

# How to make the most of cloud

Factors to consider for a successful cloud transformation



T · · Systems ·

Let's power  
higher performance

# Contents

<b>1. Introduction</b>	<b>3</b>
Customized infrastructures with the multi-cloud	3
Challenges on the migration path: Uncontrolled growth and shadow IT	3
<b>2. Making the cloud secure</b>	<b>4</b>
6 security considerations for cloud migration projects	4
1. Avoid vendor lock-in	4
2. Holistic cloud security strategy	4
3. Cloud ACT vs. DSGVO	5
4. Automation	5
5. Security by design	5
6. Lasting cloud security	5
<b>3. A guide to cloud adoption</b>	<b>6</b>
What are the steps involved to make it work?	6
<b>4. Application Examples</b>	<b>7</b>
1. Cloud-first strategy without individual data centers	7
2. T-Systems supports SAP customers on their way from on-premise via the private cloud to the public cloud	7
<b>5. The right partner in your cloud journey</b>	<b>8</b>

# 1. Introduction

”The majority of companies describe migration of the cloud as a ‘crucial’ or ‘very important’ project in their strategic annual planning. Almost three quarters (74 percent) of companies only discover that they lack the necessary internal knowledge during the migration.”

From the study “Maintaining Momentum: Cloud Migration Learnings,” Forrester Consulting

The cloud market now has an abundance of providers and solutions that are constantly changing. When selecting a provider, companies must not only consider technical and cost aspects, but also various compliance and legal requirements. And they must always keep an eye on the necessary security standards and certifications. As a result, many companies are simply overwhelmed by the task of deciding which cloud resources are best suited for which purpose and at what time. Due to high time and financial pressure, security is often assigned far too little importance in transformation projects. In retrospect, 85 percent of these projects fail because security aspects were not included in the planning early enough<sup>1</sup>.

## Customized infrastructures with the multi-cloud

Multi-cloud infrastructures offer several strategic advantages. Companies do not bind themselves to one provider and instead put together a solution from the offerings of several cloud providers that best suits their needs. In this way, the various user groups in companies get their IT resources, such as virtual machines, storage, and applications, according to their needs. These can be hosted on different cloud platforms according to governance and security requirements. In addition, with cloud computing, companies only pay for the IT capacities that they actually use.

## Challenges on the migration path: uncontrolled growth and shadow IT

In many cases, companies seem to „stumble“ into multi-cloud transformation projects rather than planning them well. The reason

for this is often a lack of overview of their own IT landscapes. In many companies, structures have grown over the years – making it difficult for anyone to have a complete overview. Gartner analysts estimate that 30 to 40 percent of IT expenditure<sup>2</sup> in companies worldwide is attributable to shadow IT. This causes frictional losses, prevents innovation, and drives up costs. “Shadow IT in a company usually comes about using cloud services with private accounts, due to missing or unknown offerings from the company’s IT department. This not only creates a considerable risk, but also wastes economies of scale when purchasing IT services,” says Paul Schöber, security expert at T-Systems.

### Numerous questions that need to be addressed:

- How can companies obtain a complete overview of their own IT landscape over the long term?
- What are the differences between cloud providers, and which solution best fits the requirements?
- What are the migration and operating costs for each cloud provider?
- What are the factors that must be considered to ensure a robust and secure cloud transformation?
- Does the technology partner have sufficient expertise and experience to not only implement all cloud solutions, but also to manage them permanently?

<sup>1</sup> <https://www.computerwoche.de/a/die-5-haeufigsten-gruende-warum-cloud-projekte-scheitern,3549661>

<sup>2</sup> <https://www.everestgrp.com/2017-04-eliminate-enterpriseshadow-sherpas-blue-shirts-39459.html/>

## 2. Making the cloud secure

Many companies are paying little attention to the topic of cloud security in their migration projects. One common reason for this is a certain amount of overload: The multitude of products and providers makes decision-making for the right solution complex. As the number of solutions, services, and providers grows, so does the potential for risk.

Through 2025, more than 99 percent of cloud breaches will be traced back to preventable misconfigurations or mistakes by end users<sup>3</sup>. Hence, it is becoming increasingly difficult to comply with

corporate compliance regulations such as regional regulations, data protection classes, or password guidelines. In summary, the more complex the IT or cloud infrastructure, the more security expertise is required. However, specialists are in short supply. 86 percent of IT decision makers believe that the shortage of skilled workers will slow down cloud projects in companies worldwide this year. This concern is also absolutely justified<sup>4</sup>. Due to the lack of expertise, many companies are unable to address fundamental challenges in cloud security because they simply do not know the dangers.

### 6 security considerations for cloud migration projects:

#### 1. Avoid vendor lock-in

Multi is often preceded by mono: Many companies initially take the first step into the cloud with a single provider. This poses the danger of so-called vendor lock-in, i.e. dependence on this provider. For example, if the provider has developed its own interfaces, tools, and templates for its platforms, which only work there. Those who only use the proprietary services of one cloud provider run the risk of spending a lot of time and money when switching to another provider. In addition, the well-known American hyperscalers are subject to the regulations of the so-called Cloud ACT (more on this in tip 3).



