UP KRITIS

Checkliste zur Auswahl eines Cloud-Dienstes

Version 1.0

Freigegeben vom Plenum des UP KRITIS, Sitzung 2022-1, 31.03.2022

Themenarbeitskreis „Nutzung cloudbasierter Dienste“ des UP KRITIS

www.upkritis.de

Download dieses Dokuments unter https://www.bsi.bund.de/dok/1043078

Inhalt

1 Zusammenfassung/Management Summary

Zielgruppe dieses Dokuments sind kleine und mittelständische Unternehmen aus den Sektoren der Kritischen Infrastrukturen, welche beabsichtigen, Cloud-Dienste künftig zu nutzen oder dies bereits tun, unabhängig davon, ob das Unternehmen nach BSI-KritisV eine Kritische Infrastruktur ist.

Liegen bei einem Unternehmen gesetzliche oder regulatorische Besonderheiten vor, besteht die Möglichkeit, dass diese Besonderheiten in diesem Dokument unberücksichtigt sind.

Dieses Dokument

- soll Unternehmen dabei unterstützen, notwendige Aspekte bei der Nutzung von Cloud-Dienstleistungen zu prüfen und zu planen.
- erhebt keinen Anspruch auf Vollständigkeit. Es stellt keine abschließende Checkliste oder Testatgrundlage dar.
- definiert nicht einen Stand der Technik bei der Nutzung von Cloud-Dienstleistungen.

2 Lebensnutzungszyklus eines Cloud-Dienstes

2.1 Nutzeranforderung, fachliche Bewertung, Produktvorauswahl, Marktsichtung

- Für welche Anforderung wird eine Lösung gesucht? Benötigen wir fachlich diese Lösung?
- Welche Lösungen bietet der Markt?

2.2 Bewertungen (technisch-organisatorisch), Datenschutz, Informationssicherheit

- Können wir die angedachten Lösungen in unserem Unternehmen integrieren?
- Welche Risiken existieren und wie gehen wir damit um?

2.3 Managementbewertung, Managemententscheidung

- Wollen wir die Lösung unter diesen Voraussetzungen und Rahmenbedingungen?

2.4 Beschaffung

- Beschaffung einer Lösung auf dem Markt

2.5 Implementierung, Produktivabnahme

- Installieren
- Konfigurieren
- Integrieren
- Aufbauen
- Schulen
- etc.

2.6 Betrieb, Betriebsübergang/Migration, Betriebsende

- Wir nutzen die Lösung und halten sie aktuell.
- Exit-Strategie wird angewendet und Cloudlösung migriert.
- Daten auf dem Clouddienst werden dokumentiert gelöscht.

3 Hinweise zur Bearbeitung der Arbeitsschritte

3.1 Anforderung erstellen

3.1.1 Zielsetzung:

Anforderung und Sicherheitsniveau ist bekannt, Übereinstimmung mit Cloud-Strategie geprüft, fachliche Freigabe erteilt, vorläufige Budgetfreigabe erteilt, sofern erforderlich Freigabe des Datenschutzes eingeholt, sofern erforderlich Freigabe des Betriebsrats eingeholt

3.1.2 Verantwortlichkeiten

Fachbereich (Anfordernde, Nutzende, Risikoeigner), fachliche Entscheidungsgremien, Controlling

