Erwerb von Cloud-Services im öffentlichen Sektor

Handbuch – inklusive Beispielausschreibung für eine Cloud-Rahmenvereinbarung

Version 2: Februar 2022

Hinweise

Dieses Dokument dient nur zur Information. Es wurde nicht unter Berücksichtigung der gesetzlichen Bestimmungen für öffentliche Auftragsvergabe in bestimmten Regionen entwickelt. Cloud-Kunden sind selbst für ihre eigene, unabhängige Einschätzung der Informationen in diesem Dokument und für jedwede Nutzung der Produkte oder Services eines Cloud-Anbieters verantwortlich. Aus diesem Dokument entstehen keine Garantien, Erklärungen, vertraglichen Verpflichtungen, Bedingungen oder Zusicherungen.

Beispieldokumente und -formulierungen dürfen nicht als Rechtsberatung, -beistand oder -auskunft verstanden werden. Cloud-Kunden sollten ihre eigenen Rechtsberater zu ihren Verantwortlichkeiten im Rahmen des geltenden Rechts im jeweiligen Betriebsland befragen. CISPE lehnt ausdrücklich jegliche Garantien, Verantwortung oder Haftung ab, die sich aus den in diesem Dokument enthaltenen Informationen ergeben könnten oder mit ihnen in Verbindung stehen.

Über CISPE

CISPE (*Cloud Infrastructure Services Providers in Europe*, https://cispe.cloud) ist ein gemeinnütziger, unabhängiger Branchenverband. Wir vertreten die Anbieter von Cloud-Infrastrukturservices in Europa und arbeiten mit Entscheidungsträgern aus der Branche und Politik zusammen, um Beratung und Trainings zu Cloud-Services und ihrer Rolle auf Wirtschaftszweigebene, im öffentlichen Leben und in der Gesellschaft anzubieten.

Unsere wachsende Mitgliederzahl umfasst Unternehmen, die in allen EU-Ländern tätig sind und in 16 europäischen Ländern ihre weltweiten Hauptniederlassungen haben. Der Verband steht allen Unternehmen offen, vorausgesetzt, sie erklären, dass mindestens einer ihrer Services den Anforderungen des CISPE Data Protection Code of Conduct (CISPE-Verhaltenskodex zum Datenschutz) entspricht. Wir:

- sprechen uns für die Vorteile von Cloud First-Richtlinien für die Auftragsvergabe im öffentlichen Sektor innerhalb der EU und in den EU-Mitgliedsstaaten aus.
- arbeiten mit dem Cloud-Infrastruktursektor auf das Ziel hin, bis zum Jahr 2030 Klimaneutralität zu erreichen.
- fördern einheitliche EU-weite Sicherheitsanforderungen und technische Standards.
- unterstützen umfassende Datenschutzanforderungen durch einen Verhaltenskodex.
- streben danach, den Cloud-Infrastrukturmarkt der EU offen und wettbewerbsfähig zu halten, ohne Bindung an einzelne Anbieter.
- verhindern ungerechtfertigte Pflichten der Inhaltsüberwachung im EU-Rechtsrahmen.

Unsere Mitglieder liefern und verwalten die grundlegenden „IT-Bausteine“, auf Basis derer Regierungen, Behörden und Unternehmen ihre eigenen Systeme aufbauen und Milliarden von Bürgern mit wichtigen Services versorgen können. In dieser Rolle unterstützen wir die Entwicklung hochmoderner Technologien und Services, zu denen auch KI (künstliche Intelligenz), vernetzte Objekte, autonome Fahrzeuge, 5G und die nächste Generation der Mobilfunktechnologie gehören.

Verhaltenskodex für Cloud-Infrastruktur-Services

Der CISPE-Verhaltenskodex zum Datenschutz, der im September 2016 öffentlich präsentiert wurde, kam der Einführung der Datenschutz-Grundverordnung (DSGVO) der EU zuvor. Er entspricht den strengen DSGVO-Anforderungen, um Cloud-Infrastrukturanbieter bei der Operationalisierung der Einhaltung von Datenschutzrichtlinien zu unterstützen und einen zuverlässigen Rahmen zu schaffen, der Kunden die Auswahl von Cloud-Anbietern erleichtert und Vertrauen in ihre Services schafft. Der CISPE-Verhaltenskodex wurde im Mai 2021 vom Europäischen Datenschutzausschuss (EDSA) validiert und im Juni 2021 von der französischen Datenschutzkommission CNIL als zuständige Behörde bestätigt. https://www.codeofconduct.cloud/

Climate Neutral Data Centre Pact

Ende 2019 entwickelte CISPE zusammen mit der Europäischen Kommission eine Reihe von Metriken und eine Initiative zur Selbstregulierung, damit Rechenzentren bis zum Jahr 2030 klimaneutral arbeiten. Diese Initiative entstand durch die Zusammenarbeit mit der European Data Centre Association (EUDCA) und anderen Wirtschaftsverbänden sowie Marktteilnehmern der Betreiber von Datenzentren. Sie wurde im Januar 2021 als „Climate Neutral Data Centre Pact“ gelauncht. https://www.climateneutraldatacentre.net/

Initiative für faire Software

Gemeinsam mit der französischen CIO-Vereinigung CIGREF und der Unterstützung anderer CIO-Wirtschaftsverbände und Anbieter aus ganz Europa veröffentlichte CISPE die 10 Grundsätze einer fairen Software-Lizenzierung. Hierbei handelt es sich um eine Sammlung von Best Practices für Unternehmen, die mit der Cloud Wachstumsinnovation und Flexibilität erreichen und ihre Softwareanbieter zu fairen Lizenzierungsbedingungen anhalten wollen.
https://www.fairsoftware.cloud/de

GAIA-X

CISPE war eines der 22 Gründungsmitglieder von GAIA-X, der europäischen Initiative für ein offenes, transparentes und sicheres digitales Ökosystem. Als solches hat sich CISPE von Anfang an der Vision und den Prinzipien von GAIA-X verschrieben und der CISPE-Generalsekretär wurde im Juni 2021 erneut in den Vorstand gewählt. Einige Tools aus diesem Handbuch, wie der CISPE-Verhaltenskodex zum Datenschutz und der SWIPO Infrastructure as a Service (IaaS)-Verhaltenskodex, eignen sich, um die Compliance mit den GAIA-X-Prinzipien zu demonstrieren. https://www.gaia-x.eu

CISPE und der öffentliche Sektor

CISPE beteiligt sich an der Debatte um Richtlinien für den öffentlichen Sektor in Europa und arbeitet daran, ein besseres Verständnis der Rolle, des Beitrags und des Potenzials der Cloud-Infrastrukturbranche in Europa zu schaffen.

Auch wenn Modelle des öffentlichen Beschaffungswesens den Prozess zur Einführung und Nutzung von Cloud Computing zur Bedingung machen sollten, unterscheidet sich der Erwerb von Cloud-Services von den meisten Formen der herkömmlichen Technologieanschaffungen im öffentlichen Sektor. Es müssen neue Ansätze für die Auftragsvergabe in Betracht gezogen werden: CISPE ermutigt EU-Entscheidungsträger, anhand von Cloud First-Richtlinieninitiativen auf EU-Ebene einen ehrgeizigeren und zukunftsorientierten Ansatz zu entwickeln. So kann ein Beitrag geleistet werden, um das Wachstum des Binnenmarkts für Cloud-Infrastrukturen in Europa voranzutreiben und die Wachstumsziele des digitalen Binnenmarkts (DSM, Digital Single Market) zu unterstützen.

Dieses Handbuch soll Behörden der öffentlichen Hand bei der Beschaffung von Cloud-Services unterstützen.

Weitere Informationen

CISPE-Mitglieder: https://cispe.cloud/members
Vorstand: https://cispe.cloud/board-of-directors
Cloud Computing-Services, die als konform mit dem CISPE-Verhaltenskodex eingestuft wurden:
https://www.codeofconduct.cloud/public-register/

Inhaltsverzeichnis

Zusammenfassung und Zweck dieses Handbuchs

Dieses **Handbuch zum Erwerb von Cloud-Services** soll Cloud-Kunden unterstützen, die Cloud-Services über einen wettbewerbsfähigen Auftragsvergabeprozess erwerben möchten (Ausschreibung für Cloud Services bzw. **„Cloud Services Request for Proposal – RFP"**), jedoch nicht über das nötige Know-how zur Abfassung einer Cloud-Rahmenvereinbarung verfügen.

Dieses Dokument dient nur zur Information. Es wurde nicht unter Berücksichtigung der gesetzlichen Bestimmungen für öffentliche Auftragsvergabe in bestimmten Ländern oder Regionen entwickelt.

Das Handbuch enthält auch Beispielformulierungen für zusätzliche Auswahlkriterien für **Abrufe** oder **Mini-Wettbewerbe** beim Erwerb im Rahmen einer Cloud-Rahmenvereinbarung. Die Abschnitte des Handbuchs sind so organisiert, dass sie einer generischen IT-Ausschreibung ähneln. Die Beispiele zu generischen Formulierungen für Ausschreibungs- und Auswahlkriterien werden durch Kommentare ergänzt, um verständlich zu machen, warum sich eine Cloud-Ausschreibung von einer herkömmlichen IT-Ausschreibung unterscheidet.

Nach Veröffentlichung der Cloud-Strategie der Europäischen Kommission zur Modernisierung der IT-Infrastruktur europäischer Institutionen durch eine Cloud First-Herangehensweise, übergab CISPE das Handbuch im Juli 2019 an die EU-Kommission im Rahmen der Veranstaltung *„How to transform governments through a smart cloud policy"*.

Version 2 dieses Handbuchs enthält neue Hilfestellungen zu Datenschutz (Abschnitt 2.3.1.1), Wechsel des Cloud-Anbieters und Data Porting (Abschnitt 2.3.1.2), Software-Geschäftsbedingungen (Abschnitt 2.5.2), Nachhaltigkeit in der Cloud (Abschnitt 3.6) und einen überarbeiteten Anhang B zur technischen Live-Bewertung.

„Cloud-Services" bezeichnet alle Cloud-Technologien und zugehörigen Services, auf die ein Endbenutzer möglicherweise Zugriff benötigt. Dazu gehören neben der Cloud-Infrastruktur selbst Beratungsdienste oder Professional/Managed Services für die Unterstützung und Ausführung der Migration in die Cloud, Support für Workloads in der Cloud sowie Cloud-Marketplace-Services wie Software-as-a-Service-Produkte (SaaS-Produkte).

Indem Cloud Computing als Standardoption für die IT des öffentlichen Sektors hervortritt, bietet sich die Möglichkeit, vorhandene Beschaffungsstrategien zu modernisieren. Cloudzentrierte Akquisitionsprozesse ermöglichen es Organisationen des öffentlichen Sektors, alle Vorteile der Cloud zu nutzen – wie etwa den Zugang zu neuesten Innovationen, die höhere Geschwindigkeit und Flexibilität, mehr Sicherheit und besseres Compliance-Management – und dabei gleichzeitig mehr Effizienz und Kosteneinsparungen zu realisieren.

Herkömmliche Methoden der IT-Beschaffung für den Einkauf von Hardware, Software und Rechenzentren lassen sich nicht auf den Kauf von Cloud-Services übertragen. Bei einem Cloud-Modell ergeben sich neue Ansätze zu Preisgestaltung, Vertrags-Governance, Geschäftsbedingungen, Sicherheit, technischen Anforderungen, SLAs und vielem mehr. Gleichzeitig reduziert oder eliminiert die Anwendung herkömmlicher Methoden der Beschaffung letztendlich die Vorteile, die die Cloud bietet.

Eine der besten Möglichkeiten für eine effektive Akquisition von Cloud-Services im öffentlichen Sektor ist eine **Cloud-Rahmenvereinbarung** – eine Vergabe für eine breite Palette von Cloud-Lösungen über mehrere Anbieter hinweg. Aus diesem Angebot können die berechtigten Käufer innerhalb der einkaufenden Organisationen diejenigen Cloud-Technologien und damit verbundene Services erwerben, die ihren jeweiligen Anforderungen entsprechen. Als Instrument für Cloud-Verträge ermöglichen solche Rahmenvereinbarungen den effizienten und effektiven Einkauf von Cloud-Services. So wird gewährleistet, dass einkaufende Organisationen und Endbenutzer-Unternehmen Zugriff auf eine umfassende Auswahl von Cloud-Services haben und letztendlich die Vorteile der Cloud voll ausschöpfen können: Flexibilität, enorme Größenvorteile, Skalierbarkeit für bessere Verfügbarkeit zu geringeren Kosten, große Funktionsvielfalt, hohes Innovationstempo und Anpassungsfähigkeit an neue Regionen.

Beachten Sie, **dass sich dieser Artikel auf den Erwerb von Cloud-Technologien in den Bereichen Infrastructure as a Service (IaaS) und Platform as a Service (PaaS) konzentriert, die von einem *„Cloud Infrastructure Service Provider" (CISP, Cloud-Infrastrukturservice-Anbieter)* bereitgestellt werden.** Solche Cloud-Technologien können direkt bei einem CISP oder einem CISP-Vertriebspartner erworben werden. *Für Distributoren von Cloud Marketplace Services (PaaS und SaaS) und Cloud-Beratungsdiensten sind bei der Ausschreibung zusätzliche Überlegungen erforderlich.*

Beachten Sie auch, dass dieses Dokument nicht jeden Aspekt der Erstellung einer End-to-End-Rahmenvereinbarung für die Cloud-Auftragsvergabe abdeckt. Es gibt zahlreiche weitere Dokumente aus der Branche und von Analysten, die Themen wie Best Practices für die Cloud-Auftragsvergabe, das Budget für die Cloud, die Cloud-Governance usw. behandeln. Wir empfehlen dringend, diese Ratschläge und Dokumente bei der Entwicklung einer allgemeinen Strategie für die Cloud-Auftragsvergabe zu berücksichtigen.
Tabelle 1 unten enthält eine Übersicht über das Ausschreibungshandbuch für Cloud-Services und Angaben dazu, wo Sie Beispielformulierungen für Ausschreibungen zu jeder Komponente einer Cloud-Services-Ausschreibung finden.

Tabelle 1 – Zusammenfassung der Abschnitte im Ausschreibungshandbuch für Cloud-Services

Abschnitt	Überblick und Beispielformulierungen für Ausschreibungen
1.0 Überblick über eine Cloud-Rahmenvereinbarung	Ein allgemeiner Überblick über das Modell einer Cloud-Rahmenvereinbarung (LOTs, Wettbewerbsstrategien und Vertragsabschlüsse)
2.0 Ausschreibung für Cloud-Services – Überblick	Allgemeine Beispiele für Formulierungen in einer Ausschreibung, die die folgenden Abschnitte abdecken, sowie Kommentare, die die Gründe für die Struktur und Formulierungen dieser Cloud-Services-Ausschreibung erläutern.
2.1 Erstellung einer Ausschreibung für Cloud-Services	**2.1.1** Einführung und strategische Ziele **2.1.2** Zeitrahmen für Antworten auf die Ausschreibung **2.1.3** Definitionen **2.1.4** Detaillierte Beschreibung des Kaufmodells und Wettbewerbs innerhalb der Rahmenvereinbarung **2.1.5** Mindestanforderungen Bieter – Verwaltung
2.2 Technische Aspekte	**2.2.1** Mindestvoraussetzungen **2.2.2** Vergleich zwischen Anbietern **2.2.3** Vertragsabschluss
2.3 Sicherheit	**2.3.1** Mindestvoraussetzungen 2.3.1.1 Datenschutz 2.3.1.2 Wechsel des Cloud-Anbieters und Data Porting 2.3.2 Vergleich zwischen Anbietern **2.3.3** Vertragsabschluss
2.4 Preise	**2.4.1** Mindestvoraussetzungen **2.4.2** Vergleich zwischen Anbietern
2.5 Vertragsabwicklung/Geschäftsbedingungen	**2.5.1** Geschäftsbedingungen 2.5.2 Software-Geschäftsbedingungen 2.5.3 So wählen Sie zwischen Teilnehmern aus 2.5.4 On-Boarding und Off-Boarding
3.0 Best Practices/Erkenntnisse	3.1 Cloud-Governance **3.2** Budgetierung für die Cloud **3.3** Verständnis des Partnergeschäftsmodells **3.4** Cloud-Broker **3.5** Beschaffung vor der Ausschreibung/Marktforschung 3.6 Nachhaltigkeit
Anhang A – Technische Anforderungen für den Vergleich zwischen Bietern	Eine Liste allgemeiner Anforderungen an die Cloud-Technologie für Abrufe oder Mini-Wettbewerbe
Anhang B – Technische Live-Bewertung	Ein Beispielskript für die Bewertung einer Cloud-Technologiedemonstration (Cloud-Demos als Teil eines Abrufs oder Mini-Wettbewerbs)

1.0 Überblick über eine Cloud-Rahmenvereinbarung

Eine gut durchdachte Cloud-Rahmenvereinbarung ermöglicht den Erwerb von Cloud-Services auf eine Weise, die sowohl den teilnehmenden Organisationen des öffentlichen Sektors als auch den Cloud-Anbietern zugutekommt. Zu den Vorteilen einer gut konzipierten Cloud-Rahmenvereinbarung gehören:

- Fokus auf Kooperation:
    - Wenn mehrere Organisationen für einen ähnlichen Bedarf gemeinsam Bestellungen aufgeben, können sie dadurch von erhöhter Zweckmäßigkeit, Effizienz, geringeren Kosten und einem vereinfachten Bestellprozess profitieren. So bietet sich eine effektive Möglichkeit, die Nachfrage mehrerer Organisationen im öffentlichen Sektor nach verbreiteten Cloud-Technologien und entsprechenden Cloud-Services wie Marketplace-Lösungen und Beratung zu bündeln.
- Umfassendes Angebot an Cloud-Services:
    - Dieses kann alle Beratungsdienste/Professional Services/Managed Services umfassen, die für die vollständige Unterstützung und Durchführung der Migration zur Cloud und für die Unterstützung von Workloads in der Cloud erforderlich sind, zusätzlich zu vom CISP bereitgestellten Cloud-Technologien und Marketplace-Services.
    - Cloud-Technologien können direkt bei einem CISP oder über einen designierten Vertriebspartner erworben werden.
- Vertrags-Governance:
    - Koordiniert verschiedene Organisationen/Einkäufer im Rahmen gemeinsamer Geschäftsbedingungen und einer einzelnen Muster-Auftragsvergabe, anstatt mehrerer unterschiedlicher für jede Organisation.
    - Auch für die Anbieter ergeben sich Vorteile aus den standardisierten Akquiseprozessen, Geschäftsbedingungen sowie einem einheitlichen Bestellmechanismus, statt unterschiedlicher Regelungen und Prozesse für jede Organisation des öffentlichen Sektors.
    - Das sorgt für Flexibilität. Das Erstellen, Genehmigen und Umsetzen eines effektiven Cloud-Vertrags im Rahmen bestehender behördlicher Richtlinien/Vorschriften erfordert Experimente und die Fähigkeit, sich schnell anzupassen. Es ist wesentlich vorteilhafter, eine Rahmenvereinbarung zu erstellen, die es dem öffentlichen Sektor und den Cloud-Anbietern ermöglicht, den Vertrag gemeinsam zu verbessern – im Sinne einer vertragsrechtlichen, mechanischen und effizienten Optimierung. Ein mehrjähriger Vertrag, der weder gut funktioniert noch angepasst werden kann, zieht eine schlechte Erfahrung für die Endbenutzer im öffentlichen Sektor, die Beschaffungsorganisationen und die Cloud-Anbieter nach sich.

- Auswahl:
    - Verschafft den Käufern die Auswahl aus mehreren qualifizierten CISPs und setzt hohe Maßstäbe sowohl für alle Cloud-Services als auch damit verbundene Services wie einen PaaS-/SaaS-Marketplace und Beratung für die Cloud.
    - Ermöglicht die Kontrolle über die Anzahl der Anbieter innerhalb einer Rahmenvereinbarung, da sichergestellt ist, dass der Standard jedes Teilnehmers angemessen geprüft wird.

Eine Rahmenvereinbarung zum Erwerb von Cloud-Services funktioniert am besten, wenn sie zentrale, vom CISP bereitgestellte IaaS-/PaaS-Technologien und einen PaaS-/SaaS-Marketplace sowie Beratungsdienste umfasst, auf die Endbenutzer im öffentlichen Sektor bei Bedarf zugreifen können, damit sie bei der Planung, Umstellung, Nutzung und Verwaltung ihrer Workload in der Cloud unterstützt werden. Wir schlagen daher vor, dass eine Cloud-Services-Ausschreibung zur Schaffung einer Cloud-Rahmenvereinbarung in drei Bereiche wie im Folgenden aufgeteilt wird:

- BEREICH 1 – CLOUD-TECHNOLOGIEN
  Cloud-Technologien, die direkt von einem CISP oder über einen designierten CISP-Vertriebspartner erworben werden

- BEREICH 2 – MARKETPLACE
  Zugang zu einem Marketplace mit PaaS- und SaaS-Services

- BEREICH 3 – CLOUD-BERATUNG
  Cloudbezogene Beratungsdienste (Schulungen, Professional Services, Managed Services usw.) und technischer Support

*Wie zuvor erwähnt, konzentriert sich dieses Dokument auf den Erwerb von IaaS- und PaaS-Cloud-Technologien (**BEREICH 1**), wie sie von einem CISP (direkt bei einem CISP oder über einen CISP-Vertriebspartner) angeboten werden. Für die Qualifizierung von Anbietern in den Bereichen 2 und 3 einer Cloud-Services-Ausschreibung sind separate Anforderungen erforderlich.*

Abbildung 1 bietet nachstehend einen allgemeinen Überblick darüber, wie eine gut strukturierte Ausschreibung für Cloud-Services, die in diese drei Bereiche unterteilt ist, zu einer Cloud-Rahmenvereinbarung führen kann, die Einrichtungen des öffentlichen Sektors Flexibilität (technisch und vertraglich), Transparenz und Kontrolle über die Ausgaben und die Cloud-Nutzung sowie die Möglichkeit bietet, auf alle Cloud-Services zurückzugreifen, die für den Aufbau und die Wartung der von ihnen benötigten Lösungen erforderlich sind.

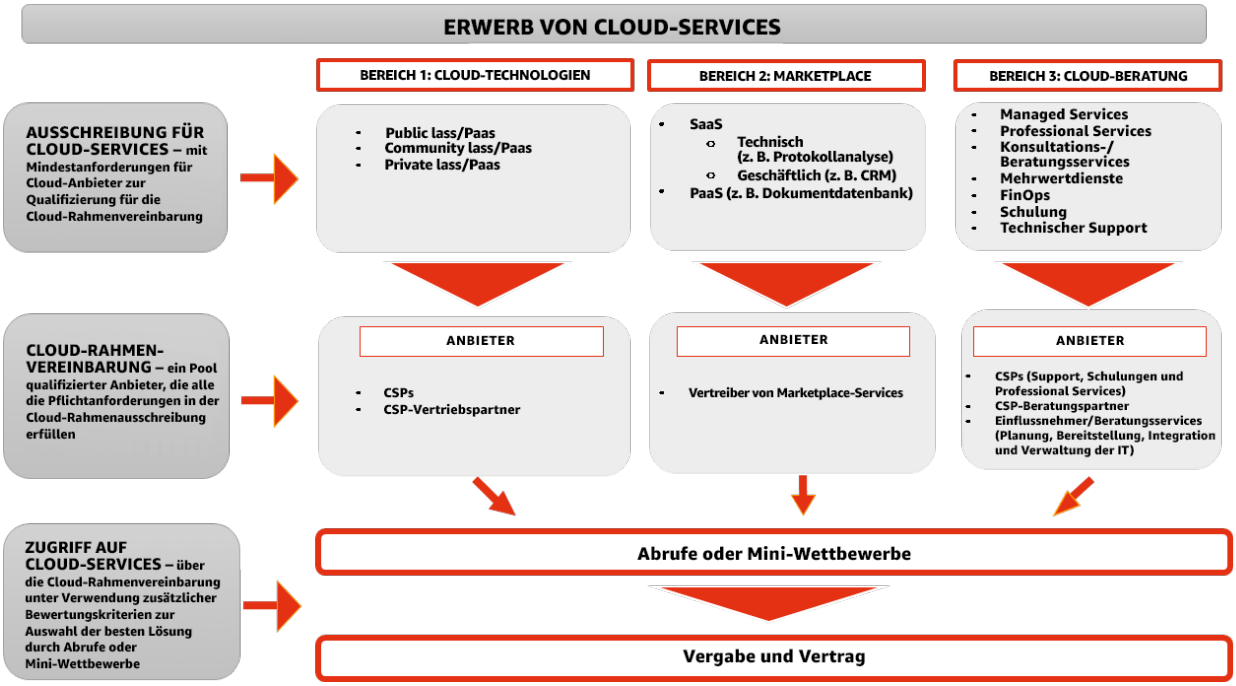

Abbildung 1: Eine erfolgreiche Cloud-Services-Ausschreibung ist in 3 Bereiche unterteilt. Jeder Bereich enthält wiederum Kategorien oder „Angebotstypen", um zu gewährleisten, dass bei Käufen innerhalb der Cloud-Rahmenvereinbarung die technischen und vertraglichen Anforderungen der Endbenutzer erfüllt werden.

Hinweis:

- Jeder Bereich wird mehrfach vergeben.
- BEREICH 3 kann möglicherweise über eine weitere Ausschreibung oder gegebenenfalls über einen bestehenden Vertrag für Beratungsdienste vergeben werden.

Kategorien BEREICH 1

In erfolgreichen Cloud-Rahmenvereinbarungen werden CISPs dazu aufgefordert, das Modell der von ihnen angebotenen Cloud zu beschreiben, eingeteilt in Kategorien innerhalb jedes Bereichs. Wir empfehlen die Verwendung des Branchenstandards für Cloud Computing – die essentiellen Cloud-Eigenschaften des NIST (National Institute of Standards and Technology) – für die Definitionen von **Public** Cloud, **Community** Cloud und **Private** Cloud. Indem eine Cloud-Rahmenvereinbarung auf diese Art strukturiert wird, können die einkaufende Organisation und die öffentlichen Einrichtungen je nach Anforderung aus einer Vielzahl von Cloud-Modellen innerhalb der Rahmenvereinbarung auswählen.

Die NIST-Definition der einzelnen Cloud-Modelle unter BEREICH 1 (Public IaaS/PaaS, Community IaaS/PaaS und Private IaaS/PaaS) finden Sie in *Abschnitt **2.1.3** Definitionen*.

Wie werden die Anbieter ausgewählt – Abrufe oder Mini-Wettbewerbe?

Die Qualifizierungskriterien für eine Cloud-Services-Ausschreibung sollten nur die zentralen Punkte und Mindestanforderungen abdecken und keine optionalen Elemente enthalten. Werden die

Mindestanforderungen um weniger essenzielle Elemente erweitert, können unter Umständen manche Anbieter, die eigentlich für die Rahmenvereinbarung infrage kämen, nicht mitbieten und fallen für den Käufer aus der Auswahl.

Nach der Ausschreibung und der nachfolgenden Einigung auf die Cloud-Rahmenvereinbarung können öffentliche Einrichtungen, die Teil der Rahmenvereinbarung sind, die benötigten Cloud-Services bei Bedarf bestellen oder „abrufen". Ein Abrufvertrag im Rahmen einer Rahmenvereinbarung ermöglicht es Käufern, bei einem Abruf die Anforderungen mit zusätzlichen funktionalen Spezifikationen zu verfeinern, während die über die Rahmenvereinbarung angebotenen Vorteile erhalten bleiben.

Falls erforderlich, kann ein Mini-Wettbewerb abgehalten werden, um den besten Anbieter für eine bestimmte Workload oder ein bestimmtes Projekt zu ermitteln. Ein Mini-Wettbewerb bedeutet, dass ein Kunde im Zuge der Rahmenvereinbarung einen weiteren Wettbewerb ausruft, indem er alle Anbieter für einen Bereich dazu einlädt, auf eine Reihe von Anforderungen zu reagieren. Der Kunde lädt alle infrage kommenden Anbieter innerhalb des Bereichs ein, ein Angebot abzugeben. Daher ist es wichtig, bei einer Cloud-Services-Ausschreibung die Mindestanforderungen für die Teilnehmer zu definieren: So wird für jeden Bereich eine qualitativ hochwertige Auswahl an Optionen gewährleistet.

*Beachten Sie, dass für jeden dieser Bereiche **unterschiedliche Vertragsbedingungen** gelten, siehe Abbildung 1 weiter oben. Der Versuch, alle Bereiche mit einheitlichen Vertragsbedingungen abzudecken, führt zu Problemen in Bezug auf technische Machbarkeit und Kompatibilität.*

2.0 Ausschreibung für Cloud-Services – Überblick

In diesem Abschnitt werden das Modell und der Umfang einer Cloud-Services-Ausschreibung beschrieben, einschließlich strategischer Ziele, Teilnehmer, Definitionen, Zeitplan und administrativer Mindestanforderungen. Auch hier liegt der Schwerpunkt dieses Handbuchs auf BEREICH 1 – CLOUD-TECHNOLOGIEN.

2.1 Erstellung einer Ausschreibung für Cloud-Services

Wir empfehlen Organisationen aus dem öffentlichen Sektor dringend, in der Einführung einer Cloud-Services-Ausschreibung ihre übergeordneten Ziele und Anforderungen klar zu formulieren.

2.1.1 Einführung und strategische Ziele

Um bei strategischen Zielen Klarheit zu erlangen, empfiehlt es sich, in der Einleitung einer Ausschreibung für Cloud-Services folgende Punkte zu definieren: **(1)** die Geschäftsziele und Vorteile, die das Unternehmen durch die Nutzung der Cloud erreichen möchte, **(2)** die Struktur der Rahmenvereinbarung – wer kauft, wer betreibt, wer verwaltet Budgets usw., **(3)** ein klares Verständnis des Modells der geteilten Verantwortung zwischen dem öffentlichen Sektor und den Cloud-Anbietern, welches das Kernstück erfolgreicher Cloud-Käufe und -Nutzung bildet, und **(4)** die Art der Beziehung zwischen Cloud-Service-Anbietern (CISPs), Vertreibern von Marketplace-Services, Beratungspartnern, öffentlichen Beschaffungsstellen/Vertragsagenturen und behördlichen Endnutzern. Die Formulierung dieser vier Punkte hilft Organisationen bei der Entwicklung einer Ausschreibung, die ihren Anforderungen am besten entspricht, und stellt gleichzeitig sicher, dass sowohl Kunden als auch Anbieter klar über die gewünschten Ergebnisse informiert sind.

Eine Cloud-Ausschreibung unterscheidet sich absichtlich von herkömmlichen IT-Ausschreibungen. Cloud-Technologie ist nicht einfach nur ein Ersatz für herkömmliche Computertechnologie, sondern eröffnet einen völlig neuen Zugang zur Nutzung von Technologie. Gut durchdachte Ausschreibungen für Cloud-Services können Organisationen des öffentlichen Sektors dabei unterstützen, schnell von der Cloud zu profitieren.

Von allen Aspekten beim Cloud-Erwerb, die sich aus unserer Sicht bewährt haben, ist ein klares Verständnis des Modells der geteilten Verantwortung sicherlich der beste Startpunkt. Das Modell der geteilten Verantwortung[1] wird hauptsächlich im Zusammenhang mit der Sicherheit und Compliance in der Cloud verwendet, jedoch gilt diese Abgrenzung von Verantwortlichkeiten für alle Aspekte von Cloud-Technologien. Eine Cloud-Services-Ausschreibung sollte klar definieren, was in einer Cloud-Umgebung zum Aufgabenbereich des CISP gehört, und was weiterhin der Verantwortung des Kunden unterliegt. Ein CISP bietet beispielsweise die Möglichkeit, Ressourcen und Anwendungen zu überwachen, die in der Cloud ausgeführt werden. ***Aber*** es liegt in der Verantwortung des Kunden, diese vom CISP bereitgestellten Funktionen tatsächlich zu nutzen, da ein CISP, der im großen Maßstab arbeitet, dies nicht für Millionen von Kunden leisten kann.

[1] Siehe Abschnitt 5 des CISPE-Verhaltenskodex für Anbieter von Cloud-Infrastrukturservices: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

Darüber hinaus sollten Cloud-Kunden verstehen, wie das Partnernetzwerk eines CISP sie dabei unterstützt, die Cloud zu nutzen und ihre Verantwortlichkeiten zu verwalten. Beispielsweise kann ein Managed Service Provider (MSP) für Clouds einem Kunden bei der Konfiguration und Verwendung von CISP-Überwachungsfunktionen helfen, um dessen individuelle Compliance- und Audit-Anforderungen zu erfüllen.

Einfach ausgedrückt, sind die Verantwortlichkeiten im Cloud-Modell wie folgt verteilt:

Ein CISP stellt Cloud-Technologie bereit.

Ein Kunde nutzt Cloud-Technologie.

Beratungsunternehmen (falls vorhanden) helfen einem Kunden dabei, auf die Cloud-Technologie zuzugreifen und diese zu nutzen.

> ***„Beratungsunternehmen"*** *sind Anbieter von Beratungsdiensten und Managed/Professional Services, die Kunden beim Design, der Gestaltung, Erstellung, Migration und Verwaltung ihrer Workloads und Anwendungen in der Cloud unterstützen. Zu diesen Unternehmen gehören Systemintegratoren, strategische Beratungsunternehmen, Agenturen, Managed Service Provider und Wiederverkäufer.*

Stellen Sie sich den „Einkauf" von Cloud-Services wie einen Einkauf in einem Baumarkt vor. In einem Baumarkt steht eine Vielzahl von Materialien und Werkzeugen zur Verfügung, mit denen Sie das bauen können, was Sie benötigen. Sie können einen Schrank, einen Swimmingpool oder ein ganzes Haus bauen – Sie haben die Wahl. Wenn Sie die Materialien und Werkzeuge kaufen, können die Mitarbeiter im Baumarkt Hilfestellungen und Fachwissen liefern, aber sie kommen nicht nach Hause und bauen etwas für Sie auf. Daher haben Sie folgende Möglichkeiten:

1. Sie kaufen die Materialien und Werkzeuge selbst und bauen eigenhändig etwas daraus.
2. Sie kaufen die Materialien und Werkzeuge selbst und beauftragen jemanden damit, etwas für Sie zu bauen und/oder zu betreiben.
3. Sie beauftragen jemanden damit, etwas für Sie zu bauen/zu betreiben und bitten ihn, die Materialien und Werkzeuge als Teil des Gesamtangebots bereitzustellen.

Wenn ein Unternehmen intern über die Fähigkeiten verfügt, seine Cloud-Umgebung und -Lösungen selbst zu erstellen und zu verwalten, muss es im Grunde nur auf die standardisierten Cloud-Technologien und -Tools des CISP zugreifen (direkt bei einem CISP oder über einen CISP-Vertriebspartner – siehe **BEREICH 1**). Erforderliche SaaS- und PaaS-Software sollte auf einem Cloud-Marketplace verfügbar sein (**BEREICH 2**). Wo darüber hinaus Bedarf an Beratung, Migration, Implementierung und/oder Verwaltungshilfe besteht, kommt hier das Partnernetzwerk eines CISP ins Spiel (**BEREICH 3**).

Beispielformulierungen für die Ausschreibung: Einleitung und strategische Ziele

Cloud Computing bietet Organisationen des öffentlichen Sektors schnellen Zugriff auf eine breite Palette flexibler und kostengünstiger IT-Ressourcen, die nutzungsbasiert bezahlt werden. Organisationen können Art und Umfang der Ressourcen, die sie für die Umsetzung ihrer neuesten Ideen oder den Betrieb ihrer IT-Abteilungen benötigen, nach Bedarf einkaufen, sodass große Investitionen in Hardware- und/oder langfristige Softwarelizenzverträge entfallen.

***<ORGANISATION>** hat Bedarf an dieser Art von kommerziell verfügbaren Cloud-Technologien, um die geschäftlichen Anforderungen in einem breiten Spektrum von verbundenen Organisationen zu erfüllen.*

*Das Hauptziel dieser Ausschreibung ist die Vergabe einer nicht exklusiven, parallelen **<RAHMENVEREINBARUNG>** mit bis zu **<x>** Anbietern, die verschiedene Cloud-Technologien und cloudbezogene Services anbieten.*

1. ***BEREICH 1.** CISPs (Cloud-Service-Anbieter) oder CISP-Vertriebspartner für den Erwerb von Cloud-Technologien.*
2. ***BEREICH 2.** Anbieter von Marketplace-Services.*
3. ***BEREICH 3.** Anbieter von Beratungsdienstleistungen, die zusätzliches Fachwissen für die Migration zu diesen CISP-Angeboten und deren Nutzung bereitstellen.*

*In Bezug auf **BEREICH 1** müssen interessierte Organisationen (CISPs oder CISP-Vertriebspartner) nachweisen, wie ihr Angebot die folgenden Ziele erfüllt:*

- ***Agilität:** IT-Ressourcen werden Endbenutzern innerhalb von Minuten anstatt der üblichen Wochen und Monate zur Verfügung gestellt.*
- ***Innovation:** Sofortiger Zugriff auf die neueste und innovativste Technologie auf dem Markt.*
- ***Kosten:** Variable Ausgaben statt Vorabkosten (z. B. Betriebs- anstelle von Investitionsaufwand), Bezahlung nur für tatsächlich genutzte Dienste.*
- ***Budgetierung:** Anzeige von Rechnungs- und Nutzungsdaten sowohl auf detaillierter als auch auf zusammenfassender Ebene, Visualisierung von Ausgabenentwicklung sowie Prognose künftiger Ausgaben.*
- ***Elastizität:** Niedrigere variable Kosten durch die erweiterten Größenvorteile der Cloud.*
- ***Kapazität:** Exakte Bestimmung der Anforderungen an die Infrastrukturkapazität.*
- ***Unabhängigkeit von Rechenzentren:** Konzentration auf die Bedürfnisse unserer Bürger statt auf den umständlichen Aufbau und Betrieb von Server-Racks und -Stacks.*
- ***Sicherheit:** Formalisieren von Kontodesigns mit mehr Transparenz und Auditierbarkeit von Ressourcen sowie Eliminierung der Kosten für den Schutz von Anlagen und physischer Hardware.*
- ***Geteilte Verantwortung:** Weniger betrieblicher Aufwand. Der CISP betreibt, verwaltet und steuert die Komponenten des Hostbetriebssystems und der Virtualisierungsebene und sorgt zudem für die physische Sicherheit der Standorte, an denen der Service betrieben wird.*
- ***Automatisierung:** Integrierte Automatisierung für die Cloud-Architektur, um die sichere Skalierung schneller und kostengünstiger gestalten zu können.*
- ***Cloud-Governance:** (1) anfänglich vollständige Bestandsaufnahme aller IT-Ressourcen; (2) zentrales Verwalten all dieser Komponenten; und (3) Erstellen von Warnmeldungen zu Nutzung/Abrechnung/Sicherheit usw., jeweils mit Funktionen für Bestandsverfolgung,*

Bestandsmanagement, Änderungsmanagement, Protokollmanagement und -analyse sowie Gesamttransparenz und Cloud-Governance.

