Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Cloud - Interoperabilität Theorie und Praxis

Omnisecure 2025 - Berlin, 20. bis 22.01.2025

Bild: ©gettyimages, Yuichiro Chino

Cloud – Interoperabilität Theorie und Praxis hier: Theorie

Christoph Pfeifer – BSI Referat Virtualisierung und Trennungsmechanismen

Sebastian Temme – BSI Referat Cloud-Sicherheit

Was ist Interoperabilität? (I/II)

Zu dem Begriff Interoperabilität (von lateinisch opus ‚Arbeit' und inter ‚zwischen') existieren zwei unterschiedliche, jedoch sinngleiche Definitionen:

- Als Interoperabilität bezeichnet man die Fähigkeit zum **Zusammenspiel verschiedener Systeme**, Techniken oder Organisationen. Dazu ist in der Regel die **Einhaltung gemeinsamer technischer Normen notwendig**. Wenn zwei Systeme miteinander vereinbar sind, nennt man sie auch interoperabel.
- Interoperabilität ist die Fähigkeit unabhängiger, heterogener Systeme, nahtlos zusammenzuwirken, um Daten auf effiziente und verwertbare Art und Weise auszutauschen bzw. dem Benutzer zur Verfügung zu stellen, **ohne** dass dazu **besondere Adaptierungen** notwendig sind.

(Quelle: Wikipedia, Website)

Was ist Interoperabilität? (II/II)

Ermöglichen der Eigenschaft, den Cloud-Dienst über andere Cloud-Dienste oder IT-Systemen der Cloud-Kunden ansprechen zu können, die gespeicherten Daten bei Beendigung des Auftragsverhältnisses zu beziehen und beim Cloud-Anbieter sicher zu löschen.
(Quelle: BSI, C5:2020, Seite 92, Domäne PI)

Wechselfähigkeit zwischen Cloud-Anbietern – ein Wechsel zwischen Cloud-Anbietern ist <aus Sicht des Nutzers/Anwenders> technisch möglich
(Quelle: Cloud-Reallabor, Dokument „Cloud-Reallabor: YEAR ONE Erfahrungen nach einem Jahr Projektarbeit“)

Interoperabilität ist die Fähigkeit von Anwendungen und Systemen, Daten sicher und automatisch auszutauschen, unabhängig von geografischen, politischen oder organisatorischen Grenzen.
(Quelle: AWS, Website)

Was ist Interoperabilität nicht?

Interoperabilität ist kein „Universal-Konverter“, der einen Cloud-Service oder eine Anwendung die einen Cloud-Service beim Anbieter A läuft, diesen automatisch auch bei einem beliebigen Anbieter B „lauffähig“ oder nutzbar macht.

Interoperabilität ist hingegen eine Fähigkeit, die an **unterschiedlichen Stellen implementiert** werden muss:

- im **Service** (Bereitstellung von Schnittstellen, Nutzung von Standards, …),
- in der jeweiligen **Applikation** selbst (z.B. Entwicklung für den Betrieb in einer Cloud),
- aber **auch** beim **Nutzer** bzw. dessen Organisation (im weitesten Sinne)

Cloud-Strategie

Lebenszyklus Cloud-Nutzung

Planungsphase

- **Cloud-Strategie**
- Sicherheitsrichtlinie
- Sicherheitskonzept
- Vorrausschauend handeln: z.B. bereits Beendigungsphase berücksichtigen
- …

Beschaffungsphase

- Umsetzung der Sicherheitsanforderungen (Nachweis z.B. durch **C5-Testat**)
- Umgang mit Unterauftragnehmer
- Lokation der Datenverarbeitung
- …

Einsatzphase

- Einbindung in das eigene ISMS
- Überwachung und Überprüfung der Vertragsleistungen
- Auswertung von Sicherheitsnachweisen (Nachweise und Berichte müssen vom Cloud-Dienstleister ausgewertet werden)
- …

Beendigungsphase

- Datenrückgabe bei Beendigung
- Datenlöschung bei Beendigung
- Migration zu einem anderen Cloud-Anbieter / On-Prem
- …

Cloud-Strategie (I/II)