3.1.3 Anforderungsinhalte (mindestens)

- Verwendungszweck/Einsatzzweck der IT-Ressource definieren
- Unterstützte Geschäftsprozesse definieren
- Informationen, die verarbeitet werden sollen, sind zu beschreiben, inklusive der Informationsklassifizierung (z.B. öffentlich, intern, vertraulich, streng vertraulich).
- Kritikalität für alle betroffenen Geschäftsprozesse gemäß den eigenen Vorgaben aus dem Risiko-Management bestimmen
- Ermitteln, ob mittels Cloud-Dienstleistung unterstützte Geschäftsprozesse zur Erbringung von kritischen Dienstleistungen (nach BSI-KritisV § 1) eingesetzt werden.
- Vorgaben (z. B. aus branchenspezifischen Sicherheitsstandards) sollten berücksichtigt werden.
- Generell sollte der Stand der Technik eingehalten werden. Für die Erbringung kritischer Dienstleistungen (nach BSI-KritisV) muss der Stand der Technik eingehalten werden.
- Sollen personenbezogene Daten (z.B. Identitätsdaten) verarbeitet werden, ist die Einbindung des Datenschutzbeauftragten sicherzustellen.
- Prüfung, ob eine Mitbestimmungspflicht des Betriebsrats besteht und ggf. einholen
- Prüfung ob Speicherort der Daten relevant ist, insbesondere wegen Datenschutz. Ggf. Berücksichtigung des US CLOUD Act
- Bei Nutzung von Cloud-Services muss eine Cloud-Strategie existieren.
- Die Cloud-Strategie muss im Einklang mit der IT-Sicherheitsstrategie sein.
- Einordnung des Projekts in die organisationsinterne Cloud-Strategie
- Schutzbedarfsanforderungen: Verfügbarkeitsanforderung, Integritätsanforderung, Vertraulichkeitsanforderung, ggf. Authentizitätsanforderungen definieren

3.1.4 Bewertung der Anforderung

- mögliche Kriterien:
  - fachlich sinnvoll,
  - Auswirkungen auf betroffene Geschäftsprozesse absehbar (positiv/negativ),

    - Betroffenheit von kritischen Dienstleistungen nach BSI-KritisV,
    - Ähnliches schon vorhanden,
    - wirtschaftlich (Make or Buy),
    - wirtschaftliche Rahmenbedingungen bei der Nutzung eines Cloud-Dienstes vorklären (Übergang von Investitionskosten (Softwarebeschaffung) zu Betriebskosten (Bezahlung nach Nutzung)),
    - notwendige Personalressourcen für die Einführung/Betrieb
    - Geschätztes Budget für Investitionskosten, Sachmittel inkl. Wartung
- Sind die Unternehmensvorgaben ausreichend berücksichtigt und lassen diese die Verarbeitung in einem Cloud-Dienst zu?
- Sind die gesetzlichen und regulatorischen Vorgaben berücksichtigt und lassen diese die Verarbeitung in einem Cloud-Dienst zu?
- Prüfung, welche Rollen in der Anforderungserstellung beteiligt sind und wer welche Verantwortlichkeiten übernimmt. Den Rollen müssen Personen zugeordnet werden.
- Sollten kritische Dienstleistungen erbracht werden, ist zu beachten, dass der Betreiber die Verantwortung für die Erbringung der kritischen Dienstleistung nicht abgeben kann.

3.2 Produktvorauswahl Marktsichtung

3.2.1 Zielsetzung

- Lösungen auf dem Markt finden, die integriert werden können. Gewinnen von Erkenntnissen, welche Rahmenbedingungen im Unternehmen geschaffen werden müssen, damit eine digitale Unterstützung erfolgen kann.

3.2.2 Verantwortlichkeiten

- Fachbereich

3.2.3 Anforderungsinhalte (mindestens)

- Z. B. vor einer Ausschreibung oder Angebotseinholung findet eine Marktsichtung statt. Im Anschluss an die Marktsichtung kann für die in Frage kommenden Produkte die nachfolgende technisch-organisatorische Integrationsbewertung durchgeführt werden.
- Evtl. ist es bereits bei Angebotseinholung sinnvoll, eine Produkt- und Lieferantenbewertung bezüglich Informationssicherheit zu erstellen.