- ***Kontrolle:*** *Vollständige Übersicht über die Nutzung von IT-Services und deren potenzielle Optimierung für Sicherheit, Zuverlässigkeit, Leistung und Kosten.*
- ***Reversibilität:*** *Portabilitätstools und -services, die die Migration zur und von der CISP-Infrastruktur erleichtern, die Anbieterbindung minimieren und den Verhaltenskodex der Branche respektieren.*
- ***Datenschutz:*** *Fähigkeit, die Compliance mit der Datenschutz-Grundverordnung (DSGVO) über einen speziellen Branchenverhaltenskodex für Cloud-Infrastrukturservices nachzuweisen: den CISPE-Verhaltenskodex zum Datenschutz.*
- ***Transparenz:*** *Kunden sollten berechtigt sein, den Standort der Infrastrukturen zu kennen (Stadtgebiet), die zur Verarbeitung und Speicherung ihrer Daten verwendet werden.*
- ***Klimaneutralität:*** *Kunden sollten mit CISPs arbeiten, die nachweislich konkrete Schritte unternehmen, um bis zum Jahr 2030 Ziele der Klimaneutralität zu erfüllen, und den Climate Neutral Data Centre Pact unterzeichnet haben. Dies hilft Kunden dabei, ihre eigenen Ziele der Klimaneutralität zu erreichen.*

2.1.2 Zeitrahmen für Antworten auf die Ausschreibung

Es empfiehlt sich bei der Erstellung einer Cloud-Rahmenvereinbarung und der zugehörigen Ausschreibung der Cloud-Services, den Bietern einen Zeitrahmen für die Reaktion auf die Ausschreibung mitzuteilen. Je stärker die Zusammenarbeit mit der Branche, desto besser, denn dadurch wird gewährleistet, dass alle Parteien die Anforderungen der Ausschreibung verstehen und genau nachvollziehen können, wie alle Anbieterservices in das Cloud-Servicemodell passen.

Beachten Sie, dass der Zeitrahmen für die Ausschreibung lokalen Gesetzen und rechtlichen Verpflichtungen unterliegt. Die folgende Aufzählung ist als Best-Practice-Leitfaden gedacht und stellt keine verbindliche Liste von Aktivitäten und Zeitrahmen dar.

Beispielformulierungen für die Ausschreibung: Zeitrahmen für die Antwort

Siehe den nachstehenden Zeitplan für die Cloud-Services-Ausschreibung:

Zeitplan für Cloud-Services-Ausschreibung
• *Veröffentlichung Informationsanfrage:* • *Antwort auf die Informationsanfrage:* • *Veröffentlichung Entwurf einer Ausschreibung:* • *Fälligkeit Antwort auf Entwurf einer Ausschreibung:* • *Branchenberatungsphase: <Zeitpläne>* • *Präqualifikation Veröffentlichung Ausschreibung:* • *Präqualifikation Antwort auf Ausschreibung:* • *Veröffentlichung Ausschreibung:* • *Fälligkeit Fragen Runde 1:* • *Antworten Runde 1:* • *Fälligkeit Fragen Runde 2:*

- *Antworten Runde 2:*
- *Fälligkeit Antwort auf Ausschreibung:*
- *Zeitraum für Klärung des Angebots:*
- *Verhandlungszeitraum:*
- *Datum der Absicht zur Vergabe:*
- *Auftragsvergabe:*
- *Dauer des Vertrags (Verlängerungsoptionen):*

Beachten Sie, dass der Zeitrahmen für die Ausschreibung lokalen Gesetzen und rechtlichen Verpflichtungen unterliegt. Die folgende Aufzählung ist als Best-Practice-Leitfaden gedacht und stellt keine verbindliche Liste von Aktivitäten und Zeitrahmen dar.

2.1.3 Definitionen

Eine Ausschreibung für Cloud-Services sollte eine detaillierte Liste von Definitionen enthalten. Diese Liste umfasst Anbieterrollen (z. B. Cloud-Service-Anbieter, Cloud-Vertriebspartner, Anbieterpartner), allgemeine Technologiekonzepte (Datenverarbeitung, Speicher, IaaS/PaaS, SaaS) und andere wichtige Vertragsbestandteile. Im Folgenden finden Sie eine Liste mit Beispieldefinitionen:

Beispielformulierungen für die Ausschreibung: Definitionen

Im Folgenden sind die Definitionen des National Institute of Standards and Technology (NIST) für Cloud Computing angegeben.[2]

- ***Infrastructure as a Service (IaaS).*** *Die dem Verbraucher bereitgestellten Kapazitäten betreffen die Verarbeitung, den Speicher und die Vernetzung sowie weitere unerlässliche Datenverarbeitungsressourcen, mit denen der Verbraucher beliebige Software, einschließlich Betriebssystemen und Anwendungen, bereitstellen und ausführen kann. Der Verbraucher verwaltet oder steuert nicht die zugrunde liegende Cloud-Infrastruktur, hat jedoch die Kontrolle über Betriebssysteme, Speicher und bereitgestellte Anwendungen sowie möglicherweise eine begrenzte Kontrolle über ausgewählte Netzwerkkomponenten (z. B. Host-Firewalls).*

- ***Platform as a Service (PaaS).*** *Die dem Verbraucher bereitgestellten Kapazitäten bestehen darin, auf der Cloud-Infrastruktur vom Verbraucher erstellte oder erworbene Anwendungen bereitzustellen, die mithilfe von Programmiersprachen, Bibliotheken, Services und Tools erstellt worden sind, die vom Anbieter unterstützt werden. Der Verbraucher verwaltet oder steuert nicht die zugrunde liegende Cloud-Infrastruktur, einschließlich Netzwerk, Servern, Betriebssystemen oder Speicher, hat jedoch die Kontrolle über die bereitgestellten Anwendungen und möglicherweise Konfigurationseinstellungen für die Hostingumgebung der Anwendungen.*

[2] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

- ***Software as a Service (SaaS).*** *Die dem Verbraucher bereitgestellten Kapazitäten bestehen darin, Anwendungen des Anbieters zu nutzen, die in einer Cloud-Infrastruktur ausgeführt werden. Der Zugriff auf die Anwendungen kann von verschiedenen Kundengeräten aus über eine Thin-Client-Schnittstelle, z. B. einen Webbrowser (z. B. webbasierte E-Mail), oder eine Programmschnittstelle erfolgen. Der Kunde verwaltet oder steuert die zugrunde liegende Cloud-Infrastruktur nicht selbst, einschließlich Netzwerk, Servern, Betriebssystemen, Speicher oder sogar einzelnen Anwendungsfunktionen, mit der möglichen Ausnahme begrenzter benutzerspezifischer Konfigurationseinstellungen für Anwendungen.*

- ***Public Cloud.*** *Die Cloud-Infrastruktur wird für die öffentliche Nutzung durch die Allgemeinheit bereitgestellt. Sie kann Eigentum eines Unternehmens, einer akademischen oder staatlichen Organisation oder einer Kombination dieser Organisationen sein, bzw. von diesen verwaltet und betrieben werden. Sie existiert auf dem Gelände des Cloud-Anbieters.*

- ***Community Cloud.*** *Die Cloud-Infrastruktur wird für die exklusive Nutzung durch eine bestimmte Gruppe von Verbrauchern aus Organisationen bereitgestellt, die gemeinsame Anliegen haben (z. B. Mission, Sicherheitsanforderungen, Richtlinien und Compliance-Aspekte). Sie kann Eigentum einer oder mehrerer Organisationen innerhalb der Gruppe, einer dritten Partei oder einer Kombination daraus sein und von diesen verwaltet und betrieben werden und sie kann auf dem Gelände der betroffenen Organisation(en) oder an einem anderen Ort existieren.*

- ***Hybrid Cloud.*** *Die Cloud-Infrastruktur ist eine Kombination aus zwei oder mehr unterschiedlichen Cloud-Infrastrukturen (Private, Community oder Public), die zwar eigenständige Einheiten bleiben, aber durch standardisierte oder proprietäre Technologie miteinander verbunden sind, wodurch Daten- und Anwendungsportabilität ermöglicht wird (z. B. Cloud Bursting für das Load Balancing zwischen Clouds).*

- ***Private Cloud.*** *Die Cloud-Infrastruktur wird für den exklusiven Gebrauch durch eine einzelne Organisation bereitgestellt, die aus mehreren Verbrauchern besteht (z. B. Geschäftsbereichen). Sie kann Eigentum der Organisation, einer dritten Partei oder einer Kombination daraus sein und von diesen verwaltet und betrieben werden und sie kann auf dem Gelände der betroffenen Organisation oder an einem anderen Ort existieren.*

2.1.4 Detaillierte Beschreibung des Kaufmodells und Wettbewerbs innerhalb der Rahmenvereinbarung

Wie zuvor erwähnt, sollten Organisationen des öffentlichen Sektors definieren, nach welchem Modell eine Rahmenvereinbarung als Kaufmechanismus für Cloud-Technologien und zugehörige Implementierungs- und Management-Services funktionieren soll. Dies sollte in der Ausschreibung für die Cloud-Services deutlich gemacht werden, damit Anbieter von Cloud-Technologien, zugehörige Beratungsunternehmen, Marketplace-Vertreiber und kaufende Organisationen ihre jeweiligen Rollen verstehen.

Im Hinblick auf den Umfang der Rahmenvereinbarung und darauffolgender Abrufe oder Mini-Wettbewerbe sollten Organisationen Folgendes bedenken:

- Wer wird im Rahmen des Vertrags für Integration und Managed Services im Zusammenhang mit den Cloud-Technologien verantwortlich sein?
- Muss ein CISP-Vertriebspartner/-Partner Mehrwertdienste bereitstellen, die über die Aufrechterhaltung einer vertraglichen Beziehung zum CISP, die Bereitstellung konsolidierter Fakturierung und den zeitnahen und direkten Zugriff auf Nutzungs- und Abrechnungsdaten im Zusammenhang mit der Nutzung der Cloud-Anbieter-Services hinausgehen?

- Besteht die Notwendigkeit für einen Full-Service-Wiederverkäufer, Systemintegrator oder Managed Service Provider oder eine andere Art Anbieter von IT-Dienstleistungen?

Beachten Sie, dass es sich bei einem CISP nicht um einen Systemintegrator (SI) oder Managed Service Provider (MSP) handelt. Viele Kunden aus dem öffentlichen Sektor benötigen einen CISP für ihre IaaS/PaaS-Nutzung und sie lagern die Beratung und eigentliche Planungs-, Migrations- und Managementaufgaben an einen SI oder MSP aus. Abbildung 2 zeigt eine Darstellung der Rollen und Verantwortlichkeiten in einem Cloud-Servicemodell.

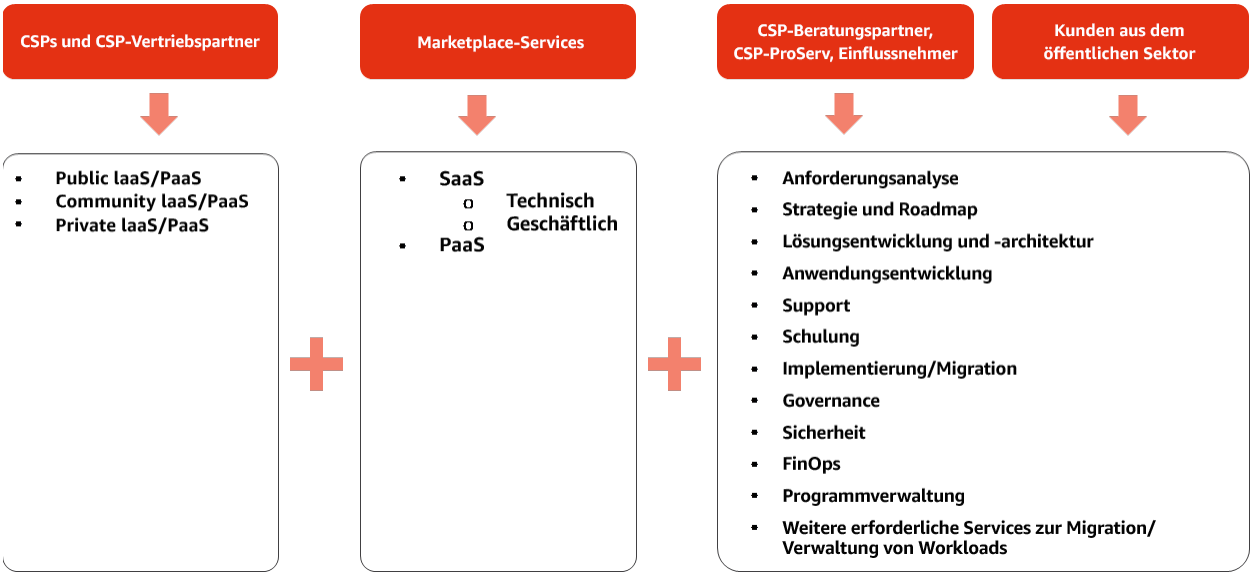

Abbildung 2: Eine Ausschreibung für Cloud-Services sollte Endbenutzern eine Palette aller von ihnen benötigten Cloud-Services zur Verfügung stellen. Kunden aus dem öffentlichen Sektor benötigen einen CISP für Cloud-Technologien und unter Umständen einen Marketplace für PaaS- und SaaS-Produkte. Dann kann der Kunde selbst bestimmen, welche Rolle er bei der Bereitstellung von Cloud-Services übernehmen möchte und wie viel er an Beratungsunternehmen/Systemintegratoren/Managed Service Providers usw. auslagern möchte.

Die folgenden Beispielformulierungen beziehen sich auf die Rollen und Verantwortlichkeiten aus Abbildung 2. Eine Cloud-Rahmenvereinbarung und die damit verbundene Ausschreibung für Cloud-Services sollten dafür sorgen, dass Käufer in der Lage sind, die Angebote der einzelnen Anbieter angemessen zu bewerten, sodass sie unter den für die Workload/das Projekt geeigneten Services die passenden auswählen können. Wie bereits besprochen, lässt sich dies am besten erreichen, indem die Services in verschiedene Bereiche aufgeteilt werden und klar definiert wird, wie unter der Rahmenvereinbarung Abrufe und Mini-Wettbewerbe durchgeführt werden.

Beispielformulierungen für die Ausschreibung: Einkaufsmodell

*Dieser Vertrag dient als **Rahmenvereinbarung** für Einkäufe. Diese Cloud-Rahmenvereinbarung umfasst mehrere **Bereiche**, gemäß der Definition von **<ORGANISATION>**, für Cloud-Technologien und zugehörige Marketplace-Services/-Produkte, Beratungsdienste, Professional Services/Systemintegration/Managed Services/Migration, Schulungen und Support, gemäß den Definitionen von **<ORGANISATION>**, und kann von mehreren berechtigten Einkäufern in Anspruch genommen werden, die mit **<ORGANISATION>** verbunden sind. Dadurch werden gleichzeitig der Beschaffungsprozess vereinfacht und Größenvorteile generiert.*

Sobald diese Rahmenvereinbarung in Kraft getreten ist, kann eine Organisation mit ihrer Hilfe die gewünschten spezifischen Cloud-Technologien und cloudbezogenen Services erwerben, und zwar zum gewünschten Zeitpunkt, anstatt sie durch einzelne Beschaffungsvorgänge zu erwerben. Ein solcher Ansatz reduziert die administrativen Anforderungen, die Komplexität der Auftragsvergabe und die Zykluszeit erheblich.

*Die Laufzeit der Rahmenvereinbarung beträgt maximal **<X>** Jahre, einschließlich aller Verlängerungen. Die maximale Dauer eines Abrufvertrags innerhalb der Rahmenvereinbarung beträgt in der Regel **<x>** Monate. Dieser kann um **<x>** Monate und dann um weitere **<x>** Monate verlängert werden, wobei ggf. die entsprechenden internen Genehmigungen für die Vertragsverlängerung vorliegen müssen. Dies wird in jedem spezifischen **Abruf** festgelegt.*

*Die RAHMENVEREINBARUNG ist in **3 (drei) Bereiche** unterteilt.*

1. *BEREICH 1: CLOUD-TECHNOLOGIEN – voller Umfang an Cloud-Anbieter-Technologien (direkt vom CISP, Vertriebspartner oder Vertriebspartner mit Mehrwertdiensten/Support):*
    i. *IaaS- und PaaS-Services – eine Auswahl aus Cloud-Technologien, z. B. Datenverarbeitung, Speicher, Netzwerke, Datenbanken, Analysen, Anwendungsservices, Bereitstellung, Verwaltung, Entwicklung, Internet of Things (IoT) usw. Umfasst Komplettlösungen für Cloud-Technologie wie DR/COOP, Archivspeicher, Big Data & Analytics, DevOps usw.*
2. *BEREICH 2: MARKETPLACE – voller Umfang an PaaS- und SaaS-Services/-Produkten wie Buchhaltung, CRM, Design, HR, GIS und Mapping, HPC, BI, Content Management, Protokollanalyse usw.*
3. *BEREICH 3: CLOUD-BERATUNG – voller Umfang an Beratungsdiensten (Managed Services, Professional Services, Consulting-/Beratungsdienste, Mehrwertdienste, FinOps, technischer Support) im Zusammenhang mit der Migration zur Cloud und ihrer Nutzung. Diese Services können Folgendes umfassen: Planung, Design, Migration, Verwaltung, Support, Qualitätssicherung, Sicherheit, Schulungen usw.*

Anbieter können ihre Angebote für mehrere Bereiche einreichen.

Anbieter reichen ihre Angebote und zugehörigen Preise in ihrem bevorzugten Format ein.

WETTBEWERBE INNERHALB DER RAHMENVEREINBARUNG UND VERGABE VON AUFTRÄGEN

ABRUFE

Öffentliche Einrichtungen, die an der Rahmenvereinbarung beteiligt sind, können die benötigten Services bei Bedarf bestellen oder „abrufen". Durch das Abschließen eines Abrufvertrages im Kontext der Rahmenvereinbarung können Käufer die Anforderungen im Zuge eines Abrufs mit zusätzlichen funktionalen Spezifikationen verfeinern und gleichzeitig die in der Rahmenvereinbarung angebotenen Leistungen beibehalten.

Aufträge, die im Kontext der Rahmenvereinbarung vergeben werden, verfügen über einen eindeutigen Audit-Trail hinsichtlich der Anforderungen, die zur Auswahl des Anbieters in den einzelnen Bereichen verwendet wurden. Die Endkunden führen Aufzeichnungen über die Kommunikation mit den Anbietern, einschließlich aller frühen Interaktionen am Markt, Fragen zur Klärung, E-Mails und persönlichen Gespräche.

1. SCHREIBEN VON ABRUFANFORDERUNGEN UND ERSUCHEN DER INTERNEN GENEHMIGUNG FÜR DEN EINKAUF

Alle Endkunden, die zur Nutzung der Rahmenvereinbarung berechtigt sind, erstellen gemeinsame Teams aus Endbenutzern, Einkaufsspezialisten und technischen Experten, um eine Liste der Dinge zu erstellen, die sie unbedingt brauchen, sowie derer, die zwar erfreulich wären, aber nicht unbedingt notwendig sind. Diese Anforderungen helfen bei der Entscheidung, welche Bereiche relevant sind und welcher Anbieter am besten für die Erfüllung der Anforderungen qualifiziert ist. Beim Entwurf von Anforderungen berücksichtigen Einkäufer Folgendes:

- *Verfügbare Mittel zur Nutzung des Services*
- *Technische und Beschaffungsanforderungen des Projekts*
- *Kriterien, auf denen die Auswahl basiert*

2. SUCHE NACH SERVICES

Käufer im Kontext der Rahmenvereinbarung verwenden einen Online-Rahmenkatalog (ein Portal, in dem über die Rahmenvereinbarung qualifizierte Anbieter und deren Services aufgeführt werden), um Produkte/Services zu finden, die ihren jeweiligen Anforderungen entsprechen. Sie wählen die zutreffenden Bereiche aus und suchen dann nach Services.

3. PRÜFUNG UND BEWERTUNG DER SERVICES

Käufer im Kontext der Rahmenvereinbarung prüfen die Servicebeschreibungen, um die Services zu finden, die ihren Bedarf am besten erfüllen, und zwar basierend auf den Anforderungen und dem Budget. Jede Servicebeschreibung enthält Folgendes:

- *Dokument zur Definition des Services oder Links zu Definitionen des Services*
- *Dokument mit den Geschäftsbedingungen*
- *Preisdokument (Links zu öffentlichen Preisen sind akzeptabel, wenn davon ausgegangen wird, dass eine vollständige Preisliste/ein Preisdokument auf Anfrage verfügbar ist.)*

Der Preis entspricht den Kosten für die am häufigsten verwendete Konfiguration des Services. Die Preisgestaltung ist jedoch in der Regel volumenbasiert. Käufer sollten sich also stets das Preisdokument des Anbieters oder die öffentlichen Preise ansehen und Tools zur Preisberechnung verwenden, um den tatsächlichen Preis des gekauften Produkts und den Gesamtwert für den Käufer zu ermitteln (z. B. Services zur Optimierung und daraus resultierende Kostensenkungen).

Käufer im Kontext der Rahmenvereinbarung können mit Anbietern sprechen, um sie zu bitten, ihre Servicebeschreibung, Geschäftsbedingungen, Preise oder Dokumente/Modelle zur Servicedefinition zu erläutern. Alle Gespräche mit Anbietern werden aufgezeichnet.

4. EINEN SERVICE AUSWÄHLEN UND EINEN AUFTRAG VERGEBEN

Ein Anbieter

Wenn nur ein Anbieter die Anforderungen erfüllt, kann ein Auftrag an diesen vergeben werden.

Mehrere Anbieter

Sind mehrere Anbieter in der engeren Auswahl, wählt der Käufer das wirtschaftlich günstigste Angebot aus (MEAT, Most Economically Advantageous Tender). Die Bewertung des wirtschaftlich günstigsten Angebots ist

den Kriterien in der folgenden Tabelle zu entnehmen. Käufer können entscheiden, welche detaillierten Eigenschaften sie für die Auswahl verwenden und wie sie gewichtet werden sollen.

Beachten Sie, dass der Käufer u. U. Folgendes tun muss:

- *Kombinationen aus verschiedenen Anbietern in Betracht ziehen*
- *spezifische Informationen zu Volume- oder Unternehmensrabatten sowie Services zur Kostenoptimierung von Anbietern einholen*

Die Bewertung von Anbietern sollte immer fair und transparent erfolgen. Es wird das passendste Angebot ausgewählt und Anbieter/Services werden nicht ausgeschlossen, ohne auf die Projektanforderungen zu verweisen.

Tabelle 2: Bewertung anhand des wirtschaftlich günstigsten Angebots (MEAT)

Vergabekriterien
Kosten über die gesamte Lebensdauer: *Kosteneffizienz, Preis und Betriebskosten*
Technische Vorzüge und funktionale Eignung: *Abdeckung, Netzwerkkapazität und Leistung gemäß den relevanten Service-Levels*
Kundendienst-Servicemanagement: *Helpdesk, Dokumentation, Kontoverwaltungsfunktionen und Sicherstellung der Versorgung einer Vielzahl von Services*
Nicht-funktionale Eigenschaften

MINI-WETTBEWERBE

Falls erforderlich, kann ein Mini-Wettbewerb abgehalten werden, um den besten Anbieter für eine bestimmte Workload oder ein bestimmtes Projekt zu ermitteln. Ein Mini-Wettbewerb bedeutet, dass ein Kunde im Zuge der Rahmenvereinbarung einen weiteren Wettbewerb ausruft, indem er alle Anbieter für einen Bereich dazu einlädt, auf eine Reihe von Anforderungen zu reagieren. Der Kunde lädt alle befähigten Anbieter innerhalb des Bereichs dazu ein, ein Angebot abzugeben. Weitere Vergleichsinformationen finden Sie in den folgenden Abschnitten zu Technik, Sicherheit und Preis/Wert.

VERTRAG

Sowohl der Käufer als auch der Anbieter unterzeichnen ein Exemplar des Vertrags, bevor der Service genutzt werden kann. Die maximale Dauer eines Vertrags innerhalb der Rahmenvereinbarung beträgt in der Regel ***<x>*** *Monate. Diese kann um* ***<x>*** *Monate und dann um weitere* ***<x>*** *Monate verlängert werden, wobei ggf. die entsprechenden internen Genehmigungen für die Vertragsverlängerung vorliegen müssen.*

Ein Exemplar des Vertrags muss von allen interessierten Parteien (Käufer und Anbieter) unterzeichnet werden, bevor der Service genutzt werden kann.

2.1.5 Mindestanforderungen Bieter – Verwaltung

Durch eine einfache und klare Formulierung der Qualifizierungskriterien für die Rahmenvereinbarung wird sichergestellt, dass keine Einreichungen von Anbietern herkömmlicher Rechenzentren oder Hardware eingehen, die eine herkömmliche Lösung als „Cloud" verpacken. Die Teilnehmer an der Ausschreibung sollten demonstrieren, wie sie die unten aufgeführten Mindestanforderungen an die administrativen Anforderungen für Bieter erfüllen.

Beachten Sie auch hier, dass sich dieses Dokument auf **BEREICH 1 – CLOUD-TECHNOLOGIEN** konzentriert. Wir haben jedoch zusätzliche Informationen zu **BEREICH 2 – MARKETPLACE** und **BEREICH 3 – CLOUD-BERATUNG** hinzugefügt, insofern sie helfen, den Gesamtkontext hinsichtlich der Anforderungen und des Umfangs der Ausschreibung zu verdeutlichen. Es ist beispielsweise wichtig, Mindestkriterien für die Qualifikation von CISP-Vertriebspartnern/MSP/SI/Beratungsunternehmen usw. anzugeben und sicherzustellen, dass diese (1) direkt mit dem CISP als Vertriebs- oder Channel-Partner verbunden sind, (2) von einem CISP für den Weiterverkauf des direkten Zugriffs auf CISP-Angebote an Drittunternehmen zertifiziert sind und (3) über entsprechende Zertifizierungen von diesen CISPs verfügen, die ihre Kompetenzen bestätigen.

Beispielformulierungen für die Ausschreibung: Mindestanforderungen Bieter – Verwaltung

Im Kontext dieser Rahmenvereinbarung werden Aufträge an mehrere Anbieter in den folgenden Kategorien vergeben. Bei den Anbietern muss es sich um einen kommerziellen CISP, einen externen Vertriebspartner eines CISP, einen Vertreiber von Marketplace-Services und/oder einen Anbieter von Services zur Nutzung eines CISP handeln (z. B. Beratung, Migrations-Services, Managed Services, FinOps usw.). Bitte geben Sie die Rollen an, die Sie anbieten:

BEREICH 1

____ - Direkter Anbieter (CISP) von Public-Cloud-Services (IaaS UND PaaS)

____ - Direkter Anbieter (CISP) von Community-Cloud-Services (IaaS UND PaaS)

____ - Direkter Anbieter (CISP) von Private-Cloud-Services (IaaS UND PaaS)

____ - CISP-Drittanbieter (Möglichkeit, direkten Zugriff auf Online-Cloud-Angebote eines CISP zu gewähren)

- *Geben Sie das CISP-Angebot an, das Sie per direktem Zugang zum Service weiterverkaufen: _____*
- *Weisen Sie über ein Dokument des CISP nach, dass Sie ein autorisierter Vertriebspartner für dessen Angebote sind: _____*

BEREICH 2

____ - Direkter Anbieter von Marketplace-Services, die auf einem CISP (PaaS und/oder SaaS) ausgeführt werden

____ - Vertreiber von Marketplace-Services, die auf einem CISP (PaaS und/oder SaaS) ausgeführt werden

BEREICH 3

____ - CISP für Professional Services

____ - Anbieter von technischem CISP-Support

____- CISP-Partner, der Services für die Nutzung des oder den Betrieb auf einem CISP bereitstellt

____- Einflussnehmer/Berater, der Services für die Nutzung des oder den Betrieb auf einem CISP bereitstellt

Geben Sie die Art des Angebots an:

- *Managed Services für Workloads auf einem CISP (J/N): _____*
  - *Geben Sie Ihre Spezialisierungen an (falls zutreffend): _____*
- *Professional Services: (J/N): _____*
- *Beratung – Training (J/N): _____*
- *Beratung – Strategie (J/N): _____*
- *Beratung – Migration (J/N): _____*
- *Beratung – Cloud-Governance (J/N): _____*
- *Beratung – FinOps (J/N): _____*
- *Beratung – Sonstiges (bitte angeben): _____*

Geben Sie den CISP/die CISPs an, für die Sie Services bereitstellen: _____

Weisen Sie über ein Dokument des CISP nach, welche Partnerrolle Sie im Rahmen des CISP-Modells einnehmen: _____

BEREICH 1: ADMINISTRATIVE MINDESTANFORDERUNGEN

Cloud-Service-Anbieter (CISPs)

Um sich als CISP zu qualifizieren, muss dieser die folgenden Anforderungen erfüllen.

Vorgeschlagene Qualifikationskriterien für CISP	*Grund*
Informationen zur Organisation wie Name, Rechtsform, Registrierungs-/DUNS-Nummer, USt. usw.	
Unternehmensgröße, wirtschaftliche und finanzielle Stellung[3]	*Der Kunde kann feststellen, dass der CISP in der Lage sein wird, den Vertrag zu erfüllen.*
Ausschlussgründe, z. B. kriminelle/betrügerische Aktivitäten usw.	
Fallstudien/Kundenreferenzen (erforderliche Anzahl/Art angeben)	*Der Kunde kann die Erfahrung des CISP im Bereitstellen der erforderlichen Services prüfen.*
Soziale Unternehmensverantwortung	*Dabei sollte es sich um öffentlich zugängliche Versionen handeln, die vom CISP bereitgestellt werden.*
Öffentlich verfügbare Nachhaltigkeitsverpflichtungen und -praktiken.	*Der Kunde kann sehen, dass ein CISP sich dazu verpflichtet, sein Geschäft so umweltfreundlich wie möglich zu führen.*
Der CISP muss über die letzten 5 Jahre eine nachweisliche Erfolgsgeschichte bei der Entwicklung und Veröffentlichung neuer nützlicher Services und Funktionen vorweisen können, insbesondere im Bereich PaaS, maschinelles Lernen und Analyse, Big Data, Managed	*Zeigt, dass der CISP daran arbeitet, neue Produkte schnell in die Hände der Kunden zu bringen, um diese Produkte dann schnell zu iterieren und zu verbessern. Dadurch arbeiten Kunden stets mit der modernsten IT-Infrastruktur, ohne dafür neues Kapital zu investieren.*

[3] Beachten Sie, dass für eine Ausschreibung für Cloud-Services allgemeine Informationen zum Unternehmen relevant sind und weniger Detailfragen, wie die Anzahl der Mitarbeiter im Unternehmen und die interne Teamstruktur der Mitarbeiter. Bei der Cloud-Technologie besteht kein Zusammenhang zwischen der garantierten Serviceleistung und der Anzahl der Mitarbeiter. Stattdessen betrachten Cloud-Ausschreibungen die gesamte Unternehmensgröße, um die Anforderungen (angemessene Skalierung) erfüllen zu können, sowie die nachweisbare Erfahrung/Leistung.

Services und Optimierungsfunktionen für die Cloud-Nutzung. Öffentlich zugängliche Änderungsprotokolle oder Aktualisierungs-Feeds können verwendet werden, um diesen Punkt zu belegen.	

Vertriebspartner-/Partnerbeziehung mit CISP

<ORGANISATION> verlangt, dass der Hauptauftragnehmer direkt mit dem CISP als Vertriebspartner oder Channel-Partner verbunden ist, von einem CISP für den Wiederverkauf des direkten Zugriffs auf die CISP-Angebote an Drittunternehmen zertifiziert wurde und Zertifizierungen dieser CISPs nachweisen kann, die seine Kompetenzen und sein Know-how belegen. Dadurch entfällt die Notwendigkeit für <ORGANISATION>, die Bedingungen und Services zu prüfen, die über eine zusätzliche Ebene der Untervergabe zwischen dem Hauptauftragnehmer der Rahmenvereinbarung und dem CISP stattfinden. Diese Anforderung verringert auch die Komplexität, die zusätzliche Ebenen von Vertriebspartnern generieren, wenn (1) <ORGANISATION> ihre Sorgfaltspflicht erfüllt, um eine klare Zuweisung von Verantwortlichkeiten in Bezug auf die zu erbringenden Services sicherzustellen, und (2) <ORGANISATION> tägliche Aktivitäten im Zusammenhang mit der Nutzung der Cloud-Services durchführt.

2.2 Technische Aspekte

Eine Ausschreibung für Cloud-Services sollte die Messlatte für CISPs höher legen, indem sie von diesen verlangt, die standardisierten Cloud-Technologien bereitzustellen, die ein Kunde zum Erstellen seiner individuellen Lösung benötigt. Wie bereits erwähnt, ist dieser Unterschied zwischen standardisierten und anpassbaren Komponenten für die Erstellung einer Cloud-Services-Ausschreibung sehr wichtig. CISPs bieten Millionen von Kunden standardisierte Services. Daher konzentrieren sich die individuellen Anpassungen in einer Cloud-Services-Ausschreibung auf zugeschnittene, kundenspezifische Lösungen und Ergebnisse, statt auf die dem System zugrunde liegenden Methoden, Infrastrukturen oder Hardware, welche zur Bereitstellung der eigentlichen Cloud-Services und ihrer Ergebnisse eingesetzt werden.

2.2.1 Mindestvoraussetzungen

Herkömmliche IT-Beschaffungen basieren häufig auf Geschäftsanforderungen, die in mehreren Arbeitssitzungen entwickelt werden und dokumentieren, wie die Organisation derzeit ihre Geschäfte führt. Diese Anforderungen perfekt zu formulieren, ist selbst unter den besten Umständen ein schwieriger Prozess. Wenn diese Sitzungen erfolgreich sind, dokumentieren sie den historischen Geschäftsprozess, der sich seinerseits als veraltet und ineffizient erweisen kann. Wenn diese Anforderungen dann als Teil der Ausschreibung vom CISP zu replizieren sind, muss dieser unter Umständen eine völlig individuelle Lösung konzipieren. Dieses Modell ist nicht mit der Cloud-Auftragsvergabe kompatibel.

Organisationen des öffentlichen Sektors sollten ihre Geschäftsziele und Leistungsanforderungen verstehen, jedoch in einer Ausschreibung nicht das Systemdesign und die Funktionalität vorgeben. Stattdessen sollten sie aus geschäftlicher Sicht nach dem am besten passenden Dienstleister suchen. Anstatt Angebote für Hunderte oder sogar Tausende von Anforderungen zu bewerten, die unter Umständen gar nicht zu erfolgreichen Services führen werden, sollten Organisationen Bewertungskriterien einbeziehen, die berücksichtigen, wie gut die Technologie und die zugehörigen Services die Geschäftsziele erfüllen oder verbessern, ob sie ihren Performanceanforderungen genügen oder ob die Möglichkeit zur Feinabstimmung von Geschäftsregeln durch Konfigurationen gegeben ist.

*Cloud-Ausschreibungen sollten die richtigen Fragen stellen, um die besten Lösungen zu erhalten. Da in einem Cloud-Modell keine physischen Komponenten erworben werden, sind viele herkömmliche Beschaffungsanforderungen für Rechenzentren nicht anwendbar. **Die gleichen Fragen wie bei Rechenzentren zu verwenden, führt zu wenig aussagekräftigen Antworten**. Dadurch sind CISPs oft nicht in der Lage, passende Angebote abzugeben, oder es entstehen schlecht konzipierte Verträge, mit denen Kunden aus dem öffentlichen Sektor die Möglichkeiten und Vorteile der Cloud nicht effektiv nutzen.*

Eine Ausschreibung für Cloud-Services sollte sich auf die wichtigsten Anforderungen konzentrieren, die ein CISP und seine Cloud-Services erfüllen müssen. So wird sichergestellt, dass Anbieter, die sich für BEREICH 1 qualifizieren, einen hohen Standard erfüllen. Die Anforderungen sollten auch nicht zu präskriptiv sein, um den Zugang des öffentlichen Sektors zu einer breiten Palette qualifizierter CISPs nicht zu beschneiden.

Beispielformulierungen für die Ausschreibung: Ressourcen Cloud-Anbieter

Siehe auch die obigen administrativen Mindestanforderungen an den CISP für BEREICH 1

Vorgeschlagene Qualifikationskriterien für CISP	*Grund*
Infrastruktur	
Die CISP-Infrastruktur sollte mindestens 2 Cluster von Rechenzentren bieten. Jeder Cluster muss aus mindestens 2 Rechenzentren bestehen, die über eine Verbindung mit niedriger Latenz verbunden sind, um hochverfügbare Aktiv-Aktiv-Bereitstellungen und Implementierungen von DR-BC-Szenarien zu ermöglichen. Die Rechenzentren, aus denen jeder Cluster besteht, müssen physisch isoliert und ausfallunabhängig voneinander sein.	*Der CISP muss eine Infrastruktur anbieten können, die für die Erstellung von Anwendungen mit hoher Verfügbarkeit geeignet ist, bei denen Single Points of Failure vermieden werden können.*
Der CISP sollte logisch und geografisch isolierte Regionen bereitstellen. Kundendaten dürfen außerhalb dieser Regionen nicht durch den CISP repliziert werden.	*Die Anforderungen an die Datenresidenz legen fest, dass der Kunde die vollständige Kontrolle darüber hat, wo seine Daten gespeichert werden.*
Der CISP muss direkte, dedizierte und private Verbindungen zwischen den CISP-Rechenzentren bereitstellen können.	*Private Konnektivität ist eine grundlegende Voraussetzung für den Aufbau einer hybriden, sicheren Infrastruktur.*
Der CISP sollte ausreichende Verschlüsselungsmechanismen bereitstellen, darunter die Verschlüsselung von Daten während der Übertragung.	*Der Kunde kann verlangen, dass es eine Funktion gibt, mittels derer gewährleistet wird, dass keine Daten unverschlüsselt übertragen werden können.*
Minimale CISP-Zertifizierungen	
Der CISP muss nach ISO 27001 zertifiziert sein.	*Auditing, Zertifizierung und Akkreditierung durch unabhängige Dritte stellen sicher, dass Kunden Services (und insbesondere die Plattform) hinsichtlich Qualität, Sicherheit und Zuverlässigkeit beurteilen können. Es ist wichtig, dass ein Mindestmaß an Zertifizierungen erfüllt wird.*

Der CISP muss den CISPE-Verhaltenskodex zum Datenschutz einhalten, um DSGVO-konforme Funktionen und Services anbieten zu können. Dadurch sind Kunden wiederum befähigt, DSGVO-konforme Anwendungen zu entwickeln.	*Der Kunde muss in der Lage sein, Anwendungen unter Einhaltung der DSGVO zu entwickeln und auszuführen.*
Der CISP muss von unabhängigen Dritten geprüfte Berichte wie SOC 1- und SOC 2-Berichte (die die vom Endkunden verwendeten Standorte und Services abdecken) vorweisen, um Transparenz hinsichtlich seiner Kontrollmechanismen und -verfahren zu gewährleisten.	*Der CISP muss nachvollziehbar aufzeigen, wie die Anwendung betrieben und verwaltet wird. SOC-Berichte sind entscheidend, um Vertrauen und Transparenz zu gewährleisten.*
Der CISP muss sich an den Climate Neutral Data Centre Pact halten.	*Der Climate Neutral Data Centre Pact hält den CISP dazu an, bis zum Jahr 2030 Klimaneutralität zu erreichen und so den Benutzer dabei zu unterstützen, seine eigenen Nachhaltigkeitsziele zu erfüllen. Prüfer eines Drittanbieters sind verpflichtend für Anbieter mit >250 Vollzeitbeschäftigten (keine KMU).*
Der CISP muss sich an den SWIPO IaaS Portability Code of Conduct halten.	*Der SWIPO IaaS Portability Code of Conduct stellt sicher, dass Services die Anforderungen von Artikel 6 „Data Porting" der Verordnung über den „freien Verkehr nicht-personenbezogener Daten" einhalten.*
Servicemerkmale	
Die CISP-Infrastruktur muss über Programmierschnittstellen (APIs) und eine webbasierte Managementkonsole zugänglich sein.	*Self-Service-Zugriff und Programmierschnittstellen sind ein verpflichtender Standard für CISP-Anbieter, damit möglichst viele Zugriffe durch Benutzer und den Anbieter selbst entfallen können.*
Der CISP muss eine Reihe von grundlegenden Services anbieten, darunter: Objektspeicher, verwaltete relationale Datenbank, verwaltete nicht relationale Datenbank, verwaltete Load Balancer, Überwachung und integrierte automatische Skalierung.	*Das bloße Angebot virtueller Maschinen reicht nicht aus, um einen Anbieter als Cloud-Anbieter zu qualifizieren. Cloud-Anbieter sollten eine Reihe von PAAS- und IAAS-Services anbieten, um die Anwendungen der Kunden zu beschleunigen und zu verbessern.*
Der CISP muss es dem Kunden ermöglichen, die Nutzung und Konfiguration seiner Services frei zu ändern oder Daten innerhalb und außerhalb des CISP zu verschieben (Self-Service-Angebot).	*Der Self-Service-Zugriff auf Services und Daten ist eine entscheidende Anforderung, die es dem Kunden ermöglicht, vollkommen unabhängig zu sein.*
Der CISP muss die Abrechnung der Services nach dem „Pay-per-Use"-Prinzip zulassen.	*„Pay-per-Use" ermöglicht dem Kunden die Kostenoptimierung seiner Workloads, die Minimierung von Risiken und die Nutzung des CISP für kurzlebige Anwendungen und PoCs.*
Daten- und Systemsicherheit	
Der CISP muss dem Kunden die Bewahrung der vollständigen Kontrolle über seine Daten ermöglichen, dem Kunden die Freiheit einräumen, den Speicherort der Daten auszuwählen (Stadtgebiet), und sicherstellen, dass keine Kundendaten verschoben werden, es sei denn, eine solche Verschiebung wird vom Kunden selbst initiiert.	*Der Kunde muss die Kontrolle darüber haben, wo Daten gespeichert werden, wie der Zugriff auf Inhalte verwaltet wird und wie der Benutzerzugriff auf Services und Ressourcen erfolgt.*

Der CISP muss dem Kunden die vollständige Kontrolle über seine Sicherheitsrichtlinien geben, einschließlich Vertraulichkeit, Integrität und Verfügbarkeit der Kundendaten und -systeme.	*Der Kunde muss in der Lage sein, seine Sicherheitsstandards für alle Workloads zu definieren und zu implementieren. Es reicht nicht aus, dem Anbieter zu vertrauen, mit den Kundendaten „das Richtige zu tun".*
Kostenkontrolle	
Der CISP muss über Mechanismen und Tools verfügen, die es dem Kunden ermöglichen, die Ausgaben im Zeitverlauf zu überwachen. Die Tools müssen eine grundlegende Untergliederung der Kosten basierend auf Workload, Service und Konto ermöglichen.	
Der CISP muss Tools anbieten, über die der Kunde gewarnt wird, wenn eine Kostenschwelle überschritten wird.	
Der CISP muss dem Kunden detaillierte Rechnungen vorlegen. Es muss möglich sein, die Rechnung so zu strukturieren, dass die Kosten nach Workload, Umgebung und Konto aufgeteilt werden.	

