CTO Sunday Thoughts #18

MyPlatform

Cloud Governance in Azure – what the platform gives you

Last week we covered Microsoft's position on Cloud Governance:

- Governance must be designed
- Guardrails beat gates
- Iteration beats perfection
- Platform beats project

This week we go one level down.

Because once the principles are clear, the real CTO question is simple: **What does Azure actually give me out of the box – and what does it not?**

Azure is powerful but also assumes you know what you are doing.

Azure does not "do governance" for you

Let's clear a common misconception. Azure does not automatically govern your cloud.

What Azure gives you instead are:

- Building blocks – a blank canvas
- Control mechanisms
- Enforcement engines

Governance only exists when these are **designed, connected, and operated** correctly. Azure is a toolbox.

CTO Sunday Thoughts #18

MyPlatform

The core governance primitives in Azure

Microsoft is consistent about how governance should be built in Azure.

The foundation rests on a few key constructs:

• Management Groups

- Subscriptions
- Azure Policy
- Role-Based Access Control (RBAC)
- Logging and monitoring
- Cost Management

Individually, they are simple. Together, they form the governance backbone.

Management Groups – where governance actually lives

If you understand nothing else about Azure governance, understand this:

Management Groups are where governance lives.

They allow you to:

- Structure your Azure estate hierarchically
- Apply policy and access once, and inherit everywhere
- Separate platform, workloads, and environments

Most governance failures start here:

- Flat subscription structures
- No inheritance model
- Governance applied too late

Without Management Groups, Azure governance does not scale.

Azure Policy – guardrails as code

Azure Policy is Microsoft's primary governance engine.

It allows you to:

- Control what can and cannot be deployed
- Enforce configuration standards
- Auto-remediate non-compliant resources

Policy works best when:

- Applied at Management Group level
- Designed as deny or modify – not audit-only
- Treated as platform code

Policy is powerful. It is also unforgiving if designed poorly.

CTO Sunday Thoughts #18

MyPlatform

Identity and cost – governance Azure assumes you design

Azure provides:

- Entra ID, RBAC, PIM, Conditional Access
- Cost analysis, budgets, alerts, tagging

CAF assumes:

- No permanent admin access
- Least privilege by default
- Clear ownership and consistent tagging

Azure supports this. **It does not design it for you. MyPlatform does.**

Without structure:

- Identity sprawl grows
- Cost tools become dashboards
- Dashboards do not stop overspend

The uncomfortable reality

In real organizations:

- Governance is implemented once
- Then slowly decays
- Exceptions accumulate
- New services bypass old rules

Not because Azure is weak.

But because governance is treated as a **deployment**, not an **operation**.

The key takeaway

Azure gives you everything you need to build strong cloud governance. It does not guarantee that governance stays correct, current, or consistent. CAF assumes mature platform ownership and continuous operation.

The open question remains:

How do you make Azure governance evergreen – without turning it into a permanent consulting project?