BSI C5 and DORA

18.11.2026 Digital Sovereignty Insurance & Financial Services

KEY POINTS AT A GLANCE

Independent Security Assessments for Financial Institutions

The BSI-C5 standard provides banks, insurance companies, and financial service providers with an independent basis for assessing the security and control measures of their cloud and IT service providers. DORA strengthens the requirements for digital resilience as well as for the selection, monitoring, and management of these service providers. A BSI-C5 report supplemented with DORA-relevant evidence can help financial institutions assess risks more transparently and demonstrate their compliance and audit processes.

Independent Security Assessments for Companies in the Financial Sector

The use of external IT services is indispensable today for **banks, insurance companies, and financial service providers**—ideally delivered flexibly, scalably, and securely from the cloud. At the same time, requirements for compliance, transparency, and the management of external service providers are increasing. Regulatory requirements such as DORA are increasingly bringing the following question into focus: How can banks, insurance companies, and financial firms verify and document that their IT partners have adequate security and control mechanisms in place?

The BSI C5 standard plays an important role in this regard.

What is the BSI-C5 testing standard?

The Cloud Computing Compliance Criteria Catalog (C5) published by the Federal Office for Information Security (BSI) is an established audit standard for cloud providers. It defines requirements for information security and transparency and serves as a guide for companies when selecting trustworthy IT and cloud services.

An independent audit assesses whether the defined security and control requirements are being effectively implemented. The resulting audit report provides transparency regarding an IT service provider's security and control environment and offers customers a reliable basis for their evaluation and risk assessment.

Why Is BSI C5 Particularly Relevant for Banks, Insurance Companies, and Financial Service Providers?

The industry is one of the most heavily regulated sectors of the economy. Banks, insurance companies, and financial service providers are required to assess, document, and continuously monitor the risks posed by their IT service providers.

At the same time, dependence on cloud and IT services is growing. This also increases the need for standardized evidence that transparently demonstrates security and the effectiveness of controls.

A BSI-C5 certificate can help with this,

- to better assess a service provider's security level,
- to support service provider management,
- To simplify inspection and audit processes,
- as well as to reduce the effort involved in risk and compliance assessments.

For regulated companies in particular, independently verified documentation provides significantly

greater transparency than mere self-reported information or marketing claims.

What Role Does DORA Play?

With the Digital Operational Resilience Act (DORA), the European Union has established a uniform framework for the digital resilience of financial institutions. The focus is not only on the institutions themselves, but also on the IT service providers they use.

The goal is to identify risks early on, increase resilience to disruptions, and ensure the stability of critical business processes. For banks, insurers, and financial institutions, this also means stricter requirements for selecting, monitoring, and managing their service providers.

What is crucial here is not only the implementation of appropriate measures, but also the ability to provide verifiable evidence of these measures to internal and external auditors.

How Can Safety Evidence Be Made Usable for Regulatory Purposes?

While a traditional BSI-C5 certification provides transparency regarding security and control measures, evidence that also demonstrates compliance with regulatory requirements is becoming increasingly important for banks, insurance companies, and financial institutions.

This makes it easier to integrate technical security measures into the regulatory context and apply them to **governance, risk, and compliance processes**. At the same time, standardized documentation can help reduce the effort involved in service provider evaluations and audits.

DORA-Enhanced BSI-C5 Report by Arvato Systems

Against this backdrop, Arvato Systems has expanded the reporting of its BSI-C5 certificates to include DORA-relevant evidence.

The DORA-enhanced BSI-C5 report provides independent evidence that key DORA requirements for IT service providers have been effectively implemented. This provides financial institutions with a reliable foundation for their third-party ICT risk management, as well as robust evidence to meet regulatory requirements.

Share this

Written by



Sophia Gunkel

Regulatory expert for banks and insurance companies

Sophia Gunkel is Director Regulatory Affairs for Banks and Insurance Companies at Arvato Systems. She supports financial companies in the classification and implementation of regulatory requirements for ICT services, in particular the DORA requirements. Her focus is on the combination of regulation, IT operations and governance for resilient and compliant IT operations.