- Gibt die Richtung für eine Cloud-Nutzung vor
  - Sollen Cloud-Dienste genutzt werden?
  - In welchem Umfang? In welchem Service-Modell (SaaS, PaaS, IaaS)?
  - Welche Daten sollen/dürfen verarbeitet werden?
  - Welche geographischen Einschränkungen gibt es für die Verarbeitung/Speicherung von Daten (Datenlokation), den Support, etc.
  - …
- **Die Cloud-Strategie sollte mit der Unternehmens- / Amtsleitung abgestimmt sein, bzw. von dieser vorgegeben und getragen werden.**

Cloud-Strategie (II/II)

- Auch Aspekte der **Wechselfähigkeit** sollten so früh wie möglich berücksichtigt werden:
  - Backup Strategie
  - Multi-Cloud / Hybrid-Cloud / On-Prem
  - Dateiformate
  - Exit-Strategie
  - …

Interoperabilität

Was ist für Interoperabilität notwendig? (I/II)

Standards, Standards und nochmal Standards

- Definierte und verlässliche **Schnittstellen**, auf beiden Seiten (Quell- bzw. Zielsystem) z.B. jeweils eine API, für die eine vollumfängliche Dokumentation vorliegt (sodass eine Einarbeitung in deren Nutzung möglich ist).
- Anwendung und zugehörige Daten liegen in einem **Format** vor, das einen **Austausch** über diese Schnittstellen zulässt, z.B. Entwicklung als Cloud-native Applikation, Bereitstellung als Container, Helm Charts, Bereitstellung von Daten in einem offenen, standardisierten Format, das den ungehinderten Umgang mit den Daten ermöglicht.
- …

Was ist für Interoperabilität notwendig? (II/II)

Aber nicht nur Standards von außen sind notwendig bzw. hilfreich, sondern auch:

- Dokumentation der Anwendung(en)
- Dokumentation der Service(s)
- behörden-/unternehmensinterne Vorgaben
- Wissen um zugrundeliegenden Anforderungen (funktionale, als auch nicht funktionale)
- Kennen der Eigenschaften (auch Sicherheitseigenschaften)

Für was ist Interoperabilität notwendig/wichtig?

Ist Interoperabilität jetzt nur eine Forderung akademischer Art,
die aufwändig ist und Kosten verursacht,
oder hat sie auch einen Mehrwert in der Praxis?

Interoperabilität - Vorteile

- **Standardisierung** (auch Dritte können prüfen, mitarbeiten, weiterentwickeln, ...)
- Einfachere **Einbindung** in das **SIEM** (Security Information and Event Management)
- Einfachere, da standardisierte, **Prüfmöglichkeiten**
- **Geringere Abhängigkeit** von einem Cloud-Anbieter oder einzelnem Service
  - Unterstützung einer **Dual- oder Multi-Vendor-Strategie**
  - Kann zur Erhöhung der Verfügbarkeit führen

Interoperabilität - Nachteile

- **Mehraufwand** bei der **Entwicklung**
  - aber kann durch Cloud-native Ansätze mitigiert werden

- **Erhöhte Kosten** durch die Einhaltung von Standards, Prüfungen, ein breiteres Angebotsspektrum
  - aber Aufwände sind nur einmal nötig
  - aber Anbieter können den Markt besser bedienen

- **Verfügbarkeit am Markt**? → Markt muss sich erst darauf einstellen/entwickeln
  - aber der Markt wird sich mit steigender Nachfrage dahin entwickeln

Interoperabilität - ein Beitrag zur digitalen Souveränität

Interoperabilität ist ein wichtiger Baustein zur Erhöhung der digitale Souveränität

Digitale Souveränität heißt – zumindest im Kontext der Bundesverwaltung – **nicht** alles **„selbst zu machen“**, sondern:

„Digitale Souveränität“ beschreibt „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt **selbstständig, selbstbestimmt und sicher** ausüben zu können“.

(Quelle: CIO Bund)

Digitale Souveränität bedeutet, eine oder die **Wahlmöglichkeit** zu haben.

