Bundesamt
für Sicherheit in der
Informationstechnik

Der Anforderungskatalog des BSI zur Bewertung der Informationssicherheit von Cloud-Diensten „Cloud Computing Compliance Controls Catalogue“ (C5)

Dr. Clemens Doubrava, BSI, 29.6.2016

Nachweis der Sicherheit von Cloud-Diensten - verschiedene Blickwinkel

Nachweis der Sicherheit von Cloud-Diensten - verschiedene Blickwinkel

Cloud-Anbieter

- Bestätigung der Sicherheit
- möglichst wenige Audits
- kein Zusatzaufwand durch spez. Anforderungen/Auditierungen
- Return-on-Invest auf Audits

Nachweis der Sicherheit von Cloud-Diensten - verschiedene Blickwinkel

Cloud-Anbieter

- Bestätigung der Sicherheit
- möglichst wenige Audits
- kein Zusatzaufwand durch spez. Anforderungen/Auditierungen
- Return-on-Invest auf Audits

Cloud-Kunde

- Compliance mit Anforderungen
- Vertrauenswürdiges Zertifikat zur Sicherheit und Compliance
- einfach Überprüfung des CSP

Nachweis der Sicherheit von Cloud-Diensten - verschiedene Blickwinkel

Cloud-Anbieter

- Bestätigung der Sicherheit
- möglichst wenige Audits
- kein Zusatzaufwand durch spez. Anforderungen/Auditierungen
- Return-on-Invest auf Audits

Cloud-Kunde

- Compliance mit Anforderungen
- Vertrauenswürdiges Zertifikat zur Sicherheit und Compliance
- einfach Überprüfung des CSP

Behörden

- Gesetzliche Vorgaben einhalten
- Einfache Beschaffung
- Vergleichbarkeit der Angebote
- Sicherheits-Standards von nationalen Stellen

Nachweis der Sicherheit von Cloud-Diensten - verschiedene Blickwinkel

Cloud-Anbieter

- Bestätigung der Sicherheit
- möglichst wenige Audits
- kein Zusatzaufwand durch spez. Anforderungen/Auditierungen
- Return-on-Invest auf Audits

Cloud-Kunde

- Compliance mit Anforderungen
- Vertrauenswürdiges Zertifikat zur Sicherheit und Compliance
- einfach Überprüfung des CSP

