KPMG

C5-Testate im Gesundheitswesen:

Was Cloud-Anbieter jetzt wissen und umsetzen müssen

April 2025

Inhaltsverzeichnis

1. **Hintergrund:**
   Was regelt § 393 SGB V? **4**

2. **C5-Gleichwertigkeitsverordnung:**
   Anforderungen an gleichwertigeNachweise **5**

3. **Fristen und To-dos:**
   Diese Deadlines sollten Sie kennen **6**

4. **Typ-1 vs. Typ-2:**
   Unterschiede und Prüfungsansätze **7**

5. **Unsere Empfehlung:**
   So können Sie Ihre Konformität effizient absichern **8**

Das Wichtigste in Kürze

- Seit dem 1. Juli 2024 gilt § 393 SGB V: Cloud-Dienstleister im Gesundheitswesen benötigen einen Sicherheitsnachweis auf Basis des BSI-C5-Kriterien-kataloges. Hierbei ist ein C5-Typ-1-Testat bis zum 1. Juli 2024 und ein C5-Typ-2-Testat ab dem 1. Juli 2025 erforderlich.
- Die C5-Gleichwertigkeitsverordnung (BGBl. 2025 I Nr. 91) konkretisiert das Digital-Gesetz (Di-giG) und ermöglicht übergangsweise alternative Standards:
  - ISO/IEC 27001,
  - ISO 27001 auf Basis IT-Grundschutz,
  - Cloud Controls Matrix Version 4.0.
- Voraussetzung ist ein detaillierter Maßnahmenplan zur C5-Konformität innerhalb von zwölf Monaten.
- Mit alternativen Standards ist dennoch bis spätestens 31. Dezember 2025 ein C5-Typ-1-Testat, bis 30. Juni 2026 ein C5-Typ-2-Testat vorzulegen.
- Wer jetzt handelt, sichert sich regulatorische Compliance und stärkt seine Marktposition.

So gehen Sie als Cloud-Anbieter vor

Damit Sie den Anforderungen aus § 393 SGB V und der C5-Gleichwertigkeitsverordnung strukturiert begegnen, empfehlen wir folgendes Vorgehen:

1. **Bestandsaufnahme und Readiness Check**: Analysieren Sie das vorhandene Interne Kontrollsystem (IKS) sowie Zertifizierungen (z. B. ISO/IEC 27001) und Testate (z. B. SOC 2) und beurteilen Sie, inwiefern die Anforderung des BSI-C5:2020-Kriterienkataloges erfüllt werden.
2. **Maßnahmenplan**: Entwickeln Sie einen konkreten Fahrplan zur Schließung identifizierter Lücken – inklusive Fristen und Verantwortlichkeiten. Kategorisieren und priorisieren Sie Handlungsfelder.
3. **Prüfungsvorbereitung**: Bereiten Sie sich gezielt auf die anstehenden Prüfungen für das Typ-1- und Typ-2-Testat vor.
4. **Nachweise bereithalten**: Maßnahmenplan und Testate sollten jederzeit gegenüber Cloud-Kunden sowie Aufsichtsbehörden vorgelegt werden können.

Sprechen Sie uns jetzt an und starten Sie Ihren Weg zur C5-Konformität – praxisnah und fristgerecht.

1. Hintergrund: Was regelt § 393 SGB V?

Mit dem Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) wurde § 393 SGB V eingeführt. Seit dem 1. Juli 2024 müssen alle Cloud-Dienste, die im Umfeld gesetzlicher Krankenkassen, Kassenärztlicher Vereinigungen (KVen) oder anderer Gesundheitsakteure eingesetzt werden, ein angemessenes IT-Sicherheitsniveau nachweisen. Dies erfolgt in der Regel durch ein C5-Testat oder einen anerkannten gleichwertigen Sicherheitsnachweis.

Ziel ist es, die Versorgungssicherheit sowie den Schutz sensibler Gesundheitsdaten durch einheitliche und prüfbare Standards sicherzustellen.

2. C5-Gleichwertigkeitsverordnung:

Anforderungen an gleichwertige Nachweise

Die am 19. März 2025 veröffentlichte C5-Gleichwertigkeitsverordnung (BGBl. 2025 I Nr. 91) wurde auf Grundlage des § 393 Absatz 1 Satz 3 SGB V erlassen. Sie konkretisiert, unter welchen Bedingungen alternative Sicherheitsnachweise als gleichwertig zum C5-Testat anerkannt werden können – und schafft damit die dringend erwartete Rechtsklarheit für betroffene Cloud-Anbieter.

Folgende alternative Nachweise können vorübergehend als gleichwertig zum C5-Testat anerkannt werden:

- ISO/IEC 27001
- ISO 27001 auf Basis IT-Grundschutz (BSI)
- Cloud Controls Matrix (CCM) v4.0 der CSA

Ein solcher Nachweis ist nur dann zulässig, wenn alle folgenden Bedingungen erfüllt sind:

1. **Dokumentation der C5-Basiskriterien**
   Es muss dokumentiert sein, welche Basiskriterien des C5-Kriterienkatalogs durch das IKS/Zertifikat nicht abgedeckt werden.