Standardisierung

Standards vereinfachen die Interoperabilität

- **Standards helfen dem Cloud-Nutzer und auch -Anbieter**

Standards vereinfachen die Interoperabilität

- Standards helfen dem Cloud-Nutzer und auch -Anbieter

- **Nutzer**:
  - Standards vereinfachen **Vergleichbarkeit** von Cloud-Diensten
  - Sorgen für **Transparenz**
  - Bessere **Informationslage**
  - …

Standards vereinfachen die Interoperabilität

- Standards helfen dem Cloud-Nutzer und auch -Anbieter

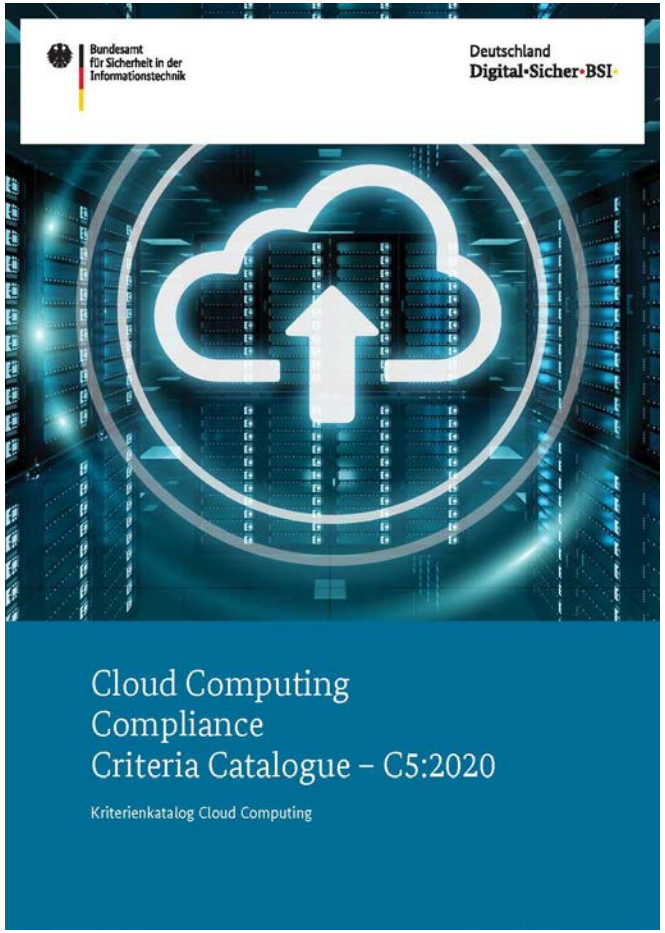
- **Anbieter**:
  - Produkte können einem **breiteren Kundenkreis** zur Verfügung gestellt werden
  - **Kommunikation** mit Kunden wird vereinfacht
  - **Sicherheitsniveau** wird gesteigert
  - …

