Erwerb von Cloud-Services im öffentlichen Sektor

Handbuch – inklusive Beispielausschreibung für eine Cloud-Rahmenvereinbarung

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-Infrastruktur-Services in Europa und arbeiten mit Entscheidungsträgern aus Industrie und Politik zusammen, um Beratung und Schulungen zu Cloud-Services und deren Rolle in Industrie, öffentlichem Leben und 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-orientierten Beschaffungsrichtlinien im öffentlichen Sektor innerhalb der EU und in den EU-Mitgliedsstaaten aus.
- fördern kohärente EU-weite Sicherheitsanforderungen und technische Standards.
- unterstützen umfassende Datenschutzanforderungen durch einen Verhaltenskodex.
- arbeiten dafür, den Cloud-Infrastrukturmarkt der EU offen, wettbewerbsfähig und herstellerungebunden zu halten.
- verhindern ungerechtfertigte Inhaltsüberwachungspflichten im EU-Rechtsrahmen.

Unsere Mitglieder liefern und pflegen die grundlegenden „IT-Bausteine“, auf deren Grundlage Regierungen, Behörden und Unternehmen ihre eigenen Systeme aufbauen und Milliarden von Bürgern mit wichtigen Services versorgen können. In dieser Rolle unterstützen wir die Entwicklung von Spitzentechnologien 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-Kodex kam der DSGVO (Datenschutz-Grundverordnung) der Europäischen Union zuvor. Er entspricht den strengen DSGVO-Anforderungen, um Cloud-Infrastrukturanbieter bei der Einhaltung von Richtlinien zu unterstützen und einen zuverlässigen Rahmen zu schaffen, der Kunden die Auswahl von Cloud-Anbietern erleichtert und Vertrauen in deren Services schafft. Bisher wurde die Konformität mit dem CISPE-Verhaltenskodex von über 100 Services erklärt, die von von mehr als 30 Cloud-Unternehmen mit Sitz in über 16 EU-Mitgliedsstaaten bereitgestellt und von Millionen von Endnutzern und Verbrauchern genutzt werden. https://cispe.cloud/code-of-conduct/

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 das öffentliche Beschaffungswesen den Prozess zur Einführung und Nutzung von Cloud-Computing zur Bedingung machen sollte, unterscheidet sich der Erwerb von Cloud-Services von den meisten herkömmlichen Technologieakquisitionen im öffentlichen Sektor. Es müssen neue Ansätze für die Auftragsvergabe in Betracht gezogen werden: CISPE ermutigt die EU-Entscheidungsträger, auf EU-Ebene einen ehrgeizigeren und zukunftsorientierten Ansatz auf Grundlage von „Cloud First“-Politikinitiativen zu entwickeln. Dies trägt dazu bei, das Wachstum des Binnenmarkts für Cloud-Infrastrukturen in Europa voranzutreiben und die Wachstumsziele des digitalen Binnenmarkts (DSM) zu unterstützen.

Dieses Handbuch soll Behörden 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 erklärt wurden: https://cispe.cloud/publicregister

Inhaltsverzeichnis

Zusammenfassung und Zweck dieses Handbuchs

Dieses **Handbuch zum Erwerb von Cloud-Services** soll Auftraggeber , die Cloud-Services über einen wettbewerbsfähigen Beschaffungsprozess erwerben möchten (Ausschreibung oder **„Cloud Services Request for Proposal – RFP“**), jedoch nicht über das nötige Know-how zur Erstellung einer Cloud-Rahmenvereinbarung verfügen, bei der Gestaltung einer Ausschreibung unterstützen.

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 gibt 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 allgemeinen IT-Ausschreibung ähneln. Beispiele für Formulierungen für generische Ausschreibungs- und Auswahlkriterien werden durch Kommentare ergänzt, um verständlich zu machen, warum sich eine Cloud-Ausschreibung von einer herkömmlichen IT-Ausschreibung unterscheidet.

> ***„Cloud-Services“*** *bezeichnet alle Cloud-Technologien und zugehörigen Services, auf die ein Endbenutzer möglicherweise Zugriff benötigt. Dazu gehören neben der Cloud-Infrastruktur selbst Beratungsleistungen 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).*

Das Aufkommen von Cloud-Computing als Standardoption für die IT des öffentlichen Sektors bietet die Möglichkeit, vorhandene Beschaffungsstrategien zu modernisieren. Cloud-zentrierte Akquisitionsprozesse ermöglichen es Organisationen des öffentlichen Sektors, alle Vorteile der Cloud zu nutzen, wie z. B. Zugang zu neuesten Innovationen, höhere Geschwindigkeit und Flexibilität, mehr Sicherheit und besseres Compliance-Management, während gleichzeitig mehr Effizienz und Kosteneinsparungen realisiert werden.