#### 2. Holistic cloud security strategy

Proven protection and cloud-specific security measures: Traditional applications such as monitoring network traffic through firewalls complement specific solutions designed specifically for use in cloud environments – from the cloud access security broker to encryption of data in SaaS applications and security for container environments. It is important to check whether virtualized security solutions offered by the cloud provider are sufficient for your own security, legal, and meet compliance requirements, or whether additional products from a specialized security provider should be purchased and, for example, deployed centrally from the corporate network.



<sup>3</sup> The Gartner Hype Cycle for Cloud Security Report, 2021

<sup>4</sup> Digitalisierungsindex Mittelstand 2019/2020, Telekom Deutschland and techconsult

### 3. Cloud ACT vs. DSGVO

Two laws, one potential conflict: While the Cloud ACT is intended to facilitate US law enforcement, the GDPR is to protect personal data in Europe. The two laws come into conflict with each other if, for example, the Cloud ACT stipulates that US authorities may also request data from US cloud providers that is stored on servers in Europe. Anyone who must play it safe and wants to exclude access by US authorities, should choose a European cloud provider for processing personal data or at least take specific security measures. Encryption offers additional protection if data is stored in encrypted form and the key is not stored in the same cloud. It is only then that access by unauthorized persons becomes difficult or even impossible.



### 4. Automation

Unify and keep pace: Ensuring network, data, and endpoint security for different processes and applications is becoming an increasingly complex task. If dynamically growing cloud resources are added – often at short notice – automation also becomes indispensable for security. The best way to keep up with the enormous pace and at the same time deliver the appropriate security is with powerful, automated tools. Appropriate solutions permanently ensure that workloads permanently meet the necessary security requirements.



### 5. Security by design

Secure right from the start: Design products and applications during the development phase in such a way that security gaps do not occur in the first place - sounds trivial but is by no means considered in all IT projects. However, especially in the age of the multi-cloud, security by design is becoming a must-have. Development cycles are becoming faster, and implementing the necessary security measures retrospectively is becoming increasingly difficult and expensive. Approaches such as DevSecOps combine well-known DevOps processes with IT security to ensure the end product has a high level of security integrated into the development.



### 6. Lasting cloud security

Don't let up: Security is not a one-time investment, but must be operated regularly and sustainably. That is because architectures and attack scenarios change daily. By 2025 cybercrime is expected to cost the world \$10.5 trillion<sup>5</sup>. As a result, companies must constantly deploy new security tools. In other words, in addition to developments based on the security by design principle, security standards must be continuously reviewed, redefined if necessary, and updated.



<sup>5</sup> <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>

## 3. A guide to cloud adoption

As cloud lays the foundation for innovation and transformation, it is crucial companies truly leverage and benefit from its potential. Whether it is driving IT productivity via [AI-supported SAP automation](#) in the cloud or improving customer experience – cloud is a starting point for success.

However, there are many questions that companies without external expertise cannot reasonably answer. And this is where Cloud Assessment from T-Systems comes in: a service that enables companies to analyze their IT landscape to consolidate and modernize it, and to benefit from the best offer for them in the long term – without creating even more shadow IT. To achieve this, T-Systems relies on a combination of a proven software tool and the experience of highly specialized experts.

First, T-Systems scans the entire IT and application landscape: data centers, virtual machines, servers, applications, and IT services of all kinds. The result is a complete inventory that shows exactly which IT resources are in use in the company and what project and operating costs are incurred. Shadow IT is uncovered during this process. Based on this information, T-Systems' cloud experts draw up a sound recommendation for how the company can modernize its IT infrastructure with the help of multiple cloud services from different providers. Cloud Assessment shows companies a clear migration path to a professional multi-cloud infrastructure, which saves time and money, considers different security requirements, and provides scope for driving digitization, developing innovations, and opening new business areas.

What are the steps involved to make it work?

### 1. Inventory and overview

of the complete IT landscape with a proven software tool: automated scan of the existing IT landscape and the resources used (data centers, virtual machines, servers, applications and services). This already shows which concrete project and operating costs are incurred in the cloud.

### 2. Intelligent simulation of business cases

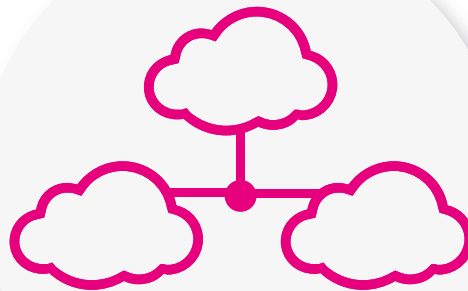
for applications that are to be migrated to the cloud, if requested also for different cloud providers, Which applications are to be migrated to which cloud, which are to be rebuilt, and which are to be shut down and replaced by cloud services?

### 3. Development of recommendations

for all the applications in a company-specific migration plan - taking into account the security strategy best suited to your company.

