BSI C5 und DORA

18.11.2026 Digitale Souveränität Versicherungen & Finanzdienstleistungen

DAS WICHTIGSTE IN KÜRZE

Unabhängige Sicherheitsnachweise für Finanzunternehmen

Der BSI-C5-Standard bietet Banken, Versicherungen und Finanzdienstleistern eine unabhängige Grundlage, um die Sicherheits- und Kontrollmaßnahmen ihrer Cloud- und IT-Dienstleister einzuschätzen. DORA stärkt die Anforderungen an digitale Resilienz sowie an Auswahl, Überwachung und Steuerung dieser Dienstleister. Ein um DORA-relevante Nachweise ergänzter BSI-C5-Bericht kann Finanzunternehmen dabei unterstützen, Risiken transparenter zu bewerten und ihre Compliance- und Prüfprozesse zu belegen.

Unabhängige Sicherheitsnachweise für Unternehmen in der Finanzbranche

Der Einsatz von externen IT-Services ist für **Banken, Versicherungen und Finanzdienstleister** heute unverzichtbar – am liebsten flexibel, skalierbar und sicher aus der Cloud erbracht. Gleichzeitig steigen die Anforderungen an Compliance, Transparenz und die Steuerung externer Dienstleister. Regulatorische Vorgaben wie DORA rücken dabei zunehmend die Frage in den Fokus: Wie können Banken, Versicherungen und Finanzunternehmen nachvollziehen und dokumentieren, dass ihre IT-Partner über angemessene Sicherheits- und Kontrollmechanismen verfügen?

Eine wichtige Rolle spielt dabei der BSI C5 Standard.

Was ist der BSI-C5-Prüfungsstandard?

Der Cloud Computing Compliance Criteria Catalogue (C5) des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist ein etablierter Prüfstandard für Cloud-Anbieter. Er definiert Anforderungen an Informationssicherheit und Transparenz und dient Unternehmen als Orientierung bei der Auswahl vertrauenswürdiger IT- und Cloud-Services.

Im Rahmen einer unabhängigen Prüfung wird bewertet, ob die definierten Sicherheits- und Kontrollanforderungen wirksam umgesetzt sind. Das daraus resultierende Testat schafft Transparenz über das Sicherheits- und Kontrollumfeld eines IT-Dienstleisters und bietet Kunden eine verlässliche Grundlage für ihre Bewertung und Risikobetrachtung.

Warum ist BSI C5 besonders relevant für Banken, Versicherungen und Finanzdienstleister?

Die Branche zählt zu den am stärksten regulierten Wirtschaftszweigen. Banken, Versicherungen und Finanzdienstleister sind verpflichtet, Risiken ihrer IT-Dienstleister zu bewerten, zu dokumentieren und kontinuierlich zu überwachen.

Gleichzeitig wächst die Abhängigkeit von Cloud- und IT-Services. Damit steigt auch der Bedarf an standardisierten Nachweisen, die Sicherheit und Kontrollwirksamkeit transparent belegen.

Ein BSI-C5-Testat kann dabei helfen,

- das Sicherheitsniveau eines Dienstleisters besser einzuordnen,
- die Dienstleistersteuerung zu unterstützen,
- Prüf- und Auditprozesse zu vereinfachen,
- sowie den Aufwand für Risiko- und Compliance-Bewertungen zu reduzieren.

Insbesondere für regulierte Unternehmen bietet ein unabhängig geprüfter Nachweis eine deutlich

höhere Transparenz als reine Selbstauskünfte oder Marketingaussagen.

Welche Rolle spielt DORA?

Mit dem Digital Operational Resilience Act (DORA) hat die Europäische Union einen einheitlichen Rahmen für die digitale Resilienz von Finanzunternehmen geschaffen. Dabei stehen nicht nur die Institute selbst im Fokus, sondern auch die von ihnen eingesetzten IT-Dienstleister.

Ziel ist es, Risiken frühzeitig zu erkennen, die Widerstandsfähigkeit gegenüber Störungen zu erhöhen und die Stabilität kritischer Geschäftsprozesse sicherzustellen. Für Banken, Versicherer und Finanzunternehmen bedeutet dies zugleich höhere Anforderungen an die Auswahl, Überwachung und Steuerung ihrer Dienstleister.

Entscheidend ist dabei nicht nur die Umsetzung geeigneter Maßnahmen, sondern auch die Möglichkeit, diese gegenüber internen und externen Prüfern nachvollziehbar nachzuweisen.

Wie werden Sicherheitsnachweise regulatorisch nutzbar?

Während ein klassisches BSI-C5-Testat Transparenz über Sicherheits- und Kontrollmaßnahmen schafft, gewinnen für Banken, Versicherungen und Finanzunternehmen zunehmend Nachweise an Bedeutung, die zusätzlich einen Bezug zu regulatorischen Anforderungen herstellen.

Dadurch lassen sich technische Sicherheitsmaßnahmen besser in den regulatorischen Kontext einordnen und für Governance-, Risiko- und Compliance-Prozesse nutzen. Gleichzeitig können standardisierte Nachweise dazu beitragen, den Aufwand für Dienstleisterbewertungen und Prüfungen zu reduzieren.

DORA-erweiterter BSI-C5-Bericht von Arvato Systems

Vor diesem Hintergrund hat Arvato Systems die Berichterstattung seines BSI-C5-Testats um DORA-relevante Nachweise erweitert.

Der DORA-erweiterte BSI-C5-Bericht schafft einen unabhängigen Nachweis darüber, dass wesentliche DORA-Anforderungen an IT-Dienstleister wirksam umgesetzt sind. Finanzunternehmen erhalten dadurch eine verlässliche Grundlage für ihr IKT-Drittparteienrisikomanagement sowie belastbare Nachweise für regulatorische Anforderungen.

Weiterempfehlen

Verfasst von



Sophia Gunkel

Expertin für Regulatorik für Versicherungen und Finanzdienstleistungen

Sophia Gunkel ist Director Regulatorik für Banken und Versicherungen bei Arvato Systems. Sie unterstützt Finanzunternehmen bei der Einordnung und Umsetzung regulatorischer Anforderungen an IKT-Dienstleistungen, insbesondere an die DORA-Anforderungen. Ihr Fokus liegt auf der Verbindung von Regulierung, IT-Betrieb und Governance für einen resilienten und konformen IT-Betrieb.