Herkömmliche IT-Beschaffungsmethoden 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, Vetrags-Governance, Geschäftsbedingungen, Sicherheit, technischen Anforderungen, SLAs und vielem mehr. Gleichzeitig reduziert oder eliminiert die Nutzung vorhandener Beschaffungsmethoden 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 Organisationen hinweg. Aus diesem Angebot können die abrufberechtigten Stellen innerhalb der einkaufenden Organisationen diejenigen Cloud-Technologien und damit verbundenen Services erwerben, die ihren jeweiligen Anforderungen entsprechen. Als Instrument für Cloud-Verträge ermöglichen solche Rahmenvereinbarungen den effizienten und effektiven Einkauf von Cloud-Services. Dies führt dazu, dass einkaufende Organisationen und Endnutzerunternehmen 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, eine größere Funktionsvielfalt, ein hohes Innovationstempo und Anpassungsfähigkeit an neue Regionen.

Beachten Sie, dass sich dieser Artikel auf den Erwerb von Infrastructure-as-a-Service-(IaaS)- und Platform-as-a-Service-(PaaS)-Cloud-Technologien konzentriert, die von einem *„Cloud Infrastructure Service Provider" (CISP, Cloud-Infrastukturservice-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-Beratungsleistungen sind bei der Ausschreibung zusätzliche Überlegungen erforderlich.*

Beachten Sie auch, dass dieses Dokument nicht jeden Aspekt der Erstellung einer End-to-End-Rahmenvereinarung für die Cloud-Beschaffung abdeckt. Es gibt zahlreiche weitere Dokumente aus der Branche und von Analysten, die Themen wie Best Practices für die Cloud-Beschaffung, das Budget für die Cloud, die Cloud-Governance usw. behandeln. Wir empfehlen dringend, diese Ratschläge und Dokumente bei der Entwicklung einer allgemeinen Cloud-Beschaffungsstrategie zu berücksichtigen.

Tabelle 1 unten enthält eine Übersicht über das Ausschreibungshandbuch für Cloud Services und Angaben dazu, wo Sie die Beispiele für Ausschreibungsformulierungen für jede Komponente einer Cloud-Service-Ausschreibung finden.

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

Abschnitt	Überblick und Beispielformulierungen für die Ausschreibung
1.0 Überblick über eine Cloud-Rahmenvereinbarung	Ein allgemeiner Überblick über das Modell einer Cloud-Rahmenvereinbarung (Lose, 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 Zeitplan für Antworten auf die Ausschreibung 2.1.3 Definitionen 2.1.4 Detaillierte Beschreibung des Einkaufmodells 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 2.3.2. Vergleich zwischen Anbietern 2.3.3 Vertragsabschluss
2.4 Preise	2.4.1 Mindestvoraussetzungen 2.4.2 Vergleich zwischen Anbietern
2.5 Vertragsausführung/Geschäftsbedingungen	2.5.1 Geschäftsbedingungen 2.5.2 So wählen Sie zwischen Teilnehmern pro Projekt aus pro Projekt 2.5.3 On-Boarding und Off-Boarding
3.0 Best Practices/Erkenntnisse	3.1 Cloud-Governance 3.2 Budgetierung für die Cloud

Abschnitt	Überblick und Beispielformulierungen für die Ausschreibung
	3.3 Verstehen des Partnergeschäftsmodells 3.4 Cloud-Broker 3.5 Beschaffung vor der Ausschreibung/Marktforschung
Anhang A – Technische Anforderungen für den Vergleich zwischen Bietern	Eine Liste generischer Anforderungen an die Cloud-Technologie für Abrufe oder Mini-Wettbewerbe
Anhang B – Demo	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 kann den Erwerb von Cloud-Services auf eine Weise ermöglichen, die sowohl den teilnehmenden Organisationen des öffentlichen Sektors als auch den Cloud-Anbietern zugute kommt. Zu den Vorteilen einer gut konzipierten Cloud-Rahmenvereinbarung gehören:

- **Fokus auf Kooperation:**
    - Mehrere Organisationen, die Bestellungen für ähnliche Anforderungen gemeinsam aufgeben, ermöglichen Zweckmäßigkeit, Effizienz, geringere Kosten und einen vereinfachten Bestellprozess. Dies ist eine effektive Möglichkeit, die Nachfrage mehrerer Organisationen im öffentlichen Sektor nach gemeinsamen Cloud-Technologien und zugehörigen Cloud-Services wie Marketplace-Lösungen und Beratung zu bündeln.
- **Umfassendes Angebot an Cloud-Services:**
    - Dieses kann alle Beratungsleistungen/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:**
    - Organisiert verschiedene Organisationen/Einkäufer im Rahmen gemeinsamer Geschäftsbedingungen und eines einzelnen Rahmenvertrags, anstatt mehrerer Verträge für jede einzelne Organisation.
    - Dies bietet auch Vorteile für die Anbieter: einen Standard-Akquiseprozess, standardisierte Geschäftsbedingungen sowie einen einheitlichen Bestellmechanismus, anstelle 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 – vertragsrechtlich,

automatisch und effizient. Ein mehrjähriger Vertrag, der nicht gut funktioniert und nicht angepasst werden kann, führt zu einer schlechten Erfahrung für die Endbenutzer im öffentlichen Sektor, die Beschaffungsorganisationen und die Cloud-Anbieter.