CISPs sollten auch Antworten auf die folgenden Fragen zu den technischen Anforderungen geben.

LÖSUNGEN

Der CISP sollte demonstrieren, wie er vorgefertigte Vorlagen und Softwarelösungen bereitstellen kann, die entweder vom CISP gehostet werden oder in diesen integriert werden, und zwar für die folgenden Lösungen:

- *Speicher*
- *DevOps*
- *Sicherheit/Compliance*
- *Big Data/Analytics*
- *Unternehmensanwendungen*
- *Telekommunikation und Netzwerke*
- *Raumbezogene Daten*
- *IoT*
- *[Sonstige]*

Geben Sie einen Überblick darüber, wie der CISP für die folgenden Workloads eingesetzt wurde:

- *Notfallwiederherstellung*
- *Entwicklung und Test*
- *Archivierung*
- *Sicherung und Wiederherstellung*
- *Big Data*
- *High Performance Computing (HPC)*
- *Internet of Things (IoT)*
- *Websites*
- *Serverless-Datenverarbeitung*
- *DevOps*
- *Bereitstellung von Inhalten*
- *[Sonstige]*

2.2.2 Vergleich zwischen Anbietern

Zusätzlich zu den Mindestanforderungen in einer Cloud-Services-Ausschreibung ist es wichtig, Kriterien anzugeben, anhand derer CISP-Technologien im Rahmen einer kompetitiven Auswertung verglichen werden können.

Ausschreibungen für Cloud-Services sollten die Cloud-Funktionen adressieren, die ein Unternehmen wirklich benötigt, unter der Voraussetzung, dass der Kunde das Recht hat, auf Grundlage dieser Funktionen seine eigenen Lösungen zu entwickeln. Funktionen, die über den Standard hinausgehen, den ein CISP bereitstellen kann (z. B. vorgefertigte Lösungen über den CISP oder Automatisierungsfunktionen), können in einer Cloud-Services-Ausschreibung zugunsten einer aussagekräftigeren Analyse von „Optionen mit Mehrwert" oder „bestem Wert" einfließen.

Der öffentliche Sektor verlangt oft einen Wettbewerb zwischen Bietern, bei dem Bewertungskriterien wie der beste Wert, das wirtschaftlich günstigste Angebot (MEAT) oder der niedrigste Preis angelegt werden. Auch bei der Planung in Hinsicht auf diesen Teil einer Cloud-Services-Ausschreibung ist es für Organisationen des öffentlichen Sektors wichtig, die einzigartigen Merkmale der Cloud zu berücksichtigen. So können Cloud-Leistungen etwa nicht über den simplen Vergleich der Einzelposten (z. B. Datenverarbeitung oder Speicher) effektiv bewertet werden. Stattdessen empfehlen wir dringend, das Augenmerk auf allgemeinere, übergeordnete Lösungen zu richten, z. B. mit Blick auf die in Abschnitt ***2.2.1*** aufgeführten Punkte. Anschließend können Organisationen des öffentlichen Sektors die cloudspezifischen Anforderungen berücksichtigen, z. B. die in *Anhang A – Technische Anforderungen für den Vergleich zwischen* Bietern aufgeführten Punkte.

Ausschreibungen sollten die wichtigsten Cloud-Merkmale benennen, die für die Erstellung ihrer Cloud-Lösung benötigt werden. Dazu können Organisationen des öffentlichen Sektors die „wichtigsten Cloud-Merkmale" des National Institute of Standards and Technology (NIST) nutzen und zusätzlich Berichte von externen Analytikern verwenden, um sicherzustellen, dass der CISP das am besten geeignete Angebot für eine „echte Cloud" liefert und dieses auch in großem Maßstab funktioniert.

Beispielformulierungen für die Ausschreibung – Vergleich zwischen Anbietern

*CISPs sollten Antworten auf ALLE Fragen zu technischen Anforderungen in **Anhang A** geben.*

Die Teilnehmer müssen über die folgenden Attribute verfügen und beschreiben, wie ihre Angebote über Cloud-Services den fünf wichtigsten Merkmalen für Cloud Computing entsprechen[4].

1) ***On-Demand-Self-Service:*** *Der Teilnehmer muss die Möglichkeit anbieten, Datenverarbeitungsfunktionen wie Serverzeit und Netzwerkspeicher nach Bedarf automatisch und einseitig bereitzustellen, ohne dass eine menschliche Interaktion mit jedem Serviceanbieter erforderlich ist. Der Teilnehmer verhilft der bestellenden Partei zu der Fähigkeit, Services einseitig (d. h. ohne Prüfung oder Genehmigung durch den Anbieter) bereitzustellen. Erklären Sie, wie dies mit Ihrem Angebot oder dem Angebot, das Sie vertreten, funktioniert.*

2) ***Universeller Netzwerkzugriff:*** *Teilnehmer müssen mehrere Optionen zur Netzwerkverbindung bereitstellen, von denen eine internetbasiert sein muss. Erklären Sie, wie dies mit Ihrem Angebot oder dem Angebot, das Sie vertreten, funktioniert.*

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

3) ***Ressourcen-Pooling:*** *Der CISP des Teilnehmers muss gepoolte Datenverarbeitungsressourcen bereitstellen, die mehrere Verbraucher bedienen. Dabei muss ein Mehrmandantenmodell verwendet werden, in dem verschiedene virtuelle Ressourcen dynamisch zugewiesen und je nach Verbrauchernachfrage umverteilt werden. Der Benutzer kann den Standort auf einer höheren Abstraktionsebene angeben (z. B. Land, Region oder Standort des Rechenzentrums). Der Teilnehmer soll die Skalierung dieser Ressourcen innerhalb von Minuten oder Stunden nach einer Bereitstellungsanfrage unterstützen. Erklären Sie, wie dies mit Ihrem Angebot oder dem Angebot, das Sie vertreten, funktioniert.*

4) ***Schnelle Elastizität:*** *Der CISP des Teilnehmers unterstützt die Bereitstellung und Beendigung von Services (Hoch- und Herunterskalieren). Dadurch wird der Service innerhalb der vorgeschriebenen Mindestzeiten (maximal „x" Stunden) ab der Bereitstellungsanfrage verfügbar gemacht. Der Teilnehmer unterstützt Anpassungen bei der Abrechnung, die sich aus diesen Bereitstellungsanfragen ergeben, auf stündlicher oder täglicher Basis.*

5) ***Messbarer Service:*** *Der Teilnehmer muss die Servicenutzung über ein Online-Dashboard oder ähnliche elektronische Mittel transparent machen.*

Darüber hinaus muss der CISP:

- *Ein anerkannter Marktführer bei der Bereitstellung von Cloud-Services sein, wie im Gartner Magic Quadrant für IaaS dargelegt[5].*
- *Branchenweit anerkannte Analystenberichte von unabhängigen Dritten vorlegen, die die nachweisbaren Fähigkeiten und die Zuverlässigkeit des CISP dokumentieren.*

Abschließend werden die CISPs anhand der in Anhang B aufgeführten Szenarien miteinander verglichen.

2.2.2.1 Service Level Agreements (SLAs)

CISPs stellen standardisierte kommerzielle SLAs für Millionen von Kunden bereit und können daher keine kundenspezifischen SLAs anbieten, wie es der Fall bei lokalen Rechenzentrumsmodellen ist. Kunden von CISPs können jedoch (oft mithilfe von CISP-Partnern) die Architektur ihrer Cloud-Nutzung so gestalten, dass die kommerziellen SLAs eines CISP wirksam genutzt und kundenspezifische Anforderungen sowie individuelle SLAS erfüllt und übertroffen werden können.

Ausschreibungen für Cloud-Services sollten sicherstellen, dass die CISPs die erforderlichen Funktionen und Hilfestellungen für die Nutzung ihrer Services sowie kommerzielle SLAs bereitstellen, damit einzelne Endbenutzer ihre Anforderungen an Leistung und Verfügbarkeit erfüllen können.

Bespielformulierungen für die Ausschreibung: Service Level Agreements

Stellen Sie Informationen und Links zum Ansatz des CISP zu Service-Level-Vereinbarungen (SLAs) bereit.

<ORGANISATION> *wird sich über die SLAs des CISP auf dem Laufenden halten und wichtige Workloads und Anwendungen so bereitstellen, dass sie auch im Falle einer Nichterfüllung eines SLA weiter funktionieren.*

<ORGANISATION> *ist für die Aufrechterhaltung entsprechender SLAs verantwortlich, die mit* ***<ORGANISATION>*** *eigenen Geräten oder von* ***<ORGANISATION>*** *betriebenen Services verbunden sind, die mit dem CISP genutzt werden.*

[5] https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb

*Der CISP muss **<ORGANISATION>** mit Möglichkeiten zur kontinuierlichen Transparenz und Berichterstattung seiner betrieblichen SLA-Performance sowie dokumentierten Best Practices ausstatten, um die CISP-Infrastruktur für die Entwicklung von Services mit Hinblick auf Performance, Beständigkeit und Zuverlässigkeit ideal zu nutzen.*

2.2.3 Vertragsabschluss

Die CISP-Geschäftsbedingungen sind so konzipiert, dass sie die Funktionsweise eines Cloud-Servicemodells widerspiegeln (physische Komponenten werden nicht erworben und CISPs wirtschaften in großem Maßstab mit standardisierten Serviceangeboten). Daher ist es wichtig, dass die Geschäftsbedingungen eines CISP im größtmöglichen Umfang integriert und genutzt werden. Im folgenden Abschnitt **2.5** finden Sie weitere Informationen zu den Geschäftsbedingungen und zum Vertragsabschluss.

2.2.3.1 Neue und sich ändernde Services

CISPs bieten Leistung über einen Service. Im Gegensatz zu herkömmlichen lokalen Lösungen, die Upgrades und auslaufende Servicewartungsverträge erfordern, stellen Cloud-Anbieter einfach den standardisierten Service bereit. Damit das Cloud-Modell Größenvorteile erzielen kann, werden Upgrades und Änderungen an der zugrunde liegenden Infrastruktur für alle bereitgestellt, nicht für einzelne Benutzer, und Kunden wählen dann die Services aus, die sie verwenden. Der Service ist reibungsloser als ältere lokale Systeme und Cloud-Anbieter fügen ständig neue und erweiterte Services hinzu, die die Kunden nach Bedarf nutzen können.

Ist es nicht möglich, nach Ablauf der Frist zur Angebotsabgabe zusätzliche oder erweiterte CISP-Services hinzuzufügen, nehmen sich Organisationen des öffentlichen Sektors die Möglichkeit, neue Services und erweiterte Funktionen zu nutzen, bis die nächste Version einer Rahmenvereinbarung veröffentlicht wird. Wir empfehlen daher nachdrücklich, dass die Regeln zur Bereitstellung der in der Rahmenvereinbarung beschriebenen Services so weit gefasst sind, dass sie das Hinzufügen neuer CISP-Services nach Ablauf der Einreichfrist ermöglichen. Das EU-Vergaberecht kann das Hinzufügen von wesentlich anderen CISP-Diensten zur Rahmenvereinbarung einschränken, aber Aktualisierungen und neue Versionen von Diensten, die nicht als wesentliche Änderungen gelten, können ohne Schwierigkeiten hinzugefügt werden.

Beispielformulierungen für die Ausschreibung: Neue und sich ändernde Services

*Der CISP stellt eine kostengünstige Lösung bereit, die sowohl bewährte als auch stabile Virtualisierungstechnik und modernste Technologien nutzt, die ständig aktualisiert werden. **<ORGANISATION>** erkennt an und stimmt zu, dass die Cloud-Technologien **<ORGANISATION>** und anderen Kunden des CISP von einer gemeinsamen Codebasis und/oder gemeinsamen Umgebung aus als Shared-Service zur Verfügung gestellt werden können und der CISP von Zeit zu Zeit die Funktionen, Eigenschaften und Leistung oder andere Merkmale der Cloud-Services ändern oder löschen kann. Falls eine solche Änderung, Ergänzung oder Löschung erfolgt, werden die Spezifikationen des Cloud-Service entsprechend angepasst.*

*Der Umfang dieses Bereitstellungsauftrags umfasst alle derzeit vorhandenen und neuen oder erweiterten CISP-Services **INNERHALB DES UMFANGS DER RAHMENVEREINBARUNG.** Vom CISP bereitgestellte Cloud-Services für gewerbliche Kunden werden **<ORGANISATION>** zur Verfügung gestellt.*

2.2.3.2 Anbieterbindung/Reversibilität

Die Cloud-Technologie verringert die Anbieterbindung, da keine physischen Komponenten erworben werden und Kunden ihre Daten jederzeit von einem Cloud-Anbieter zu einem anderen verschieben können.

Ein gewisses Maß an Anbieterbindung ist jedoch beim Erwerb von Cloud-Services unvermeidlich, da nicht alle Clouds gleich sind. Daher kann manchmal ein CISP Services und Funktionen bereitstellen, die ein anderer schlicht nicht im Angebot hat. Dadurch wird die Möglichkeit verringert, solche Dienste bei einem anderen Anbieter zu nutzen. Ein sinnvoller Ansatz besteht darin, dass CISPs die erforderlichen Funktionen und Services zum Verlassen ihrer Cloud bereitstellen müssen, sowie eine Dokumentation darüber, wie diese Services als angemessene „Exit-Strategie" verwendet werden können. Schließlich ist es einem CISP unmöglich, die einzigartige Konfiguration seiner standardisierten Services durch den Kunden zu kennen und somit einen individuellen Exit-Plan zu erstellen.

Siehe Abschnitt 2.3.1.2 für Informationen zu branchenspezifischen Verhaltenskodizes für „Data Porting" und „Wechsel von Cloud-Anbietern" zur Erfüllung der Anforderungen des Artikels 6 der EU-Verordnung über den „freien Verkehr nicht-personenbezogener Daten".

Beispielformulierungen für die Ausschreibung: Ein- und Ausstieg

<ORGANISATION> sucht nach Vorschlägen, die eine angemessene Exit-Strategie enthalten, um eine Anbieterbindung zu verhindern. <ORGANISATION> kauft keine physischen Komponenten und der CISP muss sich innerhalb des IT-Stacks nach oben und unten verschieben lassen können. Der CISP stellt Tools und Services für die Portabilität bereit, die bei der Migration zur und von der CISP-Plattform helfen und so die Anbieterbindung minimieren. Eine detaillierte Dokumentation zur Verwendung der vom CISP bereitgestellten Portabilitätstools und -services dient als angemessener Exit-Plan.

*Der CISP darf keine **Mindestverpflichtungen** oder **verpflichtenden** langfristigen Verträge verlangen.*

Daten, die bei einem Serviceanbieter gespeichert sind, können jederzeit vom Kunden exportiert werden. Der CISP ermöglicht es <ORGANISATION>, Daten nach Bedarf auf den und vom CISP-Speicher zu verschieben. Der CISP muss auch das Herunterladen und Portieren von Images virtueller Maschinen auf einen neuen Cloud-Anbieter ermöglichen. <ORGANISATION> kann die eigenen Computer-Images exportieren und lokal oder bei einem anderen Anbieter verwenden (vorbehaltlich der Softwarelizenzeinschränkungen).

2.3 Sicherheit

Sicherheits- und Compliance-Verantwortlichkeiten werden zwischen dem CISP und den Cloud-Kunden aufgeteilt. In diesem Modell steuern die Cloud-Kunden, wie sie ihre Anwendungen und Daten in der Infrastruktur erstellen und sichern, während die CISPs dafür verantwortlich sind, Services auf einer hochsicheren und kontrollierten Plattform bereitzustellen und eine Vielzahl von zusätzlichen Sicherheitsfunktionen anzubieten. Die genaue Verteilung der CISP- und Kundenverantwortlichkeiten in diesem Modell hängt vom Cloud-Bereitstellungsmodell ab (IaaS/PaaS/SaaS) und die Kunden sollten sich über ihre Verantwortlichkeiten in jedem Modell im Klaren sein.

Ein Verständnis dieses Modells der geteilten Verantwortung ist entscheidend für eine erfolgreiche Ausschreibung von Cloud-Services. Organisationen des öffentlichen Sektors sollten wissen, wofür ein CISP zuständig ist, wofür sie selbst verantwortlich sind und wo Beratungs-/ISVs-Partner und deren Lösungen zur Unterstützung eingesetzt werden sollten.

2.3.1 Mindestvoraussetzungen

Das Schlüsselwort in Bezug auf Sicherheit in der Cloud ist **Funktionalität**. Organisationen im öffentlichen Sektor sollten hohe Ansprüche an die CISPs stellen und verlangen, dass CISPs die erforderlichen Sicherheitsfunktionen bieten, um zu gewährleisten, dass die Kunden ihre Verantwortlichkeiten im Rahmen des Modells der geteilten Verantwortung erfüllen können. Wie aus der nachstehenden, repräsentativen Liste von Anforderungen hervorgeht, wird der CISP dazu angehalten, einen standardisierten Leistungsumfang bereitzustellen, mit dessen Hilfe der Kunde seine individuelle Cloud-Umgebung absichern kann.

- ***Funktionen für Netzwerk- und Webanwendungs-Firewalls*** *zur Erstellung privater Netzwerke und zur Steuerung des Zugriffs auf Instances und Anwendungen*
- ***Konnektivitätsoptionen****, die private oder dedizierte Verbindungen von Ihrem Büro oder Ihrer lokalen Umgebung ermöglichen*
- ***Funktionalität*** *für die Implementierung einer tiefgreifenden* ***Verteidigungsstrategie*** *und zur Abwehr von DDoS-Angriffen*
- ***Funktionen zur Datenverschlüsselung****, die für Speicher- und Datenbankservices verfügbar sind*
- ***Flexible Optionen für die Schlüsselverwaltung****, mit denen Sie auswählen können, ob der CISP die Verschlüsselungsschlüssel verwalten soll oder ob der Kunde die vollständige Kontrolle über die Schlüssel behalten möchte*
- ***APIs*** *für Kunden zur Integration von Verschlüsselung und Datenschutz in die in einer CISP-Umgebung entwickelten oder bereitgestellten Services*
- ***Bereitstellungstools****, um die Erstellung und Außerbetriebnahme von CISP-Ressourcen gemäß den Standards der Organisation zu verwalten*
- *Tools zur* ***Inventar- und Konfigurationsverwaltung****, um CISP-Ressourcen zu identifizieren und die Änderungen an diesen Ressourcen im Zeitverlauf nachzuverfolgen und zu verwalten*
- ***Tools und Funktionen****, mit denen Kunden genau sehen können, was in ihrer CISP-Umgebung passiert*
- ***Detaillierte Einblicke in API-Aufrufe****, einschließlich des aufrufenden Benutzers, der aufgerufenen Daten, des Zeitpunkts und Standorts des Aufrufs*
- ***Optionen zur Protokollzusammenführung****, einschließlich Angleichung von Untersuchungen und der Compliance-Berichterstellung*
- *Möglichkeit zur Konfiguration von Warnmeldungen bei bestimmten Ereignissen oder bei Überschreitung bestimmter Schwellenwerte*
- ***Funktionen*** *zum Definieren, Erzwingen und Verwalten von Benutzerzugriffsrichtlinien über CISP-Dienste hinweg*
- *Möglichkeit, einzelne* ***Benutzerkonten mit Berechtigungen für alle CISP-Ressourcen*** *zu definieren*
- *Möglichkeit zur* ***Integration und Verbindung von Firmenverzeichnissen****, um die Kosten für Administration zu verringern und das Endbenutzererlebnis zu verbessern*

Weitere Informationen zu diesen Anforderungen sind unter *Anhang A – Technische Anforderungen für den Vergleich zwischen* Bietern zu finden.

Funktionen, die über den Mindeststandard für Sicherheit hinausgehen, können in einer Cloud-Services-Ausschreibung in eine aussagekräftigere Analyse von „Optionen mit Mehrwert“ oder „bestem Wert“ einfließen. Und je mehr Funktionalität in Bezug auf die Sicherheit integriert oder automatisiert ist, desto besser. Informationen zu den Anforderungen für den Vergleich zwischen Bietern finden Sie, wie bereits erwähnt, unter *Anhang A – Technische Anforderungen für den Vergleich zwischen* Bietern.

Organisationen des öffentlichen Sektors sollten sich Zertifizierungen und Auswertungen zur Cloud-Akkreditierung ansehen, um sicherzustellen, dass die erforderlichen CISP-Sicherheitskontrollen vorhanden sind. Beispiel: Stellen Sie sich einen CISP vor, der durch einen unabhängigen Prüfer validiert und zertifiziert wurde, um seine Compliance mit dem ISO 27001-Zertifizierungsstandard zu bestätigen. ISO 27001 Anhang A, Abschnitt 14 umfasst die spezifischen Kontrollen, die ein CISP gemäß den ISO-Anforderungen bezüglich Systembeschaffung, -entwicklung und -wartung einhält. Es ist wahrscheinlich, dass diese Kontrollen die Mehrheit, wenn nicht alle, der Kontrollen rund um den Erwerb, die Entwicklung und die Wartung von Systemen abdecken, die normalerweise von einer Organisation in einer IT-bezogenen Ausschreibung angefordert werden. Aus diesem Grund ist es sinnvoll, dass eine Organisation einfach verlangt, dass ein CISP nach ISO 27001 zertifiziert ist, anstatt den Aufwand zu duplizieren und in einer Cloud-Services-Ausschreibung selbst alle Kontrollanforderungen für die Systembeschaffung, -entwicklung und -wartung aufzulisten.

Dieser Ansatz zur Nutzung von Compliance-Berichten unabhängiger Dritter kann auf die meisten Sicherheits- und Compliance-Kontrollen angewendet werden, z. B. CISPE DSGVO-Verhaltenskodex, ISO, SOC usw.

Beispielformulierungen für die Ausschreibung: Sicherheit

*Der CISP legt seine nicht proprietären Sicherheitsprozesse und technischen Einschränkungen **<ORGANISATION>** gegenüber offen, sodass zwischen **<ORGANISATION>** und dem Serviceanbieter ein angemessener Schutz und eine ausreichende Flexibilität erreicht werden können.*

Der CISP hat seine Rollen und Verantwortlichkeiten im Hinblick auf Sicherheit und Compliance anzugeben:

- *Beschreiben Sie die sicherheitsbezogenen Rollen und Verantwortlichkeiten von CISP und **<ORGANISATION>** im Angebot. Erläutern Sie die Abgrenzung der Verantwortlichkeiten und erläutern Sie die CISP-Services, die **<ORGANISATION>** beim Aufbau und bei der Automatisierung von Sicherheitsfunktionen in der Cloud-Umgebung unterstützen.*
- *Geben Sie Antworten auf die technischen Spezifikationen in **ANHANG A** mit Bezug auf die Sicherheitsanforderungen von **<ORGANISATION>**.*

EIGENTUM VON UND KONTROLLE ÜBER INHALTE VON <ORGANISATION>

*Beschreiben Sie, wie CISP-Funktionen den Datenschutz von **<ORGANISATION>** gewährleisten. Geben Sie die vorhandenen Kontrollen an, über die der Schutz von Inhalten von **<ORGANISATION>** gewährleistet wird. Der CISP muss eine starke regionale Isolierung bieten, damit Objekte, die in einer Region gespeichert sind, diese Region niemals verlassen, es sei denn, **<ORGANISATION>** überträgt sie explizit in eine andere Region.*

- *<ORGANISATION> verwaltet den Zugriff auf die eigenen Inhalte, Services und Ressourcen. Der CISP sollte erweiterte Zugriffs-, Verschlüsselungs- und Protokollierungsfunktionen bereitstellen, die **<ORGANISATION>** bei der effektiven Umsetzung unterstützen. Der Zugriff auf oder die Nutzung der Inhalte von **<ORGANISATION>** seitens des CISP geschieht zu keinen anderen als den gesetzlich vorgeschriebenen Zwecken sowie um die CISP-Dienste aufrechtzuerhalten und sie **<ORGANISATION>** und dessen Endbenutzern zur Verfügung zu stellen.*
- *<ORGANISATION> wählt die Region(en) aus, in der/denen der Inhalt gespeichert wird. Der CISP verschiebt oder repliziert Inhalte von **<ORGANISATION>** nicht außerhalb der ausgewählten Region(en), es sei denn, dies ist gesetzlich erforderlich und nötig, um die CISP-Dienste aufrechtzuerhalten und sie **<ORGANISATION>** und dessen Endbenutzern bereitzustellen.*

- *<ORGANISATION> legt fest, wie der Inhalt geschützt wird. Der CISP muss während der Übertragung und im Ruhezustand eine starke Verschlüsselung für Inhalte von <ORGANISATION> bereitstellen und die Möglichkeit bieten, dass <ORGANISATION> seine eigenen Verschlüsselungsschlüssel verwalten kann.*

- *Der CISP muss über ein Programm für die Gewährleistung der Sicherheit verfügen, das globale Best Practices zum Datenschutz und zur Datensicherheit verwendet. So wird <ORGANISATION> dabei unterstützt, die CISP-Umgebung für die Sicherheitskontrolle einzurichten, zu betreiben und nach den besten Möglichkeiten zu nutzen. Die Prozesse zur Gewährleistung und Kontrolle der Sicherheit müssen mehreren unabhängigen Prüfungen durch Dritte unterzogen werden.*

Anhand von Zertifizierungen und Auswertungen zur Cloud-Akkreditierung können Organisationen des öffentlichen Sektors sicher sein, dass die CISPs effektive physische und logische Sicherheitskontrollen einsetzen. Durch Nutzung dieser Akkreditierungen in Ausschreibungen werden der Beschaffungsprozess rationalisiert und doppelte, übermäßig aufwendige Prozesse oder Workflows für die Genehmigung vermieden, die für eine Cloud-Umgebung möglicherweise nicht erforderlich sind.

Cloud-Ausschreibungen sollten CISPs die Möglichkeit bieten, unter Beweis zu stellen, dass sie an Compliance-Akkreditierungen und -Bewertungen ausgerichtet sind. Wie bereits erwähnt, gibt es bei diesen Akkreditierungsschemata erhebliche Überschneidungen hinsichtlich Risikoszenarien und Verfahren für das Risikomanagement. Da die Kontrollen und Anforderungen in solchen Akkreditierungen gebündelt werden, ist es einfacher, in einer Ausschreibung solche Akkreditierungen als Bedingung für die Berücksichtigung eines CISP anzugeben, anstatt den bereits geleisteten Aufwand zu duplizieren und selbst individuelle Kontrollen aufzulisten. (Häufig werden diese dann von früheren Ausschreibungen übernommen, die sich noch auf lokale Rechenzentren beziehen und daher ohnehin nicht für Cloud-Umgebungen relevant sein müssen.)

HINWEIS: Es ist auch sehr wichtig zu verstehen, wie auf die unten aufgeführten Berichte zugegriffen werden kann. SOC 1- und SOC 2-Berichte sind in der Regel vertrauliche Dokumente. Beachten Sie die Vereinbarungen, die für den Zugriff auf diese erforderlich sind – z. B. eine Geheimhaltungsvereinbarung (NDA, non-disclosure agreement) – und bitten Sie nicht einfach darum, dass diese Dokumente im Rahmen des Angebots eingereicht werden. (Diese Dokumente könnten durch Open Records Acts oder eine ähnliche Gesetzgebung veröffentlicht werden, was die Cloud-Sicherheit gefährden würde.)

Beispielformulierungen für die Ausschreibung: Compliance

Die Verwendung anerkannter Sicherheits-, Compliance- und Betriebsstandards, die auf Best Practices für Cloud-Service-Abläufe beruhen – einschließlich Datenverarbeitung, Datensicherheit, Vertraulichkeit, Verfügbarkeit usw. – rationalisiert die Auftragsvergabe für Cloud-Technologie.

<ORGANISATION> bewertet individuelle Angebote anhand der akzeptierten Sicherheits-, Compliance- und Betriebsstandards, wie unten und in Anhang A beschrieben. Indem sich <ORGANISATION> bei der Bewertung des Angebots auf die Compliance-Zertifizierung für jeden Standard stützt, kann die minimale Compliance für den Standard als Grundlage für die Bewertung des Angebots verwendet werden.

Wenn der CISP die Einhaltung des Mindeststandards über die gesamte Vertragsdauer hinweg aufrechterhalten muss, hat dies den Vorteil, dass die Service-Compliance auf dem aktuellen Stand gehalten wird.

*Der CISP, der (direkt oder über einen Vertriebspartner) angeboten wird, sollte in der Lage sein, die folgenden unabhängigen Bescheinigungen, Berichte und Zertifizierungen von Dritten vorzuweisen (Hinweis: Wenn einige dieser Bescheinigungen, Berichte und Zertifizierungen aufgrund von Sicherheitsbeschränkungen nicht ohne weiteres offengelegt werden können, sucht **<ORGANISATION>** mit dem CISP zusammen nach einer Möglichkeit, einen gemeinsam vereinbarten Zugang zu erhalten):*

Zertifizierungen/Bescheinigungen	*Gesetze, Vorschriften und Datenschutz*	*Ausrichtungen/Rahmenbedingungen*
☐ *C5 (Deutschland)*		☐ *CDSA*
☐ *CISPE-Verhaltenskodex zum Datenschutz (DSGVO)*		
☐ *CNDCP (Climate Neutral Data Centre Pact)*		
☐ *DIACAP*	☐ *EU-Datenschutzrichtlinie*	☐ *CIS*
☐ *DoD SRG Level 2 und 4*	☐ *EU-Modellklauseln*	☐ *Informationen zur Strafgerichtsbarkeit. Service (CJIS)*
☐ *HDS (Frankreich, Gesundheitswesen)*		
☐ *FedRAMP*	☐ *FERPA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *DSGVO*	☐ *EU-US-Datenschutzschild*
☐ *ISO 9001*	☐ *GLBA*	☐ *EU „Safe Harbor“*
☐ *ISO 27001*	☐ *HIPAA*	☐ *FISC*
☐ *ISO 27017*	☐ *HITECH*	☐ *FISMA*
☐ *ISO 27018*	☐ *IRS 1075*	☐ *G-Cloud [UK]*
☐ *IRAP [Australien]*	☐ *ITAR*	☐ *GxP (FDA CFR 21 Teil 11)*
☐ *MTCS Tier 3 [Singapur]*	☐ *PDPA – 2010 [Malaysia]*	☐ *ICREA*
☐ *PCI DSS Stufe 1*	☐ *PDPA – 2012 [Singapur]*	☐ *IT-Grundschutz [Deutschland]*
☐ *SEC Rule 17-a-4(f)*	☐ *PIPEDA [Kanada]*	☐ *MARS – E*
☐ *SecNumCloud (Frankreich)*		
☐ *SOC1/ISAE 3402*	☐ *Privacy Act [Australien]*	☐ *MITA 3.0*
☐ *SOC2/SOC3*	☐ *Privacy Act [Neuseeland]*	☐ *MPAA*
☐ *SWIPO IaaS Code*		
	☐ *Spanische DPA-Autorisierung*	☐ *NIST*
	☐ *U.K. DPA – 1988*	☐ *Uptime Institute Tiers*
	☐ *VPAT/Abschnitt 508*	☐ *UK-Cloud-Sicherheitsrichtlinien*

Die obige Liste dient nur zur Veranschaulichung und soll nicht als erschöpfend für die Zertifizierungen und Standards angesehen werden, die für Cloud-Services gelten können.

2.3.1.1 Datenschutz

Essenziell beim Einsatz von Cloud-Services ist die Einhaltung des EU-Datenschutzgesetzes bei der Verarbeitung personenbezogener Daten. Dazu gehört auch die Datenschutz-Grundverordnung (DSGVO). Die DSGVO ist eine auf Grundsätzen aufbauende Richtlinie und bietet daher keine branchenspezifische Anleitung zur Sicherstellung der Compliance. Allerdings unterstützt die DSGVO den Einsatz von Compliance-Tools wie Verhaltenskodizes, die eine solche Anleitung bieten können. Zusammen mit der französischen Datenschutzkommission CNIL entwickelte CISPE einen Verhaltenskodex zum Datenschutz (CISPE-Kodex[6]), der vom Europäischen Datenschutzausschuss unterstützt und in Europa allgemein angewandt wird. Dieser Kodex soll CISPs bei der Einhaltung der DSGVO unterstützen und Kunden helfen zu bestimmen, ob sich CISPs für die gewünschte Form der Verarbeitung personenbezogener Daten eignen.

- Der Kodex beschränkt sich ausschließlich auf den IaaS-Sektor und behandelt die spezifischen Rollen und Aufgabenbereiche von IaaS-Anbietern.
- Er erläutert die Aspekte fairer und transparenter Verarbeitung und angemessener Sicherheitsmaßnahmen im Kontext von Cloud-Infrastrukturservices (DSGVO, Artikel 40 [2]).
- Der Kodex erklärt Kunden, wie sie die Datenhoheit behalten können, indem sichergestellt wird, dass diese innerhalb der EU bleiben.
- Er wirbt für Best Practices beim Datenschutz, welche die GAIA-X-Initiative der EU zur Entwicklung europäischer Cloud-Datenservices unterstützen.

Durch Compliance von CISPs mit Datenschutzverhaltenskodizes wie dem CISPE-Kodex wird gewährleistet, dass die Verarbeitung personenbezogener Daten in strikter Einhaltung der DSGVO geschieht.

Beispielformulierungen für die Ausschreibung: Datenschutz

Der CISP, der (direkt ober über einen Vertriebspartner) angeboten wird, sollte seine Fähigkeit unter Beweis stellen können, einen Verhaltenskodex zum Datenschutz einzuhalten, wie den CISPE-Kodex. Der Datenschutzkodex muss die im DSGVO-Rahmen dargelegten Anforderungen erfüllen. Der Kodex sollte mindestens Folgendes umfassen: (1) eine klare Definition der Rollen und Verantwortlichkeiten des CISP, (2) die Anforderung, dass der CISP Kundendaten nicht für Marketing- oder Werbezwecke einsetzt und (3) die Möglichkeit für den Kunden, CISP-Services zu wählen, durch die Daten ausschließlich im europäischen Wirtschaftsraum verarbeitet werden. Die Compliance mit dem Kodex muss durch externe unabhängige Prüfer (Überwachungsstellen) anerkannt werden, die von unabhängigen externen Prüfern der europäischen Datenschutzbehörde akkreditiert wurden.

2.3.1.2 Wechsel des Cloud-Anbieters und Data Porting

Kunden sollten frei wählen können, welche Cloud-Services sie nutzen möchten, und nicht an einen CISP oder PaaS-/SaaS-Anbieter gebunden sein („lock-in“).

[6] https://cispe.cloud/code-of-conduct/

Von CISPs bereitgestellte Cloud-Services sind standardisiert und werden auf einer „One-to-Many"-Basis angeboten, wobei der Kunde die Services konfiguriert, bereitstellt und kontrolliert. Ein Vorteil von Cloud Computing ist, dass sich Kunden die passenden standardisierten Services aussuchen können, die sie brauchen, um ihre individuellen Anwendungen und Lösungen zu entwickeln. Zu diesem Vorteil gehört auch die Möglichkeit des Wechsels zu neuen oder anderen Services, die zu unterschiedlichen Zeitpunkten die Kundenanforderungen am besten erfüllen.

Wie beim Datenschutz können Verhaltenskodizes Kunden Gewissheit und Zuversicht geben, wenn es um den Wechsel von lokaler Infrastruktur zur Cloud oder den Wechsel zwischen CISPs geht. Gemeinsam mit EuroCIO (Europäischer Verband von CIOs) war CISPE federführend bei der Entwicklung des Verhaltenskodex für Data Porting und den Wechsel von Cloud-Services für IaaS-Cloud-Services (SWIPO IaaS Code[7,8]). Die erste Version des Kodex entstand gemäß der EU-Richtlinie zum freien Datenfluss, wurde der Europäischen Kommission im November 2019 unter der finnischen EU-Präsidentschaft überreicht und vom Verband SWIPO AISBL im Mai 2020 veröffentlicht. Im April 2021 wurde den ersten Services durch SWIPO AISBL die Erfüllung des Kodex bescheinigt und im Mai 2021 wurden die ersten Services der CISPE-Mitglieder als Kodex-konform befunden.

Beispielformulierungen für die Ausschreibung: Wechsel zwischen Cloud-Anbietern und Data Porting

Der CISP, der (direkt ober über einen Vertriebspartner) angeboten wird, sollte seine Fähigkeit unter Beweis stellen können, einen Verhaltenskodex zum „Wechsel und Data Porting" einzuhalten, wie den SWIPO IaaS Code. Der Kodex muss detailliert beschreiben, wie ein CISP Kunden den sicheren Transfer von Geschäftsdaten bietet, sollte sich der Kunde zum Wechsel zu einem anderen CISP entschließen.

2.3.2 Vergleich zwischen Anbietern

Wie bei den technischen Kriterien in den obigen Abschnitten ist es wichtig, in einer Cloud-Services-Ausschreibung neben den Mindestanforderungen an die Sicherheit Kriterien anzugeben, anhand derer die CISP-Sicherheitsfunktionen und -Services im Rahmen einer kompetitiven Auswertung verglichen werden können.