3.3 Bewertung der technisch- organisatorischen Integration

3.3.1 Zielsetzung

- technische und organisatorische Einbindung und Verantwortung ist geklärt

3.3.2 Verantwortlichkeiten

- Informationstechnologie, Auftragnehmer, Fachbereich

3.3.3 Integrationsthemen (mindestens)

- Anforderungen an Netzwerke, Schnittstellen und IT- Sicherheitskomponenten durch die Cloud-Integration erarbeiten.
- Schlüssel- und Zertifikatsverwaltung (ggf. rechtliche Vorgaben beachten) für u. a. Datenhaltung, Datentransfer, Backup und weitere Themen etablieren.
- Integration in die Service-Governance-, Betriebs- und Support-Prozesse.
- Bei Betroffenheit BSI-Gesetz: Integration in das Meldewesen, inklusive Bei Betroffenheit BSI-Gesetz: Integration in das Meldewesen, inklusive Kontakte/Meldewege zum AN.
- Integration in das organisationsinterne Informationssicherheitsmanagementsystem (ISMS).
- Berücksichtigung der Cloud-Anteile bei den Nachweisen gem. § 8a Absatz 3 BSIG.
- Einsatz von Komponenten (Hardware, virtuelle Komponenten, Software, Bibliotheken) bewerten.
- Schnittstellenkonzept zu anderen internen und externen Systemen erstellen.
- Bei Bedarf E-Mail-Schnittstelle definieren (eigener/ E-Mailserver des AN).
- Definition des Zugangsweges: Installation eines Clients, Zugriff über Browser nativ oder weitere Zusatzkomponenten (Plugin, Add-On).
- Definition der Staging-Modelle: Entwicklung, Test und Produktionsbereiche
- Systemarchitekturbild erstellen
- Logmanagement und Frühwarnsysteme, Einbindung in die Security-Operationsprozesse
- Benutzer- und Berechtigungskonzept, privilegierte Rechte, Nutzerverwaltung über Identity & Access Management
- Archivierungsanforderungen definieren
- Fernwartungsanforderungen definieren
- Klärung der Verantwortlichkeiten für Risikoeigner, Asset-Eigner, Applikations-/Serviceverantwortliche (fachlich), Systembetreiber (technisch, intern/extern)

3.4 Bewertungen

3.4.1 Zielsetzung

- Lieferant ist hinsichtlich der Informationssicherheit beurteilt.
- Risiken sind bekannt und Maßnahmen benannt (Risikobewertung).
- Datenschutzrechtliche Beurteilung liegt vor.
- Managementbewertung der Risiken liegt vor (fachliche Freigabe).

3.4.2 Verantwortlichkeiten

- Einkauf, Datenschutzbeauftragter, Risikomanager, Informationssicherheitsbeauftragter, Informationstechnologie

3.4.3 Bewertungsthemen (mindestens)

3.4.3.1 Bewertung des/der Auftragnehmer(s) (wenn diese schon feststehen, ansonsten im Rahmen der Ausschreibung)

- Informationssicherheit des Auftragnehmers
- Informationssicherheit der Datenverarbeitungsanlage (RZ)
- Informationssicherheit der Softwareentwicklung
- Optional/zusätzlich: Bereits klären, ob die unternehmenseigenen Vertragsanforderungen für Cloud-Dienste durch den AN akzeptiert werden.
- Informationssicherheit und insb. Verfügbarkeit der Netzwerkverbindung zwischen dem Auftragnehmer und dem Auftraggeber
- Preisstruktur der letzten Jahre, um Preissteigerungen einkalkulieren zu können
- Übersichtlichkeit der erwarteten Kosten/Preisgestaltung
- Kundenzufriedenheit, Referenzen
- Aufwand der Migration in die Cloud, zu anderen Cloudsystemen, aus der Cloud

3.4.3.2 Bewertung der Risiken

- Risikomatrix erstellen mit Gefährdungen / Bedrohungen / Schwachstellen, Risiken, Wahrscheinlichkeit des Eintritts, Auswirkung des Ereignisses, Maßnahmen, Verantwortung
- Kompatibilität mit IT-Sicherheitskonzept des Unternehmens abgleichen

3.4.3.3 Bewertung der datenschutzrechtlichen Aspekte

Themen können sein:

- Einbeziehung des Datenschutzbeauftragten (DSB)
- Anforderungen an die Auftragsverarbeitung-Vertragsgrundlagen,
  Bewertung der technisch-organisatorischen Maßnahmen,
  Klärung des Standortes der Datenverarbeitung gemäß DSGVO
- Ggf. Datenschutzfolgeabschätzung
- Bewertung der Rückholbarkeit der Daten
- Besonders schützenswerte Daten

3.4.3.4 Beurteilung der Risiken durch das Management / Risikoeigner

Der Risikoeigner beurteilt, ob die bekannten Rest-Risiken akzeptiert werden können, und sichert die Risikomaßnahmenumsetzung zu. Hiermit erfolgt eine fachliche Freigabe unter diesen Rahmenbedingungen.