Kriterienkatalog C5

Kriterienkatalog C5

Eckpunkte

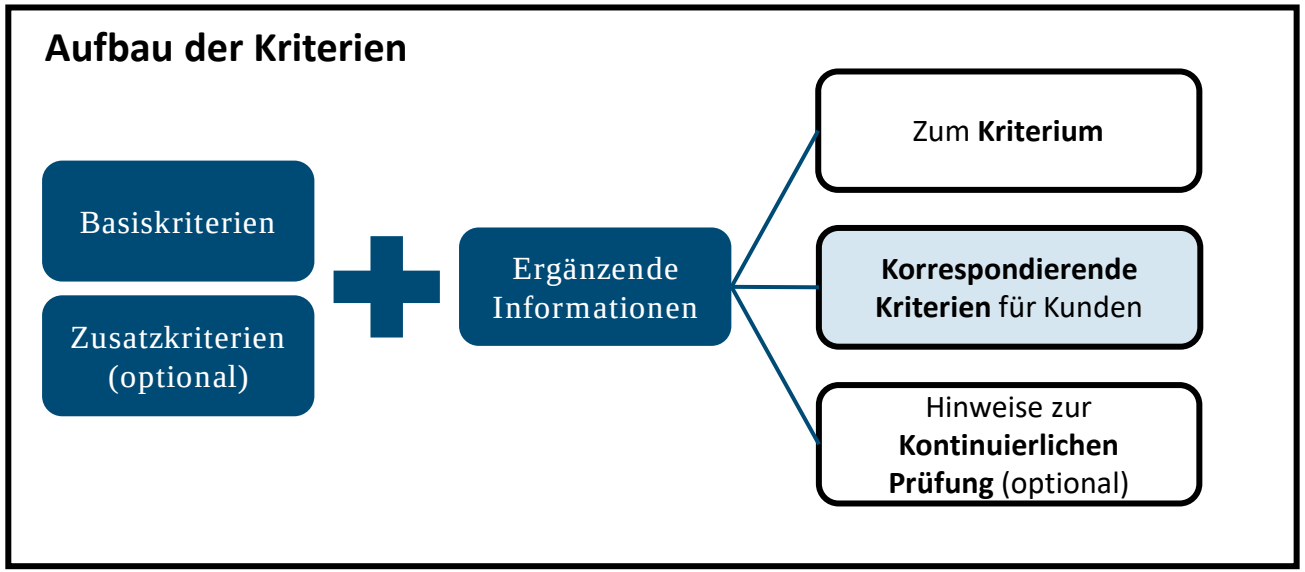
- **Cloud Computing Compliance Criteria Catalogue (C5)**
- **Zielsetzung**: Beschreibung von Mindestanforderungen an die Informationssicherheit anhand von Kriterien für Cloud-Dienste
- **Historie**:
  - Anforderungskatalog C5 (2016)
  - Überarbeitet zu Kriterienkatalog C5:2020
  - Zur Zeit in Überarbeitung
- **Grundlage des C5**: Kriterien basieren auf Anforderungen aus versch. Standards und Publikationen
- **Fokus**: Sicherheit der Cloud-Dienste, nicht des ISMS (Grundlage)
- **C5 gibt Ziele vor, nicht deren Umsetzung**



Kriterienkatalog C5

Aufbau

- Kapitel 1-3: Einleitung, Aufbau Kriterien, Details zur Prüfung
- Kapitel 4 **Rahmenbedingungen**: Angaben des Cloud-Anbieters, keine zu prüfenden Kriterien
  - **Angaben zu**:
    1. Gerichtsbarkeit und Lokationen
    2. Verfügbarkeit und Störungsbeseitigung im Normalbetrieb
    3. Wiederanlaufparametern im Notbetrieb
    4. Verfügbarkeit der Rechenzentren
    5. Umgang mit Ermittlungsanfragen staatlicher Stellen
    6. Zertifizierungen oder Bescheinigungen
- Kapitel 5 **Kriterien**:
  - **121 Kriterien** aus **17 Bereichen**
  - Bsp. Bereiche: Personal, Physische Sicherheit, Kryptographie und Schlüsselmanagement, Umgang mit Sicherheitsvorfällen, Compliance



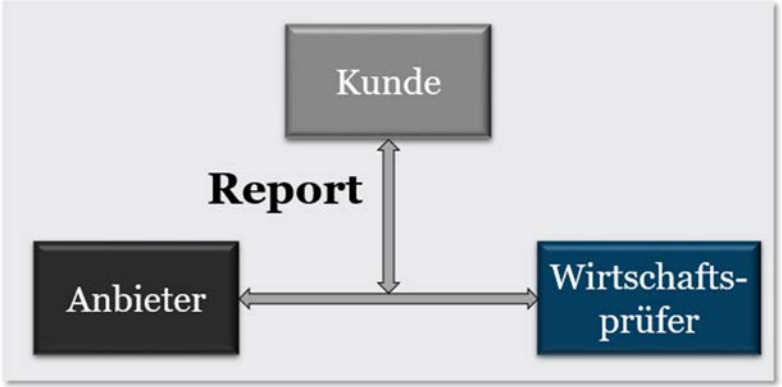
Prüfung & Testat

Prüfung

Bei einer C5-Prüfung handelt es sich immer um eine **Testierung**.