Beispiele für CISP-Sicherheitsanforderungen finden Sie unter *Anhang A – Technische Anforderungen für den Vergleich zwischen* Bietern. Wir empfehlen dringend, die folgenden Funktionalitäten als zentrale Sicherheitsüberlegungen für Organisationen des öffentlichen Sektors in die Bewertung von CISPs einfließen zu lassen:

Beispielformulierungen für die Ausschreibung: Zentrale Sicherheitsüberlegungen

- *Korrektes Verständnis des CISP vom Modell der geteilten Verantwortung und eine Dokumentation, die es Kunden erleichtert, sich einen Begriff von der Verteilung der Sicherheitsverantwortlichkeiten bei CISP-Funktionen und -Diensten zu machen (z. B. im Kontext der DSGVO)*
- *Nachgewiesene Erfolgsbilanz der Sicherheit der CISP-Infrastruktur mit öffentlich verfügbarer, nicht-proprietärer Dokumentation des CISP-Sicherheitsstatus und physischen/logischen Kontrollmechanismen*
- *CISP-Support speziell für die Cloud-Sicherheit*

[7] https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security
[8] https://swipo.eu/

- *Services, die es den Kunden ermöglichen, das Kontodesign zu formalisieren, die Kontrollen der Sicherheits- und Cloud-Governance zu automatisieren und das Auditing zu optimieren*
- *Möglichkeit, eine Sammlung von Ressourcen als Vorlagen zu erstellen, bereitzustellen und zu verwalten (einschließlich von CISP/CISP-Partnern erstellte hochwertige Standardsicherheitsvorlagen)*
- *Möglichkeit, einen verlässlichen, wiederholbaren Einsatz der Kontrollen zu etablieren*
- *Funktionen für ein kontinuierliches Auditing in Echtzeit*
- *Fähigkeit zur technischen Skripterstellung der Richtlinien zur Cloud-Governance*
- *Fähigkeit zum Erstellen von erzwingenden Funktionen, die von Nutzern ohne entsprechende Änderungsberechtigung nicht überschrieben werden können*
- *Möglichkeit, eine zuverlässige Implementierung von in der Vergangenheit festgeschriebenen Richtlinien, Standards und Regulierungen umzusetzen und gleichzeitig eine durchsetzbare Sicherheit und Compliance zu erzielen, die wiederum ein funktional zuverlässiges Cloud-Governance-Modell für IT-Umgebungen erzeugt*
- *Services zum Schutz vor gängigen, am häufigsten vorkommenden DDoS-Angriffen (Distributed Denial of Service) auf Netzwerk- und Transportebene sowie die Möglichkeit, benutzerdefinierte Regeln zu schreiben, um komplexe Angriffe auf Anwendungsebene zu mindern*
- *Services für die verwaltete Bedrohungserkennung*

2.3.3 Vertragsabschluss

Wie bereits erwähnt, sind CISP-Geschäftsbedingungen so konzipiert, dass sie die Funktionsweise eines Cloud-Servicemodells widerspiegeln (physische Ressourcen werden nicht erworben und CISPs wirtschaften in großem Umfang mit standardisierten Services). Daher ist es wichtig, dass die Geschäftsbedingungen eines CISP im größtmöglichen Umfang integriert und genutzt werden. Im folgenden Abschnitt ***2.5*** finden Sie weitere Informationen zu den Geschäftsbedingungen und zum Vertragsabschluss.

Wenn es um die Sicherheit geht, empfehlen wir erneut nachdrücklich, dass CISPs die Möglichkeit haben sollten, ihre Angebote ständig zu aktualisieren oder dass Anbieter nach Ablauf der Einreichfrist Produkte hinzufügen dürfen, solange sie den ursprünglichen Parametern der Ausschreibung entsprechen. Das liegt daran, dass sich Sicherheitsfunktionen und -services schnell entwickeln und CISPs häufig sicherheitsbezogene Services veröffentlichen, die in vielen Fällen kostenlos genutzt werden können. Beachten Sie, dass es wichtig ist, über eine minimale Sicherheitsstufe zu verfügen (siehe die Mindestanforderungen oben), um sicherzustellen, dass Änderungen an Sicherheitsangeboten nicht nachteilig sind.

Das Modell der geteilten Verantwortung ist natürlich das Herzstück des Aspekts der Sicherheit in einer Cloud-Services-Ausschreibung. Jede Partei muss sich über ihre Sicherheitsverantwortlichkeiten im Klaren sein und CISPs müssen die jeweiligen Sicherheitsverantwortlichkeiten des CISP/Kunden für vom CISP bereitgestellte Cloud-Technologien dokumentieren. Weiterhin ist erforderlich, dass sie eine Dokumentation zur Unterstützung der Kunden beim Aufbau und bei der Automatisierung von Best Practices für die Sicherheit bereitstellen.

Eine Cloud-Rahmenvereinbarung sollte die Flexibilität bieten, einen Anbieter zu entfernen, wenn er die Mindestanforderungen an Sicherheit und Compliance nicht mehr erfüllt, wie sie in der Ausschreibung für Cloud-Services dargelegt wurden.

2.4 Preise

Um bei der Vereinbarung über Cloud-Technologie eine schwankende Nachfrage zu berücksichtigen, benötigen Organisationen des öffentlichen Sektors einen Vertrag, mit dem sie Services abhängig von der tatsächlichen Nutzung bezahlen können – mit der erforderlichen Cloud-Governance und -Transparenz hinsichtlich Nutzung und Ausgaben.

Wichtig ist dabei, dass die Cloud-Services-Ausschreibungen den Wert und die Gesamtbetriebskosten (TCO, total cost of ownership) betrachten sollten, im Gegensatz zum simplen Vergleich der Preise pro Einheit. Diese traditionelle Vorgehensweise, bei der nach dem günstigsten Preis pro Einheit gesucht wird, ist nicht auf das Cloud-Modell übertragbar und führt daher nicht zum wirtschaftlich günstigsten Angebot oder dem insgesamt niedrigsten Preis.

*Bei der CISP-Preisbewertung hilft es, zunächst eine CISP-Vorqualifikation oder -Shortlist mit **minimalen Preisanforderungen** zu erstellen, damit CISPs mit vergleichbaren Funktionalitäten für die Rahmenvereinbarung infrage kommen. Beim Evaluierungsprozess für Abrufe und Mini-Wettbewerbe kann dann eine Auswahl an typischen Cloud-Beispielarchitekturen und **Preisszenarien** verwendet werden, die einigen typischen Workloads des öffentlichen Sektors entsprechen und von den CISPs bepreist werden müssen. Live-Testdemos werden ebenfalls empfohlen, um einen Vergleich der Leistung und Elastizität der von CISPs bereitgestellten Cloud-Technologieservices zu ermöglichen. In Anhang B finden Sie ein beispielhaftes Testskript für Cloud-Technologien.*

2.4.1 Mindestvoraussetzungen

Der Abschnitt „Preise“ einer Cloud-Services-Ausschreibung umfasst vier Hauptelemente:

1. **Nutzungsbasierte Preisgestaltung:** Cloud-Kunden verwenden ein nutzungsabhängiges Zahlungsmodell, bei dem sie einfach am Ende jedes Monats für die genutzten Services zahlen – optimal für Nutzungs- und Ressourcenmetriken.
2. **Transparente Preisgestaltung:** CISP-Preise sollten öffentlich verfügbar und transparent sein.
3. **Dynamische Preisgestaltung:** Modelle sollten Flexibilität bieten, durch die die Preise der Cloud je nach Marktpreis variiert werden können. Dieser Ansatz nutzt die dynamische und wettbewerbsorientierte Preisentwicklung im Cloud-Bereich und unterstützt Innovation und Preissenkungen.
4. **Kontrolle über die Ausgaben:** Die CISPs sollten Berichts-, Überwachungs- und Prognosetools bereitstellen, die Kunden ermöglichen, (1) Nutzung und Ausgaben sowohl in zusammenfassender als auch detaillierter Weise zu überwachen, (2) Benachrichtigungen zu erhalten, wenn die Nutzung und Ausgaben definierte Schwellenwerte erreichen, und (3) die Nutzung und Ausgaben zu schätzen, um künftige Cloud-Budgets planen zu können.

Beispielformulierungen für die Ausschreibung: Preise

<ORGANISATION> erbittet, dass antwortende CISPs ihren Vorschlag zu Methode und Modell für die Preisgestaltung angeben, die sie für die Bereitstellung der einzelnen Services für Endbenutzer als kommerzielle Cloud-Funktion nutzen möchten.

Der CISP gibt Folgendes an:

- *Dokument zur Definition des Services oder Links zu Definitionen des Services*
- *Dokument mit den Geschäftsbedingungen*
- *Preisdokument (Links zu öffentlichen Preisen sind akzeptabel, wenn davon ausgegangen wird, dass eine vollständige Preisliste/ein Preisdokument auf Anfrage verfügbar ist.)*

Der Preis entspricht den Kosten für die am häufigsten verwendete Konfiguration des Services. CISPs sollten Optionen volumenbasierter Rabatte und Tools zur Preisberechnung anbieten, um den tatsächlichen Preis des gekauften Produkts und den Gesamtwert für den Käufer zu ermitteln (z. B. Services zur Optimierung und daraus resultierende Kostensenkungen).

Käufer im Kontext der Rahmenvereinbarung können mit Anbietern sprechen, um sie zu bitten, ihre Servicebeschreibung, Geschäftsbedingungen, Preise oder Dokumente/Modelle zur Servicedefinition zu erläutern. Alle Gespräche mit Anbietern werden aufgezeichnet.

Zusätzliche Preisanforderungen

- *Bereitstellung von Cloud-Technologien mit einem dynamischen Preismodell, das maximale geschäftliche Flexibilität bietet und Skalierbarkeit und Wachstum ermöglicht.*
- *Die Preisattribute müssen Folgendes umfassen:*
  - *Werden die Preise in Form eines bedarfsorientierten, nutzungsabhängigen „pay-as-you-go"-basierten Services bereitgestellt? Erläutern Sie Ihr Preismodell.*
  - *Können Sie weitere Rabatte anbieten, wenn Nutzung und/oder Kauf in großen Mengen erfolgen? Geben Sie Details dazu an.*
  - *Sind die Preise öffentlich verfügbar und transparent? Bitte fügen Sie Links zu öffentlich verfügbaren Preisen hinzu.*
  - *Ist die Preisgestaltung dynamisch und reagiert schnell und effizient auf den Wettbewerb am Markt?*
  - *Stellen Sie Best Practices und Ressourcen bereit, um Ausgaben zu verfolgen?*
  - *Stellen Sie Best Practices und Ressourcen für die Kostenoptimierung bereit?*

Preistransparenz

Aufgrund des ständigen Abwärtstrends bei den Preisen für kommerzielle Cloud-Technologien, der durch Innovation und Wettbewerb vorangetrieben wird, dürfen die von <ORGANISATION> unter der Rahmenvereinbarung gezahlten, gemessenen Einheitenkosten für den CISP-Service niemals die auf der Cloud-Anbieter-Website veröffentlichten Einheitenpreise überschreiten, die zum Zeitpunkt der Nutzung der Serviceeinheit durch den Kunden wirksam sind.

Budgetierung und Warnmeldungen/Berichte zur Abrechnung

Um die Bereitstellung und Nutzung von Cloud-Technologien nachzuweisen, sollten CISPs <ORGANISATION> die Tools zur Erstellung detaillierter Abrechnungsberichte bereitstellen, die die Kosten nach Stunde, Tag oder Monat, nach jedem Konto in einer Organisation, nach Produkt oder Produktressource oder nach benutzerdefinierten Kriterien aufschlüsseln. <ORGANISATION> ist sich bewusst, dass <ORGANISATION> im Rahmen des Cloud-Modells der geteilten Verantwortung für die Verwendung der Budgetierungs- und

Abrechnungsfunktionen und -tools verantwortlich ist, die von CISPs bereitgestellt werden, um die individuellen Anforderungen an Prognosen und Berichte zu erfüllen.

- *Geben Sie Informationen dazu an, wie **<ORGANISATION>** Abrechnungsinformationen sowohl auf detaillierter als auch auf zusammenfassender Ebene aufrufen und dabei die Ausgabenentwicklung für CISP-Ressourcen sowie die Prognose zukünftiger Ausgaben visualisieren kann.*
- *Geben Sie an, wie **<ORGANISATION>** die Nutzungs-/Abrechnungsansicht nach Service, nach verknüpftem Konto oder nach benutzerdefinierten Tags für Ressourcen filtern und Abrechnungs-Warnmeldungen erstellen kann, die Benachrichtigungen senden, wenn die Nutzung von Diensten die von **<ORGANISATION>** definierten Schwellenwerte/Budgets erreicht oder überschreitet.*
- *Geben Sie an, wie **<ORGANISATION>** auf der Grundlage der bisherigen Nutzung prognostizieren kann, wie intensiv Cloud-Services über einen definierten Prognosezeitraum voraussichtlich genutzt werden. Der CISP sollte eine **Schätzung** darüber vorlegen, wich hoch die CISP-Rechnung von **<ORGANISATION>** sein wird und es **<ORGANISATION>** ermöglichen, Alarme und Budgets für die voraussichtlich aufzuwendenden Beträge einzusetzen, um eine bessere Governance über Kosten und Ausgaben zu erreichen.*

2.4.2 Vergleich zwischen Anbietern

Organisationen des öffentlichen Sektors verlangen oft einen Wettbewerb zwischen Bietern, bei dem Bewertungskriterien wie der beste Wert, das wirtschaftlich günstigste Angebot (MEAT) oder der niedrigste Preis angelegt werden. Es ist wichtig, dass der Ansatz, den man bei der Planung für die Preisgestaltung von Abrufen oder Mini-Wettbewerben innerhalb der Rahmenvereinbarung entwickelt, die einzigartigen Merkmale der Cloud berücksichtigt. Beachten Sie beispielsweise, dass der einfache Vergleich von Einzelposten zwischen den Angeboten von Cloud-Anbietern (z. B. Datenverarbeitung oder Speicher) keine effektive Vergleichsgröße darstellt, da er nicht Funktionen wie Leistung, Kostenoptimierung mithilfe von cloudnativen Services und CISP-Überwachungstools berücksichtigt oder Services mit einbezieht, die CISPs evtl. kostenlos anbieten. Darüber hinaus kann der Katalogpreis eines CISP Zehntausende von Einzelposten umfassen. Die Preismodelle unterscheiden sich dabei von einem Service und von einem Anbieter zum anderen.

Analyse der TCO

Wir empfehlen Ihnen, sich auf die Gesamtbetriebskosten (TCO) definierter Anwendungsbeispiele zu konzentrieren, die alle Aspekte einer Cloud-Lösung berücksichtigen (einschließlich Partnerservices, standardisierter CISP-Rabatte, technischer Funktionen, die die Leistung steigern können, Kosten senken/optimieren usw.).

Vergleich anhand von Szenarien

Der Bewertungsprozess kann auch typische Szenarien berücksichtigen, die auf den häufigsten Systemen oder Anwendungen basieren. Solche Szenarien (z. B. Webhosting oder die Implementierung eines Personalsystems mit einer Anzahl von x Benutzern) können Variablen wie die Geschwindigkeit und das Ausmaß von Ressourcen, die Leistung der Anwendung oder Lösung, Speicherzugriffszeiten, komplexe Daten mit geringem Volumen im Vergleich zu einfachen Rechenaufgaben mit hohem Volumen usw. beinhalten. Andere typische Szenarien für die Anwendungen oder Systeme können Dinge wie die Verarbeitung großer Datenvolumen bei Steuererklärungen oder Notfallbenachrichtigungen wie Hochwasserwarnungen sein. Die Szenarien sollten umfassend sein, um den gesamten Umfang der Technologien und Services abzudecken, die der Kunde während des Projekts brauchen könnte. Auf diese Weise kann der Kunde die geschätzten Gesamtkosten des Projekts vergleichen.

Szenarien finanziell und technisch vergleichen

Beim Vergleich der Preise verschiedener CISP-Angebote ist es auch wichtig, die technischen Vorteile zu berücksichtigen. Beispielsweise kann ein bestimmter CISP es Kunden ermöglichen, eine Aktiv-Aktiv-Topologie zur Notfallwiederherstellung (DR, Disaster Recovery) zu erstellen, da sich seine Rechenzentren in Clustern innerhalb einer geografischen Region befinden. Ein CISP, der nicht über diese Art von Redundanz und Rechenzentrumskonfiguration verfügt, könnte aufgrund der zusätzlichen Kosten für die DR-Anforderungen um x % teurer sein. Ein Beispiel dafür, warum eine ganzheitliche Preisgestaltung, die weitere technische Merkmale berücksichtigt, für die Bewertung von CISPs entscheidend ist, lässt sich durch die folgende Alternative zu einem direkten Vergleich einzelner Komponenten illustrieren.

Beispiel: Ein Kunde möchte den Preis von Objektspeichern, die von qualifizierten CISPs in einer Rahmenvereinbarung bereitgestellt werden, vergleichen. Der Preis für den Artikel „Speichereinheit" von CISP 1 beträgt 0,023 € pro GB. Der Preis für dieselbe „Einheit" bei CISP 2 beträgt 0,01 € pro GB. Bei einem einfachen Vergleich der Einheiten stellt der Kunde keine wichtigen Fragen wie:

1. Wie viele redundanten Kopien des Objekts stehen bei einem Ausfall zur Verfügung? Im obigen Beispiel ist CISP 1 so konzipiert, dass der gleichzeitige Datenverlust in zwei verschiedenen Einrichtungen verkraftet wird und mehrere Kopien der Daten aufbewahrt werden. Bei CISP 2 werden keine redundanten Kopien erstellt.
2. Wie hoch ist der Grad der Dauerhaftigkeit gespeicherter Objekte? CISP 1 liegt bei 99,999999999 %, CISP 2 bei 99 %.
3. Berücksichtigen Sie die Kosten über die gesamte Lebensdauer des Projekts oder der Workload und wie Funktionen zur Kostenoptimierung die Ausgaben für die Speicherung und Verwendung von Daten senken können (z. B. kann die gesteigerte Verwendung von Serverless-Funktionen eines CISP die Kosten um x % senken).

Dies sind nur einige unter vielen anderen technischen Aspekten, die in die Preisgestaltung einfließen, insbesondere im Hinblick auf Sicherheit und Compliance.

Überlegungen für Preisszenarien

Basispreise: Dies sind im Wesentlichen öffentliche Preise von CISPs. CISPs sollten diese Preise öffentlich angeben. Wie oben angegeben, können Kunden jedoch, um CISPs effektiv zu vergleichen, verlangen, dass alle Anbieter etwa 3 bis 5 spezifische Szenarien (oder eine andere Anzahl, die für den Kunden sinnvoll ist) bepreisen. Die Szenarien sollten umfassend sein und die ganze Bandbreite an Services und Technologien umfassen, die der Kunde im Laufe des Projekts wahrscheinlich nutzen wird. Auf diese Weise kann der Kunde die geschätzten Gesamtkosten des Projekts vergleichen. Vergleiche auf Einzelposten-/SKU-Ebene sind für Kunden und Anbieter eher problematisch als hilfreich (Die Kunden müssten Zehntausende von Einzelposten über alle CISPs hinweg vergleichen und die Anbieter müssten diesen Grad an Details bereitstellen und verwalten, obwohl der Preis später nur anhand der Servicenutzung bestimmt wird.)

Die Bewertung der übergreifenden Funktionalitäten eines CISP ist ein Muss für Cloud-Kunden, die den besten Wert erhalten möchten. CISPs können beispielsweise eine Reihe von Services anbieten, die entweder kostenlos oder so gut wie kostenlos sind. Eine Preisbewertung sollte diese Services ebenso berücksichtigen wie die Tatsache, dass andere CISPs unter Umständen ähnliche Funktionen in Rechnung stellen.

Bewertungskriterien können so geschrieben werden, dass die CISPs ihre standardmäßig enthaltenen Funktionen angeben können und wie sich diese Services auf die Gesamtkosten auswirken. Die Bewertungskriterien können auch volumenbasierte/gestaffelte Preise von CISPs sowie kommerziell verfügbare Rabatte wie Reserved Instances bzw. Spot-Instances berücksichtigen. Beispiel:

- Einsparungen von x %, wenn Kunden reservierte Rechenkapazität kaufen (1 Jahr, 3 Jahre usw.)
- x % Rabatt auf gestaffelte Preise/Volumenrabatte
- Einsparungen von x % basierend auf Architekturprüfungen und der Optimierung der Infrastruktur, z. B. dem Wechsel auf eine passendere Option für Datenverarbeitung.
- Berücksichtigen Sie, wie oben erwähnt, die Kosten für die gesamte Lebensdauer und wie Sie mit Funktionen zur Kostenoptimierung Ausgaben senken können.

PREISSZENARIO
Die Bieter müssen die Preise für das folgende Szenario nur zu Bewertungszwecken angeben. Der tatsächliche Preis basiert auf der tatsächlichen Nutzung von Services in einem nutzungsabhängigen On-Demand-Modell.

Im Folgenden finden Sie repräsentative Anforderungen zum Zwecke der Preisfindung. Sie sind ausdrücklich so zu verstehen, dass sich diese nominalen Anforderungen während der Vertragslaufzeit ändern werden. Bitte geben Sie die Preise für 12 und 36 Monate On-Demand- sowie für 12 und 36 Monate reservierte Kapazität an.

Geben Sie Folgendes an:

- *Name der vorgeschlagenen Lösung(en):*
- *Bestpreisgestaltung des Bieters:*

- *Servicezeiten: täglich rund um die Uhr*
- *Serviceverfügbarkeit: 99,95 %*

Preisszenarien können auch Beispiele von bestehenden Kunden mit ähnlichen Workloads enthalten, die ihre Ausgaben über 1/2/3 Jahre optimiert haben – durch die Verwendung von CISP-Überwachungs- und Optimierungstools, die Einführung von optimierten cloudnativen Lösungen und CISP-Preissenkungen.

2.5 Vertragsabwicklung/Geschäftsbedingungen

Von CISP bereitgestellte Cloud-Technologien und -Prozesse sind bewusst standardisiert, daher sind auch die Vertragsbedingungen standardisiert. Es besteht jedoch die Möglichkeit, diese Verträge geringfügig anzupassen, um sich an die lokalen gesetzlichen und behördlichen Gegebenheiten anzupassen.

Häufig enthalten herkömmliche IT-Beschaffungsmethoden strenge Regeln, die von den Antragstellern verlangen, viele oder alle angegebenen Anforderungen zu erfüllen, um nicht

abgelehnt zu werden. Oder sie enthalten womöglich eine bestimmte Teilmenge strikter, zwingender Voraussetzungen. Wird diese Vorgehensweise auf Cloud-Technologien übertragen, bei denen es sich im Grunde um eine Reihe standardisierter Komponenten und Tools handelt, die Sie bei der Entwicklung einer kundenspezifischen Lösung unterstützen, schlagen Beschaffungen häufig fehl.

2.5.1 Geschäftsbedingungen

Der erste Schritt bei der Vertragsvergabe bei einer Cloud-Services-Ausschreibung besteht darin, die bestehenden kommerziellen CISP-Geschäftsbedingungen zu prüfen und zu verstehen. In vielen Fällen sind diese öffentlich auf den CISP-Websites zu finden. Organisationen des öffentlichen Sektors sind mehr und mehr dazu übergangen, die Geschäftsbedingungen von CISPs ohne Vorbehalte zu akzeptieren. Ein Teil des Bestrebens, die Geschäftsbedingungen richtig einzuordnen, besteht darin, sich mit CISPs und ihren Partnern zu treffen, um sich eingehend mit ihren Ansätzen vertraut zu machen. Die wichtigste Frage ist, „warum" CISPs mit bestimmten Bedingungen arbeiten. Einige dieser Begriffe scheinen sich von den herkömmlichen IT-Bedingungen zu unterscheiden, aber es gibt sehr spezifische Gründe, „warum" sie Teil eines Cloud-Vertrags sind. Wenn die öffentlich zugänglichen Bedingungen nicht akzeptabel sind, halten CISPs häufig leicht veränderbare Vereinbarungen für Unternehmenskunden bereit, die in Betracht gezogen werden können.

Neben der Prüfung der Geschäftsbedingungen des CISP ist es wichtig, die bestehenden Richtlinien, Vorschriften und/oder Gesetze (z. B. solche bezüglich Technologien, Datenklassifizierung, Datenschutz, Mitarbeiter usw.) zu verstehen. Häufig existieren Richtlinien/Vorschriften/Gesetze, die für den Kauf und die Nutzung herkömmlicher IT-Angebote entwickelt wurden. Diese können zu dem CISP-Modell im Widerspruch stehen. Es kann zum Beispiel sein, dass nur die Nutzung von Cloud-Technologien zugelassen ist, die bereits im ursprünglichen Angebot für eine Rahmenvereinbarung (Antwort auf die Cloud-Services-Ausschreibung) enthalten waren. Die CISPs fügen jedoch ständig neue Services und Funktionen hinzu. Werden die IT-Produkte auf die herkömmliche Art aktualisiert, wird der Zugriff auf diese neuen Services erschwert, was für den Endkunden nicht sinnvoll ist. Sollte dies der Fall sein, ist es wichtig, mit CISPs eingehende Gespräche darüber zu führen, wie mit diesen Richtlinien/Vorschriften und/oder Gesetzen umgegangen werden kann.

Nutzen Sie die Vorteile von Gesprächen vor der Ausschreibung

Nehmen Sie sich vor dem Entwurf einer Ausschreibung die Zeit, sich mit CISPs und zugehörigen Anbietern zu treffen, um deren Geschäftsbedingungen zu verstehen und sie über den Ansatz, die Richtlinien, Vorschriften und Gesetze Ihrer Organisation zu informieren. Der wichtigste Teil dieser Gespräche besteht darin, dass beide Seiten verstehen, „warum" die relevanten Bedingungen zu ihrer Anwendung kommen. Die Geschäftsbedingungen für die Cloud unterscheiden sich beispielsweise von den Bedingungen für herkömmliche Rechenzentren, Managed Services, Hardware, physisch verpackte Software und Systemintegration. Da es sich um Einzelmodelle handelt, die ständige Innovation bedingen, funktionieren die zugehörigen Geschäftsmodelle nur, wenn im Rahmen eines flexiblen Ausschreibungsprozesses Verhandlungen oder klärende Gespräche möglich sind.

Durch die Möglichkeit, die allgemeinen Geschäftsbedingungen in Gesprächen oder Verhandlungen zu klären, gewinnen Organisationen des öffentlichen Sektors ein besseres Verständnis für die

Cloud-Modelle und vermeiden es, versehentlich geeignete Anbieter abzulehnen. Ein typischer Prozess besteht darin, dass die Organisation bestimmte Bedingungen im Voraus identifiziert, die sie vor der Vergabe besprechen und verhandeln möchte. Durch die Verhandlung akzeptabler Bedingungen mit dem/den Bieter(n) im Voraus stellt die Organisation sicher, dass sie den idealen Anbieter findet, und löst Konflikte, die andernfalls zu einer Ablehnung eines leistungsfähigen Angebots führen könnten. Organisationen des öffentlichen Sektors können auch ihre Richtlinien, Vorschriften und Gesetze prüfen und beide Seiten können verstehen, wie die Nutzung der Cloud in diese Modelle passt. Oft gibt es Möglichkeiten, mit den vorhandenen Klauseln zu arbeiten. Wenn es jedoch einen problematischen Bereich gibt, können beide Seiten zusammenarbeiten, um eine Lösung zu finden. (Es ist besser, diese Gespräche vor jeder Ausschreibung und der anschließenden Vertragsverhandlung zu führen.)

Flexibilität bei Verhandlungen

Damit die Verträge immer im Einklang mit der lokalen Gesetzgebung sind, sollte sich zwar grundsätzlich auf die standardisierten Vertragsbedingungen des CISP gestützt werden, jedoch ist es zusätzlich empfehlenswert, (1) von Bewerbern deren Standardvertrag anzufordern, (2) beim Erstellen der Rahmenvereinbarung für die Cloud-Services-Ausschreibung keine ungeeigneten Vertragsbedingungen durchzusetzen und (3) eine Verhandlungsoption für alle Bestimmungen der Beratung und Angebote zu bieten, die zu der Rahmenvereinbarung führen werden (mit Ausnahme der obligatorischen, gesetzlich vorgeschriebenen Klauseln).

Hinweis: Der Gültigkeitsbereich der geteilten Verantwortung ist fester Bestandteil des Cloud-Modells und sollte in den Vertragsbedingungen berücksichtigt werden (z. B. bestätigt der CISP, dass die Kunden Eigentümer ihrer Daten sind und wo sich diese befinden, und stellt Tools bereit, mit denen sichergestellt wird, dass die Auswahl der Datenstandorte begrenzt ist – **ABER**: Es liegt in der Verantwortung des Kunden oder Partners, diese Tools zu verwenden.)

*Beachten Sie, dass für jeden der Bereiche einer Cloud-Rahmenvereinbarung **unterschiedliche Vertragsbedingungen** gelten. Der Versuch, alle Bereiche mit einheitlichen Vertragsbedingungen abzudecken, führt zu Problemen in Bezug auf technische Machbarkeit und Kompatibilität.*

Wie bereits erwähnt, führen Ausschreibungen mit nicht verhandelbaren Bedingungen dazu, dass eigentlich geeignete Angebote abgelehnt werden können. Organisationen des öffentlichen Sektors sollten die Konsequenzen von nicht verhandelbaren Bedingungen sorgfältig prüfen, **es sei denn, es handelt sich um eine gesetzliche Anforderung**. Organisationen sollten sich immer darüber im Klaren sein, ob ihre nicht verhandelbaren Anforderungen oder Bedingungen wirklich notwendig sind, da sie damit ein mögliches Nachverhandeln im Vorhinein verhindern. Die Verwendung nicht verhandelbarer Anforderungen oder Bedingungen sollte auf ein absolutes Minimum beschränkt werden, um der Organisation die Flexibilität zu bieten, die für den Erwerb der besten Technologie und Lösung erforderlich ist.

Denken Sie daran, dass Cloud-Technologien von CISPs vollständig standardisiert und automatisiert bereitgestellt werden. Daher ist ein CISP nicht in der Lage, Änderungen an den Geschäftsbedingungen vorzunehmen, wenn dies eine Anpassung des zugrunde liegenden Dienstes erfordern würde. Darüber hinaus sind die Preise der Services in der Regel öffentlich und für alle

Benutzer standardisiert, was bedeutet, dass ein CISP die Preise nicht anpassen kann, um im Namen eines bestimmten Kunden ein höheres Risiko zu übernehmen.

Indirekte Käufe

Eine alternative Möglichkeit dazu, Cloud-Technologien direkt von einem CISP zu erwerben, besteht darin, sie stattdessen bei einem CISP-Vertriebspartner zu erwerben. Weitere Informationen zu CISP-Vertriebspartnern finden Sie weiter oben in Abschnitt ***2.1.3***.

Beispielformulierungen für die Ausschreibung: Geschäftsbedingungen

CISPs oder repräsentierende Anbieter müssen ihre öffentlich zugänglichen Geschäftsbedingungen bereitstellen und Feedback zu den wichtigsten Geschäftsbedingungen von ***<ORGANISATION>*** geben.

<ORGANISATION> beabsichtigt, einen schriftlichen Vertrag mit dem erfolgreichen Bieter auf der Grundlage der Vertragsbedingungen des Bieters abzuschließen. ***<ORGANISATION>*** *sollte die vorgeschlagenen Vertragsbedingungen durch den Bieter zur Prüfung erhalten, worin sich sein bestes kommerzielles und rechtliches Angebot widerspiegelt. Die Anbieter und <ORGANISATION> können beide Sätze von Bedingungen während der Phase <GESPRÄCH/VERHANDLUNG> besprechen.*

- *Allgemeine Bedingungen für die Rahmenvereinbarung bestehen höchstens aus den folgenden Komponenten:*
  - *Rahmenvereinbarung zur Dauer*
  - *Rahmenvereinbarung zur Governance*
  - *Rahmenvereinbarung zur Leistung*
  - *Rahmenvereinbarung zur Kündigung*
  - *Umfang der Rahmenvereinbarung*
  - *Bestellvorgang*
  - *Vertraulichkeitsbestimmungen*
  - *Kategoriespezifische IP und Informationen*
  - *Technische Mindestanforderungen, die von CISPs erfüllt werden müssen, z. B. Qualitätsstandards, Akkreditierung, Sicherheit und Datenschutz*
- *Für jeden Bereich der Rahmenvereinbarung bestehen unterschiedliche Bedingungen*
- *Besonderheiten des CISP-Services können berücksichtigt werden und werden beim Abruf behandelt.*
- *Lassen Sie Vertragsänderungen zu: Die Bedingungen dürfen Kunden und Anbieter nicht davon abhalten, sich auf Vertragsänderungen zu einigen, um neue Services oder Verbesserungen hinzuzufügen. Cloud-Services entwickeln sich ständig weiter, sodass Serviceverbesserungen kontinuierlich verfügbar werden, die den Kunden zu mehr Effizienz verhelfen können.*
- *Service Level Agreements (SLAs) sollten nicht vom Kunden festgelegt werden. Die Geschäftsbedingungen des Kunden sollten keine auftragsspezifischen, maßgeschneiderten SLAs definieren, die sich von den Standardmodellen für die Servicebereitstellung der CISPs unterscheiden. Werden die Standard-SLAs der CISPs akzeptiert, können die CISPs die Kosten niedrig halten und die Ersparnisse an die Kunden weitergeben, während diese sich darauf verlassen können, dass der CISP die SLA einhalten kann.*
- *Haftungsobergrenzen sollten verhältnismäßig sein. Die Haftung sollte im Verhältnis zu den erworbenen Leistungen stehen und es sollte keine unverhältnismäßig hohen Haftungsobergrenzen geben. Wenn die Obergrenzen unverhältnismäßig hoch sind, werden die CISPs davor zurückschrecken, Projekte mit niedrigem Wert anzunehmen. Diese Projekte sind oft ein nützliches Einführungs- und „Test"-Szenario für Kunden, um festzustellen, ob bestimmte Cloud-Lösungen für ihr Unternehmen effektiv sind.*
- *Kunden sollten Eigentümer ihrer eigenen Daten sein. Sie sollten ihre Daten kontrollieren und besitzen und in der Lage sein, den geografischen Standort zu bestimmen, an dem sie gespeichert sind. Dadurch können Kunden eine Anbieterbindung vermeiden und Daten frei an neue Anbieter übertragen.*

2.5.2 Software-Geschäftsbedingungen

Zwar konzentriert sich dieses Handbuch auf den Erwerb von IaaS- und PaaS-Cloud-Technologien von einem CISP. Es sollten jedoch auch Software-Geschäftsbedingungen hervorgehoben werden, die Organisationen des öffentlichen Sektors beim Kauf von Software von Anbietern in Betracht ziehen können. Siehe Abbildung 1 (Seite 5) für den Kauf von Software als Teil einer gut strukturierten Cloud-Services-Ausschreibung.

Software spielt eine entscheidende Rolle in fast jedem Unternehmen, auch im öffentlichen Sektor. Indem Verpflichtungen wie Software-Lizenzbedingungen in Ausschreibungen für Cloud-Services aufgenommen werden, wird dafür gesorgt, dass Organisationen des öffentlichen Sektors beim Kauf von Software den besten Wert erhalten und Anbieter frei wählen können.

Weitere Informationen finden Sie in den „10 Grundsätzen einer fairen Softwarelizenzierung für Cloud-Kunden“[9]. Die Prinzipien entstanden durch eine Kooperation von Cigref[10] – einem Verband führender französischer Unternehmen und Behörden, der Benutzer digitaler Technologien vertritt – und CISPE und die Unterstützung weiterer europäischer CIO- und Anbieterverbände. Sie sollten Praktiken thematisieren, die von beiden Verbänden als schädlich für die digitale Transformation von Organisationen aller Größen betrachtet werden, die zur Cloud wechseln.

Beispielformulierungen für die Ausschreibung: Software

<ORGANISATION> beabsichtigt, einen schriftlichen Vertrag mit dem erfolgreichen Bieter auf der Grundlage der Vertragsbedingungen des Bieters abzuschließen. ***<ORGANISATION>*** *sollte die vorgeschlagenen Vertragsbedingungen durch den Bieter zur Prüfung erhalten, worin sich sein bestes kommerzielles und rechtliches Angebot widerspiegelt. Die Softwareanbieter und <ORGANISATION> können beide Sätze von Bedingungen während der Phase <GESPRÄCH/VERHANDLUNG> besprechen.*

Anforderung 1.0. *Softwareanbieter müssen klare Lizenzbedingungen angeben, einschließlich einer Kostenaufschlüsselung auf zusammenfassender und detaillierter Ebene.*

Anforderung 1.1. *Sämtliche Kosten in Verbindung mit einer Nichteinhaltung der Lizenzbedingungen müssen auf zusammenfassender und detaillierter Ebene angegeben werden.*

Anforderung 2.0. *Softwarelizenzen müssen <Organisation> die Möglichkeit geben, die lizenzierte Software von einem lokalen Standort zu einer Cloud seiner Wahl zu migrieren, ohne den Kauf separater, doppelter Lizenzen für dieselbe Software zu erfordern.*

Anforderung 2.1. *Softwarelizenzen müssen frei von Lizenzeinschränkungen und gesteigerten Kosten sein, die die Fähigkeit von <Organisation> beeinträchtigen, die lizenzierte Software in der gewählten Cloud auszuführen.*

Anforderung 3.0. *Softwarelizenzen müssen es <Organisation> erlauben, die lizenzierte Software sowohl auf der eigenen Hardware (gemeinhin als „On-Premises-Software“ bezeichnet) als auch in der gewählten Cloud auszuführen.*

Anforderung 4.0. *Softwarelizenzen dürfen nicht verlangen, dass die lizenzierte Software ausschließlich auf <Organisation> vorbehaltener Hardware ausgeführt wird.*

[9] https://www.fairsoftware.cloud/de/10-grundsaetze/
[10] https://www.cigref.fr/

Anforderung 5.0. *Softwareanbieter dürfen keine Strafe gegen <Organisation> verhängen, falls die lizenzierte Software des Anbieters in der Cloud eines anderen Anbieters genutzt wird – beispielsweise wenn sie sich das Recht auf steigende oder aufdringliche Software-Audits vorbehalten oder höhere Software-Lizenzgebühren verhängen.*
Anforderung 6.0. *Verzeichnis-Software muss offene Standards für das Synchronisieren und Authentifizieren von Benutzeridentitäten mit anderen Identität-Services auf eine nicht-diskriminierende Weise unterstützen.*
Anforderung ***7.0.*** *Softwareanbieter dürfen keine unterschiedlichen Preise für dieselbe Software verlangen, wenn der einzige Unterschied darin liegt, wer der Besitzer der Hardware ist, auf dem sie installiert ist.* ***Anforderung 7.1.*** *Preise für Software dürfen keinen Unterschied machen zwischen Software, die im eigenen Rechenzentrum von <Organisation> installiert ist, in einem Rechenzentrum eines Drittanbieters, auf von einem Drittanbieter gemieteten Computern oder in der Cloud eines von <Organisation> gewählten Anbieters.*
Anforderung 8.0. *Während der Vertragslaufzeit dürfen Softwareanbieter keine wesentlichen Änderungen an den Linzenzbedingungen vornehmen, die <Organisation> in den zuvor gestatteten Nutzungen einschränken, sofern dies nicht gesetzlich oder aufgrund von Sicherheitsbedenken erforderlich ist.*
Anforderung 9.0. *Softwareanbieter dürfen <Organisation> nicht irreführen, indem sie erklären, dass Softwarelizenzen den von <Organisation> in den <Anforderungen der Organisation> beschriebenen Einsatz der Software decken, wenn hierfür der Kauf zusätzlicher Lizenzen erforderlich ist.*
Anforderung 10.0. *Sollte <Organisation> das Recht zum Weiterverkauf und zur Übertragung von Softwarelizenzen haben, müssen Softwareanbieter weiterhin unter fairen Bedingungen Support und Patches für <Organisation> bereitstellen, dessen weiterverkaufte Lizenz legal erworben wurde.*

2.5.3 So wählen Sie zwischen Teilnehmern pro Projekt aus

Einrichtungen des öffentlichen Sektors, die Teil der Rahmenvereinbarung sind, können die benötigten Services bei Bedarf bestellen oder „abrufen“. Ein Abrufvertrag im Rahmen einer Rahmenvereinbarung ermöglicht es Käufern, bei einem Abruf die Anforderungen mit zusätzlichen funktionalen Spezifikationen zu verfeinern, während die über die Rahmenvereinbarung angebotenen Vorteile erhalten bleiben.