- Auswahl:
    - Ermöglicht den Käufern die Auswahl aus mehreren qualifizierten CISPs und setzt hohe Maßstäbe für alle Cloud-Services und zugehörigen Services wie einen Cloud-PaaS-/SaaS-Marketplace und Beratung.
    - Ermöglicht die Kontrolle über die Anzahl der Lieferanten innerhalb einer Rahmenvereinbarung, indem sichergestellt wird, dass der Standard jedes Dienstleisters entsprechend überprüft wird.

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

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

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

- LOS 3 – CLOUD-BERATUNG
  Cloud-bezogene Beratungsleistungen (Schulungen, Professional Services, Managed Services usw.) und technischer Support

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

Abbildung 1 unten bietet einen allgemeinen Überblick darüber, wie eine gut strukturierte Ausschreibung für Cloud-Services, die in diese drei Lose 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, alle für den Aufbau und die Wartung der von ihnen benötigten Lösungen erforderlichen Cloud-Services zu ihrer Verfügung zu haben.

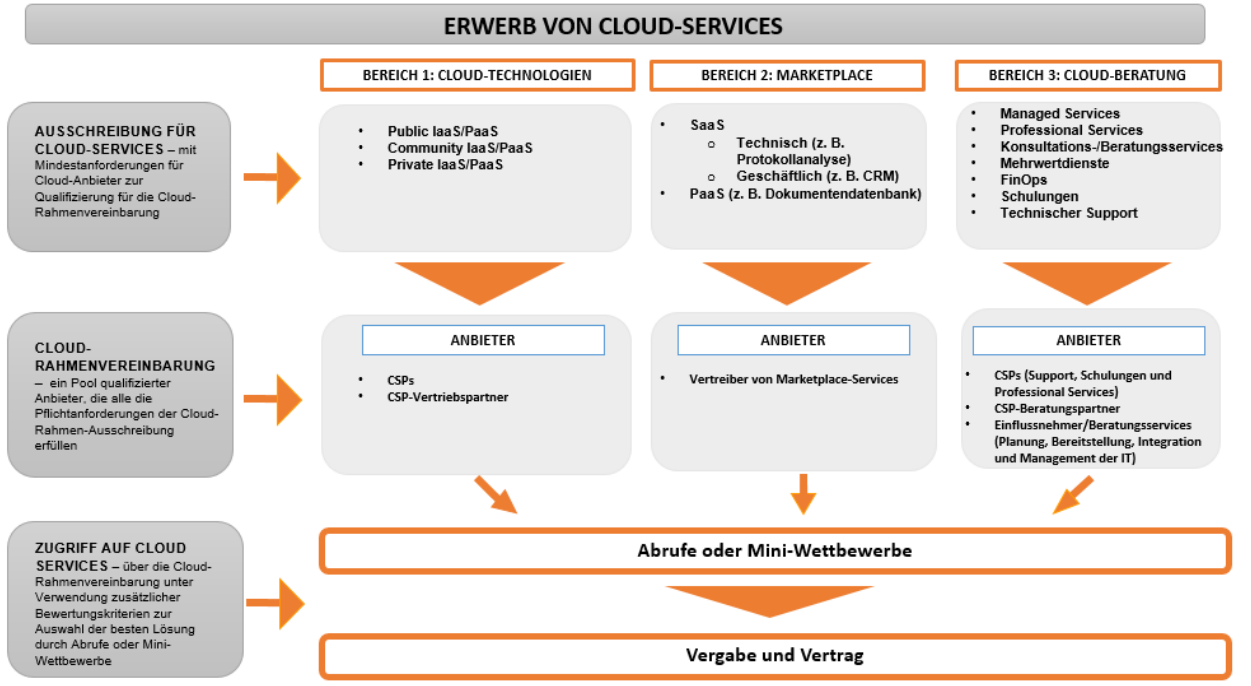

Abbildung 1: Eine erfolgreiche Cloud-Services-Ausschreibung ist in 3 Lose unterteilt. Jedes Los enthält wiederum Kategorien oder „Angebotstypen", um sicherzustellen, dass bei Abrufen innerhalb der Cloud-Rahmenvereinbarung die technischen und vertraglichen Anforderungen der Endbenutzer erfüllt werden.

Hinweis:

- Jedes Los wird an mehrere Anbieter vergeben.
- Los 3 kann über eine separate Ausschreibung oder möglicherweise über einen bestehenden Vertrag für Beratungsleistungen vergeben werden.