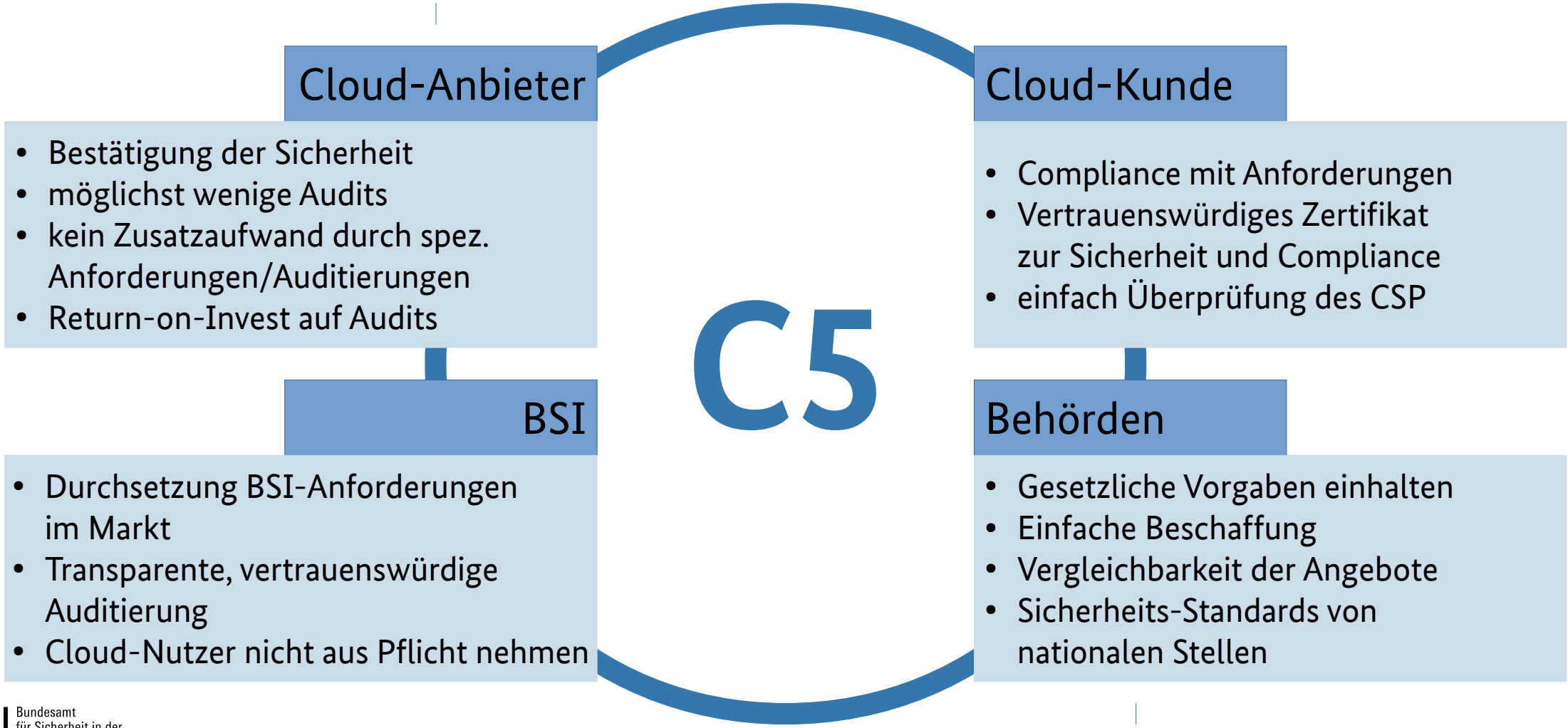
BSI

- Durchsetzung BSI-Anforderungen im Markt
- Transparente, vertrauenswürdige Auditierung
- Cloud-Nutzer nicht aus Pflicht nehmen

Behörden

- Gesetzliche Vorgaben einhalten
- Einfache Beschaffung
- Vergleichbarkeit der Angebote
- Sicherheits-Standards von nationalen Stellen

Nachweis der Sicherheit von Cloud-Diensten - verschiedene Blickwinkel



Existierende Standards/Zertifizierungen zur Cloud Sicherheit

Zusammenstellung der ENISA CCSL

- TÜV Rheinland - Certified Cloud Service
- CSA OCF – Self Assessment, Certification, Attestation
- EuroCloud - Self Assessment, Star Audit Certification
- ISO/IEC 27001
- PCI DSS
- Leet Security Rating Guide
- AICPA - Service Organization Control (SOC) 1, 2, 3
- Cloud Industry Forum Code of Practice

Weitere

- ANSSI - Certification Secure Cloud (plus)
- FEDRAMP
- Cloud Ecosystem e.V. - Trust in cloud
- France IT – Label cloud
- Trusted Cloud – Trusted cloud Label
- German Cloud
- BSI IT-Grundschutz
- …
- …
- …

Erfolgsfaktoren C5

Anforderungen

- Müssen anerkannt sein
- Möglichst aus existierenden Standards nehmen
- Ziele vorgeben und Umsetzung frei lassen
- Basis + zusätzliche Anforderungen
- Individuell erweiterbar
- Transparenz schaffen

Limitierungen

- Beschränkt auf Informationssicherheit
- Kein Datenschutz
- Keine Vertragsdetails

Auditierung

- Selbstauskunft ist nicht ausreichend
- Kein neues Verfahren einführen
- Keine neuen Strukturen aufbauen
- Vertrauenswürdigkeit bereits erwiesen
- Vollständig transparentes Verfahren
- Neutralität und Kompetenz des BSI muss sich widerspiegeln
- Für Unternehmen unterschiedlichster Größe

Anforderungen an die Informationssicherheit des Cloud-Dienstes

117 Anforderungen in 17 Kontrollbereichen

- Organisation der Informationssicherheit
- Sicherheitsrichtlinien und Arbeitsanweisungen
- Anforderungen an das Personal
- Asset Management
- Physische Sicherheit
- Maßnahmen für den Regelbetrieb
- Identitäts- und Berechtigungsmanagement
- Kryptographie und Schlüsselmanagement
- Kommunikationssicherheit
- Portabilität und Interoperabilität
- Beschaffung, Entwicklung und Änderung von Informationssystemen
- Steuerung und Überwachung von Dienstleistern und Lieferanten
- Security Incident Management
- Sicherstellung des Geschäftsbetriebes und Notfallmanagement
- Sicherheitsprüfung und -nachweis
- Compliance und Datenschutz
- Mobile Device Management