2. **Maßnahmenplan zur Schließung der C5-Lücken**
   Für jede identifizierte Lücke sind konkrete Maßnahmen zu dokumentieren, mit denen die vollständige C5-Konformität erreicht werden soll. Auch bereits begonnene Vertragsverhandlungen mit einer Wirtschaftsprüfungsgesellschaft gehören zu den Maßnahmen.

3. **Meilensteinplanung zur Umsetzung der Maßnahmen**
   Die Maßnahmen müssen innerhalb von zwölf Monaten nach Erstellung des Maßnahmenplans umgesetzt werden.

4. **Verpflichtung zur C5-Testierung**
   Es muss sichergestellt sein, dass:

   - innerhalb von 18 Monaten ein C5-Typ-1-Testat vorliegt und
   - innerhalb von 24 Monaten ein C5-Typ-2-Testat erfolgt.

Darüber hinaus verlangt die Verordnung, dass der Maßnahmenplan sowie die Nachweise auf Verlangen unverzüglich den Kranken- und Pflegekassen, die den Cloud-Computing-Dienst beauftragen, sowie den zuständigen Aufsichtsbehörden vorgelegt werden.

Fazit: Gleichwertigkeit bedeutet nicht Gleichartigkeit. Die C5-Gleichwertigkeitsverordnung schafft keine Abkürzung, sondern einen klar geregelten Pfad zur vollständigen C5-Konformität.

3. Fristen und To-dos:

Diese Deadlines sollten Sie kennen

Die C5-Gleichwertigkeitsverordnung definiert **verbindliche Fristen**, innerhalb derer betroffene Cloud-Anbieter ihre **C5-Konformität vollständig nachweisen** müssen. Die Fristen gelten **rückwirkend ab dem 1. Juli 2024**, dem Inkrafttreten des § 393 SGB V.
Die Fristen nach C5-Gleichwertigkeitsverordnung (12/18/24 Monate) beginnen erst mit Erstellung des Maßnahmenplans. Allerdings ist dieser Plan Voraussetzung dafür, dass ein alternativer Nachweis überhaupt als gleichwertig anerkannt wird. Anbieter, die sich ab dem 1. Juli 2024 auf zum Beispiel ISO 27001 berufen wollen, müssen den Maßnahmenplan bis zu diesem Datum vollständig vorlegen können.

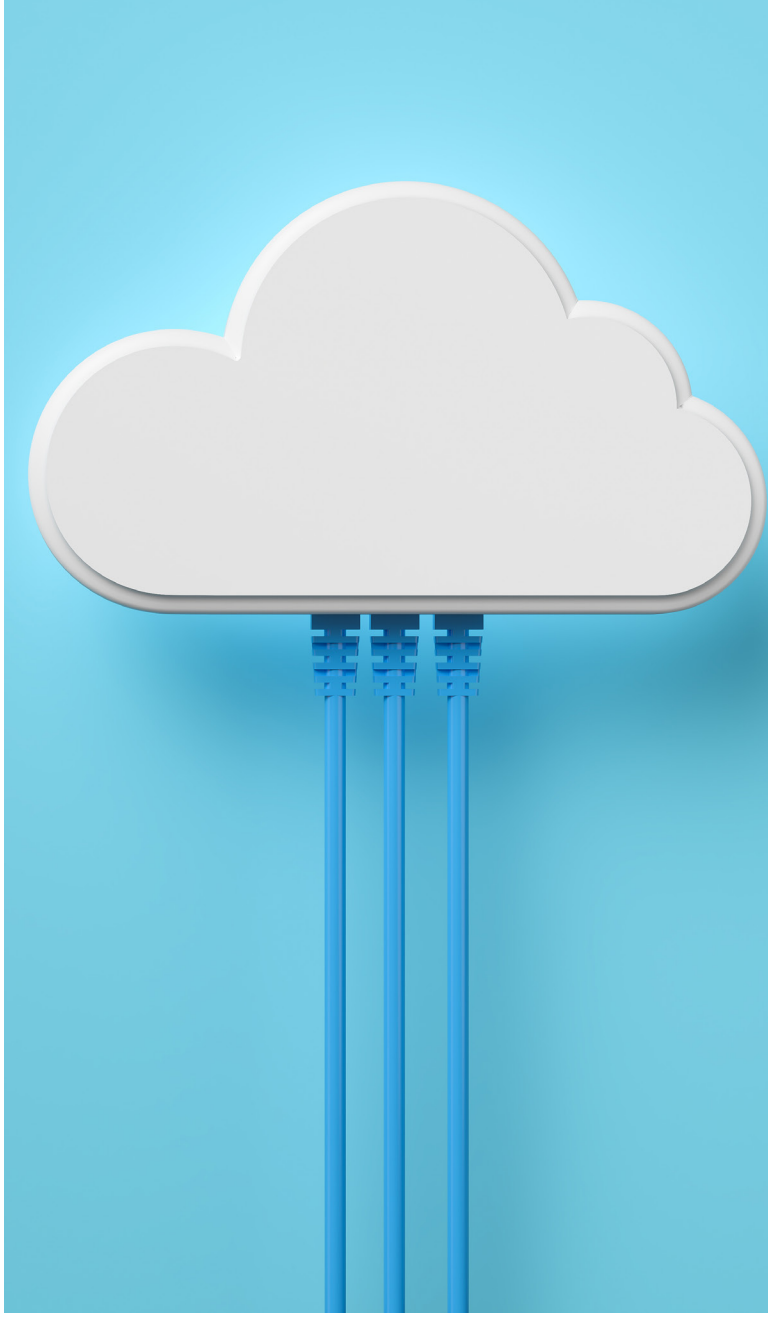
Wichtig: Wer die Fristen versäumt, kann nicht mehr als gleichwertig anerkannt werden – und läuft Gefahr, Aufträge im Gesundheitswesen zu verlieren oder regulatorische Sanktionen zu riskieren.