Falls erforderlich, kann ein Mini-Wettbewerb abgehalten werden, um den besten Anbieter für eine bestimmte Workload oder ein bestimmtes Projekt zu ermitteln. Ein Mini-Wettbewerb bedeutet, dass ein Kunde im Kontext der Rahmenvereinbarung einen weiteren Wettbewerb ausruft, indem er alle Anbieter für einen Bereich dazu einlädt, auf eine Reihe von Anforderungen zu reagieren. Der Kunde lädt alle infrage kommenden Anbieter innerhalb des Bereichs ein, ein Angebot abzugeben. Daher ist es wichtig, bei einer Cloud-Services-Ausschreibung die Mindestanforderungen für die Teilnehmer zu definieren: So wird für jeden Bereich eine qualitativ hochwertige Auswahl an Optionen gewährleistet.

Bitte beachten Sie nochmals, dass für jede der Bereichskategorien von Angebotstypen (z. B. Public IaaS/PaaS, Community IaaS/PaaS, Private IaaS/PaaS) unterschiedliche Vertragsbedingungen gelten, da eine „Einheitslösung“ für jeden Bereich zu Problemen in Bezug auf technische Machbarkeit und Kompatibilität führt.

In Abschnitt ***2.1.4*** finden Sie Beispiele für die Formulierung von Ausschreibungen, wenn es um die Auswahl zwischen Teilnehmern geht.

2.5.4 On-Boarding und Off-Boarding

Bei der Erstellung einer Cloud-Rahmenvereinbarung sollte die Option eines dynamischen Einkaufssystems (Dynamic Purchasing System, DPS) in Erwägung gezogen werden. Bei einem DPS-Modell werden alle Anbieter, die die Mindestanforderungen für die Rahmenvereinbarung erfüllen, in die Rahmenvereinbarung aufgenommen. Es gibt keine feste Grenze von Anbietern, die der Rahmenvereinbarung beitreten können. Im Gegensatz zum herkömmlichen Modell einer Rahmenvereinbarung können Anbieter sich auch während der gesamten Lebensdauer für die „DPS-Rahmenvereinbarung" bewerben.

Wir empfehlen Einrichtungen des öffentlichen Sektors dringend, hohe Standards zu setzen, um die Qualität und Service-Gewährleistung von qualifizierten Anbietern sicherzustellen, aber nicht zu spezifisch zu sein und dadurch CISPs auf eine Weise zu disqualifizieren, die keinen fairen Wettbewerb garantiert. Das Ziel besteht letztendlich darin, den Endbenutzer nicht mit einer Vielzahl von Optionen zu überfordern und gleichzeitig den Standard der verfügbaren Cloud-Technologien hoch zu halten.

3.0 Best Practices/Erkenntnisse

Im Folgenden werden wir einige unserer gesammelten Erkenntnisse dazu vorstellen, wie man mit einer gut formulierten Cloud-Services-Ausschreibung eine erfolgreiche Cloud-Rahmenvereinbarung realisiert.

3.1 Cloud-Governance

Governance in der Cloud unterliegt einer gemeinsamen Verantwortung. CISPs bieten Funktionen und Services, um die Cloud-Governance in jeden Aspekt einer Cloud-Umgebung zu integrieren. Im Gegenzug bringen Kunden ihre bestehenden Cloud-Governance-Standards mit und lernen, wie die Cloud die Cloud-Governance ermöglicht.

Kunden haben in der Cloud die Möglichkeit, die IT-Umgebung nach ihren Vorstellungen aufzubauen, anstatt einfach nur die vorhandene zu verwalten. Die Cloud bietet Kunden folgende Vorteile: (1) Sie verfügen ab Tag 1 über einen kompletten IT-Komponentenbestand, (2) sie verwalten alle diese Komponenten zentral und (3) sie können Warnungen für Nutzungs-, Gebühren- und Sicherheitslimits erstellen. Diese entscheidenden Cloud-Vorteile geben Kunden die Möglichkeit, eine optimierte – und soweit wie möglich automatisierte – Architektur zu nutzen, für die nicht laufend neue Hardware angeschafft und installiert werden muss. Diese Aufgaben werden vom CISP übernommen, sodass Kunden ihren eigenen Schwerpunkt von einer undifferenzierten Infrastrukturverwaltung auf die geschäftskritische Betriebstätigkeit verlagern können.

Im Grunde genommen lässt sich eine CISP-Cloud als sehr große API denken: Ob Sie nun einen neuen Server starten oder eine Sicherheitseinstellung ändern – Sie führen nur API-Aufrufe aus. Jede Änderung an der Umgebung wird erfasst und protokolliert (das heißt, für jede Änderung wird erfasst, was und wo geändert wurde, wer die Änderung vorgenommen hat und zu welchem Zeitpunkt die Änderung erfolgte). Dieses Maß an Cloud-Governance, Kontrolle und Transparenz ist nur in einer Cloud-Umgebung möglich. Sie ermöglicht es Kunden, ihre bestehenden

IT-Governance-Modelle zu überdenken und zu definieren, wie diese angesichts der Vorteile der Cloud optimiert und verbessert werden können.

Cloud-Governance kann auch bedeuten, die positiven Prozessänderungen und neuen Kompetenzen, die mit der Cloud einhergehen, zu kommunizieren und zu integrieren. Projektmanager sind z. B. monatelange Wartezeiten gewohnt, bis eine IT-Umgebung aufgebaut ist, und könnten daher möglicherweise die Zeitpläne für die Erstellung einer Entwicklungs- oder Testumgebung in der Cloud deutlich überschätzen (denn diese dauert mit der Cloud unter Umständen nur wenige Minuten). Sich an diese neue Agilität zu gewöhnen, wird ein evolutionärer Prozess sein und passiert von Programm zu Programm. Solche gesammelten Erkenntnisse sollten weitergegeben werden, damit eine Cloud-Rahmenvereinbarung so weiterentwickelt werden kann, dass die Anforderungen auf diese neuen Prozesse und Agilität abgestimmt werden.

3.2 Budgetierung für die Cloud

Wenn es um die passende Strukturierung der nutzungsabhängigen Cloud-Preise für die Anforderungen der Akquise und Budgetierung im öffentlichen Sektor geht, haben wir festgestellt, dass es hilft, CISP-Services in einem einzigen Posten zu bündeln (Datenverarbeitung, Speicher, Netzwerk, Datenbank, IoT usw.), und zwar alles unter dem Begriff **Cloud-Technologien**. So kann die Flexibilität garantiert werden, den Benutzern alle aktuellen und neuen CISP-Technologien in Echtzeit anzubieten, und ermöglicht ihnen schnellen Zugriff auf die erforderlichen Ressourcen, wann immer sie sie benötigen. Dieser Ansatz berücksichtigt auch eine schwankende Nachfrage und sorgt so für eine optimierte Auslastung und niedrige Kosten.

Organisationen des öffentlichen Sektors können zusätzliche Einzelposten für Aufträge aus anderen Bereichen zu einer Cloud-Rahmenvereinbarung hinzufügen, wenn sie Beratungsdienste, Professional oder Managed Services, Software von einem Marketplace, Cloud-Support-Services und Schulungen zu CISP-Angeboten benötigen.

Zusätzliche Flexibilität beim Vertragsabschluss kann durch die Verwendung optionaler Vertragspositionen in den entsprechenden Ressourcenkategorien gewährleistet werden, um so zukünftiges Wachstum zu berücksichtigen. Wenn ein Unternehmen Cloud-Technologien mit Beratungsdiensten/Professional Services/Managed Services in einem Posten bündeln möchte, kann dies auch unter einem Oberbegriff wie „Cloud-Technologien und Zusatzaufwand“ erfolgen.

Im Folgenden finden Sie ein repräsentatives Beispiel für diesen Ansatz. Im nachstehenden Beispiel entspricht jede Einheit des Einzelpostens 1001 – Cloud-Technologien einem Wert von 1,00 € für genutzte „Cloud-Technologien“. Jeden Monat können Bestellzuwächse auf der Grundlage aktueller und vorhergesagter Nutzungsprognosen finanziert werden.

Tabelle 3 – Beispiel für eine Preisstruktur für Einzelposten.

POSTEN-NR.	LIEFERUNGEN/SERVICES	STÜCKZAHL	EINHEIT	PREIS PRO EINHEIT	BETRAG
1001	Cloud-Technologien	1 000	Jede Einheit	1 €	1 000 €
1002	Beratungsservices	1	Pro Woche	3 000 €	3 000 €
1003	Cloud-Support	1	Pro Monat	1 000 €	1 000 €
1004	Cloud-Schulungen	1	Pro Tag	3,00 €	3 000 €
1005	Cloud-Marketplace	10	Jede Einheit	10 €	100 €

Ein Beispiel dafür, wie diese Struktur funktionieren kann: Eine Organisation des öffentlichen Sektors kontaktiert einen CISP, um einzuschätzen, wie viele Cloud-Technologieservices die Organisation nutzen wird. Die Organisation einigt sich mit dem Anbieter, z. B. auf 10 Millionen Euro über 5 Jahre, was 2 Millionen Euro pro Jahr entspricht. Die Organisation verpflichtet sich, den anfänglichen Jahresbetrag von 2 Millionen Euro zu begleichen. Jeden Monat gibt es eine Rechnung und das Geld wird aus dem Fonds zur Zahlung genommen. Dieses Konto wird belastet. Die verbleibenden Mittel werden mithilfe von CISP-Überwachungs- und Prognosetools auf die Verbrauchsrate hin überwacht. Wenn die verbleibenden Mittel niedrig werden, fordert die Organisation zusätzliche Mittel vom CFO an, die zur Aufrechterhaltung der Services eingesetzt werden können.

Beispielformulierungen: Preise – Vertragsabschluss

ZAHLUNGSBEDINGUNGEN
*Die Zahlungsbedingungen müssen so strukturiert werden, dass **<ORGANISATION>** nur für die Ressourcen bezahlt, die wie unten angegeben verwendet werden:*

1. *Die monatliche Zahlung basiert auf der tatsächlichen Nutzung/dem Verbrauch von Services und den öffentlich verfügbaren Preisen der CISPs.*

MINDESTGARANTIE UND MAXIMALE AUSGABEN
*Da es für **<ORGANISATION>** unmöglich ist, genau vorherzusagen, wie viele der Ressourcen eines bestimmten Cloud-Service-Anbieters über einen bestimmten Zeitraum verbraucht werden, werden Bestellungen als Stückmengen eines einzelnen fest bepreisten Postens für „Cloud-Technologien" angegeben.*

*Jede Einheit des bestellten Postens entspricht einem Wert von **<1,00 €>** der bestellten Cloud-Technologien. Inkrementelle Bestellungen werden regelmäßig über eine Anpassung dieser Bestellung mit verschiedenen Mengen aufgegeben, um **<ORGANISATION>** die Flexibilität zu bieten, verschiedene „Euro-Betrag"-Mengen von CISP-Cloud-Technologien basierend auf der geschätzten Nutzung für Anforderungen unterschiedlicher Dauer vorzubestellen. Die Artikel werden von **<ORGANISATION>** in regelmäßigen Abständen in Mengen vorbestellt, die ausreichen, um die geschätzten Kosten für Cloud-Technologien abzudecken, die für eine Vielzahl von Anforderungen verwendet werden.*

Posten-Nr.	Beschreibung	Menge	Einheit	Preis
01	CISP-Cloud-Technologien	1 000	Stk	1 000,00 €

MINDESTBESTELLUNG/INKREMENTELLE BESTELLUNG
*Bestellungen werden in regelmäßigen Abständen für verschiedene Mengen von <10 000> Posteneinheiten aufgegeben, basierend auf der geschätzten Nutzung von Cloud-Technologien durch **<ORGANISATION>**. Diese Vereinbarung bietet **<ORGANISATION>** die Flexibilität, bei Bedarf **<10 000>** Einheiten von „Cloud-Technologien" vorzubestellen, um den Betrieb zu unterstützen und dabei im Einklang mit den kommerziellen nutzungsabhängigen „pay-as-you-go"-Verfahren des Cloud Computing zu operieren.*

*Zum Zeitpunkt der Aufgabe des Abrufs wird eine anfängliche Stückzahl von **<100 000>** Einheiten zu einem Preis von **<100 000 €>** bestellt. Die Mindestanzahl der gesamten Posteneinheiten, die mit einem oder mehreren Einzelposten in einem einzelnen inkrementellen Auftrag platziert werden können, beträgt **<x>.** Die maximale Anzahl an Einheiten, die im Rahmen des Bereitstellungsauftrags bestellt werden, darf **<x>** nicht überschreiten. Zusätzlich darf die Anzahl, kombiniert mit allen zuvor bestellten Einheiten, niemals den Abrufwert überschreiten.*

<ORGANISATION> ist dafür verantwortlich, dass alle Aufträge innerhalb der in diesem Abschnitt festgelegten Grenzen liegen.

MAXIMALER BESTELLWERT
Der maximale Gesamtbestellwert <x> besteht aus bis zu <x> Einheiten eines Einzelpostens, der mit <x> pro Einheit berechnet wird. Der Wert basiert auf einer Schätzung der Anforderungen von <ORGANISATION> über den Leistungszeitraum hinweg, kann jedoch nicht garantiert werden.

3.3 Verständnis des Partnergeschäftsmodells

Einrichtungen des öffentlichen Sektors sollten sich mit den verschiedenen Angebotsmodellen der CISPs vertraut machen und beachten, dass Partner eine entscheidende Rolle in Beratung, Managed Services, Wiederverkauf und vielen weiteren Bereichen spielen. Viele Kunden benötigen einen Cloud-Anbieter für ihre Infrastruktur. Die „praktische" Planung, Migration und Verwaltung wird dabei an einen System-Integrator (SI) oder Managed Service Provider ausgelagert. Aufgrund dieser Mischung aus Services gelten manche Anforderungen möglicherweise nicht für Cloud-Anbieter, wie z. B. die Weitergabe von Vertragsklauseln an Subunternehmer.

Am Beispiel dieser Klauseln lässt sich erkennen, warum es wichtig ist, zu verstehen, wie Partner und Vertriebspartner mit CISPs zusammenarbeiten. In manchen Beschaffungsfällen gibt es etwa Klauseln, die vorsehen, dass der Hauptauftragnehmer einige erforderliche Klauseln an Partner/Subauftragnehmer weitergibt. In der Regel stellen CISPs ihre Services nicht wie formelle Subunternehmer bereit und geben keine entsprechenden Angebote ab, da sie einen standardisierten Service in großem Umfang anbieten, der nicht auf die individuellen Anforderungen eines bestimmten Endkunden ausgerichtet ist (die Anforderungen von Kunden des öffentlichen Sektors mit einem entsprechenden Vertrag für den öffentlichen Sektor sind hierin eingeschlossen). In einem indirekten Beschaffungsmodell (Beschaffung von Cloud-Services über einen CISP-Vertriebspartner) kann der CISP diese Klauseln von seinem Vertriebspartner mit der Begründung ablehnen, dass sie auf einen kommerziellen Serviceanbieter der „zweiten Stufe" nicht anwendbar sind. In einem solchen Fall führt der CISP den vertraglich vereinbarten Leistungsumfang nicht selbst aus, sondern ein CISP-Partner nutzt zu diesem Zwecke die Infrastruktur eines CISP. Daher gilt der CISP als kommerzieller Anbieter (und nicht als Subunternehmer) für die Leistungen des Partners. In einem direkten Beschaffungsmodell (Beschaffung von Cloud-Services direkt von einem CISP) lehnt der CISP diese „erforderlichen" Vertragsklauseln, die für einen normalen Subunternehmer bei Verbrauchsgütern typisch sind, in der Regel mit einem Verweis auf den kommerziellen Charakter der vertraglich vereinbarten Services ab, sowie aufgrund der Tatsache, dass die meisten CISPs für die Bereitstellung ihrer kommerziellen Services keine Subunternehmer benötigen.

3.4 Cloud-Broker

Das Konzept eines Cloud-Brokers als Mittel zur Reduzierung einer möglichen Anbieterbindung kann problematisch sein. Ein Cloud-Broker mag in der Theorie sinnvoll erscheinen, in der Praxis würde er jedoch wahrscheinlich mehr Komplexität und Verwirrung bringen als wirklichen Nutzen.

Anwendungen auf mehreren Clouds gleichzeitig oder austauschbar auszuführen, führt unweigerlich zu Kompromissen bezüglich der Funktionalität. (Für die Cloud gibt es kein Universalkonzept.) Ein solcher Ansatz kann zu unnötiger Komplexität zwischen Kunden des öffentlichen Sektors und

ihren Cloud-Services führen, was ggf. die Effizienz- und Sicherheitsvorteile wieder zunichtemacht, die man sich eigentlich erhofft hatte. Die Folgen: eine geringere Skalierbarkeit und Flexibilität, höhere Kosten und verlangsamte Innovationen.

3.5 Beschaffung vor der Ausschreibung/Marktforschung

Wenn eine Organisation des öffentlichen Sektors eine Ausschreibung für Cloud-Services plant, sollte sie von Anfang an Stakeholder aus allen Bereichen der Organisation einbeziehen – die Führungskräfte sowie die Stakeholder in den Bereichen Technologie, Geschäft, Finanzen, Beschaffung, Recht und Verträge. Dadurch wird sichergestellt, dass sich alle Stakeholder einen Begriff des Cloud-Modells machen und folglich eine fundierte Einschätzung zur Neubewertung herkömmlicher IT-Beschaffungsmethoden geben können.

Für den Dialog mit der Branche empfehlen wir Organisationen des öffentlichen Sektors dringend, sich die Zeit zu nehmen, fundierte Gespräche zu führen, um so Feedback zu sammeln – von CISPs, CISP-Partnern, PaaS-/SaaS-Marketplace-Anbietern und Branchenexperten. Ein solcher Dialog kann beispielsweise in Form von Branchentagen oder Sicherheits- und Beschaffungsworkshops stattfinden. Eine weitere effektive Möglichkeit, ein tiefergehendes Verständnis der Cloud-Beschaffung zu gewinnen, ist die Abgabe einer Informationsanfrage oder idealerweise eines Entwurfsdokuments für eine Ausschreibung. Häufig enthalten diese potenzielle Probleme, die identifiziert, diskutiert und angepasst werden können, bevor die endgültige Ausschreibung für Cloud-Services veröffentlicht wird.

3.6 Nachhaltigkeit

Nachhaltigkeit ist ein inhärenter Teil von Cloud Computing und der Wechsel zur Cloud steigert die Energieeffizienz im Vergleich zu lokalen Servern oder Rechenzentren von Unternehmen. Indem ein CISP gefunden wird, der Nachhaltigkeit priorisiert und der sich öffentlich Nachhaltigkeitsziele gesetzt hat, kann weiter dafür gesorgt werden, dass die Cloud nachhaltig ist. Europäische CISPs und Betreiber von Rechenzentren entwickelten (mit der Unterstützung der Europäischen Kommission) den Climate Neutral Data Centre Pact[11]. Diese Selbstregulierungsinitiative soll klare, einfache und weitreichende Nachhaltigkeitskriterien für die Rechenzentrumsbranche aufstellen und dafür sorgen, dass Betreiber und Cloud-Service-Anbieter bis zum Jahr 2030 Klimaneutralität erreichen. Die Initiative setzt für Rechenzentren klare Ziele hinsichtlich Energieeffizienz, Wasserverbrauch, Wiederverwendung und Reparatur von Servern und Einsatz kohlenstofffreier Energie zum Betreiben von Rechenzentren. CISPs, die bei der Selbstregulierungsinitiative mitmachen, stimmen diesen Zielen zu und akzeptieren die Bedingungen, um als klimaneutrale Betreiber anerkannt zu sein.

Eine Cloud-Services-Ausschreibung sollte fragen, ob sich CISPs solchen Kriterien verschrieben haben, insbesondere, ob sie einer Selbstregulierung zugestimmt haben und wann dies geschah.

Beispielformulierungen für die Ausschreibung: Nachhaltigkeit

Haben Sie sich im Rahmen der Selbstregulierungsinitiative Climate Neutral Data Centre dazu verpflichtet, klimaneutrale Rechenzentren zu betreiben? Wenn ja, wann haben Sie unterzeichnet?

Können Sie beweisen, dass Ihnen das Siegel des Climate Neutral Data Centre Pact verliehen wurde?

[11] https://www.climateneutraldatacentre.net/self-regulatory-initiative/

Anhang A – Technische Anforderungen für den Vergleich zwischen Bietern

Im Folgenden finden Sie einige allgemeine Anforderungen an die Cloud-Technologie, die für den Vergleich von CISPs während Abrufen oder Mini-Wettbewerben in einer Cloud-Rahmenvereinbarung verwendet werden können.

1. Profil des Cloud-Anbieters

	Anforderung
1.	***MARKTERFAHRUNG:*** *Wie viele Jahre ist der Cloud-Anbieter im Cloud-Marktsegment tätig?*
2.	***OFFENHEIT UND DATENSICHERHEIT:*** *Hält der Cloud-Anbieter sich an die Verhaltenskodizes für Datenschutz oder Reversibilität in der Branche? Hält der Cloud-Anbieter die Open Source- und Open-API-Entwicklungsprinzipien ein?*

2. Globale Infrastruktur

	Anforderung
1.	***GLOBALE REICHWEITE:*** *Bietet der Cloud-Anbieter eine globale Infrastruktur, mit der Benutzer eine niedrige Latenz und einen hohen Durchsatz erzielen können?*
2.	***REGIONEN:*** *Verfügt der Cloud-Anbieter über eine regionale Präsenz in den benötigten geografischen Gebieten?*
3.	***DOMÄNEN/ZONEN:*** *Implementiert der Cloud-Anbieter das Konzept von Domänen oder Zonen, in denen mehrere Rechenzentren durch ein Netzwerk mit niedriger Latenz gruppiert werden, um ein höheres Maß an Verfügbarkeit und Fehlertoleranz zu bieten?* • *Wenn ja, geben Sie bitte die Anzahl der Domänen oder Zonen und die Anzahl der Rechenzentren innerhalb der erforderlichen geografischen Region an.*
4.	***DISTANZ DOMÄNEN/ZONEN:*** *Baut der Cloud-Anbieter seine Domänen oder Zonen mit physisch voneinander getrennten Rechenzentren auf, um Redundanz, Hochverfügbarkeit und geringe Latenz zu unterstützen?*
5.	***BAU RECHENZENTREN:*** *Bietet der Cloud-Anbieter Rechenzentren, die vor Ausfällen in anderen Rechenzentren durch redundante Stromversorgung, Kühlung und Netzwerke geschützt sind?*
6.	***REPLIKATION RECHENZENTREN:*** *Bietet der Cloud-Anbieter Datenreplikation mit automatischem Failover über Rechenzentren innerhalb einer Domäne oder Zone hinweg?*
7.	***REPLIKATION DOMÄNEN/ZONEN:*** *Bietet der Cloud-Anbieter Datenreplikation über Domänen oder Zonen innerhalb einer Region hinweg?*

3. Infrastruktur

3.1 Datenverarbeitung

	Anforderung
1.	***DATENVERARBEITUNG – NORMALE INSTANCE – ALLGEMEINE ZWECKE:*** *Bietet der Cloud-Anbieter die folgenden Instance-Typen an?* • *Allgemeine Zwecke – optimiert für generische Anwendungen, mit ausgewogenem Verhältnis von Rechen-, Arbeitsspeicher- und Netzwerkressourcen* o *Wenn ja, welche ist die größte Instance?*
2.	***DATENVERARBEITUNG – NORMALE INSTANCE – ARBEITSSPEICHEROPTIMIERT:*** *Bietet der Cloud-Anbieter die folgenden Instance-Typen an?* • *Arbeitsspeicheroptimiert – optimiert für arbeitsspeicherintensive Anwendungen* o *Wenn ja, welche ist die größte Instance?*
3.	***DATENVERARBEITUNG – NORMALE INSTANCE – DATENVERARBEITUNGSOPTIMIERT:*** *Bietet der Cloud-Anbieter die folgenden Instance-Typen an?* • *Datenverarbeitungsoptimiert – optimiert für rechenintensive Anwendungen* o *Wenn ja, welche ist die größte Instance?*
4.	***DATENVERARBEITUNG – NORMALE INSTANCE – SPEICHEROPTIMIERT:*** *Bietet der Cloud-Anbieter die folgenden Instance-Typen an?* • *Speicheroptimiert – enthält eine große Menge lokaler Speicherkapazität* o *Wenn ja, wie hoch ist die maximale Speicherkapazität (d. h. 5, 10, 20, 50 TB) und die maximale Anzahl an Festplatten (HDDs/SSDs), die bereitgestellt und an eine Instance angehängt werden können?*
5.	***DATENVERARBEITUNG – NORMALE INSTANCE – GRAFIKOPTIMIERT:*** *Bietet der Cloud-Anbieter die folgenden Instance-Typen an?* • *Kostengünstige Grafik – bietet er kostengünstige Grafikbeschleunigung zur Verarbeitung von Instances?* o *Wenn ja, welche ist die größte Instance?*
6.	***DATENVERARBEITUNG – NORMALE INSTANCE – GPU-OPTIMIERT:*** *Bietet der Cloud-Anbieter die folgenden Instance-Typen an?* • *GPU – enthält Hardware-GPUs (Graphics Processing Units) für grafikintensive Anwendungen* o *Wenn ja, wie viele GPUs und welche GPU-Modelle kann der Cloud-Anbieter pro Instance anbieten?*
7.	***DATENVERARBEITUNG – NORMALE INSTANCE – FPGA-OPTIMIERT:*** *Bietet der Cloud-Anbieter die folgenden Instance-Typen an?* • *FPGA – enthält lokal programmierbare Gate-Arrays (FPGA, Field Programmable Gate Arrays) für die Entwicklung und Bereitstellung benutzerdefinierter Hardwarebeschleunigung für Anwendungen* o *Wenn ja, wie viele FPGAs kann der Cloud-Anbieter pro Instance anbieten?*

8.	*DATENVERARBEITUNG – BURSTFÄHIGE INSTANCE:* *Bietet der Cloud-Anbieter burstfähige Instances, die ein Baseline-Level der CPU-Leistung (Central Processing Unit) mit der Möglichkeit bieten, diese Baseline mittels „Bursting" zu überschreiten?* • *Wenn ja, welche ist die größte burstfähige Instance?*
9.	*DATENVERARBEITUNG – E/A-INTENSIVE INSTANCE:* *Bietet der Cloud-Anbieter Instances, die SSDs (Solid State Drives) mit Non Volatile Memory Express (NVMe) verwenden, welche für eine geringe Latenz, eine sehr hohe beliebige E/A-Leistung und einen hohen sequenziellen Lesedurchsatz optimiert sind?* • *Wenn ja, wie hoch ist die maximale IOPS-Kapazität (Input/Output Operations Per Second) der größten Instance?*
10.	*DATENVERARBEITUNG – TEMPORÄRE LOKALE SPEICHER:* *Unterstützt der Cloud-Anbieter lokalen Speicher für Datenverarbeitungs-Instances, die für die temporäre Speicherung von Informationen verwendet werden, die sich häufig ändern?*
11.	*DATENVERARBEITUNG – UNTERSTÜTZUNG MEHRERER NICs:* *Unterstützt der Cloud-Anbieter mehrere (primäre und zusätzliche) Netzwerk-Schnittstellenkarten (NICs, Network Interfaces Cards), die einer bestimmten Instance zugeordnet werden?* • *Wenn ja, wie viele NICs pro Instance sind maximal zulässig?*
12.	*DATENVERARBEITUNG – INSTANCE-AFFINITÄT:* *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, Instances innerhalb eines Rechenzentrums logisch zu gruppieren?*
13.	*DATENVERARBEITUNG – INSTANCE-ANTI-AFFINITÄT:* *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, Instances logisch zu gruppieren und in verschiedenen Rechenzentren innerhalb einer Region zu platzieren?*
14.	*DATENVERARBEITUNG – SELF-SERVICE-BEREITSTELLUNG:* *Bietet der Cloud-Anbieter die gleichzeitige Self-Service-Bereitstellung für mehrere Instances, entweder über eine Programmschnittstelle, eine Verwaltungskonsole oder ein Webportal?*
15.	*DATENVERARBEITUNG – ANPASSUNG:* *Bietet der Cloud-Anbieter anpassbare Instances, d. h. die Möglichkeit, Konfigurationseinstellungen wie virtuelle Prozessoren (vCPUs, Virtual Central Processing Units) und Arbeitsspeicher (RAM, Random Access Memory) zu ändern?*
16.	*DATENVERARBEITUNG – MANDANTENFÄHIGKEIT:* *Bietet der Cloud-Anbieter Instances für einen einzelnen Mandanten, die also auf Hardware ausgeführt werden, die einem einzelnen Benutzer zugewiesen ist?* • *Wenn ja, wie groß ist die größte verfügbare Instance für einen einzelnen Mandanten?*
17.	*DATENVERARBEITUNG – HOST-AFFINITÄT:* *Bietet der Cloud-Anbieter die Möglichkeit, eine Instance zu starten und anzugeben, dass diese Instance immer auf demselben physischen Host gestartet wird?*
18.	*DATENVERARBEITUNG – HOST-ANTI-AFFINITÄT:* *Bietet der Cloud-Anbieter die Möglichkeit, bestimmte Instances auf verschiedene physische Hosts aufzuteilen und zu hosten?*

19.	*DATENVERARBEITUNG – AUTOMATISCHE SKALIERUNG:* *Bietet der Cloud-Anbieter die Möglichkeit, die Anzahl der Instances automatisch während Bedarfsspitzen zu erhöhen, um die Leistung aufrechtzuerhalten (d. h. durch „aufskalieren")?*
20.	*DATENVERARBEITUNG – MECHANISMUS ZUM IMPORT VON IMAGES:* *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, ihre vorhandenen Images zu importieren und als neue, privat verfügbare Images zu speichern, die dann später für die Bereitstellung von Instances verwendet werden können?* • *Wenn ja, welche Formate werden unterstützt?*
21.	*DATENVERARBEITUNG – MECHANISMUS ZUM EXPORT VON IMAGES:* *Unterstützt der Cloud-Anbieter die Möglichkeit, eine vorhandene, ausgeführte Instance oder eine Kopie einer Instance in ein virtuelles Maschinenformat zu exportieren?* • *Wenn ja, welche Formate werden unterstützt?*
22.	*DATENVERARBEITUNG – SERVICEUNTERBRECHUNG:* *Bietet der Cloud-Anbieter Mechanismen zur Vermeidung von Instance-Ausfällen oder Ausfallzeiten, wenn der Anbieter jegliche Hardware- oder Servicewartung auf Hostebene durchführt?*
23.	*DATENVERARBEITUNG – INSTANCE-NEUSTART:* *Bietet der Cloud-Anbieter Mechanismen für den automatischen Neustart von Instances auf einem fehlerfreien Host, wenn der ursprüngliche physische Host ausfällt?*
24.	*DATENVERARBEITUNG – BENACHRICHTIGUNGEN:* *Ist der Cloud-Anbieter im Fall eines Ereignisses, das die Datenverarbeitung beeinträchtigen könnte, in der Lage, den Benutzer über ein solches Ereignis zu benachrichtigen, und kann der Benutzer diese Kommunikation über Self-Service-Methoden aktivieren oder deaktivieren?*
25.	*DATENVERARBEITUNG – EREIGNISZEITPLAN:* *Bietet der Cloud-Anbieter die Möglichkeit, Ereignisse für die Instances des Benutzers zu planen, z. B. Neustart, Anhalten, Starten oder Stilllegen der Instance?*
26.	*DATENVERARBEITUNG – SICHERUNGS- UND WIEDERHERSTELLUNGSMECHANISMUS:* *Bietet der Cloud-Anbieter einen integrierten Mechanismus für Sicherung und Wiederherstellung?*
27.	*DATENVERARBEITUNG – SNAPSHOT-MECHANISMUS:* *Bietet der Cloud-Anbieter einen manuellen On-Demand-Snapshot-Mechanismus?*
28.	*DATENVERARBEITUNG – METADATEN:* *Bietet der Cloud-Anbieter einen Instance-Metadatenservice, mit dem Benutzer beliebige Schlüssel/Wert-Paare für die Instance festlegen können?*
29.	*DATENVERARBEITUNG – METADATENABRUF:* *Bietet der Cloud-Anbieter einen Instance-Metadatenservice, der eine Programmierschnittstelle (API) bereitstellt, welche die Instance aufrufen kann, um Informationen über sich selbst zu erhalten?*
30.	*DATENVERARBEITUNG – ANGEBOTSMECHANISMUS:* *Bietet der Cloud-Anbieter einen Angebotsmechanismus für kostengünstigere Instances, die sofort instanziiert werden können, um nicht geschäftskritische Workloads zu hosten?*
31.	*DATENVERARBEITUNG – ZEITPLANMECHANISMUS:* *Bietet der Cloud-Anbieter eine Möglichkeit, regelmäßig, d. h. täglich, wöchentlich oder monatlich, zusätzliche Rechenkapazität zu planen und zu reservieren?*
32.	*DATENVERARBEITUNG – RESERVIERUNGSMECHANISMUS:*

	Bietet der Cloud-Anbieter eine Möglichkeit, zusätzliche Rechenkapazität für die Zukunft zu reservieren (d. h. auf 1 Jahr, 2 Jahre, 3 Jahre usw.)?
33.	***DATENVERARBEITUNG – LINUX-BETRIEBSSYSTEM:*** *Unterstützt der Cloud-Anbieter die letzten zwei langfristig unterstützten Versionen von mindestens einer Enterprise Linux-Distribution (wie Red Hat, SUSE) und einer gängigen kostenlosen Linux-Distribution (wie Ubuntu, CentOS und Debian)?*
34.	***DATENVERARBEITUNG – WINDOWS-BETRIEBSSYSTEM:*** *Unterstützt der Cloud-Anbieter die letzten beiden relevanten Windows Server-Versionen (Windows Server 2017 und Windows Server 2016)?*
35.	***DATENVERARBEITUNG – LIZENZPORTABILITÄT:*** *Bietet der Cloud-Anbieter Lizenzportabilität und zugehörigen Support?* • *Wenn ja, geben Sie bitte den Softwareanbieter, die Softwarenamen, die Editionen und zugehörigen Versionen an.*
36.	***DATENVERARBEITUNG – SERVICE-LIMITS:*** *Unterliegt der Cloud-Anbieter jeglichen Einschränkungen (d. h. Service-Limits) in Bezug auf den oben aufgeführten Abschnitt zum Thema Datenverarbeitung?* *Beispiel:* *Maximale Anzahl von Instances pro Konto* *Maximale Anzahl dedizierter Hosts pro Konto* *Maximale Anzahl reservierter IP-Adressen*

3.2 Netzwerk

	Anforderung
1.	***NETZWERK – VIRTUELLE NETZWERKE:*** *Unterstützt der Cloud-Anbieter die Erstellung eines logischen, isolierten virtuellen Netzwerks, das das organisationseigene Netzwerk in der Cloud repräsentiert?*
2.	***NETZWERK – KONNEKTIVITÄT IN DERSELBEN REGION:*** *Unterstützt der Cloud-Anbieter die Verbindung von zwei virtuellen Netzwerken innerhalb derselben Region, um Datenverkehr mithilfe von IP-Adressen zwischen ihnen zu routen?*
3.	***NETZWERK – ÜBERREGIONALE KONNEKTIVITÄT:*** *Unterstützt der Cloud-Anbieter die Verbindung von zwei virtuellen Netzwerken über verschiedene Regionen hinweg, um Datenverkehr mithilfe von IP-Adressen zwischen ihnen zu routen?*
4.	***NETZWERK – PRIVATES SUBNETZ:*** *Bietet der Cloud-Anbieter die Möglichkeit, vollständig isolierte (private) virtuelle Netzwerke und Subnetze zu erstellen, in denen Instances ohne IP-Adresse oder Internet-Routing bereitgestellt werden können?*
5.	***NETZWERK – VIRTUELLE NETZWERK-ADRESSBEREICHE:*** *Unterstützt der Cloud-Anbieter IP-Adressbereiche, die in RFC 1918 (Request for Comments) angegeben sind, sowie öffentlich routingfähige CIDR-Blöcke (Classless Inter-Domain Routing)?*
6.	***NETZWERK – MEHRERE PROTOKOLLE:***

	Unterstützt der Cloud-Anbieter mehrere Protokolle, einschließlich TCP (Transmission Control Protocol), UDP (User Datagram Protocol) und ICMP (Internet Control Message Protocol)?
7.	*NETZWERK – AUTOMATISCHE ZUWEISUNG VON IP-ADRESSEN:* *Unterstützt der Cloud-Anbieter die automatische Zuweisung von IP-Adressen zu Instances?*
8.	*NETZWERK – RESERVIERTE STATISCHE IP-ADRESSEN:* *Unterstützt der Cloud-Anbieter IP-Adressen, die mit einem Benutzerkonto verknüpft sind, nicht mit einer bestimmten Instance? Die IP-Adresse sollte bis zur expliziten Freigabe mit dem Konto verknüpft bleiben.*
9.	*NETZWERK – IPV6-SUPPORT:* *Unterstützt der Cloud-Anbieter das Internetprotokoll Version 6 (IPv6) entweder auf Gateway- oder Instance-Ebene und stellt diese Funktionalität Benutzern zur Verfügung?*
10.	*NETZWERK – MEHRERE IP-ADRESSEN PRO NIC:* *Unterstützt der Cloud-Anbieter die Zuweisung einer primären und einer sekundären IP-Adresse zu einer Netzwerk-Schnittstellenkarte (NIC), die mit einer bestimmten Instance verbunden ist?*
11.	*NETZWERK – MEHRERE NICS:* *Unterstützt der Cloud-Anbieter die Möglichkeit, einer bestimmten Instance mehrere Netzwerk-Schnittstellenkarten (NICs) zuzuweisen?*
12.	*NETZWERK – NIC- UND IP-MOBILITÄT:* *Unterstützt der Cloud-Anbieter die Möglichkeit, Netzwerk-Schnittstellenkarten (NICs) und IP-Adressen zwischen Instances zu verschieben?*
13.	*NETZWERK – SUPPORT VON SR-IOV:* *Unterstützt der Cloud-Anbieter Funktionen wie SR-IOV (Single Root Input/Output Virtualization) für höhere Leistung – z. B. Pakete pro Sekunde (PPS, Packets Per Second), geringere Latenz und weniger Jitter?*
14.	*NETZWERK – INGRESS-FILTER:* *Unterstützt der Cloud-Anbieter das Hinzufügen oder Entfernen von Regeln, die für eingehenden Datenverkehr (Ingress) zu Instances gelten?*
15.	*NETZWERK – EGRESS-FILTER:* *Unterstützt der Cloud-Anbieter das Hinzufügen oder Entfernen von Regeln, die für ausgehenden Datenverkehr (Egress) von Instances gelten?*
16.	*NETZWERK – ACL:* *Bietet der Cloud-Anbieter Zugriffskontrolllisten (ACLs, Access Control Lists) zur Steuerung des ein- und ausgehenden Datenverkehrs zu Subnetzen?*
17.	*NETZWERK – SUPPORT VON FLUSSPROTOKOLLEN:* *Bietet der Cloud-Anbieter die Möglichkeit, Flussprotokolle für den Netzwerk-Datenverkehr zu erfassen?*
18.	*NETZWERK – NAT:* *Stellt der Cloud-Anbieter einen Managed Gateway-Service für die Netzwerkadressübersetzung (NAT, Network Address Translation) bereit, um Instances in einem privaten Netzwerk die Verbindung mit dem Internet oder anderen Cloud-Services zu ermöglichen, aber das Internet daran zu hindern, eine Verbindung zu diesen Instances herzustellen?*
19.	*NETZWERK – QUELL-/ZIELORTPRÜFUNG:* *Kann der Cloud-Anbieter die Quell-/Zielprüfung auf Netzwerk-Schnittstellenkarten (NICs) deaktivieren?*