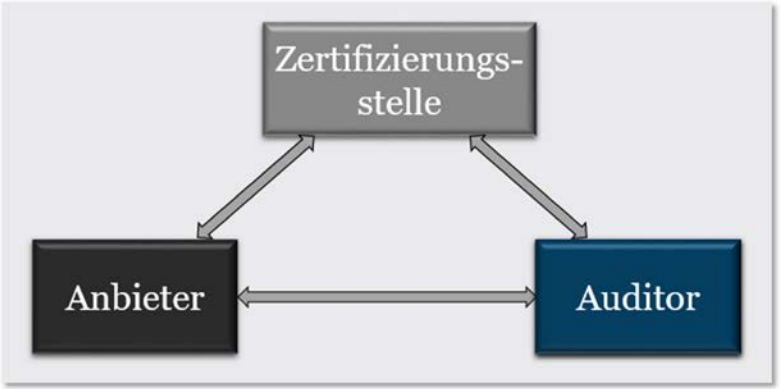
➢ Es gibt nur **C5-Testate**, keine C5-Zertifikate.

Testierung



vs.

Zertifizierung

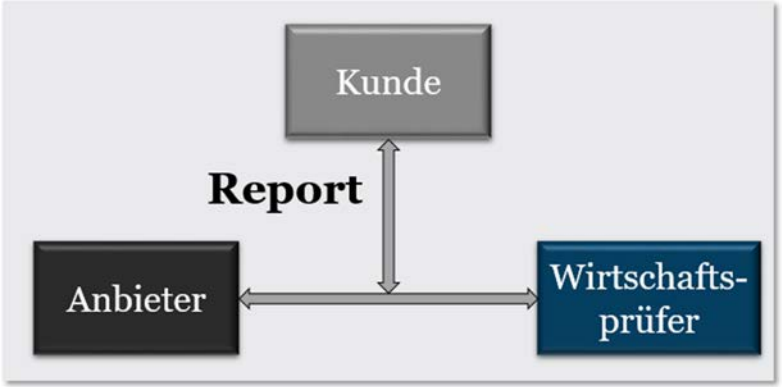


Prüfung & Testat

Prüfung

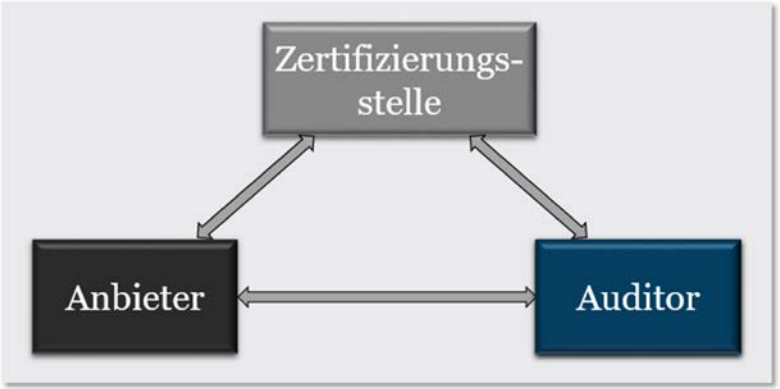
- **Wirtschaftsprüfer** prüfen **alle (Basis-)Kriterien** nach internationalen Standards (ISAE 3000), stellen Testat aus und haften für Prüfaussagen
- **Prüfungsformen (Typ 1 und Typ 2)**:
  - **Typ 1** prüft Erfüllung der Kriterien zu einem **Zeitpunkt** (Angemessenheitsprüfung)
  - **Typ 2** prüft Erfüllung der Kriterien über einen **Zeitraum** (3-12 Monate der Vergangenheit) (Wirksamkeitsprüfung)
- **Prüfungshandlungen** und **-ergebnisse** werden in einem **Bericht** dokumentiert
  - Cloud-Anbieter kann diesen an Kunden weitergeben
- Wirtschaftsprüfer stellt **C5-Testat** aus
  - Testate werden für einen oder mehrere Cloud-Dienste, **nicht** für den Cloud-Anbieter selbst ausgestellt
- **Haftung**: Wirtschaftsprüfer haftet für Prüfaussagen
- **Rolle BSI**: Erstellung des Kataloges, nicht in Prüfungsprozess involviert

Testierung



vs.