3.5 Ausschreibungsprozess

3.5.1 Zielsetzung

Finden einer geeigneten fachlichen, technischen und dem gewünschten Sicherheitsniveau entsprechenden Lösung.

3.5.2 Verantwortlichkeiten

Fachbereich, Einkauf, Rechtsabteilung, Informationstechnologie

3.5.3 Ausschreibungsthemen

Folgende Anforderungen sind mindestens bei Ausschreibung und Auswahl zu berücksichtigen:

- Fachspezifisch
- Sicherheit
- Datenschutz
- Infrastruktur
- Vertragsgestaltung

Siehe auch Kapitel 4.1, die dort genannten Punkte sind im Rahmen einer Ausschreibung oder Angebotseinholung zu berücksichtigen.

Bei Ausschreibungen/Einholung von Angeboten müssen die Anforderungen an Testate/Zertifikate für die Cloud-Dienstleistung Teil der Ausschreibung und mit den Unternehmensvorgaben harmonieren.

Vorkehrungen für eine Exit-Strategie sind in der Ausschreibung zu berücksichtigen

3.6 Bestellvorgang

3.6.1 Zielsetzung

Freigegebene Bestellung

3.6.2 Verantwortlichkeiten

Fachbereich, Einkauf

3.6.3 Bestellvorgang

Siehe Kapitel 4.1 für ein Beispiel einer Vertragsgestaltung (Themenpunkte und Inhalte)

Es müssen sich mindestens die Maßnahmen aus der Risikobewertung wiederfinden, entweder in den Verträgen und/oder in den Leistungsanforderungen.

3.6.4 Beurteilung der getroffenen Vereinbarungen und der Maßnahmenbeachtung

Durch den Einsatz von freigegebenen Standardmaßnahmen kann die Beurteilung beschleunigt werden:

a) Fachliche Beurteilung Fachbereich
b) Technische Beurteilung
c) Beurteilung Informationssicherheit
d) Beurteilung der relevanten Vorgaben und Richtlinien (Compliance, u. a. Datenschutz durch den DSB)

3.7 Implementierung der IT-Ressource

3.7.1 Zielsetzung

Implementierte IT-Ressource vor Inbetriebnahme, aktualisierte Risikobewertung durch den Implementierenden

3.7.2 Verantwortlichkeiten

Informationstechnologie

3.7.3 Themen bei der Implementierung

- Berücksichtigung der Maßnahmen aus der Risikobewertung und der vertraglichen Vereinbarungen.
- Schulung der Entwickler, Administratoren und Anwender
- Dokumentation

3.8 Inbetriebnahme, Betriebsabnahme, Produktionsabnahme

3.8.1 Zielsetzung

Freigabe der IT-Ressource in den produktiven Betrieb

3.8.2 Verantwortlichkeiten

Fachbereich, Informationstechnologie, Informationssicherheit

3.8.3 Bewertung der Umsetzung

- Prüfung der Maßnahmenumsetzung aus Risikobewertung und vertraglicher Vereinbarung
- Technisches Audit: Schwachstellentest, Penetrationstest
- Fachliche Abnahme durch Fachabteilung
- Technische Abnahme durch Systembetreiber / Service Manager / Applikationsverantwortlichen
- Nacharbeit, wenn notwendig, evtl. Folgebewertung
- Beurteilung der Risiken durch das Management / Risikoeigner:
  Der Risikoeigner beurteilt, ob die bekannten Restrisiken übernommen werden oder nicht.