20.	*NETZWERK – VPN-SUPPORT:* *Unterstützt der Cloud-Anbieter Virtual Private Network (VPN)-Verbindungen zwischen dem Cloud-Anbieter und dem Rechenzentrum des Benutzers?*
21.	*NETZWERK – VPN-TUNNEL:* *Unterstützt der Cloud-Anbieter mehrere Virtual Private Network (VPN)-Verbindungen pro virtuellem Netzwerk?*
22.	*NETZWERK – IPSEC-VPN-SUPPORT:* *Ermöglicht der Cloud-Anbieter Benutzern den Zugriff auf Cloud-Dienste über einen IPsec-VPN-Tunnel (IPsec, Internet Protocol Security) oder SSL-VPN-Tunnel (SSL, Secure Sockets Layer) über das öffentliche Internet?*
23.	*NETZWERK – BGP-SUPPORT:* *Nutzt der Cloud-Anbieter BGP (Border Gateway Protocol), um das Failover über IPsec-VPN-Tunnel (Virtual Private Network) hinweg zu verbessern?*
24.	*NETZWERK – PRIVATE DEDIZIERTE KONNEKTIVITÄT:* *Bietet der Cloud-Anbieter einen direkten privaten Konnektivitätsservice zwischen den Standorten des Cloud-Anbieters und der Rechenzentrums-, Büro- oder Colocation-Umgebung eines Benutzers, der große und schnelle Datenübertragungen ermöglicht?*
25.	*NETZWERK – LOAD BALANCER FÜR FRONT-END:* *Bietet der Cloud-Anbieter einen Load-Balancer-Service für das Front-End (mit dem Internet verbunden), der Anfragen von Clients über das Internet annimmt und diese Anfragen auf Instances verteilt, die beim Load Balancer registriert sind?*
26.	*NETZWERK – LOAD BALANCER FÜR BACK-END:* *Bietet der Cloud-Anbieter einen Load-Balancer-Service für das Back-End (privat), der den Datenverkehr an Instances weiterleitet, die in privaten Subnetzen gehostet werden?*
27.	*NETZWERK – LAYER-7-LOAD-BALANCER:* *Bietet der Cloud-Anbieter einen Layer-7-HTTP-Load-Balancer-Service (Hypertext Transfer Protocol), der in der Lage ist, Load Balancing für Netzwerk-Datenverkehr über mehrere Instances hinweg auszuführen?*
28.	*NETZWERK – LAYER-4-LOAD-BALANCER:* *Bietet der Cloud-Anbieter einen Layer-4-TCP-Load-Balancer-Service (Transmission Control Protocol), der in der Lage ist, Load Balancing für Netzwerk-Datenverkehr über mehrere Instances hinweg auszuführen?*
29.	*NETZWERK – SITZUNGSAFFINITÄT FÜR LOAD BALANCER:* *Bietet der Cloud-Anbieter einen Load-Balancing-Service, der Sitzungsaffinität unterstützt?*
30.	*NETZWERK – DNS-BASIERTES LOAD BALANCING:* *Bietet der Cloud-Anbieter einen Load-Balancing-Service, der in der Lage ist, Datenverkehr per Load Balancing auf Instances weiterzuleiten, die auf mehreren Hosts gehostet werden, welche zu einer einzigen Domäne gehören?*
31.	*NETZWERK – LOAD-BALANCER-PROTOKOLLE:* *Stellt der Cloud-Anbieter Protokolle bereit, die detaillierte Informationen zu allen Anforderungen erfassen, die an einen Load Balancer gesendet werden?*
32.	*NETZWERK – DNS:* *Bietet der Cloud-Anbieter einen hochverfügbaren und skalierbaren DNS-Service (Domain Name System)?*

33.	*NETZWERK – LATENZBASIERTES DNS-ROUTING:* *Bietet der Cloud-Anbieter einen DNS-Service an, der latenzbasiertes Routing unterstützt (d. h. der DNS-Service antwortet auf DNS-Abfragen mit den Ressourcen, die die beste Latenz bieten)?*
34.	*NETZWERK – GEO-BASIERTES DNS-ROUTING:* *Bietet der Cloud-Anbieter einen DNS-Service an, der geo-basiertes Routing unterstützt (d. h. der DNS-Service antwortet auf DNS-Abfragen basierend auf der geografischen Position der Benutzer)?*
35.	*NETZWERK – FAILOVER-BASIERTES DNS-ROUTING:* *Bietet der Cloud-Anbieter einen DNS-Service an, der Failover-basiertes Routing unterstützt (d. h. der DNS-Service leitet DNS-Abfragen an die aktuell aktive Ressource weiter, während eine zweite Ressource wartet und erst bei einem Ausfall der primären Ressource aktiv wird)?*
36.	*NETZWERK – SERVICE ZUR DOMÄNENREGISTRIERUNG:* *Bietet der Cloud-Anbieter Services zur Registrierung von Domänennamen an (d. h. Benutzer können nach verfügbaren Domänennamen suchen und diese registrieren)?*
37.	*NETZWERK – DNS-ZUSTANDSPRÜFUNGEN:* *Bietet der Cloud-Anbieter einen DNS-Service an, der mithilfe von Zustandsprüfungen den Zustand und die Leistung von Ressourcen überwacht?*
38.	*NETZWERK – DNS- UND LOAD-BALANCER-INTEGRATION:* *Bietet der Cloud-Anbieter einen DNS-Service, der in den Load Balancer des Cloud-Anbieters integriert werden kann?*
39.	*NETZWERK – VISUELLER EDITOR:* *Bietet der Cloud-Anbieter ein Tool, mit dem Benutzer Richtlinien für die Verwaltung des Datenverkehrs erstellen können?*
40.	*NETZWERK ZUR BEREITSTELLUNG VON INHALTEN (CDN):* *Bietet der Cloud-Anbieter einen CDN-Service (Content Delivery Network) zur Verteilung von Inhalten mit geringer Latenz und hoher Datenübertragungsgeschwindigkeit an?*
41.	*NETZWERK – CDN-CACHE-ABLAUF:* *Bietet der Cloud-Anbieter einen CDN-Service, mit dem ein Objekt vor seinem Ablauf aus dem Edge-Cache entfernt werden kann, einschließlich Funktionen wie das Ungültigmachen von Objekten und Objekt-Versioning?*
42.	*NETZWERK – EXTERNE CDN-URSPRÜNGE:* *Bietet der Cloud-Anbieter einen CDN-Dienst an, der einen benutzerdefinierten Ursprung, d. h. einen HTTP-Server, unterstützt?*
43.	*NETZWERK – CDN-OPTIMIERUNG:* *Bietet der Cloud-Anbieter einen CDN-Service mit detaillierter Kontrolle für die Konfiguration mehrerer Ursprungsserver und Caching-Eigenschaften verschiedener URLs (Uniform Resource Locators)?*
44.	*NETZWERK – GEO-BESCHRÄNKTES CDN:* *Bietet der Cloud-Anbieter einen CDN-Service, der geografische Beschränkungen unterstützt, d. h. Benutzer in bestimmten Regionen daran hindert, auf Inhalte zuzugreifen?*
45.	*NETZWERK – CDN-TOKENS:* *Bietet der Cloud-Anbieter einen CDN-Service an, der signierte URLs unterstützt, die in der Regel zusätzliche Informationen wie Ablaufdatum/-zeit enthalten, um Benutzern mehr Kontrolle über den Zugriff auf ihre Inhalte zu geben?*

46.	***NETZWERK – CDN-ZERTIFIKATE:*** *Bietet der Cloud-Anbieter einen CDN-Service, der benutzerdefinierte SSL-Zertifikate unterstützt, um Inhalte sicher über HTTPS (Hypertext Transfer Protocol Secure) von Edge-Standorten bereitzustellen?*
47.	***NETZWERK – MEHRSCHICHTIGER CDN-CACHE:*** *Bietet der Cloud-Anbieter einen CDN-Service, der einen mehrschichtigen Cache-Ansatz mit regionalen Edge-Caches nutzt, um die Latenz zu reduzieren?*
48.	***NETZWERK – CDN-KOMPRIMIERUNG:*** *Bietet der Cloud-Anbieter einen CDN-Service, der Dateikomprimierung unterstützt?*
49.	***NETZWERK – CDN-VERSCHLÜSSELTE UPLOADS:*** *Bietet der Cloud-Anbieter ein CDN, mit dem Benutzer ihre sensiblen Daten sicher hochladen können, sodass diese nur von bestimmten Komponenten und Services in der Ursprungsinfrastruktur des Benutzers angezeigt werden können?*
50.	***NETZWERK – ENDPUNKTE:*** *Bietet der Netzwerkservice des Cloud-Anbieters Benutzern Endpunkte, die den Datenverkehr über die interne Netzwerkkonnektivität des Anbieters (d. h. private Konnektivität) leiten können, um die Kommunikationskosten zu senken und die Traffic-Sicherheit zu verbessern?*
51.	***NETZWERK – SERVICE-LIMITS:*** *Unterliegt der Cloud-Anbieter jeglichen Einschränkungen (d. h. Service-Limits) in Bezug auf den oben aufgeführten Netzwerkbereich?* *Beispiel:* *Maximale Anzahl virtueller Netzwerke pro Konto* *Maximale Größe eines virtuellen Netzwerks* *Maximale Anzahl von Subnetzen pro Konto* *Maximale Anzahl von Load Balancern pro Konto* *Maximale Anzahl von ACL-Einträgen* *Maximale Anzahl von VPN-Tunneln* *Maximale Anzahl von Ursprüngen pro Distribution* *Maximale Anzahl von Zertifikaten pro Load Balancer*

3.3 Speicher

	Anforderung
1.	***BLOCKSPEICHERSERVICE:*** *Bietet der Cloud-Anbieter Speicher-Volumes auf Blockebene für die Verwendung mit Datenverarbeitungs-Instances?*
2.	***BLOCKSPEICHER – IOPS:*** *Bietet der Cloud-Anbieter die Möglichkeit, explizite Performance-Ziele oder -Stufen auf Blockspeicher-Volumes zu erwerben, z. B. eine bestimmte Anzahl von Eingabe-/Ausgabevorgängen pro Sekunde (IOPS) oder einen Durchsatz in Megabyte pro Sekunde (MB/s)?*

3.	***BLOCKSPEICHER – SOLID STATE DRIVES:*** *Unterstützt der Cloud-Anbieter SSD-gestützte Speichermedien, die Latenzen im einstelligen Millisekundenbereich bieten?* • *Wenn ja, wie viele SSDs können pro Instance maximal angehängt werden?*
4.	***BLOCKSPEICHER – SKALIERUNG:*** *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, die Größe eines vorhandenen Blockspeicher-Volumes zu erhöhen, ohne ein neues Volume bereitstellen und die Daten kopieren/verschieben zu müssen?*
5.	***BLOCKSPEICHER – SNAPSHOTS:*** *Verfügt der Cloud-Anbieter über Snapshot-Funktionen für seinen Blockspeicherservice?*
6.	***BLOCKSPEICHER – VOLLSTÄNDIGE DATENLÖSCHUNG:*** *Unterstützt der Cloud-Anbieter die vollständige Löschung von Daten, sodass Daten nicht mehr lesbar oder für unbefugte Benutzer und/oder Dritte zugänglich sind?*
7.	***BLOCKSPEICHER – VERSCHLÜSSELUNG IM RUHEZUSTAND:*** *Bietet der Cloud-Anbieter die serverseitige Verschlüsselung von Daten im Ruhezustand in Bezug auf Daten, die auf Volumes und deren Snapshots gespeichert sind?* • *Wenn ja, welcher kryptografische Algorithmus wird eingesetzt?*
8.	***OBJEKTSPEICHERSERVICE:*** *Bietet der Cloud-Anbieter einen sicheren, belastbaren und hochgradig skalierbaren Objektspeicher zum Speichern und Abrufen beliebiger Datenmengen aus dem Internet?*
9.	***OBJEKTSPEICHER – UNREGELMÄSSIGER ZUGRIFF:*** *Bietet der Cloud-Anbieter eine kostengünstigere Speicher-Servicestufe, die darauf abzielt, weniger häufig genutzte Objekte und Dateien zu speichern?*
10.	***OBJEKTSPEICHER – GERINGERE BESTÄNDIGKEIT:*** *Bietet der Cloud-Anbieter eine Stufe mit reduzierter Redundanz, in der ein Benutzer nicht kritische, einfach reproduzierbare Objekte zu einem niedrigeren Preis speichern kann?*
11.	***OBJEKTSPEICHER – WENIGER HÄUFIGER ZUGRIFF:*** *Bietet der Cloud-Anbieter eine Stufe für Daten, auf die seltener zugegriffen wird, die aber dennoch einen schnellen Zugriff erfordern?*
12.	***OBJEKTSPEICHER – OBJEKTSTAFFELUNG:*** *Bietet der Cloud-Anbieter eine Funktion zur Objektspeicher-Staffelung, d. h. die Möglichkeit, eine Empfehlung darüber auszusprechen, ein Objekt basierend auf seiner Zugriffshäufigkeit zwischen Objektspeicherklassen oder Stufen zu verschieben?*
13.	***OBJEKTSPEICHER – LEBENSZYKLUSVERWALTUNG:*** *Unterstützt der Cloud-Anbieter die Verwaltung des Lebenszyklus eines Objekts mithilfe einer Lebenszykluskonfiguration, die definiert, wie Objekte während ihrer Lebensdauer von der Erstellung bis zur Löschung verwaltet werden?*
14.	***OBJEKTSPEICHER – RICHTLINIENGESTEUERTE VERWALTUNG:*** *Bietet der Cloud-Anbieter die Möglichkeit, Richtlinien zur Verwaltung gespeicherter Daten, ihres Lebenszyklus und ihrer Stufeneinstellungen zu erstellen und zu verwenden?*

15.	*OBJEKTSPEICHER – STANDORT- UND ZEITBASIERTE RICHTLINIEN:* *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, Richtlinien zu erstellen, die den Zugriff auf Daten auf Grundlage des Standorts des Benutzers und der Zugriffszeit einschränken können?*
16.	*OBJEKTSPEICHER – WEBSITE-HOSTING:* *Unterstützt der Cloud-Anbieter das Hosten statischer Websites aus seinem Objektspeicherservice?*
17.	*OBJEKTSPEICHER – VERSCHLÜSSELUNG IM RUHEZUSTAND:* *Unterstützt der Cloud-Anbieter die serverseitige Verschlüsselung (SSE, Server-Side Encryption) von Daten im Ruhezustand, wobei er die Verschlüsselungsschlüssel verwaltet?* • *Wenn ja, welcher kryptografische Algorithmus wird eingesetzt?*
18.	*OBJEKTSPEICHER – VERSCHLÜSSELUNG MIT BENUTZERSCHLÜSSELN:* *Bietet der Cloud-Anbieter serverseitige Verschlüsselungsfunktionen mit vom Kunden bereitgestellten kryptografischen Schlüsseln an?*
19.	*OBJEKTSPEICHER – MANAGED SERVICE FÜR SCHLÜSSEL:* *Unterstützt der Cloud-Anbieter die serverseitige Verschlüsselung mithilfe eines Schlüsselverwaltungsservices, der Verschlüsselungsschlüssel erstellt, Richtlinien definiert, die steuern, wie Schlüssel verwendet werden können, und die Schlüsselverwendung prüft, um nachzuweisen, dass sie korrekt verwendet werden?*
20.	*OBJEKTSPEICHER – CLIENTSEITIGER MASTERSCHLÜSSEL:* *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, die Kontrolle über die Verschlüsselungsschlüssel zu behalten und die Verschlüsselung/Entschlüsselung von Objekten auf Clientseite durchzuführen?*
21.	*OBJEKTSPEICHER – HOHE KONSISTENZ:* *Unterstützt der Cloud-Anbieter die Read-after-Write-Konsistenz für PUT-Vorgänge bei neuen Objekten?*
22.	*OBJEKTSPEICHER – DATENLOKALITÄT:* *Bietet der Cloud-Anbieter eine starke regionale Isolierung, sodass Objekte, die in einer Region gespeichert sind, die Region niemals verlassen, es sei denn, der Benutzer überträgt sie explizit in eine andere Region?*
23.	*OBJEKTSPEICHER – REPLIKATION:* *Bietet der Cloud-Anbieter eine regionsübergreifende Replikationsfunktion, mit der Objekte automatisch über vom Benutzer ausgewählte Regionen hinweg repliziert werden?*
24.	*OBJEKTSPEICHER – VERSIONING:* *Unterstützt der Cloud-Anbieter das Versioning, d. h. die Möglichkeit, mehrere Versionen eines Objekts zu speichern und zu verwalten?*
25.	*OBJEKTSPEICHER – MARKIERUNG VON ELEMENTEN ALS UNLÖSCHBAR:* *Erlaubt der Cloud-Anbieter einem Benutzer, ein Element als nicht löschbar zu markieren?*
26.	*OBJEKTSPEICHER – LÖSCHEN MIT MFA:* *Unterstützt der Cloud-Anbieter Multi-Faktor-Authentifizierung (MFA, Multi-Factor Authentication) als zusätzliche Sicherheitsoption für Löschvorgänge?*
27.	*OBJEKTSPEICHER – MEHRTEILIGE UPLOADS:* *Ermöglicht der Cloud-Anbieter das Hochladen eines Objekts in mehreren Teilen, wobei jeder Teil ein zusammenhängender Abschnitt der Objektdaten ist und diese Objektteile unabhängig und in beliebiger Reihenfolge hochgeladen werden können?*

28.	*OBJEKTSPEICHER – TAGS:* *Bietet der Cloud-Anbieter die Möglichkeit, veränderbare, dynamische Tags auf Objektebene zu erstellen und zuzuordnen?*
29.	*OBJEKTSPEICHER – BENACHRICHTIGUNGEN:* *Bietet der Cloud-Anbieter die Möglichkeit, Benachrichtigungen zu senden, wenn bestimmte Ereignisse auf Objektebene stattfinden (d. h. Hinzufügungs-/Löschvorgänge)?*
30.	*OBJEKTSPEICHER – PROTOKOLLE:* *Bietet der Cloud-Anbieter die Möglichkeit, Audit-Protokolle zu erstellen, die Details zu einer einzelnen Zugriffsanfrage enthalten, z. B. den Anforderer, die Anfragezeit, die Anfrageaktion, den Antwortstatus und den Fehlercode?*
31.	*OBJEKTSPEICHER – INVENTORY FÜR OBJEKTE:* *Bietet der Cloud-Anbieter Inventory-Funktionen, mit denen Benutzer Objekte und deren Status schnell visualisieren können, sodass die Benutzer Objekte mit öffentlichem Zugriff schnell erkennen können?*
32.	*OBJEKTSPEICHER – INVENTORY FÜR METADATEN:* *Bietet der Cloud-Anbieter Inventory-Funktionen, mit denen Benutzer die Metadaten von Objekten schnell visualisieren können?*
33.	*OBJEKTSPEICHER – OPTIMIERTES HOCHLADEN:* *Hat der Cloud-Anbieter die Möglichkeit, Daten mithilfe eines optimierten Netzwerkpfads von Edge-Standorten zum Speicherservice weiterzuleiten?*
34.	*OBJEKTSPEICHER – ABFRAGEFÄHIGKEIT:* *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, seinen Objektspeicherservice mithilfe von SQL-Anweisungen (Structured Query Language) abzufragen?*
35.	*OBJEKTSPEICHER – ABRUFEN VON TEILMENGEN:* *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, mithilfe einfacher SQL-Ausdrücke nur eine Teilmenge von Daten aus einem Objekt abzurufen?*
36.	*DATEISPEICHERSERVICE:* *Bietet der Cloud-Anbieter einen einfachen und skalierbaren Dateispeicherservice für die Verwendung mit Datenverarbeitungs-Instances in der Cloud?*
37.	*DATEISPEICHER – REDUNDANZ:* *Speichert der Cloud-Anbieter die Dateisystemobjekte (z. B. Verzeichnis, Datei und Link) redundant über mehrere Rechenzentren oder Einrichtungen hinweg, um eine höhere Verfügbarkeit und Beständigkeit zu erreichen?*
38.	*DATEISPEICHER – VOLLSTÄNDIGE DATENLÖSCHUNG:* *Unterstützt der Cloud-Anbieter die vollständige Löschung von Dateispeicherdaten, sodass diese nicht mehr lesbar sind oder nicht mehr für nicht autorisierte Benutzer oder Dritte zugänglich sind?*
39.	*DATEISPEICHER – HOHE VERFÜGBARKEIT:* *Bietet das vom Cloud-Anbieter verwaltete Dateisystem ein hohes Maß an Hochverfügbarkeit?*
40.	*DATEISPEICHER – NFS:* *Unterstützt der Cloud-Anbieter das NFS-Protokoll (Network File System)?*
41.	*DATEISPEICHER – SMB:* *Unterstützt der Cloud-Anbieter das SMB-Protokoll (Server Message Block)?*

42.	*DATEISPEICHER – VERSCHLÜSSELUNG IM RUHEZUSTAND:* *Unterstützt der Dateispeicherservice des Cloud-Anbieters die Verschlüsselung im Ruhezustand?*
43.	*DATEISPEICHER – VERSCHLÜSSELUNG WÄHREND DER ÜBERTRAGUNG:* *Unterstützt der Dateispeicherservice des Cloud-Anbieters die Verschlüsselung von Daten während der Übertragung?*
44.	*DATEISPEICHER – DATENMIGRATIONSTOOL:* *Bietet der Cloud-Anbieter ein Datenmigrationstool, mit dem Benutzer Daten von lokalen Systemen in das cloudbasierte Dateisystem verschieben können?*
45.	*ARCHIVSPEICHERSERVICE:* *Bietet der Cloud-Anbieter einen sehr kostengünstigen Speicherservice an, der auf die Archivierung von weniger häufig abgerufenen und nahezu unveränderbaren Objekten und Dateien abzielt?*
46.	*ARCHIVSPEICHER – FEHLERTOLERANZ:* *Bietet die Architektur des Cloud-Anbieters Fehlertoleranz für seinen Archivspeicherservice?*
47.	*ARCHIVSPEICHER – UNVERÄNDERBARKEIT:* *Unterstützt der Cloud-Anbieter die Unveränderbarkeit der archivierten Objekte und Dateien?*
48.	*ARCHIVSPEICHER – WORM:* *Bietet der Cloud-Anbieter WORM-Funktionen (Write Once, Read Many)?*
49.	*ARCHIVSPEICHER – ABRUF VON TEILMENGEN:* *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, mithilfe einfacher SQL-Ausdrücke nur eine Teilmenge von Daten aus einem archivierten Objekt abzurufen?*
50.	*ARCHIVSPEICHER – SCHNELLERES ABRUFEN:* *Bietet der Cloud-Anbieter Benutzern mehrere Optionen für den Datenabruf, mit jeweils unterschiedlichen Kosten und Abrufzeiten?*
51.	*ARCHIVSPEICHER – VERSCHLÜSSELUNG IM RUHEZUSTAND:* *Unterstützt der Archivspeicherservice des Cloud-Anbieters die Verschlüsselung im Ruhezustand?*
52.	*SPEICHER – SERVICE-LIMITS:* *Unterliegt der Cloud-Anbieter jeglichen Einschränkungen (d. h. Service-Limits) in Bezug auf den oben aufgeführten Abschnitt zum Thema Speicher?* *Beispiel:* *Maximale Volume-Größe* *Maximale Anzahl an Laufwerken, die an eine Instance angehängt sind* *Maximale Eingabe-/Ausgabevorgänge pro Sekunde (IOPS)* *Maximale Objektgröße* *Maximale Anzahl von Objekten pro Speicherkonto* *Maximale Anzahl von Snapshots*

4. Administration

	Anforderung
1.	***ADMINISTRATION – BENUTZER UND GRUPPEN:*** *Bietet der Cloud-Anbieter einen Service zur Erstellung und Verwaltung von Benutzern und Gruppen von Benutzern seiner Infrastruktur und seiner Ressourcen?*
2.	***ADMINISTRATION – PASSWORT ZURÜCKSETZEN:*** *Erlaubt der Cloud-Anbieter Benutzern, ihr eigenes Passwort in einem Self-Service-Verfahren zurückzusetzen?*
3.	***ADMINISTRATION – BERECHTIGUNGEN:*** *Bietet der Cloud-Anbieter die Möglichkeit, Benutzern und Gruppen auf Ressourcenebene Berechtigungen hinzuzufügen?*
4.	***ADMINISTRATION – TEMPORÄRE BERECHTIGUNGEN:*** *Bietet der Cloud-Anbieter die Möglichkeit, Berechtigungen zu erstellen, die für ein bestimmtes Zeitintervall gültig sind?*
5.	***ADMINISTRATION – TEMPORÄRE ANMELDEDATEN:*** *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, temporäre sichere Anmeldedaten für vertrauenswürdige Benutzer zu erstellen und bereitzustellen, die für eine Dauer von wenigen Minuten bis zu mehreren Stunden konfiguriert sind?*
6.	***ADMINISTRATION – ZUGRIFFSKONTROLLE:*** *Bietet der Cloud-Anbieter detaillierte Zugriffskontrollen für seine Infrastrukturressourcen?* • *Wenn ja, welche Bedingungen können von diesen Kontrollen genutzt werden (z. B. Tageszeit, ursprüngliche IP-Adresse usw.)?*
7.	***ADMINISTRATION – INTEGRIERTE RICHTLINIEN:*** *Enthält die Infrastruktur des Cloud-Anbieters integrierte Richtlinien zur Zugriffskontrolle, die Benutzern und Gruppen hinzugefügt werden können?*
8.	***ADMINISTRATION – BENUTZERDEFINIERTE RICHTLINIEN:*** *Ermöglicht die Infrastruktur des Cloud-Anbieters die Erstellung und Anpassung von Zugriffskontrollrichtlinien, die Benutzern und Gruppen hinzugefügt werden können?*
9.	***ADMINISTRATION – RICHTLINIENSIMULATOR:*** *Bietet der Cloud-Anbieter einen Mechanismus zum Testen der Auswirkungen von Zugriffskontrollrichtlinien, bevor diese Richtlinien in die Produktion übernommen werden?*
10.	***ADMINISTRATION – CLOUD-MFA:*** *Unterstützt der Cloud-Anbieter die Verwendung der Multi-Faktor-Authentifizierung als zusätzliche Ebene der Zugriffskontrolle und Authentifizierung für seine Infrastruktur?*
11.	***ADMINISTRATION – SERVICE-LIMITS:*** *Unterliegt der Cloud-Anbieter jeglichen Einschränkungen (d. h. Service-Limits) in Bezug auf den oben aufgeführten Abschnitt zum Thema Administration?* *Beispiel:* *Maximale Anzahl der Benutzer* *Maximale Anzahl der Gruppen* *Maximale Anzahl verwalteter Richtlinien*

5. Sicherheit

	Anforderung
1.	***SICHERHEIT – HINTERGRUNDPRÜFUNGEN:*** *Werden alle Mitarbeiter des Cloud-Anbieters, die Zugang zur Serviceinfrastruktur haben (physisch oder nicht physisch), Hintergrundprüfungen unterzogen?*
2.	***SICHERHEIT – PHYSISCHER ZUGANG:*** *Schränkt der Cloud-Anbieter den Zugriff von Mitarbeitern auf die Serviceinfrastruktur ein, es sei denn, es gibt ein bestimmtes Problemticket, eine Änderungsanfrage oder eine ähnliche formale Autorisierung?*
3.	***SICHERHEIT – ZUGRIFFSPROTOKOLLE:*** *Protokolliert der Cloud-Anbieter Mitarbeiterzugriff über seine Infrastruktur, wobei dieser Zugriff immer protokolliert wird und Protokolle mindestens 90 Tage aufbewahrt werden?*
4.	***SICHERHEIT – HOST-ANMELDUNGEN:*** *Schränkt der Cloud-Anbieter die Anmeldung seiner Mitarbeiter bei Datenverarbeitungs-Hosts ein und automatisiert stattdessen alle Aufgaben, die auf dem Datenverarbeitungs-Host ausgeführt werden, wobei die Inhalte dieser automatisierten Jobs protokolliert und die Protokolle mindestens 90 Tage aufbewahrt werden?*
5.	***SICHERHEIT – KRYPTOGRAFISCHE SCHLÜSSEL:*** *Bietet der Cloud-Anbieter einen Service zur Erstellung und Steuerung der kryptografischen Schlüssel, die zur Verschlüsselung von Benutzerdaten verwendet werden?*
6.	***SICHERHEIT – VERWALTUNG VON ZUGRIFFSSCHLÜSSELN:*** *Bietet der Cloud-Anbieter die Möglichkeit, zu bestimmen, wann ein Zugriffsschlüssel zuletzt verwendet wurde, alte Schlüssel zu rotieren und inaktive Benutzer zu entfernen?*
7.	***SICHERHEIT – VOM KUNDEN BEREITGESTELLTE SCHLÜSSEL:*** *Ermöglicht der Cloud-Anbieter Benutzern den Import von Schlüsseln aus der eigenen Schlüsselverwaltungsinfrastruktur in den Schlüsselverwaltungsservice des Cloud-Service-Anbieters?*
8.	***SICHERHEIT – INTEGRATION DES SERVICES FÜR KRYPTOGRAFISCHE SCHLÜSSEL:*** *Lässt sich der Schlüsselverwaltungsservice des Cloud-Anbieters in andere Cloud-Services integrieren, um Verschlüsselungsfunktionen für Daten im Ruhezustand bereitzustellen?*
9.	***SICHERHEIT – HSM:*** *Bietet der Cloud-Anbieter dedizierte Hardware-Sicherheitsmodule (HSM), d. h. Hardware-Appliances, die sichere Schlüsselspeicherung und kryptografische Prozesse innerhalb eines manipulationssicheren Hardwaremoduls bereitstellen?*
10.	***SICHERHEIT – BESTÄNDIGKEIT KRYPTOGRAFISCHER SCHLÜSSEL:*** *Unterstützt der Cloud-Anbieter die Beständigkeit von Schlüsseln, einschließlich der Speicherung mehrerer Kopien, damit Schlüssel bei Bedarf verfügbar sind?*
11.	***SICHERHEIT – SSO:*** *Bietet der Cloud-Anbieter einen verwalteten SSO-Service (Single Sign-on), mit dem Benutzer den Zugriff auf mehrere Konten und Geschäftsanwendungen zentral verwalten können?*
12.	***SICHERHEIT – ZERTIFIKATE:*** *Bietet der Cloud-Anbieter einen Managed Service für die Bereitstellung und Verwaltung von SSL-/TLS-Zertifikaten (Secure Sockets Layer / Transport Layer Security)?*

13.	*SICHERHEIT – ERNEUERUNG VON ZERTIFIKATEN:* *Ermöglicht der Zertifikatverwaltungsdienst des Cloud-Anbieters die Erneuerung von Zertifikaten?*
14.	*SICHERHEIT – PLATZHALTERZERTIFIKATE:* *Unterstützt der Zertifikatverwaltungsdienst des Cloud-Anbieters die Verwendung von Platzhalterzertifikaten?*
15.	*SICHERHEIT – ZERTIFIZIERUNGSSTELLE:* *Fungiert der Zertifikatverwaltungsdienst des Cloud-Anbieters auch als Zertifizierungsstelle (CA, Certificate Authority)?*
16.	*SICHERHEIT – ACTIVE DIRECTORY:* *Bietet der Cloud-Anbieter einen verwalteten Microsoft Active Directory-Service (AD-Service) in der Cloud an?*
17.	*SICHERHEIT – LOKALES ACTIVE DIRECTORY:* *Unterstützt der verwaltete Microsoft Active Directory-Service des Cloud-Anbieters die Integration in lokales Microsoft Active Directory (AD) vor Ort?*
18.	*SICHERHEIT – LDAP:* *Unterstützt der verwaltete Microsoft Active Directory-Service des Cloud-Anbieters das Lightweight Directory Access Protocol (LDAP)?*
19.	*SICHERHEIT – ACTIVE DIRECTORY:* *Unterstützt der verwaltete Microsoft Active Directory-Service des Cloud-Anbieters die Security Assertation Markup Language (SAML)?*
20.	*SICHERHEIT – MANAGEMENT VON ANMELDEINFORMATIONEN:* *Bietet der Cloud-Anbieter einen Managed Service, mit dem Benutzer Anmeldeinformationen wie API-Schlüssel, Datenbank-Anmeldeinformationen und andere Secrets einfach rotieren, verwalten und abrufen können?*
21.	*SICHERHEIT – WAF:* *Bietet der Cloud-Anbieter eine Webanwendungs-Firewall (WAF), die Webanwendungen vor gängigen Internet-Bedrohungen schützt, die sich auf die Anwendungsverfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen verbrauchen könnten?*
22.	*SICHERHEIT – DDOS:* *Bietet der Cloud-Anbieter einen Service zum Schutz vor gängigen, am häufigsten auftretenden DDoS-Angriffen (Distributed Denial of Service) auf Netzwerk- und Transportebene sowie die Möglichkeit, benutzerdefinierte Regeln zu schreiben, um komplexe Angriffe auf Anwendungsebene zu mindern?*
23.	*SICHERHEIT – SICHERHEITSEMPFEHLUNGEN:* *Bietet der Cloud-Anbieter einen Service zur automatischen Bewertung potenzieller Schwachstellen in Anwendungen und Ressourcen?*
24.	*SICHERHEIT – BEDROHUNGSERKENNUNG:* *Bietet der Cloud-Anbieter einen verwalteten Service zur Erkennung von Bedrohungen?*
25.	*SICHERHEIT – SERVICE-LIMITS:* *Unterliegt der Cloud-Anbieter jeglichen Einschränkungen (d. h. Service-Limits) in Bezug auf den oben aufgeführten Abschnitt zum Thema Sicherheit?* *Beispiel:* *Maximale Anzahl der Kunden-Masterschlüssel* *Maximale Anzahl von Hardwaresicherheitsmodulen (HSMs)*

6. Compliance

Die folgende Liste dient nur zur Veranschaulichung und soll nicht als erschöpfend für die Zertifizierungen und Standards angesehen werden, die für Cloud-Services gelten können.

Bitte geben Sie an, welche internationalen und branchenspezifischen Compliance-Standards der Cloud-Anbieter erfüllt hat:

Zertifizierungen/Bescheinigungen	*Gesetze, Vorschriften und Datenschutz*	*Ausrichtungen/Rahmenbedingungen*
☐ *C5 [Deutschland]*	☐ *EU-Datenschutzrichtlinie*	☐ *CDSA*
☐ *CISPE-Verhaltenskodex zum Datenschutz*	☐ *EU-Modellklauseln*	
☐ *CNDCP (Climate Neutral Data Centre Pact)*		
☐ *DIACAP*	☐ *FERPA*	☐ *CIS*
☐ *DoD SRG Level 2 und 4*	☐ *DSGVO*	☐ *Informationen zur Strafgerichtsbarkeit. Service (CJIS)*
☐ *FedRAMP*	☐ *GLBA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *HIPAA*	☐ *EU-US-Datenschutzschild*
☐ *HDS (Frankreich, Gesundheitswesen)*	☐ *HITECH*	☐ *EU „Safe Harbor"*
☐ *ISO 9001*	☐ *IRS 1075*	☐ *FISC*
☐ *ISO 27001*	☐ *ITAR*	☐ *FISMA*
☐ *ISO 27017*	☐ *PDPA – 2010 [Malaysia]*	☐ *G-Cloud [UK]*
☐ *ISO 27018*	☐ *PDPA – 2012 [Singapur]*	☐ *GxP (FDA CFR 21 Teil 11)*
☐ *IRAP [Australien]*	☐ *PIPEDA [Kanada]*	☐ *ICREA*
☐ *MTCS Tier 3 [Singapur]*	☐ *Privacy Act [Australien]*	☐ *IT-Grundschutz [Deutschland]*
☐ *PCI DSS Stufe 1*	☐ *Privacy Act [Neuseeland]*	☐ *MARS – E*
☐ *SEC Rule 17-a-4(f)*	☐ *Spanische DPA-Autorisierung*	☐ *MITA 3.0*
☐ *SOC1/ISAE 3402*	☐ *U.K. DPA – 1988*	☐ *MPAA*
☐ *SOC2/SOC3*	☐ *VPAT/Abschnitt 508*	☐ *NIST*
☐ *SWIPO IaaS Code*		
		☐ *Uptime Institute Tiers*
		☐ *UK-Cloud-Sicherheitsrichtlinien*

Durch die Nutzung der oben genannten Compliance-Berichte können Organisationen des öffentlichen Sektors einzigartige Angebote im Hinblick auf anerkannte Sicherheits-, Compliance- und Betriebsstandards auswerten. Solche Berichte können zeigen, dass der CISP aufgrund seiner Compliance mit ihnen die unten aufgeführten Betriebskontrollen für Rechenzentren erfüllt, die von einem Public-Cloud-Service-Anbieter gefordert werden. Indem Konformität mit solchen Berichten gefordert wird, können Einrichtungen des öffentlichen Sektors sicherstellen, dass die unten aufgeführten Kontrollen vorhanden sind.

- ***Geprüfter Zugang:*** *Der CISP sollte den physischen Zugang auf Personen beschränken, die aus berechtigten geschäftlichen Gründen an einem Standort sein müssen. Wenn der Zugang gewährt wird, sollte er widerrufen werden, sobald die erforderlichen Arbeiten abgeschlossen sind.*

- ***Zutrittskontrolle und -überwachung:*** *Das Betreten des Umfelds des physischen Rechenzentrums sollte ein kontrollierter Prozess sein. Der CISP sollte an den Zugangstoren Sicherheitskräfte einsetzen, die ebenso wie die Besucher durch Aufsichtspersonal über Sicherheitskameras überwacht werden. Wenn genehmigte Personen vor Ort sind, sollten sie einen Ausweis erhalten, der eine Multi-Faktor-Authentifizierung erfordert und den Zugang auf vorab genehmigte Bereiche beschränkt.*

- ***CISP-Mitarbeiter in Rechenzentren:*** *CISP-Mitarbeiter, die regelmäßig Zugang zu einem Rechenzentrum benötigen, sollten entsprechend ihrer Tätigkeit Berechtigungen für relevante Bereiche der Einrichtung erhalten, wobei der Zugang regelmäßig geprüft wird. Mitarbeiterlisten sollten regelmäßig von einem zuständigen Bereichsleiter überprüft werden, um sicherzustellen, dass die Autorisierung jedes Mitarbeiters weiterhin erforderlich ist. Wenn ein Mitarbeiter keine andauernden geschäftlichen Gründe hat, sich in einem Rechenzentrum aufzuhalten, sollte er den Besucherprozess zu durchlaufen.*

- ***Überwachung auf unberechtigten Zutritt:*** *CISPs sollten kontinuierlich das Grundstück des Rechenzentrums auf unberechtigten Zugang überwachen. Dazu werden System für Videoüberwachung, Einbruchmeldung und Zugriffsprotokollüberwachung verwendet. Eingänge sollten mit Vorrichtungen gesichert werden, die Alarme auslösen, wenn eine Tür gewaltsam geöffnet oder offengehalten wird.*

- ***CISP Security Operations Center überwachen die globale Sicherheit:*** *CISP Security Operations Center sollten global verteilt sein und für die Überwachung, Triage und die Ausführung von Sicherheitsprogrammen für CISP-Rechenzentren verantwortlich sein. Die Center sollten die Verwaltung des physischen Zugriffs und die Reaktion auf Einbruchversuche überwachen und gleichzeitig den Sicherheitsteams des Rechenzentrums vor Ort rund um die Uhr globalen Support bieten. Sie sollten kontinuierliche Überwachungsaktivitäten wie die Verfolgung von Zugriffsaktivitäten und das Widerrufen von Zugriffsberechtigungen bereitstellen und für die Reaktion auf und Analyse von potenziellen Sicherheitsvorfällen verfügbar sein.*

- ***Zugriffsüberprüfung auf mehreren Ebenen:*** *Der Zugriff auf die Infrastrukturebene sollte je nach geschäftlichen Anforderungen eingeschränkt werden. Durch die Implementierung einer Zugriffsüberprüfung auf mehreren Ebenen wird niemandem ein standardmäßiges Recht gewährt, auf jede Ebene zuzugreifen. Der Zugriff auf eine bestimmte Ebene sollte nur gewährt werden, wenn ein bestimmter Bedarf für den Zugriff auf diese bestimmte Ebene besteht.*

- ***Die Wartung der Geräte ist Teil des regulären Betriebs:*** *CISP-Teams sollten Diagnosen an Computern, Netzwerken und Backup-Geräten durchführen, um sicherzustellen, dass sie jetzt und im Notfall ordnungsgemäß funktionieren. Routinemäßige Wartungsprüfungen an den Geräten und Einrichtungen des Rechenzentrums sollten Teil des regulären CISP-Rechenzentrumsbetriebs sein.*

- ***Notfall-Backup-Geräte:*** *Wasser-, Strom-, Telekommunikations- und Internetverbindungen sollten redundant ausgelegt sein, damit der CISP im Notfall den kontinuierlichen Betrieb aufrechterhalten kann. Elektrische Stromversorgungssysteme sollten so ausgelegt sein, dass sie vollständig redundant sind, damit im Falle einer Störung unterbrechungsfreie Stromversorgungen für bestimmte Funktionen aktiviert werden können, während Generatoren für die gesamte Anlage eine Notstromversorgung bereitstellen. Personen und Systeme sollten die Temperatur und Luftfeuchtigkeit überwachen und kontrollieren, um eine Überhitzung zu vermeiden und mögliche Serviceausfälle weiter zu reduzieren.*

- ***Technologie und Mitarbeiter arbeiten zusammen, um die Sicherheit zu erhöhen:*** *Es sollten obligatorische Verfahren vorhanden sein, um die Autorisierung für den Zugriff auf die Datenebene zu erhalten. Dazu gehören auch die Überprüfung und Genehmigung von Zugriffsanträgen einer Person durch autorisierte Mitarbeiter. Gleichzeitig sollten Systeme zur Erkennung von Bedrohungen und elektronischen Eindringversuchen zur Überwachung*

eingesetzt werden und automatisch Warnungen zu erkannten Bedrohungen oder verdächtigen Aktivitäten auslösen. Wenn beispielsweise eine Tür aufgehalten oder gewaltsam geöffnet wird, wird ein Alarm ausgelöst. CISPs sollten Überwachungskameras einsetzen und die Aufnahmen gemäß den gesetzlichen und Compliance-Anforderungen aufbewahren.