Basis-Anforderungen und ggf. weiterführende Anforderungen

Referenz Titel	Beschreibung der Basis-Anforderung	Beschreibung optionaler, weitergehenden Anforderungen	C/A	Ergänzende Informationen zur Basis-Anforderung
PS-02 Physische Zutrittskontrolle	Zugänge zu Räumlichkeiten oder Gebäuden die sensible oder kritische Informationen, Informationssysteme oder sonstige Netzwerkinfrastruktur beherbergen, sind durch physische Zutrittskontrollen gesichert und überwacht, um unbefugten Zutritt zu verhindern.	Die physischen Zutrittskontrollen erfordern eine Zwei-Faktor-Authentifizierung.	C	

Hilfstexte

Referenz Titel	Beschreibung der Basis-Anforderung	Beschreibung optionaler, weitergehenden Anforderungen	C/A	Ergänzende Informationen zur Basis-Anforderung
KRY-01 Richtlinie zur Nutzung von Verschlüsselungsverfahren und Schlüsselverwaltung	Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für Verschlüsselungsverfahren und Schlüsselverwaltung sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt, in denen die folgenden Aspekte beschrieben sind: • das Nutzen von starker Verschlüsselungsverfahren (z. B. AES) und die Verwendung von sicheren Netzwerkprotokollen, die dem Stand der Technik entsprechen (z. B. TLS, IPsec, SSH); • Risikobasierte Vorschriften für den Einsatz von Verschlüsselung die mit Schemata zur Informationsklassifikation abgeglichen sind und den Kommunikationskanal, Art, Stärke und Qualität der Verschlüsselung berücksichtigen; • Anforderungen für das sichere Erzeugen, Speichern, Archivieren, Abrufen, Verteilen, Entziehen und Löschen der Schlüssel; • Berücksichtigung der relevanten rechtlichen und regulatorischen Verpflichtungen und Anforderungen.			Der Stand der Technik bezüglich starker Verschlüsselungsverfahren und sichere Netzwerkprotokolle ist in der jeweils aktuellen Fassung der folgenden technischen Richtlinien des BSI festgelegt: • BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ • BSI TR-02102-2 „Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)“ • BSI TR-02102-3 „Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPSec) und Internet Key Exchange (IKEv2)“ • BSI TR-02102-4 „Kryptographische Verfahren: Verwendung von Secure Shell (SSH)“

Referenzierung des Anforderungskatalogs auf internationale Standards

- Referenzierung auf Anforderungen anderer Standards
- Hinweis auf Über-/Untererfüllung

Basis-Anforderung	ISO/IEC 27001:2013		CSA Cloud Controls Matrix 3.01		AICPA - Trust Services Principles Criteria 2014		ANSSI Référentiel Secure Cloud 2.0 (Draft)		IDW ERS FAIT 5 04.11.2014		BSI IT-Grundschutz 14. EL 2014		BSI SaaS Sicherheitsprofile 2014	
Ref.	Ref.	SN	Ref.	SN	Ref.	SN	Ref.	SN	Ref.	SN	Ref.	SN	Ref.	SN
RB-10	A.12.4.1 A.12.4.2 A.12.4.3	0	IVS-01	0	CC6.1 CC6.2	-	12.6 12.7 12.9	0	Tz. 97	+	M 2.64 M 2.110 M 2.133 M 2.497 M 2.499 M 2.500 M 4.81 M 4.430 M 4.443 M 5.9 B 5.22	0	SIM-01 M1.03	-

Anforderungen an die Transparenz (Umfeldparameter)

- **Umfeldparameter** schaffen Transparenz über
  - **Systembeschreibung**: Details des Cloud-Dienstes (Infrastruktur, Standorte, Unterauftragnehmer, etc.)
  - **Gerichtsbarkeit, Datenlokationen** (auch der Sicherungen und auch von Unterauftragnehmern)
  - Bestehende **Ermittlungsbefugnisse** von oder **Offenbarungspflichten** gegenüber staatlichen Stellen (auch durch Unterauftragnehmer)
  - Vorhandene **Zertifikate** und deren Reichweite

- Umfeldparameter geben diese Eigenschaften ***nicht*** vor, sondern fordern lediglich die Transparenz

Die Prüfung

- Prüfung folgt **ISAE 3000** („International Standards for Assurance Engagements“)
  „Assurance Engagements Other than Audits or Reviews of Historical Financial Information“ umfasst:
  - allgemeine Anforderungen an die Qualifikation und das Verhalten eines Prüfers
    (z. B. sachverständige Beurteilung und Skepsis),
  - Annahme, Planung und Durchführung eines Prüfauftrags,
  - allgemeine Anforderungen an Prüfungskriterien enthalten.
- Prüfungsvorgehen, Dokumentation und Berichterstattung folgen sinngemäß der
  ISAE 3402 „Assurance Reports on Controls at a Service Organization“
  (ähnlich zu IDW PS 951 n.F. „Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen“)

- Ziel ist: **Effiziente Prüfung**
  - Prinzip „Audit Once – Certify Many“
  - Kombination mit anderen Zertifizierungen (z. B. ISO 27001/22301 oder auch Datenschutz) möglich

Das Prüfteam

- Allgemeine Anforderungen aus ISAE 3000 (bspw. zur Unabhängigkeit)
- Wird geleitet von einem **Wirtschaftsprüfer**
- Muss mindestens zur Hälfte aus Personen mit
  - mindestens 3 Jahren **Berufserfahrung** in Wirtschaftsprüfung und
  - einschlägiger **Berufsqualifizierung** bestehen, wie:
    - ISACA CISA o. CISM,
    - CSA CCSK,
    - ISO 27001 Auditoren, BSI IT-Grundschutz Auditoren,
    - ISC² CCSP.

- Komplettes Prüfteam, inklusive Berufsqualifikationen ist im Prüfbericht nachgewiesen

Der Prüfbericht

- Folgt den Vorgaben eines **ISAE 3402 / SOC 1 / SOC 2-Berichts** (SOC = „Service Organization Controls“)
- Zu jeder Anforderung gibt es **dokumentierte Prüfnachweise** (Dokumente & Interviews, Begehungen, etc.) und **Urteil**, ob die Kontrollen zu dieser Anforderung über einen Zeitraum der Vergangenheit hinweg wirksam waren.
- Es gibt die Freiheit des „Professional Judgements“. Diese sind aber eng begrenzt und insofern nicht beliebig
  - Insbesondere muss der Bericht alle Informationen enthalten, damit der sachverständige Leser das **Gesamturteil nachvollziehen** kann und in seiner Beurteilung dann zum gleichen Urteil gelangt, wie der Prüfer
  - Die Ergebnisse der Prüfung müssen mithin jederzeit den Nachfragen der Berichtsadressaten und erforderlichenfalls auch einer **gerichtlichen Überprüfung standhalten**.

- Einstieg über eine reine Prüfung der Angemessenheit möglich – Wiederholung ausgeschlossen

Umgang mit Unterauftragnehmern

- **Alle Unterauftragnehmer müssen bei den Umfeldparametern genannt werden**
- Sofern sie wesentliche Teile für den Cloud-Dienst erbringen:
  - Alle **Anforderungen werden an Unterauftragnehmer weiter gegeben**
  - **Einhaltung wird geprüft**
  - **Umfeldparameter** müssen erhoben werden
  - Einbindung des Auftraggebers ins **Incident-Handling**

- Für die **Prüfung**:
  - Entweder Prüfer prüft Unterauftragnehmer komplett mit
  - Oder Prüfer prüft nur den Auftraggeber und prüft, ob dieser die Einhaltung der Anforderungen regelmäßig prüft (z. B. durch Vorlage eines Prüfberichts nach diesem Katalog)

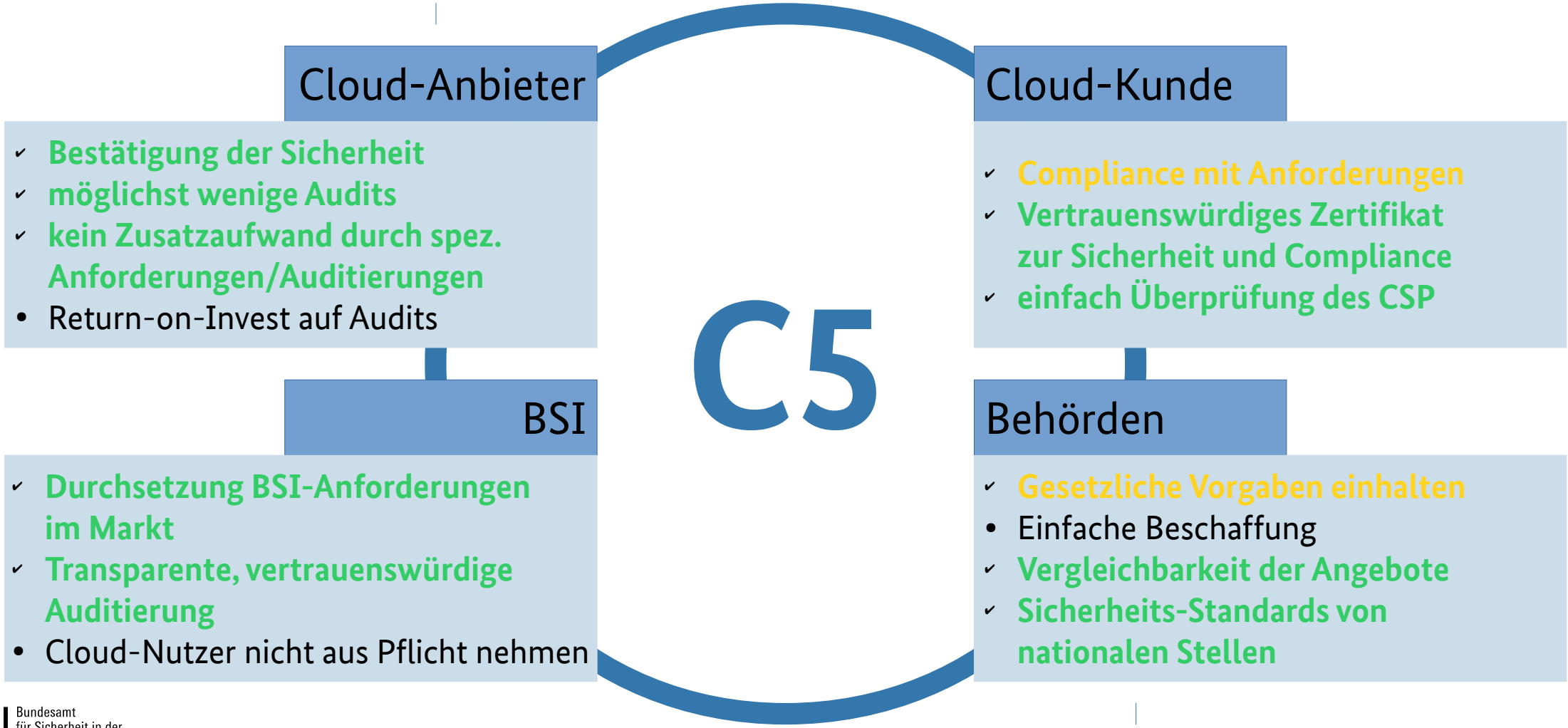
Was hat der Kunde zu tun?

- Der Kunde darf sich **nicht auf Selbstauskunft oder Testat alleine verlassen**
- Der Kunde muss Anbieter auf die **Einhaltung der Anforderungen vertraglich verpflichten**
- Der Kunde muss sich regelmäßig **Testat und Prüfbericht vorlegen lassen** und den Umgang mit Abweichungen und Änderungen regeln
- Der **Kunde sollte den Prüfbericht selbst sichten und bewerten**

Woran der Kunde sonst noch denken kann:

- Der Kunde kann **eigene, Einsatz-Szenario-abhängige Anforderungen** (oder sogar Maßnahmen) definieren
- Diese zusätzlichen Anforderungen/Maßnahmen können ggf. Gegenstand von Prüfungen werden
- Ggf. sind Teile dieser eigenen Anforderungen durch einzelne weiterführende Anforderungen adressiert

Was deckt C5 ab?



Vielen Dank
für Ihre Aufmerksamkeit!

https://www.bsi.bund.de/C5

Kontakt

Dr.-Ing. Clemens Doubrava
Referent
cloudsecurity@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik
Referat B25
Postfach 20 03 63
53133 Bonn
https://www.bsi.bund.de/cloud

Bundesamt
für Sicherheit in der
Informationstechnik