Cloud Security Assessment

360° analysis and assessment of your cloud architecture by experienced and certified security experts from Telekom Security

Give your cloud architecture a comprehensive check

The move from traditional, dedicated IT infrastructure to cloud based solutions seems unstoppable. No organization can afford to overlook the financial advantages, the increased flexibility and better agility offered by the cloud. But it is vital that cloud transformation does not compromise the security of data and applications. Are you sufficiently addressing that risk?

Today, modern and mobile IT relies on the cloud and a diversity of end devices. Use of the cloud changes demands on IT security. Telekom Security offers you a Cloud Security Assessment in which we help you look at the changes for your own company and benefit from our experiences in implementing cloud strategy for the Deutsche Telekom Group.

The Security Assessment provides a comprehensive examination and evaluation of the customer's environment by experienced and certified security consultants from Telekom Security. During the assessment, both procedural and technical security criteria of cloud security are considered. The assessment focuses on the following questions, which build on each other:

- **Foundation:** Are security requirements for the cloud defined and documented?
- **Implementation:** Are the security requirements implemented correctly and consistently?
- **Continuous control:** Are appropriate mechanisms and processes in place to maintain and improve the defined security level?

The procedure follows recognized best practices. As a result, you receive recommendations for action with possible measures, which we explain in a final presentation. The recommendations cover all vulnerabilities in your security guidelines, their implementation and the associated processes. These are sorted and prioritized by criticality.

Two phase procedure: Are you meeting your own demands? Is the security level sufficient?

- **Initial workshop: First**, we review whether the documents provided cover the relevant checkpoints and best practices. If necessary, the information already gathered is augmented with expert interviews. These can be combined with arranged appointments for technical sampling or conducted separately.
- **Security assessment:** Subsequently, technical implementation is tested on the basis of sampling. The technical samples can be collected in a joint appointment with the customer or independently by Telekom Security. The technical samples depend on the specific environment and the cloud services used. After this, the results of the assessments, including the findings and recommendations derived from them, are documented and presented in a final presentation.

·T··Systems·

Let's power
higher performance

Standard Cloud Security Assessment

When to use?	▶	Tests the security status quo of single single-cloud environments.
What is included?	🧩	• Initial assessment workshop • 360° security assessment, analysis and recommendations for one environment • Final report and presentation (about 1.5 hours)
How much does it cost?	€	Fixed price € 19,900*

Complex Cloud Security Assessment

When to use?	▶	Tests the security status quo of multi-cloud environments or those with decentral governance.
What is included?	🧩	• Assessment workshop for customer's full cloud environment • 360° assessment, detail analysis and recommendations for up to three environments • Final report and presentation (about 3 hours)
How much does it cost?	€	Fixed price € 39,500*

*All prices exclude valued added tax and travel expenses (if applicable)

The Cloud Security Assessment in detail: Who does what and how long does it last?

Duration of service delivery
- The total duration of service delivery is typically four to six weeks.

Delimitation
- The activities of the described work packages contain only recommendations. No activities are carried out to implement the recommendations in the client's systems.

Cooperation by the customer
- Provision of a central contact person (SPoC) for the duration of the service provision.

- Availability of the designated contact person and workshop participants on the specified dates
- Provision of premises for the implementation of the workshop.
- Provision of the required information for the detailed assessment (i.e., by allocating the necessary interview partners and/or sharing the necessary documentation)
- Provision of a technical contact for access to the cloud landscape.
- Provision of accounts with access rights to the relevant cloud assets to be examined or provision of the required technical contacts for joint, guided access to the cloud environment.

T **·** **·Systems·**

Let's power
higher performance