

BSI C5

Why you still need to secure your data in the cloud



Testing against the German Federal Office for Information Security's (BSI) Cloud Computing Compliance Criteria Catalog (C5) is an important indicator for cloud customers. It proves that the provider meets strict security standards and has implemented appropriate measures to protect customer data (Type I). The Type II certificate also confirms that the effectiveness of the measures has been tested over a period of time. The BSI C5 audit covers various aspects, including data protection, information security, risk management and compliance.

Security-conscious organizations should insist on C5 attestation for cloud services. At the same time, it is no guarantee that customer data is fully protected. Securing data „in the cloud“ remains the responsibility of the organization. A cloud security strategy is essential.



Understanding shared responsibility in the cloud

Security in the cloud follows the „shared responsibility“ model, where both the cloud provider and the customer must take responsibility. The exact allocation can vary depending on the cloud platform. In general, two main areas can be distinguished:

- + Infrastructure layer (hardware, network, virtualization)
- + Application layer (operating system, applications, data)

The provider does not have access to the application layer and cannot secure it. As a customer, you should ensure that you establish internal security policies, manage access controls, use data encryption, and perform regular security audits.

Would you like to find out more about how you can protect your data in the cloud?

Feel free to contact us for a free initial consultation with our security experts.

[> Learn more](#)

[> Download BSI C5 test report](#)

Provider responsibilities	Customer responsibilities
<p>+ Physical security:</p> <p>The provider is responsible for the physical security of the data centers, including access controls, monitoring and environmental security.</p> <p>+ Network infrastructure:</p> <p>The provider deploys and secures the basic network infrastructure - including shared firewalls, routers and switches - to control data traffic.</p> <p>+ Virtualization layer:</p> <p>The provider manages the virtualization layer on which customers create and run their virtual machines (VMs).</p>	<p>+ Identity and access management:</p> <p>The customer is responsible for managing user access, authentication and authorization within its cloud resources.</p> <p>+ Data:</p> <p>Customers are responsible for the security of their data, including encryption, access controls and data management.</p> <p>+ Applications:</p> <p>Securing applications running on cloud resources is the responsibility of the customer.</p>

plusserver

A sovereign, future-proof and secure cloud.

We offer German companies a sovereign and vendor-independent foundation for their digital business processes. On our secure, scalable cloud platforms, customers can implement future-proof and cost-effective digital applications. We advise our customers on cloud architectures and the integration of existing IT environments. Our approach is fast, dynamic and always personal.

Do you have any questions?

Feel free to contact us.

We are here to help - quickly and easily

+49 2203 1045 3500

sales@plusserver.com