Kategorien BEREICH 1

Erfolgreiche Cloud-Rahmenvereinbarungen fordern CISPs auf, das Modell der von ihnen angebotenen Cloud zu beschreiben, eingeteilt in Kategorien innerhalb jedes Loses. Wir empfehlen die Verwendung des Branchenstandards für Cloud Computing (die Essential Cloud Characteristics des National Institute of Standards and Technology (NIST)) 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 LOS 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 „Nice-to-have"-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 die ausschreibende Stelle 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 Lieferanten für eine bestimmte Workload oder ein bestimmtes Projekt zu ermitteln. Ein Mini-Wettbewerb bedeutet, dass ein Kunde im Rahmen der Rahmenvereinbarung einen weiteren Wettbewerb ausruft, indem er alle Lieferanten für einen Bereich dazu einlädt, auf eine Reihe von Anforderungen zu reagieren. Der Kunde lädt alle infrage kommenden Lieferanten innerhalb des Loses 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 jedes dieser Lose ***unterschiedliche Vertragsbedingungen*** *gelten, siehe Abb. 1. 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 dem **LOS 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)** eine klare Definition des Modells übergreifender Verantwortlichkeit zwischen dem öffentlichen Sektor und den Cloud-Anbietern, die 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 bedingt einen völlig neuen Zugang zur Nutzung der Technologie. Gut durchdachte Ausschreibungen für Cloud-Services können Organisationen im öffentlichen Sektor dabei unterstützen, schnell von der Cloud zu profitieren.

Von allen Aspekten beim Cloud-Einkauf, die sich aus unserer Sicht bewährt haben, ist eine klare Definition der Verantwortungsbereiche sicherlich der beste Startpunkt. Das Modell übergreifender Verantwortlichkeit[1] wird hauptsächlich im Zusammenhang mit der Sicherheit und Compliance in der Cloud verwendet. Diese Abgrenzung von Verantwortlichkeiten gilt aber für alle Aspekte der 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 Code of Conduct for Cloud Infrastructure Service Providers (CISPE-Verhaltenskodex für Cloud Infrastructure Service Provider): 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 Services Provider (MSP) für Clouds einem Kunden bei der Konfiguration und Verwendung von CISP-Überwachungsfunktionen helfen, um dessen einzigartigen 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 Beratungsleistungen und Managed/Professional Services, die Kunden bei der Entwicklung, Gestaltung, Erstellung, Migration und Verwaltung ihrer Workloads und Anwendungen in der Cloud unterstützen. Zu diesen Unternehmen gehören Systemintegratoren, strategische Beratungsunternehmen, Agenturen, Managed Services *Provider und Wiederverkäufer.*

Stellen Sie sich den Einkauf von Cloud-Services wie einen Einkauf in einem Baumarkt vor. In einem Baumarkt stehen Ihnen 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 einige Möglichkeiten:

1. Sie kaufen die Materialien und Werkzeuge selbst und bauen selbst 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 entwickeln/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 tatsächlich nur auf die standardisierten Cloud-Technologien und -Tools des CISP zugreifen (direkt bei einem CISP oder über einen CISP-Vertriebspartner – siehe **LOS 1).** Erforderliche SaaS- und PaaS-Software sollte auf einem Cloud-Marketplace verfügbar sein (**LOS 2**). Wenn zusätzliche Beratung, Migration, Implementierung und/oder Verwaltungshilfe benötigt wird, kommt hier das Partnernetzwerk eines CISP ins Spiel (**LOS 3**).

Beispielformulierungen für die Ausschreibung: Einleitung und strategische Ziele

Cloud Computing bietet Organisationen im öffentlichen Sektor 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 Cloud-bezogene Services anbieten.

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

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

- ***Flexibilität:** 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:** Gewerbekapitalausgaben durch variable Ausgaben ersetzen (z. B. Investitions- zu Betriebskosten, Bezahlung nur für tatsächlich genutzte Dienste)*
- ***Budgetierung:** Anzeige von Rechnungs- und Nutzungsdaten auf granularer und zusammenfassender Ebene, Visualisierung von Ausgabenentwicklung sowie Prognose künftiger Ausgaben*
- ***Elastizität:** Niedrigere variable Kosten durch die höheren Größenvorteile der Cloud*
- ***Kapazität:** Exakte Bestimmung von Infrastrukturkapazitätsanforderungen*
- ***Unabhängigkeit von Rechenzentren:** Konzentration auf die Bedürfnisse unserer Bürger, statt Zeit mit dem umständlichen Aufbau und Betrieb von Server-Racks und -Stacks zu verbringen*
- ***Sicherheit:** Formalisieren von Kontodesigns mit mehr Transparenz und Überprüfbarkeit von Ressourcen und Eliminierung der Kosten für den Schutz von Anlagen und physischer Hardware*
- ***Übergreifende Verantwortlichkeit:** Weniger betriebliche Verantwortung. 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) Zunächst vollständige Bestandsaufnahme aller IT-Ressourcen; (2) zentrales Verwalten all dieser Ressourcen; und (3) Erstellen von Warnmeldungen zu Nutzung/Abrechnung/Sicherheit usw. All dies 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 potenzieller Optimierung für Sicherheit, Zuverlässigkeit, Leistung und Kosten*
- ***Reversibilität:** Portabilitätstools und -services, die die Migration zur und von der CISP-Infrastruktur erleichtern, die Anbieterabhängigkeit 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 Data Protection Code of Conduct (CISPE-Verhaltenskodex zum Datenschutz)*
- ***Transparenz:*** *Kunden sollten berechtigt sein, den Standort der Infrastrukturen zu kennen, die zur Verarbeitung und Speicherung ihrer Daten (Stadtgebiet) verwendet werden*