- *Schutz vor physischen und elektronischen Eindringversuchen: Zugangspunkte zu Serverräumen sollten mit elektronischen Kontrollgeräten gesichert werden, die eine Multi-Faktor-Autorisierung erfordern. Der CISP sollte auch darauf vorbereitet sein, ein elektronisches Eindringen zu verhindern. CISP-Server sollten Mitarbeiter warnen können, wenn Versuche unternommen werden, Daten zu entfernen. Im unwahrscheinlichen Fall eines Verstoßes sollte der Server automatisch deaktiviert werden.*

- *Server und Medien werden mit peinlich genauer Aufmerksamkeit behandelt: Medienspeichergeräte, die zum Speichern von Kundendaten verwendet werden, sollten vom CISP als kritisch eingestuft und während ihres gesamten Lebenszyklus entsprechend mit höchster Umsicht behandelt werden. Der CISP sollte genaue Standards für die Installation, Wartung und schlussendlich für die Vernichtung der Geräte haben, wenn diese nicht mehr benötigt werden. Wenn ein Speichergerät das Ende seiner Nutzungsdauer erreicht hat, deaktiviert der CISP Medien mithilfe der in NIST 800-88 beschriebenen Verfahren. Medien, auf denen Kundendaten gespeichert sind, werden erst aus der Kontrolle des CISP entlassen, wenn sie sicher außer Betrieb genommen wurden.*

- *Unabhängige Prüfer verifizieren die CISP-Verfahren und -Systeme: CISPs sollten von externen Prüfern verifiziert werden, die die Rechenzentren inspizieren. Dabei muss eingehend geprüft werden, ob der CISP die für die Sicherheitszertifizierung erforderlichen festgelegten Regeln einhält. Je nach Compliance-Programm und dessen Anforderungen können externe Prüfer mit CISP-Mitarbeitern darüber sprechen, wie sie Medien handhaben und entsorgen. Prüfer können auch das Bildmaterial von Überwachungskameras kontrollieren und sich Eingänge und Korridore im gesamten Rechenzentrum ansehen. Und sie können die Ausrüstung begutachten, etwa die elektronischen Zutrittskontrollgeräte und Überwachungskameras von CISPs.*

- *Auf das Unerwartete vorbereitet: Der CISP sollte sich proaktiv auf potenzielle Umweltbedrohungen wie Naturkatastrophen und Brände vorbereiten. Die Installation von automatischen Sensoren und reaktionsfähigen Geräten sind zwei Möglichkeiten, wie der CISP Rechenzentren schützen kann. Wassermelder sollten installiert werden, um die Mitarbeiter auf Probleme aufmerksam zu machen. Zudem können automatische Pumpen dabei helfen, Flüssigkeiten zu entfernen und Schäden zu verhindern. In ähnlicher Weise reduzieren automatische Feuermelde- und -löschvorrichtungen das Risiko und können CISP-Mitarbeiter und Feuerwehrleute über ein Problem benachrichtigen.*

- *Hohe Verfügbarkeit über mehrere Availability Zones: Der CISP sollte mehrere Availability Zones bereitstellen, um eine höhere Fehlertoleranz zu erreichen. Jede Availability Zone sollte aus einem oder mehreren Rechenzentren bestehen, physisch von den anderen getrennt sein und über redundante Stromversorgung und Netzwerke verfügen. Availability Zones sollten über ein schnelles, privates Glasfasernetzwerk miteinander verbunden sein, um Anwendungen zu entwickeln, die automatisch und ohne Unterbrechung zwischen Availability Zones ein Failover ausführen.*

- *Störungssimulation und Reaktionsmessung: Der CISP sollte einen Betriebskontinuitätsplan als Prozessleitfaden haben, in dem erläutert wird, wie Störungen aufgrund von Naturkatastrophen vermieden und reduziert werden können. Darin sollte auf die detaillierten Schritte eingegangen werden, die vor, während und nach einem Ereignis ausgeführt werden. Um sich möglichst gut auf unerwartete Ereignisse vorzubereiten, sollte der CISP den Betriebskontinuitätsplan regelmäßig mit Übungen testen, die verschiedene Szenarien simulieren. Der CISP sollte dokumentieren, wie seine Mitarbeiter und Prozesse abschneiden, und anschließend die Erfahrungen und Korrekturmaßnahmen besprechen, die zur Verbesserung der Reaktionsrate erforderlich sind. Die CISP-Mitarbeiter sollten geschult werden und in der Lage sein, schnell auf Unterbrechungen zu reagieren. Dabei sollte ein methodischer Wiederherstellungsprozess verwendet werden, um weitere Ausfallzeiten aufgrund von Fehlern zu minimieren.*

- *Unterstützung beim Erreichen von Effizienzzielen: Neben dem Umgang mit Umweltrisiken sollte der CISP auch Überlegungen zur Nachhaltigkeit in die Bauweise von Rechenzentren einbeziehen. Der CISP sollte angeben, wie er seine Verpflichtung zur Nutzung erneuerbarer Energien für seine Rechenzentren umsetzt, und Informationen darüber bereitstellen, wie Kunden CO2-Emissionen im Vergleich zu ihren eigenen Rechenzentren reduzieren können.*

- *Standortauswahl: Vor der Auswahl eines Standorts sollte der CISP erste ökologische und geografische Bewertungen durchführen. Rechenzentrumsstandorte sollten sorgfältig ausgewählt werden, um Umweltrisiken wie*

Überschwemmungen, extreme Wetterbedingungen und seismische Aktivitäten gering zu halten. Availability Zones von CISPs sollten voneinander unabhängig und physisch getrennt sein.

- ***Redundanz:*** *Rechenzentren sollten so ausgelegt sein, dass Ausfälle antizipiert und toleriert werden können, wobei die Service-Level aufrechterhalten werden. Bei einem Ausfall sollten automatisierte Prozesse den Datenverkehr aus dem betroffenen Bereich entfernen. Die Kernanwendungen sollten nach einem N+1-Standard bereitgestellt werden, sodass bei Auftreten eines Rechenzentrumsausfalls ausreichend Kapazität vorhanden ist, um den Datenverkehr per Load Balancing an die verbleibenden Standorte zu leiten.*

- ***Verfügbarkeit:*** *Der CISP sollte kritische Systemkomponenten identifizieren, die zur Aufrechterhaltung der Verfügbarkeit des Systems und, bei Auftreten eines Ausfalls, zur Wiederherstellung des Services erforderlich sind. Kritische Systemkomponenten sollten über mehrere isolierte Standorte hinweg gesichert werden. Alle Standorte oder Availability Zones sollten so ausgelegt sein, dass sie unabhängig und mit hoher Zuverlässigkeit arbeiten. Availability Zones sollten verbunden werden, damit Anwendungen ohne Unterbrechung ein automatisches Failover zwischen Availability Zones durchführen können. Hochgradig ausfallsichere Systeme und folglich die Serviceverfügbarkeit sollten ein Zweck des Systemdesigns sein. Die Ausführung des Rechenzentrums mit Availability Zones und Datenreplikation sollte es CISP-Kunden ermöglichen, extrem kurze Recovery Time Objectives und Recovery Point Objectives sowie ein Höchstmaß an Serviceverfügbarkeit zu erreichen.*

- ***Kapazitätsplanung****: Der CISP sollte die Servicenutzung kontinuierlich überwachen, um die notwendige Infrastruktur bereitzustellen und so die Zusagen und Anforderungen hinsichtlich der Verfügbarkeit zu erreichen. Der CISP sollte ein Modell zur Kapazitätsplanung unterhalten, das die Nutzung und den Bedarf der CISP-Infrastruktur mindestens monatlich bewertet. Dieses Modell sollte die Planung zukünftiger Anforderungen unterstützen und Überlegungen wie Informationsverarbeitung, Telekommunikation und Audit-Protokollspeicherung enthalten.*

BETRIEBSKONTINUITÄT UND NOTFALLWIEDERHERSTELLUNG

- ***Betriebskontinuitätsplan:*** *Der CISP-Plan zur Aufrechterhaltung der Betriebskontinuität sollte Maßnahmen zur Vermeidung und Verringerung von Umweltstörungen enthalten. Er sollte operative Details zu den vor, während und nach einem Ereignis einzuleitenden Schritten enthalten. Der Betriebskontinuitätsplan sollte durch Tests unterstützt werden, die Simulationen verschiedener Szenarien einschließen. Während und nach den Tests sollte der CISP die Mitarbeiter- und Prozessleistung, Korrekturmaßnahmen und Erfahrungen dokumentieren, um kontinuierliche Verbesserungen zu erzielen.*

- ***Pandemieschutz:*** *Der CISP sollte Richtlinien und Verfahren zur Reaktion auf eine Pandemie in seine Notfallwiederherstellungsplanung integrieren, um schnell auf Bedrohungen durch den Ausbruch von Infektionskrankheiten reagieren zu können. Strategien zur Risikominderung umfassen alternative Personalmodelle zur Übertragung kritischer Prozesse auf Ressourcen außerhalb der Region sowie die Aktivierung eines Krisenmanagementplans zur Unterstützung entscheidender Geschäftsabläufe. Pandemiepläne sollten auf internationale Gesundheitsbehörden und Vorschriften verweisen, einschließlich Kontaktstellen für internationale Behörden.*

ÜBERWACHUNG und PROTOKOLLIERUNG

- ***Zugangsprüfung für Rechenzentren:*** *Der Zugang zu Rechenzentren sollte regelmäßig geprüft werden. Zugangsrechte sollten automatisch widerrufen werden, wenn die Personalakte eines Mitarbeiters im Personalverwaltungssystem des CISP gelöscht wird. Wenn die Zugangsrechte eines Mitarbeiters oder Auftragnehmers gemäß der genehmigten Antragsdauer ablaufen, sollte sein Zugangsrecht auch dann aufgehoben werden, wenn er weiterhin Mitarbeiter des CISP ist.*

- ***Rechenzentrums-Zugriffsprotokolle****: Der physische Zugriff auf CISP-Rechenzentren sollte protokolliert, überwacht und die Protokolle aufbewahrt werden. Der CISP sollte Informationen aus logischen und physischen Überwachungssystemen in Wechselbeziehung bringen, um die Sicherheit nach Bedarf zu erhöhen.*

- ***Zugangsüberwachung für Rechenzentren:*** *Die Überwachung von Rechenzentren durch den CISP sollte über globale Security Operations Center passieren, die für die Überwachung, Triage und Ausführung von Sicherheitsprogrammen zuständig sind. Die Center sollten einen weltweiten Support rund um die Uhr bereitstellen, indem sie die Zugriffsaktivitäten in den Rechenzentren verwalten und überwachen sowie lokale Teams und andere*

Supportteams so ausstatten, dass sie Sicherheitsvorfällen durch Triage, Beratung, Analyse und reaktives Handeln entgegenwirken können.

ÜBERWACHUNG und ERKENNUNG

- ***CCTV:*** *Physische Zugangspunkte zu Serverräumen sollten mit Überwachungskameras (CCTV, Closed Circuit Television Cameras) überwacht werden. Die Bilder sollten gemäß den gesetzlichen und Compliance-Anforderungen aufbewahrt werden.*

- ***Zugangspunkte zu Rechenzentren:*** *Der physische Zutritt an den Zugangspunkten zum Gebäude sollte von professionellem Sicherheitspersonal mithilfe von Videoüberwachung, Erkennungssystemen und anderen elektronischen Mitteln kontrolliert werden. Autorisierte Mitarbeiter sollten für den Zugang zu Rechenzentren Mechanismen der Multi-Faktor-Authentifizierung einsetzen. Eingänge zu Serverräumen sollten mit Geräten gesichert werden, die Alarme auslösen, um bei gewaltsam geöffneter oder offengehaltener Tür eine Vorfallsreaktion auszulösen.*

- ***Eindringungserkennung:*** *Elektronische Meldesysteme zur Erkennung von Eindringversuchen sollten auf Datenebene installiert werden, um Sicherheitsvorfälle zu ausfindig zu machen, zu erkennen und daraufhin das entsprechende Personal automatisch zu alarmieren. Eingangs- und Ausgangspunkte zu Serverräumen sollten mit Geräten gesichert werden, bei denen jede Person vor dem Betreten oder Verlassen eine Multi-Faktor-Authentifizierung durchlaufen muss. Diese Geräte geben Alarme aus, wenn die Tür ohne Authentifizierung gewaltsam geöffnet oder offengehalten wird. Die Türalarmgeräte sollten so konfiguriert werden, dass sie Fälle erkennen, in denen eine Person eine Datenschicht verlässt oder in diese eindringt, ohne dass eine Multi-Faktor-Authentifizierung erfolgt. Alarme sollten sofort an rund um die Uhr arbeitende CISP Security Operations Center weitergeleitet werden, wo sie unverzüglich protokolliert, analysiert und beantwortet werden können.*

GERÄTEMANAGEMENT

- ***Komponentenmanagement:*** *CISP-Komponenten sollten zentral über ein Bestandsverwaltungssystem verwaltet werden, das Informationen zu Eigentümer, Standort, Status, Wartung und Beschreibung für CISP-eigene Assets speichert und nachverfolgt. Nach der Beschaffung sollten die Komponenten gescannt und nachverfolgt werden und solche, die einer Wartung unterzogen werden, auf Eigentümerschaft, Status und Beendigung hin überprüft und überwacht werden.*

- ***Vernichtung von Medien:*** *Medienspeichergeräte, die zum Speichern von Kundendaten verwendet werden, sollten vom CISP als kritisch eingestuft und während ihres gesamten Lebenszyklus entsprechend mit höchster Umsicht behandelt werden. Der CISP sollte genaue Standards zur Installation, Wartung und schlussendlich für die Vernichtung der Geräte haben, wenn diese nicht mehr benötigt werden. Wenn ein Speichergerät das Ende seiner Nutzungsdauer erreicht hat, sollte der CISP Medien mithilfe der in NIST 800-88 beschriebenen Verfahren außer Betrieb nehmen. Medien, auf denen Kundendaten gespeichert sind, sollten erst aus der Kontrolle des CISP entlassen werden, wenn sie sicher außer Betrieb genommen wurden.*

BETRIEBLICHE VERSORGUNGSSYSTEME

- ***Stromversorgung:*** *Die elektrischen Stromversorgungssysteme des CISP-Rechenzentrums sollten so ausgelegt sein, dass sie rund um die Uhr vollständig redundant und ohne Auswirkung auf den Betrieb wartbar sind. Der CISP sollte dafür sorgen, dass Rechenzentren mit einer Notstromversorgung ausgestattet sind, um sicherzustellen, dass bei einem elektrischen Ausfall die Stromversorgung für den Betrieb kritischer und wichtiger Workloads in der Anlage aufrechterhalten werden kann.*

- ***Klima und Temperatur:*** *CISP-Rechenzentren sollten Mechanismen verwenden, um das Raumklima zu kontrollieren und eine angemessene Betriebstemperatur für Server und andere Hardware aufrechtzuerhalten. So wird eine Überhitzung verhindert und die Wahrscheinlichkeit von Serviceausfällen verringert. Temperatur und Luftfeuchtigkeit müssen in angemessener Weise von den Mitarbeitern und den technischen Systemen überwacht und geregelt werden.*

- ***Branderkennung und -bekämpfung:*** *CISP-Rechenzentren sollten mit automatischen Feuermelde- und -löschanlagen ausgestattet sein. Feuermeldeanlagen sollten Rauchmeldesensoren in Netzwerk-, Mechanik- und Infrastrukturbereichen verwenden. Diese Bereiche müssen zusätzlich durch Löschsysteme geschützt werden.*

- ***Leckerkennung:*** *Um Wasserlecks zu erkennen, sollte der CISP seine Rechenzentren mit Funktionen zur Erkennung von Wasseransammlungen ausstatten. Wenn das Vorhandensein von Wasser erkannt wird, sollten Mechanismen zum Entfernen des Wassers zur Verfügung stehen, um zusätzliche Wasserschäden zu vermeiden.*

INFRASTRUKTURWARTUNG

- ***Gerätewartung:*** *Der CISP sollte elektrische und mechanische Geräte überwachen und präventiv warten, um die Funktionsfähigkeit der Systeme innerhalb von CISP-Rechenzentren aufrechtzuerhalten. Wartungsverfahren für Geräte sollten von qualifizierten Personen und gemäß einem dokumentierten Wartungsplan durchgeführt werden.*

- ***Verwaltung der Umgebung:*** *Der CISP sollte elektrische und mechanische Systeme und Geräte überwachen, um Probleme sofort erkennen zu können. Dies sollte mithilfe von Tools für ein kontinuierliches Auditing sowie anhand von Informationen erfolgen, die über CISP-Systeme zur Gebäudeverwaltung und zur elektrischen Überwachung bereitgestellt werden. Es sollten vorbeugende Wartungen vorgenommen werden, um eine kontinuierliche Funktionsfähigkeit der Ausstattung sicherzustellen.*

GOVERNANCE UND RISIKO

- ***Laufendes Risikomanagement für Rechenzentren:*** *Das CISP Security Operations Center sollte regelmäßige Prüfungen zu Bedrohungen und Schwachstellen in Rechenzentren durchführen. Eine laufende Bewertung und Minderung potenzieller Schwachstellen sollte über Maßnahmen der Risikobewertung im Rechenzentrum durchgeführt werden. Diese Bewertung sollte zusätzlich zum Risikobewertungsprozess auf Unternehmensebene durchgeführt werden, der zur Identifizierung und Steuerung von Risiken verwendet wird, die im gesamten Unternehmen auftreten können. Bei diesem Prozess sollten auch regionale Vorschriften und Umweltrisiken berücksichtigt werden.*

- ***Bestätigung der Sicherheit durch Dritte:*** *Tests von CISP-Rechenzentren seitens Dritter, wie sie in dessen Berichten von unabhängigen Dritten dokumentiert werden, sollen sicherstellen, dass der CISP Sicherheitsmaßnahmen entsprechend den festgelegten Regeln implementiert hat, die für den Erhalt von Sicherheitszertifizierungen erforderlich sind. Je nach Compliance-Programm und seinen Anforderungen können externe Prüfer die Medienentsorgung testen, Aufzeichnungen von Überwachungskameras prüfen, Eingänge und Korridore im gesamten Rechenzentrum beobachten, elektronische Zugangskontrollgeräte testen und die Ausrüstung des Rechenzentrums untersuchen.*

7. Migrationen

	Anforderung
1.	***MIGRATIONSSERVICE:*** *Wie viele verschiedene Datenmigrationsservices bietet der Cloud-Anbieter?*
2.	***MIGRATIONEN – ZENTRALISIERTE ÜBERWACHUNG:*** *Bietet der Cloud-Anbieter Organisationen einen zentralisierten Service (d. h. eine zentrale Schnittstelle), mit dem sie den Status ihrer Server- und Anwendungsmigrationen verfolgen und überwachen können?*
3.	***MIGRATIONEN – DASHBOARD:*** *Bietet das Migrationstool des Cloud-Anbieters ein Dashboard zur schnellen Visualisierung des Migrationsstatus, der zugehörigen Metriken und des Migrationsverlaufs?*
4.	***MIGRATIONEN – CLOUD-ANBIETER-TOOLS:*** *Bietet das Migrationstool des Cloud-Anbieters die Integration in andere Migrationstools des Cloud-Anbieters, die Server- und Anwendungsmigrationen durchführen können?*

5.	*MIGRATIONEN – TOOLS VON DRITTEN:* *Ermöglicht das Migrationstool des Cloud-Anbieters die Integration von Migrationstools von Drittanbietern?* • *Wenn ja, welche Migrationstools von Drittanbietern werden unterstützt?*
6.	*MIGRATIONEN – MULTIREGIONALE MIGRATIONEN:* *Bietet das Migrationstool des Cloud-Anbieters die Möglichkeit, Server- und Anwendungsmigrationen in verschiedenen Regionen nachzuverfolgen und zu überwachen?*
7.	*MIGRATIONEN – SERVERMIGRATION:* *Bietet das Migrationstool des Cloud-Anbieters eine Möglichkeit, lokale virtualisierte Server in die Cloud zu migrieren?* • *Wenn ja, welche virtualisierten Umgebungen werden derzeit unterstützt?*
8.	*MIGRATIONEN – SERVERERKENNUNG:* *Verfügt das Migrationstool des Cloud-Anbieters über Erkennungsfunktionen, um automatisch lokale virtualisierte Server zu finden, die in die Cloud migriert werden sollen?*
9.	*MIGRATIONEN – SERVERLEISTUNGSDATEN:* *Verfügt das Migrationstool des Cloud-Anbieters über die Fähigkeit, die Leistung von Servern und/oder virtuellen Maschinen wie CPU und RAM zu erfassen und anzuzeigen?*
10.	*MIGRATIONEN – ERKENNUNGSDATENBANK:* *Kann das Migrationstool des Cloud-Anbieters alle erfassten Daten in einer zentralisierten Datenbank speichern?* • *Wenn ja, können Unternehmen diese Daten exportieren? In welche Formate?*
11.	*MIGRATIONEN – VERSCHLÜSSELUNG IM RUHEZUSTAND:* *Verschlüsselt der Cloud-Anbieter alle in der Erkennungsdatenbank erfassten und gespeicherten Daten im Ruhezustand?*
12.	*MIGRATIONEN – INKREMENTELLE SERVERREPLIKATION:* *Bietet das Migrationstool des Cloud-Anbieters während der Server- oder VM-Migration eine automatisierte, inkrementelle Live-Serverreplikation, um alle Änderungen am Server oder der virtuellen Maschine zu unterstützen, die im endgültigen migrierten Image enthalten sind?* • *Wenn ja, wie lange kann dieser Service ausgeführt werden?*
13.	*MIGRATIONEN – VMWARE:* *Unterstützt das Migrationstool des Cloud-Anbieters Migrationen virtueller VMWare-Maschinen von lokalen Umgebungen in die Cloud?*
14.	*MIGRATIONEN – HYPER-V:* *Unterstützt das Migrationstool des Cloud-Anbieters Migrationen virtueller Hyper-V-Maschinen von lokalen Umgebungen in die Cloud?*
15.	*MIGRATIONEN – ANWENDUNGSERKENNUNG:* *Kann das Migrationstool des Cloud-Anbieters Anwendungen erkennen und gruppieren, bevor sie migriert werden?*
16.	*MIGRATIONEN – ABHÄNGIGKEITSZUORDNUNG:* *Kann das Migrationstool des Cloud-Anbieters Abhängigkeiten zwischen Servern und Anwendungen erkennen, bevor sie migriert werden?*
17.	*MIGRATIONEN – DATENBANKMIGRATION:* *Ist das Migrationstool des Cloud-Anbieters in der Lage, lokale Datenbanken in die Cloud zu migrieren?*

18.	*MIGRATIONEN – AUSFALLZEITEN DER DATENBANKMIGRATION:* *Kann das Migrationstool des Cloud-Anbieters eine Datenbankmigration in die Cloud mit minimalen Ausfallzeiten durchführen, d. h. bleibt die Quelldatenbank während des Migrationsprozesses voll funktionsfähig?*
19.	*MIGRATIONEN – QUELLDATENBANK:* *Unterstützt das Migrationstool des Cloud-Anbieters die Migration verschiedener Datenbankquellen wie Oracle, SQL Server usw.?* • *Wenn ja, geben Sie bitte alle unterstützten Quelldatenbanken an, die in die Cloud migriert werden können.*
20.	*MIGRATIONEN – HETEROGENE MIGRATIONEN:* *Kann das Migrationstool des Cloud-Anbieters heterogene Datenbankmigrationen durchführen, d. h. von einer Art Quelldatenbank zu einer anderen Art Zieldatenbank, etwa Oracle zu SQL Server?* • *Wenn ja, listen Sie bitte alle möglichen Kombinationen aus heterogenen Datenbankmigrationen auf.*
21.	*MIGRATIONEN – DATENMIGRATION IM PETABYTE-BEREICH:* *Bietet der Cloud-Anbieter eine Datentransportlösung im Petabyte-Bereich, die sichere Geräte verwendet, um große Datenmengen in die und aus der Cloud zu übertragen?*
22.	*MIGRATIONEN – DATENMIGRATION IM EXABYTE-BEREICH:* *Bietet der Cloud-Anbieter eine Datentransportlösung im Exabyte-Bereich, um extrem große Datenmengen in die Cloud zu verschieben?*
23.	*MIGRATIONEN – ENTERPRISE-SICHERUNGEN:* *Bietet der Cloud-Anbieter einen Service zur nahtlosen Integration des Rechenzentrums eines Kunden in Cloud-Speicherservices, mit denen Daten in den Speicherservice des Cloud-Anbieters übertragen und darin gespeichert werden können?*
24.	*MIGRATIONEN – ENTERPRISE-SICHERUNGEN – OBJEKTSPEICHER:* *Bietet der Enterprise-Sicherungsservice des Cloud-Anbieters eine Integration in den Cloud-Objektspeicherservice des Anbieters?*
25.	*MIGRATIONEN – ENTERPRISE-SICHERUNGEN – DATEIZUGRIFF:* *Ermöglicht der Enterprise-Sicherungsservice des Cloud-Anbieters Benutzern das Speichern und Abrufen von Objekten mithilfe von Dateiprotokollen wie dem NFS-Protokoll?*
26.	*MIGRATIONEN – ENTERPRISE-SICHERUNGEN – BLOCKZUGRIFF:* *Ermöglicht der Enterprise-Sicherungsservice des Cloud-Anbieters Benutzern das Speichern und Abrufen von Objekten mithilfe von Blockprotokollen wie dem iSCSI-Protokoll (Internet Small Computer Systems Interface)?*
27.	*MIGRATIONEN – ENTERPRISE-SICHERUNGEN – TAPE-ZUGRIFF:* *Ermöglicht der Enterprise-Sicherungsservice des Cloud-Anbieters Benutzern, ihre Daten über eine virtuelle Tape-Bibliothek zu sichern und diese Tape-Sicherungen in der Cloud des Anbieters zu speichern?*
28.	*MIGRATIONEN – ENTERPRISE-SICHERUNGEN – VERSCHLÜSSELUNG:* *Bietet der Enterprise-Sicherungsservice des Cloud-Anbieters die Verschlüsselung von Daten im Ruhezustand und während der Übertragung?*
29.	*MIGRATIONEN – ENTERPRISE-SICHERUNGEN – INTEGRATION IN DRITTANBIETER-SOFTWARE:* *Lässt sich der Enterprise-Sicherungsservice des Cloud-Anbieters in gängige Sicherungssoftware von Drittanbietern integrieren?*

30.	***MIGRATIONEN – SERVICE-LIMITS:*** *Unterliegt der Cloud-Anbieter jeglichen Einschränkungen (d. h. Service-Limits) in Bezug auf den oben aufgeführten Abschnitt zum Thema Migrationen?* *Beispiel:* *Maximale Anzahl gleichzeitiger Migrationen virtueller Maschinen* *Maximal bestellbare Anzahl an Datentransportlösungen*

8. Rechnungsstellung

	Anforderung
1.	***RECHNUNGSSTELLUNG – NACHVERFOLGUNG UND BERICHTERSTELLUNG:*** *Bietet der Cloud-Anbieter einen Service für Nachverfolgung und Berichterstellung zu Abrechnungen, um Benutzer bei der Verwaltung und Überwachung ihrer Nutzung von Cloud-Angeboten zu unterstützen?*
2.	***RECHNUNGSSTELLUNG – ALARME UND BENACHRICHTIGUNGEN:*** *Bietet der Cloud-Anbieter Benutzern einen Mechanismus zur Einrichtung von Alarmen mit Benachrichtigungen, um sie zu warnen, wenn ihre Ausgaben einen bestimmten Schwellenwert überschritten haben?*
3.	***RECHNUNGSSTELLUNG – KOSTENMANAGEMENT:*** *Bietet der Cloud-Anbieter einen Mechanismus zum Erstellen und Anzeigen von Grafiken, die Kosten und Ausgaben zusammenfassen?*
4.	***RECHNUNGSSTELLUNG – BUDGETS:*** *Bietet der Cloud-Anbieter einen Mechanismus zur Anzeige und Verwaltung von Budgets und zur Prognose der geschätzten Kosten?*
5.	***RECHNUNGSSTELLUNG – KONSOLIDIERTE ANSICHT:*** *Bietet der Cloud-Anbieter einen Mechanismus zur Konsolidierung der Rechnungsstellung für mehrere Konten unter einem einzigen primären Zahlungskonto?*
6.	***RECHNUNGSSTELLUNG – SERVICE-LIMITS:*** *Unterliegt der Cloud-Anbieter jeglichen Einschränkungen (d. h. Service-Limits) in Bezug auf den oben aufgeführten Abschnitt zum Thema Rechnungsstellung?* *Beispiel:* *Maximale Anzahl von Konten, die gruppiert werden können* *Maximale Anzahl von Alarmen, die erstellt werden können* *Maximale Anzahl von Budgets, die verwaltet werden können*

9. Verwaltung

	Anforderung
1.	***VERWALTUNG – ÜBERWACHUNGSSERVICE:*** *Bietet der Cloud-Anbieter einen Überwachungsservice für die Verwaltung von Cloud-Ressourcen und -Anwendungen an, der anhand vordefinierter Metriken für die Datenerfassung, Überwachung und Berichterstellung eingesetzt werden kann?*

2.	*VERWALTUNG – ALARME:* *Ermöglicht der Überwachungsservice des Cloud-Anbieters Benutzern die Einrichtung von Alarmen?*
3.	*VERWALTUNG – BENUTZERDEFINIERTE METRIKEN:* *Ermöglicht der Überwachungsservice des Cloud-Anbieters Benutzern die Erstellung und Überwachung benutzerdefinierter Metriken?*
4.	*VERWALTUNG – ÜBERWACHUNG DER GRANULARITÄT:* *Bietet der Überwachungsservice des Cloud-Anbieters verschiedene Ebenen der Granularität für die Überwachung, bis hinunter zur 1-Minuten-Ebene?*
5.	*VERWALTUNG – API-NACHVERFOLGUNGSSERVICE:* *Bietet der Cloud-Anbieter einen Service, der Aktivitäten innerhalb der Cloud-Ressourcen sowohl auf Konsolen- als auch auf API-Ebene protokolliert, überwacht und speichert, um die Transparenz zu verbessern?* • *Wenn ja, welche der Services des Cloud-Anbieters lassen sich mit diesem Nachverfolgungsservice integrieren?*
6.	*VERWALTUNG – BENACHRICHTIGUNGEN:* *Bietet der Cloud-Anbieter eine Funktion für das Senden von Benachrichtigungen anhand des API-Aktivitätsgrades?*
7.	*VERWALTUNG – KOMPRIMIERUNG:* *Bietet der Cloud-Anbieter einen Mechanismus zur Komprimierung von Protokollen, die vom API-Nachverfolgungssystem generiert werden, um die mit diesem Service verbundenen Speicherkosten zu senken?*
8.	*VERWALTUNG – AGGREGIERUNG VON REGIONEN:* *Bietet der Cloud-Anbieter die Möglichkeit, API-Aktivitäten eines Kontos in allen Regionen aufzuzeichnen und diese Informationen für eine vereinfachte Nutzung aggregiert bereitzustellen?*
9.	*VERWALTUNG – RESSOURCENBESTAND:* *Bietet der Cloud-Anbieter einen Service zur Bewertung, Evaluierung und zum Auditing der von einem Benutzer bereitgestellten Ressourcenkonfigurationen?*
10.	*VERWALTUNG – KONFIGURATIONSÄNDERUNGEN:* *Zeichnet der Cloud-Anbieter automatisch eine Änderung der Ressourcenkonfiguration auf, wenn sie auftritt?*
11.	*VERWALTUNG – KONFIGURATIONSVERLAUF:* *Bietet der Cloud-Anbieter die Möglichkeit, die Ressourcenkonfiguration an einem beliebigen Zeitpunkt in der Vergangenheit zu untersuchen?*
12.	*VERWALTUNG – KONFIGURATIONSREGELN:* *Bietet der Cloud-Anbieter Richtlinien und Empfehlungen für die Bereitstellung, Konfiguration und kontinuierliche Überwachung der Compliance?*
13.	*VERWALTUNG – RESSOURCENVORLAGEN:* *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, eine Sammlung von Ressourcen in der Art und Weise von Vorlagen zu erstellen, bereitzustellen und zu verwalten?*
14.	*VERWALTUNG – REPLIKATION VON RESSOURCENVORLAGEN:* *Bietet der Cloud-Anbieter die Möglichkeit, diese Ressourcenvorlagen schnell über verschiedene Regionen hinweg zu replizieren, um sie ggf. in Situationen einer Notfallwiederherstellung (DR) zu verwenden?*

15.	*VERWALTUNG – VORLAGENDESIGNER:* *Bietet der Cloud-Anbieter ein benutzerfreundliches grafisches Tool mit Drag-and-Drop-Funktionalität, das die Erstellung solcher Ressourcenvorlagen beschleunigt?*
16.	*VERWALTUNG – SERVICEKATALOG:* *Bietet der Cloud-Anbieter einen Service zur Erstellung und Verwaltung eines Servicekatalogs, d. h. Server, virtuelle Maschinen, Software, Datenbanken usw.?*
17.	*VERWALTUNG – KONSOLENZUGRIFF:* *Bietet der Cloud-Anbieter eine webbasierte Benutzeroberfläche, um die Verwaltung und Überwachung von Cloud-Services zu vereinfachen?*
18.	*VERWALTUNG – CLI-ZUGRIFF:* *Bietet der Cloud-Anbieter ein einheitliches Tool zur Verwaltung und Konfiguration mehrerer Cloud-Services über die Befehlszeilenschnittstelle (CLI, Command Line Interface) und ermöglicht er die Automatisierung von Verwaltungsaufgaben durch den Einsatz von Skripts?*
19.	*VERWALTUNG – MOBILER ZUGRIFF:* *Bietet der Cloud-Anbieter eine Smartphone-Anwendung, mit der Benutzer eine Verbindung zum Cloud-Service herstellen und ihre Ressourcen verwalten können?* • *Wenn ja, ist diese Anwendung sowohl für iOS als auch für Android verfügbar?*
20.	*VERWALTUNG – BEST PRACTICES:* *Verfügt der Cloud-Anbieter über einen Service, mit dem Benutzer ihre Cloud-Nutzung mit Best Practices vergleichen können?*
21.	*VERWALTUNG – SERVICE-LIMITS:* *Unterliegt der Cloud-Anbieter jeglichen Einschränkungen (d. h. Service-Limits) in Bezug auf den oben aufgeführten Abschnitt zum Thema Verwaltung?* *Beispiel:* *Maximale Anzahl von Konfigurationsregeln pro Konto* *Maximale Anzahl von Alarmen, die erstellt werden können* *Maximale Anzahl an Protokollen, die gespeichert werden können*

10. Support

	Anforderung
1.	***SUPPORT – SERVICE:*** *Bietet der Cloud-Anbieter jederzeit Support, rund um die Uhr, an sieben Tagen in der Woche und an 365 Tagen im Jahr per Telefon, Chat und E-Mail?*
2.	***SUPPORT – SUPPORTSTUFE:*** *Bietet der Cloud-Anbieter verschiedene Supportstufen?*
3.	***SUPPORT – ZUWEISUNG VON STUFEN:*** *Ermöglicht der Cloud-Anbieter Benutzern die selbstständige Zuweisung der verwendeten Ressourcen/Services zu verschiedenen Supportstufen auf der Grundlage einer detaillierten Klassifizierung und nicht durch die erzwungene Notwendigkeit, separate Cloud-Konten zu unterhalten, um verschiedene Supportstufen zu erreichen und zu erhalten?*
4.	***SUPPORT – FOREN:*** *Bietet der Cloud-Anbieter öffentliche Support-Foren, in denen Kunden über ihre Probleme sprechen können?*
5.	***SUPPORT – SERVICESTATUS-DASHBOARD:*** *Bietet der Cloud-Anbieter ein Dashboard für den Servicestatus, das die aktuellsten Informationen zur Serviceverfügbarkeit in mehreren Regionen anzeigt?*
6.	***SUPPORT – PERSONALISIERTES DASHBOARD:*** *Bietet der Cloud-Anbieter ein Dashboard, das einen personalisierten Überblick über die Performance und Verfügbarkeit der Services bietet, die den spezifischen Ressourcen des Benutzers zugrunde liegen?*
7.	***SUPPORT – DASHBOARD-VERLAUF:*** *Bietet der Cloud-Anbieter einen 365-Tage-Dashboard-Verlauf für den Servicestatus an?*
8.	***SUPPORT – CLOUD-BERATER:*** *Bietet der Cloud-Anbieter einen Service, der wie ein individueller Cloud-Experte agiert und dabei hilft, die Nutzung der Ressourcen mit den Best Practices zu vergleichen?*
9.	***SUPPORT – TAM:*** *Stellt der Cloud-Anbieter einen Technical Account Manager (TAM) bereit, der technisches Know-how für das gesamte Spektrum der Cloud-Services bietet?*
10.	***SUPPORT – SUPPORT FÜR ANWENDUNGEN VON DRITTANBIETERN:*** *Bietet der Cloud-Anbieter Support für gängige Betriebssysteme und Komponenten des Anwendungs-Stacks?*
11.	***SUPPORT – ÖFFENTLICHE API:*** *Bietet der Cloud-Anbieter eine öffentliche API, die programmatisch mit Supportfällen interagiert, um solche Fälle zu erstellen, zu bearbeiten und zu schließen?*
12.	***SUPPORT – SERVICEDOKUMENTATION:*** *Bietet der Cloud-Anbieter hochwertige, öffentlich einsehbare technische Dokumentationen für alle seine Services, einschließlich, aber nicht beschränkt auf Benutzerhandbücher, Tutorials, häufig gestellte Fragen (FAQs) und Versionshinweise?*
13.	***SUPPORT – CLI-DOKUMENTATION:*** *Bietet der Cloud-Anbieter eine hochwertige, öffentlich einsehbare technische Dokumentation für seine Befehlszeilenschnittstelle (CLI)?*

14.	*SUPPORT – REFERENZARCHITEKTUREN:* *Bietet der Cloud-Anbieter eine kostenlose Online-Dokumentensammlung zu Referenzarchitekturen an, um Kunden beim Erstellen spezifischer Lösungen zu unterstützen, die viele Cloud-Services des Cloud-Anbieters kombinieren?*
15.	*SUPPORT – REFERENZBEREITSTELLUNGEN:* *Bietet der Cloud-Anbieter eine kostenlose Online-Dokumentensammlung mit detaillierten, getesteten und validierten Schritt-für-Schritt-Verfahren, einschließlich Best Practices, zur Implementierung verbreiteter Lösungen (d. h. DevOps, Big Data, Data Warehouse, Microsoft-Workloads, SAP-Workloads usw.) in seinen Cloud-Angeboten?*

Anhang B – Technische Live-Bewertung

Bei der Auswahl eines CISP ist es wichtig, die Funktionalität der Cloud-Plattform unter Verwendung der öffentlich zugänglichen Services und Infrastruktur des CISP „live" zu beurteilen. Für die technische Bewertung empfehlen wir mindestens einen ganzen Tag pro CISP in der engeren Auswahl. Während der Bewertung können Sie: 1) eine gründliche Bewertung durchführen, um einschätzen zu können, ob die demonstrierten Funktionen zu den Anforderungen Ihrer Ausschreibung und der schriftlichen Antwort des CISP passen; 2) Ihren Experten eine Plattform bieten, den CISP zu testen und so sicherzustellen, dass die spezifischen technischen Bedürfnisses Ihres Unternehmens erfüllt werden; 3) sich mit CISP-Services vertraut machen und Gewissheit darüber erlangen, dass der CISP in der Lage ist, zu skalieren, seinen Betrieb sicher und zuverlässig aufrechtzuerhalten und weiterhin Innovationen voranzutreiben, um zukünftigen Anforderungen gerecht zu werden.