3.9 Betrieb

3.9.1 Zielsetzung

Dokumentierte Kontrolle des Cloud-Dienstes und des Auftragnehmers

3.9.2 Verantwortlichkeiten

Informationstechnologie, Servicemanagement, Fachbereich

3.9.3 Themen während des Betriebs

- Regelmäßige Kontrolle der Leistungen des Auftragnehmers durch den Service Manager/ Applikationsverantwortlichen.
- Prüfung der vom Auftragnehmer zur Verfügung gestellten Informationen zu Funktionsänderungen des Angebots.
- Anlassbezogene oder regelmäßiges Lieferantenaudits
- Regelmäßige Übung der Notfall- / Geschäftsfortführungspläne.
- Bei Änderung der Systemarchitektur (beim KRITIS-Betreiber oder dem Auftragnehmer) oder Änderung der gesetzlichen Vorgaben ist eine erneute Risikobewertung mit Maßnahmenfestlegung notwendig.
- Bei Betroffenheit BSI-Gesetz: Integration in das Nachweis- und das Meldeverfahren

- Umsetzung des Cloud-Nutzungskonzepts
- Überwachung des Cloud-Dienstes, insbesondere:
    - Updates einspielen
    - Änderungen der Funktionen beim Auftragnehmer überwachen
    - Überwachung der Ereignisse
    - Rechtemanagement, insbesondere, wenn Nutzer hinzukommen oder entfallen

3.10 Betriebsübergang

U. a. Exit-Strategie anwenden

3.11 Betriebsende

U. a. dokumentierte Datenlöschung

4 Anlage

4.1 Möglicher Vertragsaufbau und zu regelnde Inhalte bei der Nutzung von Cloud-Diensten

4.1.1 Vertragsart(en) festlegen

- Mietvertrag, Einrichtung Dienstleistung, Auftragsverarbeitungs-Vertrag
- Hausvertrag, Vertrag des Auftragnehmers (evtl. individuell ergänzt), ggf. EVB IT
- Ort der Dienstleistung (Deutschland, Europa, weltweit)

Vertragsgegenstand, Art und Umfang der Leistung

- Übergabepunkt des Service festlegen
- SaaS: Bereitstellung von (Anwendungs-)Software
- IaaS/PaaS: Rechenzentrumsleistung, Service-/Wartungs-Leistung
- Leistungsbeschreibung
- Speicherort der Daten (wg. Zugriffsrechten durch Regierungen/CLOUD Act)

4.1.2 Service Level Agreement (SLA)

- Qualität der Leistung beschreiben
- Berechnungen beschreiben (z. B. Verfügbarkeit)
- Rechtsfolgen, Bonus/Malus
- Achtung bzgl. Kündigungen aufgrund mangelnder Leistung: Klärung der aufrecht-zuerhaltenden Geschäftsprozesse und Übergabe alle notwendigen Daten

4.1.3 Security Level Agreement (SecLA)

- Ggf. Nutzung der Vorlage für ein Security Level Agreement des UP KRITIS

4.1.4 Subunternehmer

- Vertragliche Regelung zu Vereinbarungen mit den eingesetzten Subunternehmen und deren Kontrolle
- Sofern sinnvoll: eine Liste erstellen mit den Subunternehmern und deren Aufgaben (immer mit direktem Leistungserbringungsbezug)
- Regelungen zum Einsatz und/oder Auswahl von Subunternehmen

4.1.5 Vergütung

- Abrechnung, Pauschalen, Preisanpassung
- Die Kündigungsfristen sind der Exit-Strategie anzupassen, wenn eine Preisanpassung einen Kündigungsgrund darstellt.