2.1.2 Zeitplan für Antworten auf die Ausschreibung

Es empfiehlt sich bei der Erstellung einer Cloud-Rahmenvereinbarung und der zugehörigen Ausschreibung der Cloud-Services, den interessierten Unternehmen einen Zeitrahmen für die Reaktion auf die Ausschreibung anzugeben. Je stärker die Zusammenarbeit mit der Branche, desto besser, da dadurch sichergestellt wird, dass alle Parteien die Anforderungen der Ausschreibung verstehen und tatsächlich wissen, 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 Zeiträumen dar.

Beispielformulierungen für die Ausschreibung: Zeitrahmen für die Antwort

Siehe nachstehenden Ausschreibungszeitplan für die Cloud-Services-Ausschreibung:

Zeitplan für Cloud-Services-Ausschreibung
• *Veröffentlichung Leistungsanfrage:* • *Antwort auf die Leistungsanfrage:* • *Veröffentlichung Entwurf einer Ausschreibung:* • *Fälligkeit Antwort auf Entwurf einer Ausschreibung:* • *Branchenberatungsphase: <Zeitplan>* • *Präqualifikation Veröffentlichung Ausschreibung:* • *Präqualifikation Antwort auf die Ausschreibung:* • *Freigabe Ausschreibung:* • *Fälligkeit Fragen Runde 1:* • *Antworten Runde 1:* • *Fälligkeit Fragen Runde 2:* • *Antworten Runde 2:* • *Fälligkeit Antwort auf Ausschreibung:* • *Angebotsklärungszeitraum:* • *Verhandlungszeitraum:* • *Datum der Absicht zur Vergabe:* • *Vertragsschluss:* • *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 Zeiträumen 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. In Folgendem finden Sie eine Liste mit Beispieldefinitionen:

Beispielformulierungen für die Ausschreibung: Definitionen

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

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

- ***Platform as a Service (PaaS).*** *Die dem Auftraggeber bereitgestellte Kapazität besteht darin, auf der Cloud-Infrastruktur vom Auftraggeber erstellte oder erworbene Anwendungen bereitzustellen, die mithilfe von Programmiersprachen, Bibliotheken, Services und Tools erstellt worden sein können, die vom Anbieter unterstützt werden. Der Auftraggeber verwaltet oder steuert nicht die zugrunde liegende Cloud-Infrastruktur, einschließlich Netzwerk, Server, Betriebssysteme oder Speicher, hat jedoch die Kontrolle über die bereitgestellten Anwendungen und möglicherweise Konfigurationseinstellungen für die Anwendungshostingumgebung.*

- ***Software as a Service (SaaS).*** *Die dem Auftraggeber bereitgestellte Kapazität besteht darin, Anwendungen des Anbieters in einer Cloud-Infrastruktur auszuführen. 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 Auftraggeber verwaltet oder steuert die zugrunde liegende Cloud-Infrastruktur nicht selbst, einschließlich Netzwerk, Server, Betriebssysteme, Speicher oder sogar einzelner 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 Nutzern 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.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 mehreren 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 entsteht (z. B. Cloud Bursting für den Lastenausgleich zwischen Clouds).*

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

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

2.1.4 Detaillierte Beschreibung des Einkaufmodells und Wettbewerbs innerhalb der Rahmenvereinbarung

Wie bereits 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-Distributoren und kaufende Organisationen ihre jeweiligen Rollen verstehen.

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

- Wer wird im Rahmen der Vereinbarung für Integration und Managed Services im Zusammenhang mit den Cloud-Technologien verantwortlich sein?
- Muss ein CISP-Vertriebspartner/-Partner Zusatzleistungen 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 Services Provider oder eine andere Art Anbieter von IT-Dienstleistungen?