Schritt	Deadline	Anforderung
Maßnahmenplan	unverzüglich	Erstellung nach Einreichung eines gleichwertigen Nachweises
Typ-1-Testat (C5)	31. Dezember 2025	Nachweis über das Design der implementierten Kontrollen
Typ-2-Testat (C5)	30. Juni 2026	Nachweis über die Wirksamkeit der Kontrollen über einen Prüfungszeitraum

4. Typ-1 vs. Typ-2:

Unterschiede und Prüfungsansätze

Die C5-Gleichwertigkeitsverordnung verpflichtet Cloud-Anbieter zur Vorlage **beider Testatstypen** – Typ 1 und Typ 2. Beide dienen als formeller Nachweis über die Umsetzung der C5-Anforderungen, unterscheiden sich jedoch in Ziel, Prüfungsgegenstand und zeitlichem Fokus.



Das Typ-1-Testat bietet eine erste Bestätigung, das Typ-2-Testat ist für die dauerhafte Anerkennung und regulatorische Konformität entscheidend.

Testattyp	Fokus	Zeitraum	Aussagekraft
Typ 1	Design der Kontrollen	Stichtag (z. B. 31. Oktober 2025)	Liefert eine erste Bestätigung über die grundsätzliche Eignung des internen Kontrollsystems
Typ 2	Design und Wirksamkeit der Kontrollen	Zeitraum: mindestens drei Monate, typischerweise 6–12 Monate (z. B. 1. Juli 2025 bis 30. Juni 2026)	Tatsächliche Umsetzung im operativen Betrieb; vollwertiger Nachweis der C5-Konformität – insbesondere für Kunden im Gesundheitswesen von zentraler Bedeutung

5. Unsere Empfehlung:

So können Sie Ihre Konformität effizient absichern

Die Anforderungen aus § 393 SGB V in Verbindung mit der C5-Gleichwertigkeitsverordnung schaffen ein klares und enges regulatorisches Korsett – aber auch eine echte Chance, sich als **verlässlicher und prüfbarer Cloud-Anbieter im Gesundheitswesen zu positionieren**.

Basierend auf unserer Projekterfahrung empfehlen wir ein **fünfstufiges Vorgehen:**

1. **Ist-Analyse und Readiness-Check:** Beurteilung, ob bestehende Zertifizierungen (z. B. ISO/IEC 27001, SOC 2) und die vorhandenen Technischen und Organisatorischen Maßnahmen (TOM) die C5-Basiskriterien ausreichend abdecken.

2. **Gap-Assessment gegen den C5-Katalog:** Strukturierter Abgleich mit dem C5-Katalog und Entwicklung eines belastbaren Maßnahmenplans.

3. **Umsetzung:** Schließung der Lücken im Design und Betrieb.

4. **Prüfungsvorbereitung:** Bereiten Sie sich gezielt auf das Typ-1- und Typ-2-Testat vor. Dazu zählen Nachweisdokumente, Prozessbeschreibungen, Kontrollnachweise.

5. **Testierung:** Zielgerichtete Unterstützung durch eine Begleitung bei der Vorbereitung und Durchführung von Typ-1 und Typ-2 Testaten.

Wir unterstützen Sie fachlich fundiert, pragmatisch und mit einem klaren Blick auf regulatorische Anforderungen und Kundenerwartungen.
Sprechen Sie uns gerne an – ob für eine Erstberatung, ein Gap-Assessment oder die Vorbereitung auf ein vollständiges C5-Testat.

Ansprechpartner

KPMG AG Wirtschaftsprüfungsgesellschaft

Sebastian Blass
Partner,
Regulatory Advisory
T +49 621 426-7298
sblass@kpmg.com

Dennis Denk
Senior Manager,
Regulatory Advisory
T +49 69 9587-1973
ddenk@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia