Cloud-Grundlagen und Definitionen

Cloud Computing Grundlagen - Bundesamt für Sicherheit in der Informationstechnik (BSI)
https://www.bsi.bund.de/dok/6622124

Tipps für den Umgang mit TOMs und ISDS-Vorgaben

- Vorgehen, Umfang und Detaillierungsgrad der Vorgaben dem Anwendungsfall bzw. Ausschreibungsgegenstand anpassen. Es gilt den Markt und die «best practices» der potenziellen Auftragnehmer zu kennen.
- Bei der Formulierung von TOMs den Zweck im Auge behalten:
  - Auftraggeber: Risikovermeidung, Dokumentationspflicht, Vorgaben an Auftragnehmer, periodische Überprüfung
  - Auftragnehmer: Risikovermeidung, Dokumentationspflicht, «Verkaufsargumente», Gewährleistung, Haftung

  Sie sind üblicherweise Anhang zu einer Auftragsdatenbearbeitungsvereinbarung (ADV)
- Für die Gesamtsicherheit einer Organisation bzw. deren Systeme sind alle TOMs wichtig, die eigenen wie diejenigen von Auftragnehmern/Providern. Eine durch «Brainstorming» gewonnen Gesamtaufstellung von TOMs eignet sich jedoch nicht als Anforderungsdokument oder Vertragsvorlage. Die vom Anbieter erwarteten TOMs sind sorgfältig auszuformulieren (richtiger Abstraktionslevel) und vor der Ausschreibung gegen den Markt zu prüfen. Anforderungen an die Zertifizierung (ISO 27001, ISO2717, ISO 27018, ISA 3402, SOC Type 2) sind hilfreich, aber als Vorgabe nicht ausreichend.
- Zur Sicherstellung der Minimalanforderungen führt kein Weg vorbei an einigen wenigen «harten» Anforderungen, üblicherweise als technische Spezifikationen formuliert (z.B. verschlüsselte Kommunikation, verschlüsselte Datenträger, verschlüsselte Datenbank, usw.). Diese müssen 100% gegen den Markt geprüft sein – ansonsten besteht das Risiko, keine Angebote zu erhalten.
- Bei der Formulierung von TOMs durch die Anbieter (AGB der Anbieter) ist ein gewisser Abstraktionslevel zu akzeptieren (ohne, dass die Definitionen komplett nichtssagend werden). Wichtiger als die Formulierung im Einzelnen ist, dass
  - Belege beigebracht werden (z.B. Zertifizierungen, Verträge mit Subunternehmern, ext. Audits)
  - Kontrollen durch den Auftragnehmer möglich sind (AGB/Vertragsbedingungen, Zugriffs-Logs)
  - die Darlegungen und Vertragsbedingungen insgesamt den «Reifegrad» des Anbieters bezeugen (→ Checkliste)
- Vorgehen bei der Evaluation und beim Vertragsabschluss
  - Technische Spezifikationen und Eignungskriterien prüfen (zwingende Vorgaben)
  - Anforderungen (Zuschlagskriterien) bewerten
  - Anbieter-TOMs (AGB, Vertragsbedingungen) gegen Anforderungen/Checkliste prüfen und nachverhandeln
  - Nachweise und periodische Re-Evaluation verlangen (z.B. externe Auditbericht)
- «Red-Flags» bei Anbieter-TOMs:
  - Subunternehmer werden nicht ausgewiesen
  - Keine Auftragskontrolle für Subunternehmer
  - keine periodische Überprüfung von Massnahmen vorgesehen
  - keine Angaben zur Behandlung von Sicherheitsvorfällen
- Best Practice bei Anbieter-TOMs:
  - Verantwortliche (DSB und ISB) sind benannt
  - Liste der internen Richtlinien/Dokumentation (IT-Security Policy, Secure Development Rules, usw.)
  - Externe Audits/Testate vorhanden und werden periodisch erneuert, sind für Auftraggeber zugänglich
  - Anbieter lässt periodisch externe Penetration-Tests durchführen
  - Angaben zu Home Office / VPN
  - Extensive Protokollierung (URL-Zugriffe, Mutationslogs, usw.)
- Wichtigste Vorgaben gemäss «12 Golden TOMs» (Rosenthal/Becker 2024)
  - IAM mit MFA für alle User mit Zugriff zu Kundendaten, TPAM für Administratoren
  - Kundenspezifische Schlüssel (Datenbank, Dokumente), Key Vault / HSM
  - Geo-Lokalisierung der Datenhaltung und (technische) Vorgaben für die Regelung grenzüberschreitender Zugriffe
  - Log-Management (nicht-modifzierbar, einsehbar durch Kunden)
  - Pen-Testing (jährlicher Nachweis)
  - Trennung von Test- und Produktivumgebungen
  - Subcontractor Risk Management