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

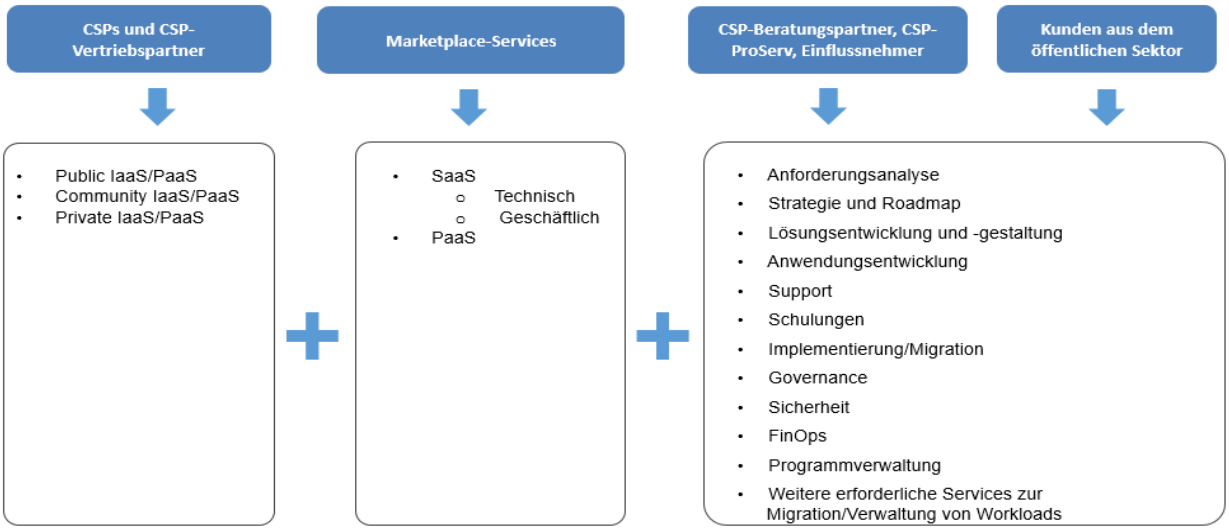

Abbildung 2: Eine Ausschreibung für Cloud-Services sollte Endnutzern eine Palette aller benötigten Cloud-Services zur Verfügung stellen. Kunden aus dem öffentlichen Sektor benötigen einen CISP für Cloud-Technologien und unter Umständen einen Marketplace für PaaS- und SaaS-Produkte. Nur dann kann der Kunde selbst bestimmen, welche Rolle er bei der Bereitstellung von Cloud-Services übernehmen möchte und wie viel er an Beratungsunternehmen/Systemintegratoren/Managed Services 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 sollte sicherstellen, dass der Auftraggeber in der Lage ist, die Angebote der einzelnen Anbieter angemessen zu bewerten, sodass sie unter den für die Workload/das Projekt geeigneten Services die passenden Anbieter auswählen können. Dies lässt sich am besten erreichen, indem die Services in verschiedene Lose aufgeteilt werden und klar definiert wird, wie unter der Rahmenvereinbarung Abrufe und Mini-Wettbewerbe durchgeführt werden.

Beispielformulierungen für die Ausschreibung: Einkaufsmodell

*Diese Vereinbarung dient als **Rahmenvertrag** für die Beschaffung von Cloud-Leistungen. Diese Cloud-*Rahmenvereinbarung *umfasst mehrere **Lose,** gemäß der Definition von **<ORGANISATION>,** für Cloud-Technologien und zugehörige Marketplace-Services/-Produkte, Beratungsleistungen, Professional Services/Systemintegration/Managed Services/Migration, Schulungen und Support, gemäß den Definitionen von **<ORGANISATION>,** und kann von mehreren berechtigten Organisationen/Behörden 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 die gewünschten spezifischen Cloud-Technologien und Cloud-bezogenen Services erwerben, und zwar zum gewünschten Zeitpunkt, anstatt sie durch einzelne Beschaffungsvorgänge zu erwerben. Ein solcher Ansatz reduziert die administrativen Anforderungen, die Komplexität der Beschaffung und den Zeitbedarf 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. Diese 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) Lose** unterteilt.*

1. ***LOS 1: CLOUD-TECHNOLOGIEN** – voller Umfang an Cloud-Anbieter-Technologien (direkt vom CISP, von einem Vertriebspartner oder von einem Vertriebspartner mit Mehrwertdiensten/Support):*
    i. ***IaaS- und PaaS-Services** – eine Auswahl aus Cloud-Technologien, z. B. Datenverarbeitung, Speicher, Netzwerke, Datenbanken, Analysen, Anwendungsservices, Bereitstellung, Verwaltung, Entwickler, „Internet of Things" (IoT) usw. Umfasst Cloudtechnologie-Komplettlösungen wie DR/COOP, Archiv, Big-Data-Analyse, DevOps usw.*
2. ***LOS 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. ***LOS 3: CLOUD-BERATUNG** – voller Umfang an Beratungsleistungen (Managed Services, Professional Services, Konsultations-/Beratungsleistungen, Mehrwertdienste, FinOps, technischer Support) im Zusammenhang mit der Migration und Nutzung der Cloud. Diese Services können Folgendes umfassen: Planung, Design, Migration, Verwaltung, Support, Qualitätssicherung, Sicherheit, Schulung usw.*

Anbieter können ihre Angebote für mehrere Bereiche einreichen.