4.1.6 Geheimhaltung, Informationssicherheit, Datenschutz

- Auftragsdatenverarbeitung abschließen (DSB)
- Verpflichtung auf technische/organisatorische Maßnahmen

- Weisungsbefugnis/Kontrollrecht des AG
- Verarbeitungsort der Informationen festlegen
- Definition des Zeitraumes der Verpflichtung zur Datenaufbewahrung mit Löschfristen vertraglich regeln

4.1.7 Urheber und patentrechtliche Nutzungsrechte

- Nutzungsrechte an den eigenen Daten klären
- Freistellung AG vor Ansprüchen Dritter bzgl. Urheber/Nutzungsrechte (Lizenzproblematiken auf AN verlagern)

4.1.8 Mitwirkungspflichten, Beistellungen, Nebenpflichten

- Mitwirkungspflichten AG zur Nutzung des Cloud-Dienstes (z. B. Internetanschluss, Firewall-Freischaltung, …)
- Nebenpflichten AG, z.B. Geheimhaltung Login-Infos, Virenschutz, … also alles, was vom AG zu Gefahren beim AN führen kann
- Mitwirkungen des AN bei Penetrationstests, Audits, Nachweiserstellung nach BSIG etc.

4.1.9 Gewährleistung, Haftung, Schadensersatz

- Ansprüche Mängel: Hier hängt es stark vom Vertragstyp ab.
- Haftungsbeschränkungen und Haftungsnachweis klären
- Vertragsstrafen: auch hier Vorsicht vor außerordentlichen Kündigungsrechten des AN
- Evtl. auch in den SLA beschrieben

4.1.10 Vertragsbeginn, -laufzeit, Beendigung

- Automatische Verlängerungen und öffentliche Vergabe berücksichtigen
- Fristen sind so zu wählen, dass Migrations-/Exit-Szenarien realistisch sind
- Außerordentliche Kündigungen und Kündigungen ohne Grund ebenfalls bzgl. Migrations-/ Exit-Szenarien realistisch festlegen
- Insolvenzfall berücksichtigen

4.1.11 Beendigungsunterstützung, Exit-Management

- Rückführung der Daten konkret regeln
- Löschen aller gespeicherte Daten beim Auftragnehmer unter Berücksichtigung der vereinbarten Lösch- und Aufbewahrungsfristen.
- Überleitung der Leistungserbringung an anderen Cloud-Dienst oder Re-Integration On Premises definieren.

- Beendigungsunterstützung des Auftragnehmers regeln: frühzeitige (gestaffelte) Herausgabe von Datenbeständen in geeigneten Formaten (Formate grob definieren, Datenbank-Backup/ Dump, CSV, XML, Online Übertragung). Vermittlung von Know-how, Dokumentation Datenaufbau, Einräumung von urheberrechtlichen Nutzungsrechten an Software, Migrationsunterstützung und übergangsweise Leistungserbringung des SaaS auch nach dem eigentlichen Vertragsende.
- Kosten und Bereitstellungsarten definieren

4.1.12 IT-/Informationssicherheit und Notfallmanagement

- Anerkannte Sicherheitsstandards als Grundlage festlegen, z. B. Datenverarbeitung in einem SOC2 / C5/ …-zertifizierten Rechenzentrum, Auftragnehmer selbst ISO 27001 zertifiziert, Softwareentwicklung etc.
- Kontrollrechte der Informationssicherheit sicherstellen, Kosten, Rollen, Umfang regeln
- Betriebsausfallrisiken analysieren und Vereinbarungen von Maßnahmen mit dem AN (Zweit-RZ, On Premises Installation…)
- Bei Betroffenheit BSI-Gesetz: Mitwirkung des AN bei der Nachweispflicht berücksichtigen
- Integration in die Notfall- und Geschäftsfortführungspläne und das Unternehmens-Krisenmanagement des AG (wenn notwendig)
- Festlegen der Kommunikation (Personen, Meldezeiten, Kanäle) bei Sicherheitsvorfällen beim AN und AG
- Integration in das Meldewesen gem. § 8b Absatz 4 BSIG
- Aufnahme des AN in den UP KRITIS prüfen (ggf. als Dienstleister)
- Vereinbarungen für das Üben der Notfall- und Geschäftsfortführungspläne
- Backup: Backuplösungen können oftmals beim AN gekauft werden, auch Speicherung in anderer Lokation. Speicherlokation prüfen

