# Governance Risk in Your Hybrid Cloud

Azure ARC is one of Microsoft's featured technologies. It allows organizations to manage any infrastructure; on-premises, multi-cloud or edge via Azure control plane. Servers, Kubernetes clusters, and even virtual machines in other clouds appear inside Azure as first-class citizens.

This unified management model is powerful. But it also hides a security paradox: when everything looks like Azure, everything is controlled *as if* it were Azure.

If governance is not enforced, ARC becomes a single, borderless control plane with the ability to reconfigure resources far beyond Azure's native scope. In practice, that means a single mistake or breach can now cross your hybrid boundaries.

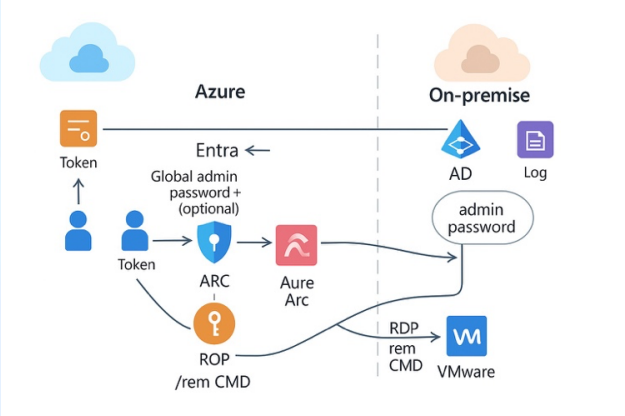
## When Convenience Collides with Control

Every ARC-connected resource authenticates through Azure AD. The ARC agent, typically registered with a service principal, acts on behalf of Azure to apply policies, deploy extensions, and collect telemetry. In principle, this architecture is secure.

In practice, most organizations grant these identities broad rights because "**it just works.**"

This is where governance fails. A service principal assigned ***Contributor*** at subscription level can deploy code, create resources, or change configurations on any connected system. Combine that with automation pipelines and delegated permissions, and you have a control plane that is nearly impossible to audit. The result: **identity overreach and invisible privilege escalation** across hybrid boundaries.

## A security example




*A sysadmin uses their laptop to run administrative tasks for both Azure and local datacenter VMs. They authenticate to Entra ID and receive an access token and a refresh token. The laptop is compromised by malware (e.g., from a phishing attachment). The attacker steals the refresh token and reuses it from an external host to request new access tokens. Because Azure Arc agents and a service principal have fairly broad rights, the attacker uses the stolen token to call Arc APIs and execute remote commands on on-prem systems — moving from cloud identity to on-prem execution and retrieving sensitive data or adding backdoors.*

The problem is not Azure ARC itself. It's the absence of an enforced Governance, Risk, and Compliance (GRC) model. When least-privilege design, role separation, and policy compliance are manual, they simply don't keep up with cloud speed.

Governance becomes a slide deck instead of a safeguard.

## The compliance problem

Traditional compliance frameworks were built for static systems. ARC lives in motion.

Every connected resource, server, VM, Kubernetes cluster can drift from baseline in hours. One configuration change on-premises or a missed patch in AWS can break policy alignment. The organization believes it is compliant, but the hybrid reality tells another story.

In regulated sectors, this drift is not theoretical. It directly affects **NIS2, CIS, and ISO 27001** controls for access management, auditability, and change traceability. Auditors now ask not only *what policies exist*, but *how continuously they are enforced*. Without automation, that question has no credible answer.

## Why the GRC model must be built-In, not bolted-on

Governance cannot be added after deployment.

Azure ARC turns Azure into the operational heart of hybrid IT — and that means the GRC layer must live inside that heart. It needs to enforce role design, policy inheritance, and compliance evidence automatically.

That is exactly what **MyPlatform** delivers.

# MyPlatform: GRC by Automation

**MyPlatform** transforms Azure GRC from a consulting exercise into an automated system.

Deployed directly through Azure Marketplace, it builds a fully governed Azure and ARC foundation in minutes. Once deployed, it continuously enforces least privilege, policy compliance, and drift remediation — across every connected environment.

**Least-Privilege by design**
**MyPlatform** creates a dedicated management group hierarchy for ARC and applies role-based access models that isolate onboarding, operations, and auditing. No user or service principal ever holds overlapping privileges. **This enforces *separation of duties* by architecture, not by policy document.**

**Policy-as-Code enforcement**
All ARC resources inherit compliance controls aligned with Microsoft's Cloud Adoption Framework, CIS, NIS2, and ISO 27001. Encryption, logging, network segmentation, and Defender integration are continuously verified. If drift occurs, remediation triggers automatically. Compliance becomes real-time, not retrospective.

**Secure identity lifecycle**
ARC onboarding and operational roles use Azure Privileged Identity Management (PIM) for time-bound access. No permanent admin accounts, no forgotten service principals. Every elevation is approved, logged, and expires automatically.

**Evergreen governance**
Because **MyPlatform** is managed as SaaS within your tenant, its baselines evolve with Microsoft. As Azure updates its security benchmarks, MyPlatform applies them automatically and keeping governance evergreen without projects, consultants, or risk of obsolescence.

## From governance cost to business control

For leadership, this is not just about security hygiene — it's about operational assurance.

Azure ARC lets organizations modernize at speed. MyPlatform ensures that modernization happens inside a **governed, auditable, and continuously compliant framework**.

Instead of expanding the attack surface, ARC becomes the safest way to unify hybrid IT — when it's governed automatically.

That's the shift from governance as paperwork to governance as code.

And that's what **MyPlatform** delivers every day.