Avoid the pitfalls of cloud transformation

These snippets, based on real-world events, highlight the challenges businesses may encounter in their journey towards cloud-based IT solutions. Cloud technology is not a problem-free miracle cure. Without the right planning, the necessary skills, and a sharp focus on security, the path to an effective cloud solution can quickly turn into an obstacle course with serious consequences for the business.

Lack of planning – when improvisation turns into chaos

"The easiest was to use the company credit card for the test subscription... So did others in the company, so why not?"

"We just implemented some demo servers. We weren't supposed to use them for production!"

"No one had the overall responsibility, so we defined our own governance model."

These statements illustrate an alarming trend: a lack of planning and an ad-hoc approach to cloud adoption. Without a clear strategy and a defined decision-making model, companies risk ending up in cloud chaos. Resources and technologies are deployed unstructured, development, testing and production environments are mixed, and security is compromised.

Often, clean-up and optimization are downgraded, even though in the long run it can lead to increased risk, inefficient finances and inappropriate technology choices. "It's too complex", "We don't have time right now" or "It costs too much" are frequent arguments for postponing the necessary clean-up. But experience shows that the overall solution quickly sands and the problems grow exponentially.

Lack of skills – when procrastination creates vulnerabilities

"We just copied our setup from our existing infrastructure!"

"The easiest thing was to build a unified solution on the same infrastructure and not use advanced services."

"We only activated the services needed to build our solution and save money!"

In pursuit of quick results and short-term cost savings, companies that lack the necessary cloud expertise may resort to procrastination. It may seem tempting to implement solutions that at first glance seem sufficient, but which in the long run turn out to be inadequate or directly harmful.

These shortcuts often lead to several serious problems. Data breaches become a real threat when there is a lack of knowledge about security best practices in cloud environments. Inadequate security measures, lack of encryption, and misconfiguration of access controls can all contribute to this.

Downtime becomes more frequent when the complexity of cloud architecture is not met with the necessary expertise, leading to design errors and unstable systems. Companies are also missing out on important features and benefits that could have optimized their business because they don't have the expertise to unlock the full potential of cloud solutions. Finally, a lack of knowledge about cloud optimization can lead to unnecessary expenses, for example through oversized resources or inefficient use of cloud services.

To avoid these pitfalls, it's crucial that businesses invest in building or attracting specialized knowledge about cloud solutions. This can be done by hiring experienced cloud specialists, training existing employees, or partnering with external consultants who possess the necessary expertise.

With the right knowledge and expertise, businesses can unlock the full potential of cloud technology and minimize the risks associated with skills shortages.

Security Issues – When Rights Become a Risk

"The security of our cloud setup is the supplier's responsibility."

"Setting up a firewall was a hassle... So we gave the developer global admin rights."

"Our license provider needed access to our cloud... so we made a central access to them..."

These statements reveal a dangerous misunderstanding of the division of responsibilities in cloud environments and a lax approach to security.

Proper management of access rights is *crucial* in cloud solutions. Poor handling of role and rights definitions can be a ticking time bomb that gives hackers free rein and can have disastrous consequences.

One of the main problems is the granting of too broad rights to employees and especially external consultants. This often happens due to a lack of guidelines or a lack of removal of privileges when an employee changes jobs or leaves the company. The result is an accumulation of unused and unnecessary rights – an open invitation to abuse. Outdated passwords, lack of two-factor authentication, no use of the latest security techniques, and systems that aren't updated – all these omissions pose serious security holes.

The consequences of these neglects can include identity theft, where hackers abuse rights to access personal information. Financial loss can occur as a result of lost revenue, recovery costs, fines, or extortion. Operational disruptions, such as breakdowns, blocking of data or sabotage, can paralyze the company. Finally, a hacker attack can have serious consequences for the company's reputation and lead to a loss of trust from customers and business partners.

Companies *must* take role and rights management seriously. This involves clear guidelines for access, granting *only* the necessary rights, ongoing clean-up of old and unnecessary rights, as well as active and properly maintained security features.

A Structured, secure and efficient cloud solution

To avoid "hitting the wall", it is crucial to establish a structured and well-documented cloud platform where Governance, Risk and Compliance (GRC) is defined based on a best practice model. Companies need to have the necessary knowledge to understand how a cloud *should* be run and what the implications of different choices are.

GRC must be anchored at management level. This involves a thorough risk assessment to identify and assess potential risks in the cloud environment. Clear security policies must be implemented covering access control, data encryption, and monitoring. Finally, the company must ensure compliance and comply with relevant laws and regulations, such as GDPR.

Through extensive experience with cloud deployments and building best practices, we have founded **MyPlatform** – a **Premium Cloud Model**. This model is offered as a 'managed solution', ensuring an efficient cloud solution with built-in GRC, while being flexible enough to support the changing needs of the business.

When the cloud meets the wall

MyPlatform

Your shortcut to a secure and efficient cloud

MyPlatform is designed to directly address the traditional cloud adoption/operational challenges, and at the same time disrupt the current habitual thinking.

Standardized and automated foundation
MyPlatform provides a standardized and automated Microsoft Azure Cloud platform. It adapts best practices, such as CAF, into an agile, standardized model, incorporating necessary local controls and identity management from the outset.

Managed cloud operation excellence
MyPlatform offers a managed cloud platform designed to keep the environment secure, compliant, and efficient. This includes an always updated - evergreen platform, proactive management, transparent configuration compliance.

Built-in governance and compliance
MyPlatform include all necessary prebuilt controls to support IAM, Cloud security, and Governance as part of its mandatory subscription service. to provide robust GRC guardrails from day one.

Transparency and faster ROI
MyPlatform emphasizes a simplified and transparent model to ensure a low barrier to entry, minimize ongoing governance costs, and allow customers to harvest value immediately with predictable maintenance costs.

Accessible onboarding
Leveraging the Azure Marketplace allows for streamlined deployment and access to the platform's management board in minutes after configuration and approval.

MyPlatform adopt and operate Microsoft Azure effectively, securely and cost-efficiently, without needing the scale or deep pockets previously required.