4.1.13 Service Governance, Eskalationsverfahren, Berichtswesen

- Festlegen von Rollen, Verantwortlichkeiten, Gremien, Kommunikationswegen und Eskalationsverfahren
- Soweit notwendig auf Seiten des AN und des AG festlegen
- Mehrstufige Eskalationsverfahren festlegen
- Monitoring und Reporting zur Qualität der Leistungserfüllung auf Basis der SLA
- Etablierung eines Berichtswesens über Sicherheitsvorfälle, Störungen u. ä. (evtl. auch bei SLA definieren)
- Berichtszeiträume und Verantwortlichkeit für Berichte festlegen

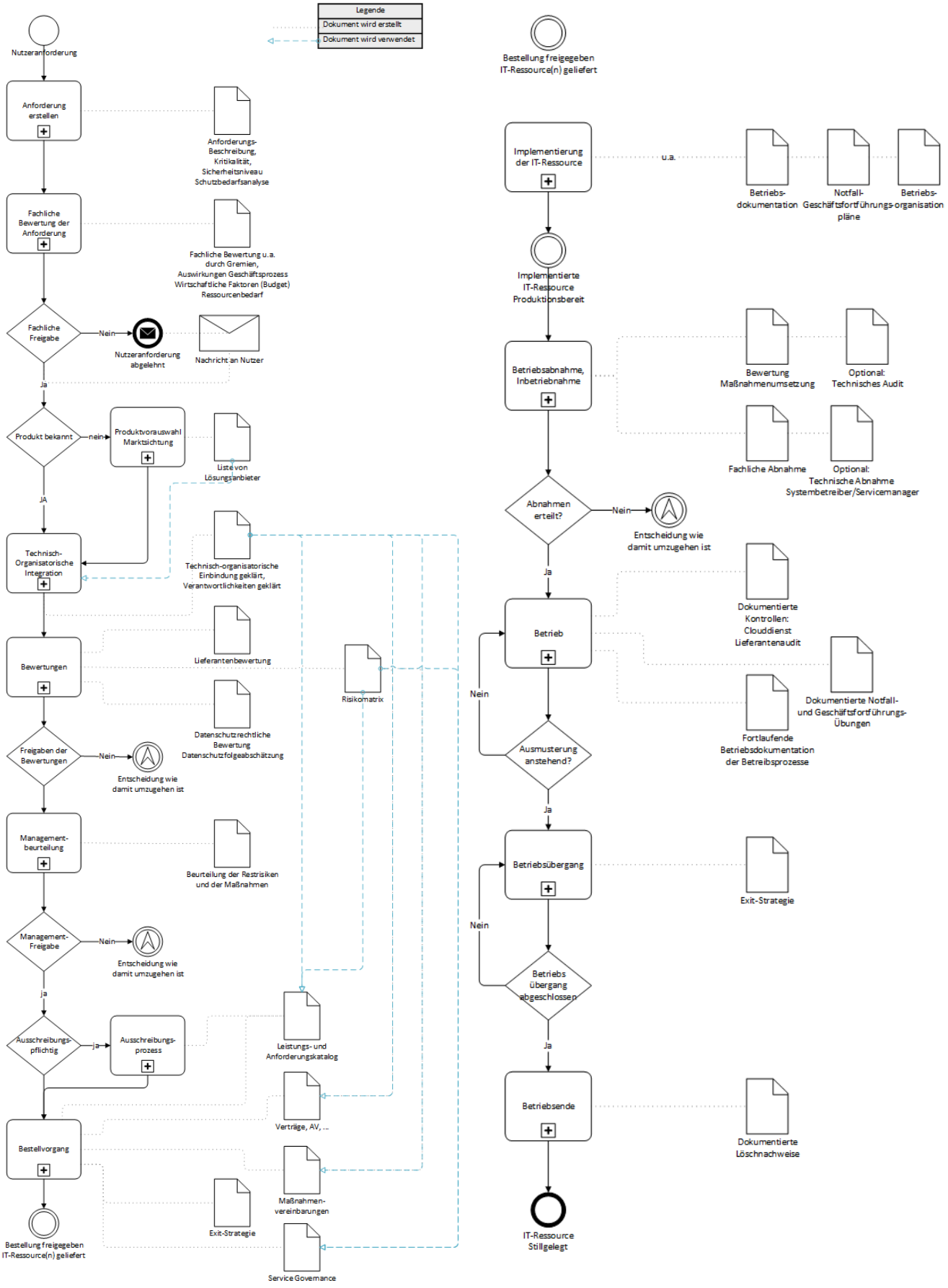
4.1.14 Service Requests

- Akzeptierte Kommunikationswege für Service Requests festlegen
- Bedingungen festlegen für Mengenerhöhung, -reduzierung, Nachbestellungen und Kündigung von Leistungen von standardisierten Einzelleistungen

4.1.15 Regulatorisches

Hinweis auf Kritische Infrastruktur und BSIG, wenn die Dienstleistung entsprechend der Kritikalität eingestuft wurde (s. hierzu die BSI-Kritisverordnung).

4.2 Detaillierter Lebensnutzungszyklus eines Cloud-Dienstes



4.3 Glossar

Abkürzungen/Begriffe	Definitionen
AG	Auftraggeber
AN	Auftragnehmer
Bot	Schadprogramm auf einem Client, das zum Aufbau fernsteuerbarer Rechnernetze (Bot-Netze) dient
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	BSI-Kritisverordnung
BSIG	BSI-Gesetz
C5	Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue) des BSI, spezifiziert Mindestanforderungen an sicheres Cloud Computing und richtet sich in erster Linie an professionelle Cloud-Anbieter, deren Prüfer und Kunden
CLOUD Act	Der US CLOUD Act ist ein US-amerikanisches Gesetz aus dem Jahr 2018. Es ermöglicht US-Behörden den Zugriff auf Daten US-amerikanischer IT-Unternehmen und Cloud-Provider, die außerhalb der USA gespeichert sind. Das Wort „CLOUD“ steht abgekürzt für „Clarifying Lawful Overseas Use of Data Act“.
