From Reactive to Proactive Cloud GRC Operations

Reflections After the Computerworl Cloud Festival in Copenhagen

After insightful days at Computerworld CloudFestival 2025 in Copenhagen, it is clear: Cloud GRC (Governance, Risk, and Compliance) is still handled reactively in many companies. What I call "Silent Drift" is not just a hypothetical risk — It is a widespread practice. Most of the leaders and specialists we spoke with confirmed our thesis: GRC is only maintained when a critical incident forces them to act.

A Key Realization: Responsibility and Misconceptions

Many organizations, especially those new to the cloud, only prioritize GRC after a serious incident occurs. This highlights the need to clarify the division of responsibility between the cloud provider and the company. A Cloud RACI (Responsible, Accountable, Consulted, Informed) model is no longer a "nice-to-have" but a necessity.

There is a common misconception that the cloud provider automatically delivers a 100% "managed service" where all GRC aspects are covered by best practices. This may be true for pure SaaS solutions, but in practice, there are always gray areas, especially within security, administration, and maintenance. This ambiguity creates uncertainty, and as we have seen with examples like Peloton open APIs or external administrative rights can lead to serious security breaches.

The conclusion is clear: Although the public cloud offers agility and scalability, IT leaders must take GRC obligations just as seriously as in traditional IT. The operational management can be outsourced, but the ownership and control remain the company's responsibility.

What Does This Mean in Practice?

For Greenfield Customers (New to Cloud):

For new cloud users, the message is simple: GRC must be integrated from day one. The platform elements; infrastructure, core services, and security frameworks, must be configured and maintained in accordance with the organization's policies and regulatory requirements. This includes:

- Identity and Access Management (IAM)
- Network Security
- Data Encryption
- Monitoring and Compliance

On top of this platform, the organization builds its workload elements (applications, services, data, and code). Here, the GRC responsibility lies more closely with the organization, as it concerns their own assets.

For Brownfield Customers (Existing Cloud Users):

For companies already in the cloud, the strategic question arises: Should we clean up or tear down and rebuild? Many choose to patch holes reactively, but the horizontal complexity of an organically grown cloud environment can make this unmanageable.

Tearing down and rebuilding may seem drastic, but it is often the most sustainable long-term solution. A well-architected GRC platform makes it possible to migrate business-critical applications and data to a secure foundation, while leaving technical debt and irrelevant systems behind.

The metaphor: It's like moving from a child's room to a teenager's room. The original solution was appropriate at the time, but over time, modernization is required to support further development.

The Solution: MyPlatform

With 10 years of specialized experience, we have developed MyPlatform, a solution that ensures a robust, maintained, and secure Azure platform based on an "opinionated configuration." This makes GRC a proactive and integrated part of the cloud strategy.

Final Reflection: How does your company handle the responsibility for GRC in the cloud today?

- Do you have full control and a proactive maintenance program?
- Or are you waiting for the next critical incident to dictate your priorities?