Aktionsplan: Implementierung C5:2026

Strategische Vorbereitung für Cloud Service Provider (CSP)

Compliance & Information Security

23. April 2026

1 Einleitung

Der BSI Cloud Computing Compliance Criteria Catalogue (C5) in der Version 2026 stellt eine signifikante Weiterentwicklung der Cloud-Sicherheit dar. Dieses Dokument dient als Leitfaden für Unternehmen, die bereits ein ISMS (z.B. ISO/IEC 27001) betreiben, um die spezifischen Anforderungen des C5:2026 zu erfüllen.

Kernänderungen gegenüber C5:2020

- **Struktur:** Ausrichtung an der ISO/IEC 27001:2022 (4 statt 14 Domänen).
- **Terminologie:** Ablösung der „Basic Conditions“ (BC) durch „General Conditions“ (GC).
- **Architektur:** Einführung der Begriffe *Partitions*, *Regions* und *Zones* zur Beschreibung der Datenlokation.
- **Souveränität:** Erhöhte Anforderungen an die technische Souveränität (Verschlüsselung, Zugriffskontrolle).
- **ESG:** Integration von Nachhaltigkeits-Reporting (GC-03).

2 Phasenmodell der Implementierung

Phase	Meilenstein	Aktivitäten	Fokus C5:2026
1. Scoping	Prüfungsgegenstand	Abgrenzung des Dienstes unter Berücksichtigung von Partitions.	Definition von Souveränitätszonen.
2. Alignment	ISMS-Update	Mapping der Controls auf ISO 27001:2022 Basis.	Anpassung an neue Control-Kategorien.
3. GC-Setup	Rahmenbedingungen	Erstellung der Transparenzangaben nach GC-01 bis GC-03.	Integration von ESG-Reporting.
4. Remediation	Tech-Implementation	Schließung technischer Lücken (Verschlüsselung, Portabilität).	Fokus auf techn. Datenhoheit.
5. Audit	Attestierung	Durchführung der Prüfung durch einen WP (ISAE 3000).	Option: Continuous Auditing.

3 Detaillierte Maßnahmen & Änderungen

3.1 Phase 1: Erweitertes Scoping (Neukonzeption)

Im C5:2026 reicht die Angabe von Standorten nicht mehr aus.

- **Partitionierung:** Identifizieren Sie logische Trennungen innerhalb Ihres Dienstes. Eine Partition beschreibt eine Umgebung, in der Daten verarbeitet werden (z.B. „Public Cloud“ vs. „Sovereign Partition“).
- **Zones & Regions:** Dokumentieren Sie exakt, welche Zonen für welche Kundendaten (Account Data vs. Cloud Service Customer Data) genutzt werden.

3.2 Phase 2: Transition der General Conditions (GC)

Die bisherigen Rahmenbedingungen wurden gestrafft und um moderne Anforderungen ergänzt:

- **GC-01 (Recht & Lokation):** Transparenz über anwendbares Recht (Jurisdiktion) des Hauptsitzes und der operativen Einheiten.
- **GC-02 (Sicherheitsparameter):** Angaben zu Zertifizierungen. Hier muss nun klarer zwischen dem CSP und Unterauftragnehmern unterschieden werden.
- **GC-03 (ESG - Neu):** Der CSP muss Angaben zu Umwelt- und Sozialstandards machen (z.B. Energieeffizienz des RZ, CSRD-Reporting).

3.3 Phase 3: Technische Souveränität (Die „Sharpening“ Kriterien)

C5:2026 führt verstärkt Kriterien ein, die die digitale Souveränität schärfen:

- **Verschlüsselung:** Implementierung von „Customer Managed Keys“ (CMK) wird zum Standard-Nachweis für Souveränität.
- **Identity Management:** Nachweis, dass administrativer Zugriff durch den CSP auf Kundendaten technisch (nicht nur organisatorisch) unterbunden werden kann.

4 Dokumentationsanforderungen

Die Systembeschreibung (Description of the System) ist das zentrale Dokument für den Prüfer. In der Version 2026 muss diese zwingend folgende Matrix enthalten:

- Zuordnung von Kriterien zu spezifischen **Partitions**.
- Detaillierte Darstellung der **Interoperabilität** (Schnittstellenbeschreibungen für den Datenexport).
- Dokumentation der Maßnahmen zur Resilienz gegen extraterritoriale Datenzugriffe.

5 Zeitplan für den Umstieg

1. **Monat 1-2:** Gap-Analyse gegen ISO 27001:2022 und C5:2026.
2. **Monat 3:** Definition der Partitions-Struktur und ESG-Datenerhebung.
3. **Monat 4-6:** Technische Umsetzung (BYOK, Portabilitäts-Tools).
4. **Ab Monat 7:** Beginn des Beobachtungszeitraums für Typ 2 Audit.