COBIT	Control Objectives for Information and Related Technology, Methode zur Kontrolle von Risiken, die sich durch den IT-Einsatz zur Unterstützung geschäftsrelevanter Abläufe ergeben
DSB	Datenschutzbeauftragte(r)
EVB-IT	Ergänzende Vertragsbedingungen für IT-Dienstleistungen
IaaS	Infrastructure as as Service, Bereitstellung von IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netzen als Dienst
IAM	Identity & Access Management, Oberbegriff für Prozesse einer Organisation zur Verwaltung und Pflege von Benutzerkonten und Ressourcen. Dazu gehört auch die Verwaltung der Berechtigungen für Benutzer auf Anwendungen und Systeme. Benutzerkonten und Zugriffsberechtigungen werden mit IAM aktuell gehalten und gemäß den Vorgaben der Organisation verwaltet.
ISMS	Informationssicherheitsmanagementsystem
ISO 27001	Internationale Norm ISO/IEC 27001 „Information technology – Security techniques – Information security management systems – Requirements“ zu Anforderungen an Managementsysteme für Informationssicherheit (ISMS)
KRITIS	Kritische Infrastrukturen

On Premises	Systeme werden lokal (auf „eigenem Gebiet“), auf eigener Hardware bzw. im eigenen Rechenzentrum betrieben.
PaaS	Platform as a Service, Bereitstellung einer kompletten Laufzeit- bzw. Entwicklungsumgebung als Dienstleistung
RZ	Rechenzentrum
SaaS	Software as a Service, Bereitstellung von IT-Anwendungen als Dienst-leistung
SecLA	Security Level Agreement
SLA	Service Level Agreement
SOC2	Service Organization Control 2 - Bericht über die Angemessenheit (Typ 1) und Wirksamkeit (Typ 2) der Kontrollen

5 Danksagung

Dieses Papier wurde aus einem Positionspapier des Universitätsklinikums Tübingen entwickelt. Der TAK dankt dem Universitätsklinikum für die Nutzungserlaubnis.