Anbieter geben 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 Dienstleistungen bei Bedarf bestellen oder „abrufen". Durch das Abschließen eines Abrufvertrages im Rahmen der Rahmenvereinbarung können Käufer die Anforderungen bei einem Abruf mit zusätzlichen funktionalen Spezifikationen verfeinern und gleichzeitig die in der Rahmenvereinbarung angebotenen Leistungen beibehalten.

Verträge, die im Rahmen der Rahmenvereinbarung vergeben werden, verfügen über ein eindeutiges Prüfprotokoll hinsichtlich der Anforderungen, die zur Auswahl des Lieferanten in den einzelnen Bereichen verwendet wurden. Die Endkunden führen Aufzeichnungen über die Kommunikation mit den Anbietern, einschließlich aller früheren Interaktionen auf dem Markt, Bieterfragen, 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 Endnutzern, Einkaufsspezialisten und technischen Experten, um eine Liste der Dinge zu erstellen, die sie unbedingt brauchen, sowie derer, die zwar positiv 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 Rahmen 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 entsprechenden Bereiche aus und suchen dann nach Services.

3. ÜBERPRÜFUNG UND BEWERTUNG DER SERVICES

Käufer im Rahmen der Rahmenvereinbarung überprüfen die Servicebeschreibungen, um die passenden Services zu finden, und zwar basierend auf den Anforderungen und dem Budget. Jede Servicebeschreibung enthält Folgendes:

- *Dokument zur Definition des Services oder Links zu Definitionen des Services*
- *Ein 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 Rahmen der Rahmenvereinbarung können mit Anbietern sprechen, um sie zu bitten, ihre Servicebeschreibungen, Geschäftsbedingungen, Preise oder Servicedefinitionsdokumente/-modelle zu erläutern. Alle Gespräche mit Anbietern werden aufgezeichnet.

4. SERVICE AUSWÄHLEN UND VERTRAG VERGEBEN

Ein Anbieter

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

Mehrere Anbieter

Sind mehrere Anbieter in der engeren Auswahl, wählt der Käufer das wirtschaftlich günstigste Angebot aus. 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 Lieferanten in Betracht ziehen*
- *Spezifische Informationen zu Mengenrabatten oder Unternehmensrabatten sowie Services zur Kostenoptimierung von Anbietern einholen*

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

Tabelle2: Bewertung des wirtschaftlich günstigsten Angebots

Vergabekriterien
Kosten über die gesamte Lebensdauer: *Kosteneffizienz, Preis und Betriebskosten*
Technische Leistungfähigkeit und funktionale Eignung: *Abdeckung, Netzwerkkapazität und Leistung gemäß den relevanten Service-Levels*

After-Sales-Servicemanagement: *Helpdesk, Dokumentation, Kontoverwaltungsfunktionen und Sicherstellung der Versorgung einer Vielzahl von Services*
Nicht-funktionale Anforderungen

MINI-WETTBEWERBE

Falls erforderlich, kann ein Mini-Wettbewerb abgehalten werden, um den besten Lieferanten für eine bestimmte Workload oder ein bestimmtes Projekt zu ermitteln. Ein Mini-Wettbewerb bedeutet, dass ein Kunde im Rahmen der Rahmenvereinbarung einen weiteren Wettbewerb ausruft, indem er alle Lieferanten für einen Bereich dazu einlädt, auf eine Reihe von Anforderungen zu reagieren. Der Kunde lädt alle befähigten Lieferanten 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 Auftraggeber als auch der Anbieter unterzeichnen eine Kopie 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.*

Eine Kopie des Vertrags muss von allen interessierten Parteien (Auftraggeber 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 Angebote von herkömmlichen Rechenzentren oder Hardwareanbietern eingereicht werden, die eine herkömmliche Lösung als „Cloud“ verpacken. Die Teilnehmer an der Ausschreibung sollten demonstrieren, wie sie die unten aufgeführten Mindestanforderungen an die Administration erfüllen.