Zertifizierung



Standards vereinfachen die Interoperabilität

- Standards helfen dem Cloud-Nutzer und auch -Anbieter

- **Nutzer**:
  - Standards vereinfachen **Vergleichbarkeit** von Cloud-Diensten
    - **C5** macht Informationssicherheit vergleichbar
  - Sorgen für **Transparenz**
    - **C5** Prüfbericht und Rahmenbedingungen
  - Bessere **Informationslage**
    - **C5** Prüfbericht: Informationen über die Informationssicherheit
    - **C5** Kriterien: Dokumentationen/Anleitungen über den Cloud-Dienst

Standards vereinfachen die Interoperabilität

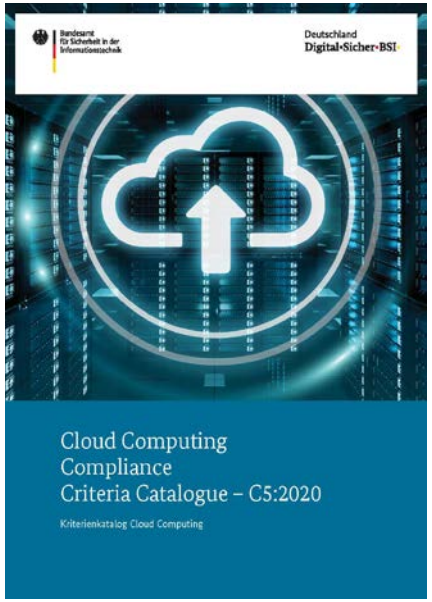
- Standards helfen dem Cloud-Nutzer und auch -Anbieter

- **Anbieter**:
  - Produkte können einem **breiteren Kundenkreis** zur Verfügung gestellt werden
  - **Kommunikation** mit Kunden wird vereinfacht
    - Anbieter kann allen Kunden den **C5** Prüfbericht zur Verfügung stellen
  - **Sicherheitsniveau** wird gesteigert
    - Für ein gutes Grundniveau: Erfüllung der **C5**-Basiskriterien

Hilfsmittel des BSI (I/III)

- **Kriterienkatalog C5**
- Kriterien C5:2020 (Editierbares Format)
- Kreuzreferenztabelle C5 zu internationalen Standards
- Kreuzreferenztabelle C5 zu ISO IEC 27001:2022

https://www.bsi.bund.de/dok/13368652



Hilfsmittel des BSI (II/III)

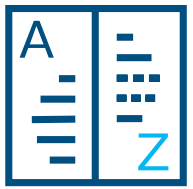
- Kurzübersicht zur Berichterstattung (Word Dokument)
- **Auswertungsleitfaden** (Excel Tabelle)

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/Auswertung/Auswertung_node.html

Hilfsmittel des BSI (III/III)

- **C5 Einführung**
  - Kunden
  - Prüfer
  - Anbieter

https://www.bsi.bund.de/dok/13447812



- **C5 FAQ**
  - 50+ Fragen & Antworten

https://www.bsi.bund.de/dok/C5-FAQ

Soweit die Theorie – gibt es Fragen?

Bundesamt
für Sicherheit in der
Informationstechnik

Vielen Dank für Ihre Aufmerksamkeit!

Christoph Pfeifer
Sachbearbeiter – Virtualisierung und Trennungsmechanismen

Sebastian Temme
Referent – Cloud-Sicherheit

cloudsecurity@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de

Follow us:

Quellen

- Wikipedia: https://de.wikipedia.org/wiki/Interoperabilit%C3%A4t
- C5: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/C5_2020.pdf?__blob=publicationFile&v=3
- Cloud-Reallabor: https://reallabor.cloud/wp-content/uploads/2024/12/Cloud-Reallabor_Year-One.pdf
- AWS: https://aws.amazon.com/de/what-is/interoperability/#:~:text=Interoperabilit%C3%A4t%20ist%20die%20F%C3%A4higkeit%20von,geografischen%2C%20politischen%20oder%20organisatorischen%20Grenzenm
- CIO Bund: https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html