Wenn CISPs auf Cloud-Services-Ausschreibungen antworten und angeben, die Anforderungen zu erfüllen, basiert dies möglicherweise auf einer sehr allgemeinen Interpretation der Anforderungen, ohne den vollständigen Kontext der Betriebsumgebung/Anwendungsanforderungen einer Organisation. Wir empfehlen die Besetzung eines Gremiums für die technische Live-Bewertung mit leitenden technischen, betrieblichen, Sicherheits- und Anwendungsexperten. Die Gutachter sollten den CISP während des gesamten Prozesses mit Herausforderungen konfrontieren und als Best Practice sollten sie CISPs unabhängig bewerten. Die Bewertung sollte auf einer Skala erfolgen, beispielsweise von 0 bis 4 (0=Inakzeptabel, 1=Grenzwertig, 2=Akzeptabel, 3=Gut, 4=Hervorragend). Anschließend können die Bewertungen konsolidiert werden. Die Durchschnittsbewertung jedes Szenarios fließt in die Gesamtbewertung des CISP ein. Szenarien mit einer starken Standardabweichung sollten vor der Fertigstellung im Bewertungsteam diskutiert werden. Nach der Konsolidierung der Bewertungen kann eine Gewichtung basierend auf der Kritikalität des Szenarios erfolgen.

Was den Umfang der Demonstration betrifft, empfehlen wir einen ganzheitlichen Blick auf die Plattform des CISP, mit einer anschließenden genaueren Bewertung bestimmter Workloads, die auf der Plattform ausgeführt werden. Unten finden Sie eine Beispielübersicht für eine Plattform- und Workloadbewertung. Organisationen können auf dieser Grundlage aufbauen und sie anpassen, um sicherzustellen, dass der gewählte CISP ihren speziellen funktionalen und nicht funktionalen Anforderungen entspricht. Als Best Practice kann man es Anbietern, denen die Liste von Szenarien vorgelegt wurde, gestatten, eine Agenda für die Live-Bewertung vorzuschlagen, mit deren Hilfe möglichst viel behandelt werden kann und worin 20 % der Zeit für Fragen und Antworten vorgesehen ist.

Plattformbewertung: Mehrere CISPs haben den Begriff „Well Architected" übernommen und beschreiben damit eine Herangehensweise an die Cloud, die den Wert optimiert und das Risiko minimiert. Well-Architected-Szenarien können bei einer technischen Live-Demonstration Folgendes umfassen:

1. **Sicherheit:** Identität, zentralisierte Governance, automatische Bedrohungserkennung, Datenschutz, Ereignisbereitschaft
2. **Leistungseffizienz:** Passende Dimensionierung, Skalierbarkeit/Elastizität, Serverless
3. **Zuverlässigkeit:** Hohe Zuverlässigkeit (Fehlerresilienz), Verminderung des Änderungsrisikos, Notfallwiederherstellung, Sicherung
4. **Kostenmanagement:** Finanzgeschäfte, geschäftliche Optimierung, Budgets und Kostenzuordnung
5. **Hochwertiger Betriebsumfang:** Automatisierung, Überwachung, Support, Management und Funktionalität für die Migration zu und den Betrieb innerhalb der Cloud

Workloadbewertung: Eine gängige Auswahl an Anwendungsarten für die Demonstration umfasst:

- **Webanwendung:** Öffentliches Hosten einer dynamischen Website, einschließlich Back-End-Datenbank und statischem Objektspeicher.
- **Datenanalytik:** Eine Data-Lake- oder Lake-House-Architektur, welche die Konsolidierung von Daten verschiedenartiger Datenanbieter ermöglicht sowie die Fähigkeit zum Umgang mit hohen Volumes (TB/PB von Daten), hoher Vielfalt (strukturiert, unstrukturiert, unterschiedliche Formate usw.) und hoher Geschwindigkeit (Rate der Datengenerierung, Änderungs- und Abfragemuster).
- **Plattform für Datenwissenschaft:** Eine Plattform, die die Entwicklung, Bereitstellung und den Einsatz von KI-/ML-basierten Funktionen überall in Ihrer Organisation ermöglicht.
- **IoT-Anwendung:** Eine IoT-Plattform/-Funktionalität, die die Cloud, eine Netzwerkfunktion und die entsprechenden Geräte umfasst.

Für jede repräsentative Workload, die für Ihre Organisation wichtig ist, können Sie die Szenarien definieren, die vom CISP demonstriert werden sollen. Die Szenarien sollten allgemeine Fähigkeiten aufzeigen, mit denen die Bereitstellung der Workload nach dem Well-Architected-Prinzip ermöglicht wird. Auf den folgenden Seiten finden Sie Beispielkriterien einer technischen Live-Demonstration für 1) die Plattform des CISP und 2) eine Muster-Workload einer Webanwendung.

Plattform – Beispiel für technische Live-Bewertung

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
Platt.Sich.1	Identitätsverbund	4	Demonstration der Fähigkeit, von einem bestehenden Identitätsspeicher zum Cloud-Service zu föderieren.	• Unterstützung von Standardprotokollen wie SAML. • Unterstützung von SCIM-basierter Identitätsreplikation. • Die Fähigkeit, innerhalb des Identitätsspeichers des Unternehmens verschiedene Zugriffsebenen zu definieren und diese beim Cloud-Anbieter anzuwenden. • Die Fähigkeit, bestimmte Teams/Einzelpersonen auf bestimmte Konten/Projekte/Workloads zu beschränken. • Unterstützung von attributbasierter Zugriffskontrolle (Attribute-Based Access Control, ABAC) und Einsatz dieser Attribute im Identity and Access Management-System (IAM) des Cloud-Anbieters, um den Zugriff auf Cloud-Ressourcen zu kontrollieren.
Platt.Sich.2	Zentrale Governance	4	Demonstration der Fähigkeit zur Definition von Richtlinien und Anforderungen auf zentraler Ebene, betrieblicher Ebene (globale Richtlinien) sowie Geschäftsbereichs- und Projektebene.	• Richtlinien sollten enthalten: Aktivieren/Deaktivieren von Services, Anwendung geografischer Einschränkungen (Begrenzung von Regionen). • Die Richtlinien sollten auch Benutzer – einschließlich Administratoren – darin einschränken, Auditing-/Governance-Kontrollen zu deaktivieren.
Platt.Sich.3	Einschränkung von Benutzerberechtigungen	3	Demonstration der automatischen Empfehlungen für die Eingrenzung von Benutzerberechtigungen.	• Fähigkeit, aktuelle Berechtigungen mit erforderlichen Berechtigungen zu vergleichen. • Automatische Erstellung von Richtlinien zur Förderung des Prinzips der geringsten Berechtigung.

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
Platt.Sich.4	Audit-Protokollierung	4	Demonstration der Audit-Protokollierung von Cloud-Aktivität, einschließlich erlaubter und unerlaubter Aktionen.	• Zentralisierte Protokolle für die gesamte Organisation. • Konto-/Projektspezifische Protokolle zur Unterstützung allgemeinerer Funktionen für Nachverfolgung und Verantwortlichkeit. • Tools zum Aktivieren von Protokollabfragen. • Tools zum Aktivieren von Maßnahmen, die basierend auf bestimmten Ereignissen/Protokolleinträgen ausgelöst werden. • Möglichkeit, die Support-Aktivitäten des Anbieters anzusehen. • Möglichkeit, das Löschen von Protokollen zu verhindern, auch durch Administratoren.
Platt.Sich.5	Netzwerkisolation	4	Demonstration und, wo möglich, Belege für die Isolierung verschiedener Mandanten innerhalb der Cloud. Demonstration der Konfigurierung isolierter (ohne Konnektivität), privater (ohne Internet) und öffentlicher (mit Internetzugang) Subnetze.	• Trennung von Mandanten, auch auf Services via VPN und Querverbindungen. • Fähigkeit, den Datenverkehrsfluss von außerhalb der Cloud-Infrastruktur (On-Premises), darin und zum Internet zu kontrollieren. • Wie die Trennung im Falle der Verwendung von Shared Services angewendet wird, etwa bei Container-Hosting oder Function as a Service.
Platt.Sich.6	Verschlüsselung von Daten im Ruhezustand	4	Demonstration der Fähigkeit, Daten im Ruhezustand zu verschlüsseln, einschließlich der Optionen für Bring Your Own Keys (BYOK) und clientseitige Verschlüsselung.	• Fähigkeit, die Verschlüsselung sensibler Daten zu erforderlich zu machen. • Fähigkeit, entweder vom Anbieter verwaltete Schlüssel oder vom Kunden verwaltete Schlüssel einzusetzen. • Einhaltung von FIPS 140-2. • Fähigkeit, bei Nichteinhaltung von Verschlüsselungsanforderungen

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
				Warnungen auszulösen und diese zu protokollieren. • Zusätzliche Kostenauswirkungen. • Leistungsauswirkungen. • Unterstützung von quantensicheren Algorithmen und Schlüsselgrößen.
Platt.Sich.7	Verschlüsselung während der Übertragung	4	Demonstration der Fähigkeit zur Verschlüsselung von Daten während der Übertragung.	• Verschlüsselung als Standard für Service-APIs. • Fähigkeit, die Verschlüsselung während der Übertragung (TLS) auf Load Balancern und verwalteten APIs zu aktivieren. • Unterstützung für gegenseitige (Client und Server) Authentifizierung.
Platt.Sich.8	Schlüsselverwaltung	4	Demonstration von Funktionen der Schlüsselverwaltung. Einbindung des vollständigen Schlüssel-Lebenszyklus. Einbindung der Integration mit Cloud-Services.	• Protokollierung der Erstellung, Benutzung, Rotation und Vernichtung von Schlüsseln.
Platt.Sich.9	Konfigurationsmanagement	3	Demonstration der Funktionen des Konfigurationsmanagements der Cloud-Plattform.	• Verwaltung akkurater CMDB (Configuration Management Databases). • Prüfung der Compliance. • Automatisches Auslösen von Aktionen basierend auf Nicht-Compliance. • Fähigkeit, Änderungen an der Konfiguration im Vergleich zu Best Practices oder benutzerdefinierten Richtlinien zu prüfen.
Platt.Sich.10	Netzwerksicherheit	3	Demonstration der Funktion der Webanwendungs-Firewall und allgemeinen Firewall, einschließlich der Integration mit Regelsätze/Firewalls von Drittanbietern und volumetrischem Angriffsschutz.	• Webanwendungs-Firewall (WAF): Skalierbarkeit. • Support für private und öffentliche Netzwerke. • Fähigkeit, Branchen-/Anbieter-Feeds zu abonnieren, um Regelsätze zu erhalten.

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
				• Automatisches Auslösen von Aktionen innerhalb der Infrastruktur basierend auf Ereignissen bei der WAF. • Firewall-Funktionen, Skalierbarkeit. • Hostbasierte und netzwerkbasierte Firewalls. • Fähigkeit, auf logische Gruppen oder Objekte zu verweisen, zusätzlich zu der Fähigkeit, CIDR-IP-Blöcke anzugeben. • Anzahl von Regeln, die für jede Ebene/jede Komponente unterstützt werden. • Möglichkeit der Unterstützung eines verteilten Betriebsmodells (Netzwerkteam + Entwicklungsteam) durch Richtlinien und Netzwerkkonfiguration.
Platt.Sich.11	Netzwerkkonnektivität	3	Demonstration der Fähigkeit, Verbindungen zu lokalen Netzwerken herzustellen, sowie der Fähigkeit von Endpunkten/Clients, Verbindungen zu privaten Netzwerken innerhalb der Cloud herzustellen.	• Private Konnektivität (hohe Bandbreite > 10 GB/s). • Möglichkeit, Routing- und Firewall-Richtlinien über die gesamte Organisation hinweg zu steuern. • VPN-Konnektivität (Site-to-Site und clientbasiert). • IPV6-Support.
Platt.Sich.12	Instance-Verwaltung	3	Demonstration von Instance-Verwaltungsfunktionen.	• Möglichkeit, den Patch-Status einer großen Menge von Instances zu überwachen und zu verwalten. • Support für die Patch-Verwaltung in Linux- und Windows-Betriebssystemen. • Fähigkeit, Befehle über eine Flotte von Servern hinweg auszuführen, ohne die Notwendigkeit von SSH. • Fähigkeit, den Remote-Zugriff auf virtuelle Maschinen zentral zu kontrollieren und zu prüfen.

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
				• Fähigkeit, via Konsole, CLI und API die Größe einer Instance zu ändern, zusätzliche Volumes anzuhängen, Netzwerkkonfigurationen zu ändern, usw.
Platt.Sich.13	Richtlinienanwendung	3	Demonstration der Fähigkeit, Services so zu konfigurieren, dass der Zugriff aus dem öffentlichen Internet verhindert wird.	• Fähigkeit, beim Vorliegen von Services, die wahrscheinlich kritische/vertrauliche Daten enthalten, den Datenverkehr auf private Netzwerke zu isolieren. • Fähigkeit, Richtlinien zu definieren, die den Zugriff auf Daten basierend auf dem Quellnetzwerk kontrollieren. • Anwendung dieser Zugriffseinschränkungen auf alle Benutzer, einschließlich solcher mit weit gefassten Berechtigungen.
Platt.Sich.14	Scanning nach Schwachstellen	2	Demonstration der Fähigkeit, Images (Container oder VM) nach Schwachstellen zu scannen.	• Fähigkeit, Container in einem Verzeichnis automatisch zu scannen. • Fähigkeit, virtuelle Maschine nach bekannten Schwachstellen zu scannen. • Fähigkeit, Netzwerk-Scans durchzuführen.
Platt.Sich.15	Netzwerkinspektion	2	Demonstration der Fähigkeit, Netzwerk-Datenverkehr von innerhalb einer Kundenumgebung aus zu erfassen/spiegeln (NetFlow und vollständige Pakete).	• Fähigkeit, den Datenverkehr innerhalb der Infrastruktur des Cloud-Anbieters (aus Sicht eines Kundenmandaten) teilweise/vollständig zu spiegeln, einschließlich der vollständigen Paketerfassung. • Möglichkeit einer einfachen Auswahl des Datenverkehrs, der erfasst werden soll. • Möglichkeit des Skalierens auf sehr hohe Datenverkehrvolumes (>50 GB/s).
Platt.Sich.16	Bedrohungserkennung	3	Demonstration der Fähigkeit der Plattform zur Eindringungserkennung,	• Fähigkeit, verdächtige Aktivitäten wie „Mining“ zu erkennen.

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
			einschließlich Bedrohungen von einem Netzwerk, Einsatz von Berechtigungen und Analyse von Nutzungsmustern.	• Fähigkeit, Brute-Force-Authentifizierungs-Angriffe wie SSH-Anmeldungen zu erkennen. • Fähigkeit, den Verlust oder Missbrauch von Anmeldeinformationen zu erkennen. • Anwendung von ML, Analyse großer Mengen von Ereignissen und Hervorheben priorisierter Ereignisse. • Bestrebung nach Aktivierung/Konfiguration (einfacher ist besser). • Fähigkeit der Integration mit externen Services und Benachrichtigungen über Auslöser. • Fähigkeit, die IDs auf globaler Ebene für alle Projekte/Konten zu konfigurieren.
Platt.Leist.1	Optimierung der Datenverarbeitung	2	Demonstration automatischer Empfehlungen für die Optimierung der Kosten für virtuelle Maschinen und Function as a Service.	• Empfehlungen basierend auf tatsächlichen Auslastungs- und Workload-Mustern. • Empfehlungen umfassen geschätzte Ersparnisse und Erkenntnisse über zu erwartende Load-Level/technische Auswirkungen. • Optimierungen sollten sowohl Einsparungen enthalten als auch „Leistungsrisiken“ mit einbeziehen, solche Umstände also, in denen sich virtuelle Maschinen womöglich als für ihre Aufgaben zu klein dimensioniert herausstellen könnten.
Platt.Leist.2	Umgebungsoptimierung	2	Demonstration automatischer Empfehlungen für andere Cloud-Komponenten wie Load Balancer, Netzwerke, Datenbanken, Speicher usw.	• Empfehlungen identifizieren Ersparnisse und potentielle Verbesserungsmöglichkeiten der Leistungseffizienz in anderen Komponenten neben der Kerndatenverarbeitung.

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
Platt.Leist.3	Automatische Skalierung der Datenverarbeitung	4	Demonstration von Möglichkeiten zur automatischen Skalierung einer Anwendung, die in einer virtuellen Datenverarbeitungsumgebung hinter einem Load Balancer bereitgestellt wird. Demonstration der verschiedenen verfügbaren Optionen/Ansätze und der Möglichkeit, vor/nach Skalierungsereignissen weitere (optionale) Maßnahmen auszulösen, etwa eine Benachrichtigung.	• Verschiedene Optionen für die Skalierung: auslöserbasiert, zeitbasiert, manuell oder durch intelligentere Herangehensweisen, die maschinelles Lernen zur Vorhersage der nötigen Kapazität einsetzen. • Vollautomatische Skalierung, einschließlich der Registrierung bei einem Load Balancer und Zustandsprüfungen. • Fähigkeit, einen zufälligen Teil des Codes an bestimmten Punkten des Skalierungslebenszyklus auszuführen.
Platt.Leist.4	Online-Skalierung für Speicher	3	Demonstration der Fähigkeit, sowohl die Kapazität als auch den Durchsatz des Blockspeichers ohne Unterbrechung der Workload zu skalieren.	• Fähigkeit, den Blockspeicher auf verschiedene Speichertypen umzustellen, ohne Services komplett neu erstellen zu müssen. • Fähigkeit, die Größe von Volumes zu erhöhen, die VMs verarbeiten sollen.
Platt.Leist.5	Automatische Skalierung für Managed Services	3	Demonstration der Fähigkeit des Objektspeichers, des API-Gateways, der FaaS-Plattform und der NoSQL-Datenbank, von wenigen (Dutzende) auf viele (Tausende) gleichzeitige Nutzer zu skalieren.	• Reibungsloses automatisches Skalieren, idealerweise ohne das Eingreifen eines Administrators. • Konsistente Leistung während einer hochfahrenden und -skalierenden Phase, die sich an den Skalierungsanforderungen der Produktion ausrichtet. • Bei manchen Komponenten, wie FaaS, sollten bei Bedarf Optionen des Aufwärmens und der Verwaltung gleichzeitiger Ausführungslimits begutachtet werden.

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
Platt.Leist.6	Containerbasierte Workloads	3	Demonstration der Fähigkeit, containerbasierte Workloads zu hosten.	• Optionen für Container-Hosting-Plattformen. • Integration mit anderen IaaS-Komponenten, wie Load Balancern. • Verfügbarkeit einer Service-Mesh-Lösung. • Nicht proprietäre Optionen für Container-Hosting, wie Kubernetes. • Nativer Support für Hochverfügbarkeit auf der Container-Steuerebene. • Fähigkeit, lokale Container-Hosts zu verwalten.
Platt.Zuverl.1	Regionale Resilienz	4	Demonstration des automatischen Failovers einer relationalen Datenbank-Instance innerhalb einer Region, wenn ein geografisch lokalisierter Ausfall (etwa ein Stromausfall) simuliert wird.	• Automatisiertes Failover. • Isolierte Fehlerzonen innerhalb einer Cloud-Region. • Klare Demarkierung und einfaches Erstellen, im Sinne der Hochverfügbarkeit.
Platt.Zuverl.2	Automatische Wiederherstellung von Instances	2	Demonstration der automatischen Wiederherstellung einer Instance/Reihe von Instances nach einer fehlerhaften Zustandsprüfung.	• Konfigurierbare Zustandsprüfungen. • Vollautomatische. Wiederherstellung/erneute Bereitstellung von Instances.
Platt.Zuverl.3	Load Balancer-Zustandsüberwachung	3	Demonstration, wie ein Load Balancer automatisch eine fehlerhafte Instance erkennt und den Datenverkehr zu anderen, fehlerfreien Hosts umleitet.	• Konfigurierbare Zustandsprüfungen. • Automatisiertes Routing von Datenverkehr zu fehlerfreien Hosts.
Platt.Zuverl.4	Regionale Failover	3	Demonstration einer multiregionalen Architektur, einschließlich automatischer	• Globale Zustandsprüfungen. • Automatisierte Routing-Optionen: Latenz, gewichtet und Failover. • Unterstützung sowohl für Workloads virtueller Maschinen als auch für Managed

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
			Umleitung des Datenverkehrs in eine sekundäre Region.	Services wie Objektspeicher-/NoSQL-Datenbank-Services.
Platt.Zuverl.5	Sichern und wiederherstellen	4	Demonstration der Sicherungs- und Wiederherstellungsoptionen für: virtuelle Maschinen, Datenbanken und Managed Services.	• Level an Automatisierung. • Fähigkeit des Wiederherstellens in derselben/einer anderen Cloud-Region. • Fähigkeit, Sicherungen in eine andere Cloud-Region zu kopieren.
Platt.Kost.1	Budgets	3	Demonstration der Fähigkeit der Budgetverwaltung, einschließlich einer Demonstration der Strukturierung für Unterkonten und Projekte.	• Untersuchen Sie die Möglichkeiten der Steuerung und Überwachung des Budgets auf den verschiedenen Ebenen Ihres Unternehmens. • Achten Sie auf Flexibilität, etwa auf die Möglichkeit, Komponenten zu gruppieren (durch Tags), Budgets für bestimmte Cloud-Services festzulegen und Schwellenwerte für Warnungen/Überwachung zu konfigurieren.
Platt.Kost.2	Budgetzuweisung	1	Demonstration der Bereitstellung einer neuen Projektumgebung (Konto), einschließlich des Prozesses der Budgetzuweisung für das Projekt. Die Bereitstellung sollte manuelle Bestätigungsschritte für 1) technische Prüfung/IT, 2) geschäftliche Prüfung/Finanzen einschließen.	• Möglichkeit der eigenständigen Bereitstellung, mit den entsprechenden Genehmigungen. • Automatisierung der Konfiguration der entsprechenden Budgeteinstellungen, Benachrichtigung oder Budgetrichtlinien, gemäß den Anforderungen Ihrer Organisation.
Platt.Kost.3	Budget-Berichterstattung	2	Demonstration von Möglichkeiten zur Budget-Berichterstattung für die gesamte Organisation. Berichterstattung an eine bestimmte Abteilung im Gegensatz zur gesamten Organisation (Need-to-	• Möglichkeit, auf verschiedenen Ebenen der Organisation Einsicht zu gewähren und Bewusstsein und Transparenz zu schaffen, jedoch auf Need-to-know-Basis. • Prognosen sollten auf aktuellen und vergangenen Verbrauchstrends basieren

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
			know-Basis). Die Berichterstattung sollte „tatsächliche" Zahlen enthalten, ebenso wie vorhergesagte/geschätzte Werte.	und frühzeitig vor möglichen Budgetüberschreitungen warnen.
Platt.Kost.4	Budgetkontrollen	1	Demonstration der Fähigkeit, Maßnahmen zu ergreifen, wenn eine Budgetschwelle erreicht wird. Aktionen können umfassen: Benachrichtigungen, Anwenden von Einschränkungen oder aktive Intervention, um eine Budgetüberschreitung zu verhindern.	• Möglichkeit, Maßnahmen auf einfache Art für unterschiedliche Projekte zu definieren. • Möglichkeit, die Maßnahmen je nach Projekt variieren zu lassen, um etwa zwischen Auswirkungen auf die Entwicklung und auf die Produktion zu unterscheiden. • Möglichkeit, für dasselbe Budget/Projekt mehrere Maßnahmen und Schwellen zu definieren. • Möglichkeit, zusätzlich zu Standardfunktionen benutzerdefinierte Maßnahmen zu definieren.
Platt.Kost.5	Budgetperiodizität	1	Demonstration der Möglichkeit, Budgets für unterschiedliche Zeiträume festzulegen (täglich/monatlich/jährlich usw.). Demonstration der Möglichkeit, bei jährlichen Budgets eine variable Verteilung der erwarteten Ausgaben im Verlauf des Jahres festzulegen.	• Möglichkeit, Budgets für unterschiedliche Zeiträume zu definieren. • Möglichkeit, bei jährlichen Budgets die Ausgaben über das Jahr hinweg zu verteilen. Dies ist besonders wichtig für saisonale/hochelastische Workloads, wie eine jährliche Steuererklärung.
Platt.Kost.6	Drittanbieter-Marketplace	3	Demonstration der Möglichkeit, Produkte von Drittanbietern zu kaufen und einzusetzen. Demonstration einer Budgetfestlegung für eine Reihe von Drittanbieterprodukten, die über einen Marketplace verfügbar sind, sowie die Möglichkeit, die	• Möglichkeit, ein Budget für ein bestimmtes Produkt festzulegen; ein globales Budget und ein Budget für eine Reihe von Projekten/Konten. • Möglichkeit, Cloud-Benutzern nur einen Teil des Marketplace zugänglich zu machen.

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
			verfügbaren Produkte einzuschränken.	
Platt.Kost.7	Preismodelle für Datenverarbeitung	3	Demonstration der verschiedenen Preis-/Geschäftsmodelle, die auf virtuelle Maschinen angewandt werden können.	• Die Möglichkeiten sollten On-Demand-Modelle einschließen, ohne erforderliche langfristige Verpflichtung und mit granularer Preisbildung (pro Minute/Stunde). • Optionale langfristige Bindungen im Gegenzug für einen Preisnachlass. • Möglichkeit zum Kauf von Instances mit der Bereitschaft, Unterbrechungen zu tolerieren, im Gegenzug für einen Preisnachlass. • Wichtig: Es sollte möglich sein, diese Modelle innerhalb desselben Projekts/Kontos zu mischen und die Vorteile auch über verschiedene Konten hinweg zu teilen.
Platt.Kost.8	Geschäftliche Optimierungsempfehlungen	3	Demonstration der Möglichkeit, geschäftliche Optimierungsempfehlungen zu erhalten, um so die Ausgaben zu optimieren (ohne technische Änderungen vornehmen zu müssen).	• Ganzheitliche Empfehlungen für mehrere Services, wie zum Beispiel virtuelle Maschinen und verwaltete Datenbanken. • Möglichkeit, Empfehlungen einfach umzusetzen und die erwarteten Einsparungen/Vorteile zu verstehen.
Platt.Kost.9	Dedicated Hosts	4	Demonstration der Möglichkeit, einen Dedicated Host für lokale Lizenzierungen bereitzustellen, die an einen bestimmten Host gebunden sind.	• Benutzerfreundlichkeit der Bereitstellung. • Fähigkeit, die Auslastung des Hosts zu verwalten. • Fähigkeit, den Host über verschiedene Projekte/Mandanten hinweg zu teilen.
Platt.Opt.1	Migration virtueller Maschinen	3	Demonstration des Imports einer virtuellen Maschine von einem lokalen zu einem cloudbasierten VM-Service.	• Fähigkeit, sowohl Windows- als auch Linux-basierte Betriebssysteme zu importieren. • Fähigkeit, mehrere Maschinen gleichzeitig zu importieren.

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
				• Fähigkeit, eine Replikationssitzung aufrechtzuerhalten, um ein schnelles „Failover" zur Cloud zu ermöglichen.
Platt.Opt.2	DevOps- und Automatisierungfähigkeiten	4	Demonstration von DevOps-/Automatisierungsfähigkeiten, einschließlich der Demonstration, wie Umgebungen als Code definiert werden, sowie des Supports von vollautomatischen Bereitstellungen, automatisierten Tests und Rollbacks.	• Fähigkeit, alle Systemkomponenten als Code zu definieren, einschließlich der Netzwerke, virtuellen Maschinen, Speicher, Datenbanken. • Fähigkeit, eine Pipeline zu erstellen. • Fähigkeit, ein Code-Repository zu erstellen. • Fähigkeit, Builds zu automatisieren. • Fähigkeit, Blau/Grün-Bereitstellungen durchzuführen. • Fähigkeit, mehrere Umgebungen zu erstellen und mehrere Stufen einer Bereitstellung zu durchlaufen. • Automatisches Rollback fehlerhafter Bereitstellungen.
Platt.Opt.3	Anwendungs-Hosting	2	Demonstration des Hostings einer einfachen 2-Schichten-Anwendung in einem Low-Code-/Plattform-Service. Einschließen einer relationalen Datenbank und automatischen Skalierung für Anwendungs-/Web-Schicht.	• Einfache Konfiguration über die UI. • Einbindung von Zustandsprüfungen, Skalierung, Hochverfügbarkeit. Plattform-Support, Windows und Linux.
Platt.Opt.4	Sicherheitsintegration	2	Demonstration der Integrationsmöglichkeiten der Plattform aus der Perspektive von Sicherheitsvorfalls- und Ereignisverwaltung.	• Fähigkeit, sicherheitsbezogene Protokolle des Cloud-Anbieters leicht zu integrieren und zu nutzen, sowie APIs für die Integration.
Platt.Opt.5	ITSM-Integration	3	Demonstration der Integrationsmöglichkeiten der Plattform aus ITSM-Perspektive (IT Service Management).	• Möglichkeit, einen Supportfall über eine API zu erstellen, zu überwachen und zu aktualisieren.

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
				• Möglichkeit der Bereitstellung von Services oder Reihen von Services als „Produkte“ über eine API.
Platt.Opt.6	Support	4	Demonstration des Supportangebots.	• Unterschiedliche Stufen des Supports für verschiedene Arten von Workloads. • Fähigkeit, je nach Bedarf auch Support für das Betriebssystem, die Datenbank-Engine usw. eines bestimmten Services zu bieten. • Fähigkeit, ein erstklassiges Angebot mit genannten Support-Führungskräften für kritische Workloads zu unterbreiten. • Fähigkeit, einen strukturierten Prozess für die Ereignisbereitschaft und Architekturprüfung anzubieten. • Einblick in die Roadmap des Anbieters.
Platt.Opt.7	Auditierbarkeit	4	Demonstration der vorhandenen Tools zur Unterstützung von Compliance-Audits.	• Möglichkeit, Details zu Compliance-Audits über die Konsole abzurufen. • Möglichkeit, Umgebungs-Audits zu verwalten und zu automatisieren.
Platt.Opt.8	VM zu Container	1	Demonstration der Konvertierung einer Anwendung auf einer virtuellen Maschine zu einem Container, und die Bereitstellung mithilfe der Container-Plattform des Cloud-Anbieters.	• Benutzerfreundlichkeit der Konvertierung. • Dauer der Konvertierung. • Plattform-Support, .Net und Java.

Workload: Webanwendung – Beispiel für technische Live-Bewertung

Der folgende Bereich stellt einen Bewertungsbogen für eine spezifische „Webanwendungs“-Workload bereit. Bei der Ausarbeitung eines Bewertungsbogens für eine bestimme Anwendung ist es empfehlenswert, die Benutzer, Entwickler und Administratoren der Anwendung mit einzubeziehen. Diese haben meist die umfassendsten Kenntnisse der Anforderungen, derzeitigen Herausforderungen und Einschränkungen.

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
Web.Sich.1	Sicherheit – Anwendungsschutz	3	Demonstration der Fähigkeit, böswillige Versuche zu blockieren, die darauf abzielen, die Anwendung durch SQL-Injection-, XSS-Scripting- oder andere Angriffe auszunutzen.	• Fähigkeit, durch Standardregeln/-funktionen sofort einsatzbereiten Schutz („out of the box") gegen häufige Angriffe bieten zu können. • Fähigkeit zum Erstellen benutzerdefinierter Prüfungen/Regeln/Funktionen.
Web.Sich.2	Sicherheit – Ratenbasierter Schutz	3	Demonstration der Fähigkeit, Angriffe auf eine Anwendung abzuwehren oder dagegen zu schützen, die große Anforderungsraten oder Datenvolumes nutzen.	• Fähigkeit, Limits zu konfigurieren und Anforderungsraten für eine bestimmte IP-Adresse oder Liste von Adressen einzuschränken.
Web.Sich.3	Sicherheit – Quellenbasierter Schutz	3	Demonstration der Fähigkeit, Zugriffe anhand der Quelle (Netzwerk/Standort) einzuschränken.	• Fähigkeit, Einschränkungen nach dem Netzwerkblock oder der Liste von Netzwerkblöcken zu erheben. • Fähigkeit, Einschränkungen nach Ursprungsland zu erheben (ohne die Notwendigkeit, IP-Listen zu verwalten).
Web.Sich.4	Sicherheit – Netzwerksegmentierung	4	Demonstration der Möglichkeit, Komponenten (Webserver, Anwendungsserver/DB-Server) zu isolieren/schützen, um sowohl gegen Nord-Süd- als auch Ost-West-Ausbreitung durch die Infrastruktur zu schützen.	• Fähigkeit, Komponenten in unterschiedliche Subnetze zu platzieren und den Datenverkehrsfluss zwischen Subnetzen zu steuern. • Fähigkeit, den Datenverkehrsfluss auf Ebene der Netzwerkschnittstelle zu steuern. • Fähigkeit, sowohl auf logische Gruppen als auch CIDR-Blöcke zu verweisen.
Web.Sich.5	Sicherheit – TLS-Unterstützung und Zertifikatverwaltung	4	Demonstration der Fähigkeit, einen TLS-gesicherten Endpunkt bereitzustellen und die unterstützenden Komponenten dafür automatisch zu verwalten, einschließlich beispielsweise der automatischen Rotation von Zertifikaten.	• Unterstützung der neuesten TLS-Protokolle und die Fähigkeit, Legacy-Versionen zu deaktivieren, falls nötig. • Einfache Zertifikaterstellung, -verwaltung und -rotation (idealerweise vollautomatisch).

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
Web.Leist.1	Leistung – Skalierbarkeit	4	Demonstration der Fähigkeit, durch dynamische automatische Skalierung von 10 auf 100 000 gleichzeitige Benutzer der Anwendung zu skalieren.	• Fähigkeit, sowohl zeitbasierte als auch auslöserbasierte Skalierungsregeln zu definieren. • Nahtloses Skalieren für den Endbenutzer und Administrator. Automatisches Aufskalieren bei steigender Last, bzw. automatisches Abskalieren bei sinkender Last. • Gewährleistung von Skalierbarkeit auf jeder Ebene der Webanwendung (Load Balancer, Webebene, Datenebene, usw.). • Verfügbarkeit von Caching-Services auf verschiedenen Ebenen der Anwendung, wie jeweils anwendbar.
Web.Leist.2	Leistung – Globale Bereitstellung	3	Demonstration der CDN-Fähigkeiten, darunter auch die Darstellung der Latenz von verschiedenen Punkten weltweit, einschließlich: Australien, Asien, Afrika, Naher Osten, Nordamerika, Südamerika und Europa.	• Fähigkeit, ein CDN durch die CISP-Konsole/ -APIs zu erstellen und zu konfigurieren. • Konfigurierbare Verteilungsregeln für unterschiedliche geografische Regionen. • Konfigurierbares Caching für unterschiedliche Anwendungsfälle/Anwendungen.
Web.Zuverl.1	Zuverlässigkeit – Resilienz in einer einzelnen Region	4	Demonstration der Fähigkeit, lokale Ereignisse zu tolerieren, wie etwa der Verlust der Netzwerkverbindung zum CISP-Rechenzentrum.	• Automatisiertes Failover und Hochverfügbarkeit innerhalb einer Cloud-Region (Stadt).
Web.Zuverl.2	Zuverlässigkeit – Multiregionale Bereitstellung	3	Demonstration einer multiregionalen Bereitstellung einer Webanwendung, einschließlich einer global replizierten Datenbank.	• Fähigkeit, eine multiregionale Anwendung programmatisch bereitzustellen. • Replikation zwischen den Regionen für den Datenspeicher. • Automatisches Routing von Benutzern zur optimalen Region.
Web.Zuverl.3	Zuverlässigkeit – Multiregionales Failover	3	Demonstration des automatischen Failovers einer Webanwendung im Falle eines Service-Problems mit regionalen Auswirkungen.	• Automatisiertes Failover und Hochverfügbarkeit über mehrere Cloud-Regionen hinweg.

Szenario-ID	Szenarioname	Kritikalität (1=Gering, 4=Kritisch)	Demonstrationsanforderungen	Überlegungen zur Bewertung
Web.Kost.1	Kosten – Sichtbarkeit	2	Demonstration der Fähigkeit zur Kostenverfolgung je Anwendung.	• Möglichkeit, den Kostenverlauf einer bestimmten Anwendung einzusehen, darunter auch die Phasen, in denen die Anwendung hoch- bzw. herunterskaliert.
Web.Kost.2	Kosten – Budgets	2	Demonstration der Möglichkeit, Budgets und damit verbundene Warnungen je Anwendung festzulegen.	• Konfigurieren von Budgets je Anwendung und die Möglichkeit, Maßnahmen/Warnungen anhand von festgelegten Schwellenwerten auszulösen.
Web.Ops.1	Ops – Wartungsfenster	3	Demonstration der Möglichkeit, Wartungsfenster festzulegen und mit Geschäftserfordernissen abzustimmen, insbesondere bei Wartungen, die die Verfügbarkeit der Anwendung beeinträchtigen können.	• Konfigurierbare Wartungsfenster für Komponenten, wie einen Service für relationale Datenbanken.
Web.Ops.2	Ops – Protokollierung	3	Demonstration der Fähigkeit, die Protokollierung für eine Anwendung mit mehreren Komponenten zu zentralisieren, einschließlich der langfristigen Speicherung von Protokollen nach der Beendigung/dem Ausfall einer virtuellen Maschine.	• Möglichkeit, einen zentralisierten Protokoll-Service zu konfigurieren, der gemeinsam mit den Anwendungsanforderungen skaliert. • Die Möglichkeit, Regeln/Filtern zu definieren, die Warnungen oder Maßnahmen basierend auf bestimmten Protokollereignissen auslösen.
Web.Ops.3	Ops – Überwachung	3	Demonstration der Überwachung der Anwendung, einschließlich Leistung, Verfügbarkeit, Reaktionszeit, Fehleranzahl usw., und der Funktionalität, basierend auf unterschiedlichen Metrik-Schwellenwerten Maßnahmen zu ergreifen oder Benachrichtigungen auszulösen.	• Verfügbarkeit einer Sammlung von Standardmetriken, wie Datenträger-E/A, Datenbankmetriken, Netzwerk, Load Balancer usw. • Möglichkeit, benutzerdefinierte Metriken und Schwellenwerte zu definieren. • Möglichkeit, ein benutzerdefiniertes Dashboard zu erstellen, das die wichtigsten Metriken darstellt, und diese Dashboards mit den relevanten Benutzern zu teilen.