### 4. Identification of savings potentials

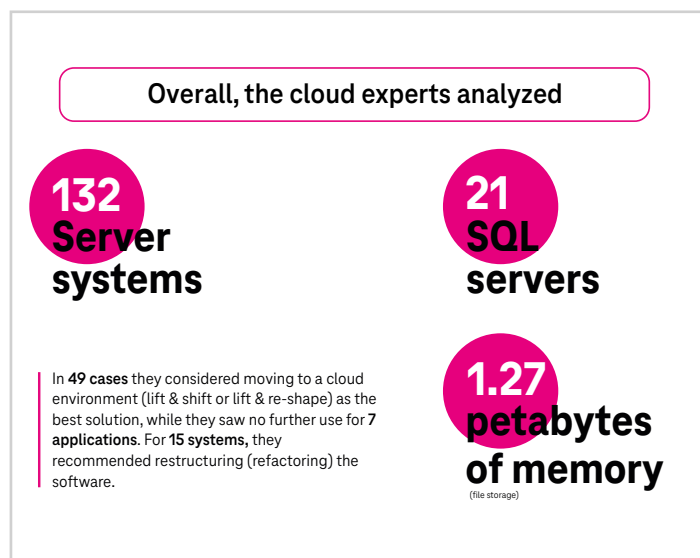
based on an automatic capacity planning. With T-Systems's Cloud Assessment, time savings of up to 65 percent can be achieved and costs reduced by up to 45 percent (on the basis of more than 1,000 Cloud Assessments performed).



# 4. Application Examples

## 1. Cloud-first strategy without individual data centers

At a major supplier of foundry chemicals, an analysis of the entire IT landscape was required: the company wanted to close its own data centers and adopt a cloud-first strategy, and be advised on the selection of the right supplier. T-Systems carried out the Cloud Assessment. Among the systems to be analyzed by the specialist chemicals supplier were Microsoft Exchange and SharePoint as well as SAP systems. In less than eight weeks, T-Systems developed a migration strategy for the cloud.



In addition, the cloud experts provided the chemical company with a precise breakdown of the costs that would arise from implementing the proposed cloud strategy. To this end, they conducted a detailed comparison of the offers of Amazon Web Services (AWS) and Microsoft Azure. Based on a complete inventory of its IT landscape, the chemical company was thus able to carry out a fast and thorough migration of its systems and save costs by using cloud-native services.

## 2. T-Systems supports SAP customers on their way from on-premise via the private cloud to the public cloud

One of the world's largest sportswear manufacturer needed a highly dynamic SAP multi-cloud concept and wanted to ramp-up their private cloud environment within three months. To enable this, T-Systems implemented S4/HANA in a greenfield approach for 1,500 SAP users. Within six weeks, T-Systems extended and connected the private cloud SAP landscape to Azure. All QAS & DEV SAP systems were migrated to Azure and are now operated by the same SAP operations team. By coupling the hybrid cloud to Azure and Gbit/s connection to private cloud environment in the T-Systems data center, the customer was able to achieve flexibility and agility in modelling its business processes. Additionally, faster installation and deployment of SAP test systems and reduced IT costs with the "pay-as-you-use" model enabled the customer to expand their cloud environment and integrate innovative services in the further development of its products.



## 5. The right partner in your cloud journey

To modernize your company's IT infrastructure in the long term, it is advisable to have a partner that has both the appropriate software tools and sufficient cloud and security expertise in-house to be able to provide adequate advice. Because one thing is clear: Only with the right cloud strategy, which also takes security aspects into account from the start, can migration succeed, and potentials be leveraged. As an enabler for multi-cloud and digitalization, T-Systems has been reliably supporting companies for decades on their path to greater performance and security.

And when it comes to taking advantage of the public cloud without compromising on data security and compliance requirements, the new T-Systems Sovereign Cloud powered by Google Cloud, now available in the German market, offers full compliance with the

requirements of German regulators – while retaining the public cloud functionality and flexibility of a hyperscaler.

An ecosystem of digitalization partners provides the right cloud solution for every need – from infrastructure to platform to software-as-a-service (IaaS, PaaS, SaaS). Beyond that, T-Systems has its own cloud offerings such as the Open Telekom Cloud, hosted in German data centers or the private cloud solution, Future Cloud. T-Systems experts always identify exactly the right cloud solution for companies to meet their individual business and security requirements. They work with you to define your cloud security strategy, find suitable solutions, and help implement it. In this way, companies are optimally prepared for the cloud world.





# Next Steps

To help you plan your migration needs and gain an overview of your landscape's maturity, we recommend a [Cloud Assessment](#). Because no matter where you are in your cloud migration journey, there is support at every stage.

## Contact

T-Systems International GmbH  
Hahnstraße 43d  
60528 Frankfurt am Main, Germany  
Tel: 00800 33 090300  
E-Mail: [info@t-systems.com](mailto:info@t-systems.com)  
Internet: [www.t-systems.com](http://www.t-systems.com)

## Publisher

T-Systems International GmbH  
Marketing  
Hahnstraße 43d  
60528 Frankfurt am Main, Germany