Beachten Sie auch hier, dass sich dieses Dokument auf LOS 1 – CLOUD-TECHNOLOGIEN konzentriert. Wir haben jedoch zusätzliche Informationen zu LOS 2 – MARKETPLACE und LOS 3 – CLOUD-BERATUNG immer dann hinzugefügt, wenn es hilft, den Gesamtkontext hinsichtlich der Anforderungen und des Umfangs der Ausschreibung zu verdeutlichen. Es ist beispielsweise wichtig, Mindestqualifizierungskriterien für CISP-Vertriebspartner/MSP/SI/Beratungsunternehmen usw. anzugeben und sicherzustellen, dass diese (1) direkt mit dem CISP als Vertriebspartner 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: Bieter-Mindestanforderungen – Verwaltung

Im Rahmen dieser Rahmenvereinbarung werden Verträge an mehrere Anbieter in den folgenden Kategorien vergeben. Bei den Anbietern muss es sich um einen kommerziellen CISP, einen externen Vertriebspartner eines CISP, einen Distributor 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:

LOS 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 vertreiben: _____*
- *Weisen Sie über ein Dokument des CISP nach, dass Sie ein autorisierter Vertriebspartner für dessen Angebote sind: _____*

LOS 2

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

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

LOS 3

____ - CISP für Professional Services

____ - Anbieter des technischen CISP-Supports

____- CISP-Partner, der Services für die Nutzung oder den Betrieb eines CISP bereitstellt

___- Einflussnehmer/Berater, der Services für die Nutzung oder den Betrieb auf einem CISP erbringt

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: _____

LOS 1: ADMINISTRATIVE MINDESTANFORDERUNGEN

Cloud-Service-Anbieter (CISPs)
Um sich als CISP zu qualifizieren, muss dieser die folgenden Anforderungen erfüllen.

Vorgeschlagene Anforderungen für CISP	*Grund*
Informationen zur Organisation wie Name, rechtliche Struktur, Registrierungs-/DUNS-Nummer, USt. usw.	

Unternehmensgröße, wirtschaftliche und finanzielle Leistungsfähigkeit[3]	*Der Kunde kann feststellen, dass der CISP den Vertrag ausführen kann.*
Ausschlussgründe, z. B. kriminelle/betrügerische Aktivitäten usw.	
Fallstudien/Kundenreferenzen (erforderliche Anzahl/Typ angeben)	*Der Kunde kann die Erfahrung des CISP im Bereitstellen der erforderlichen Services prüfen.*
Soziale Unternehmensverantwortung	*Diese sollten öffentlich zugängliche Versionen sein, die vom CISP bereitgestellt werden.*
Öffentlich verfügbare Nachhaltigkeitsverpflichtungen und -praktiken.	*Der Kunde kann sehen, dass ein CISP sich verpflichtet hat, sein Geschäft so umweltfreundlich wie möglich zu führen.*
Der CISP muss in den letzten 5 Jahren eine nachweisliche Erfolgsgeschichte bei der Entwicklung und Veröffentlichung neuer nützlicher Services und Funktionen vorweisen können, insbesondere im Bereich PAaaS, maschinelles Lernen und Analyse, Big-Data, Managed Services und Optimierungsfunktionen für die Cloud-Nutzung. Öffentlich zugängliche Änderungsprotokolle oder Aktualisierungs-Feeds können verwendet werden, um diesen Punkt zu belegen.	*Zeigt, dass der CISP daran arbeitet, neue Produkte schnell in die Hände der Kunden zu bringen und diese Produkte dann schnell zu iterieren und zu verbessern. Dadurch arbeiten Kunden stets mit der modernsten IT-Infrastruktur, ohne dafür neues Kapital zu investieren.*

Vertriebspartner-/Partnerbeziehung mit CISP

<ORGANISATION> *verlangt, dass der Hauptauftragnehmer direkt mit dem CISP als Vertriebspartner oder Wiederverkäufer 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 Unterauftragsebene zwischen dem Hauptauftragnehmer der* ***Rahmenvereinbarung*** *und dem CISP stattfinden. Diese Anforderung verringert auch die Komplexität, die zusätzliche Vertriebspartnerebenen 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 Aufbau 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 der Lösungen und Ergebnisse in einer Cloud-Services-Ausschreibung auf eine vergleichsweise allgemeine Ebene und nicht auf die dem System zugrundeliegenden Methoden, Infrastrukturen oder Hardware, die zur Bereitstellung der eigentlichen Cloud-Services eingesetzt werden.

[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 Mitarbeiterteamstruktur. 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/Performance.

2.2.1 Mindestvoraussetzungen

Herkömmliche IT-Beschaffungen basieren häufig auf Geschäftsanforderungen, die in mehreren Arbeitssitzungen entwickelt wurden 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 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 neue Lösung konzipieren. Dieses Modell ist nicht mit Cloud-Anschaffungen kompatibel.

Organisationen des öffentlichen Sektors sollten ihre Geschäftsziele und Leistungsanforderungen verstehen, jedoch nicht in einer Ausschreibung ein konkretes Systemdesign und Funktionalitäten vorgeben. Stattdessen sollten sie 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 die Bewertungskriterien darauf basieren, wie gut die Technologie und die zugehörigen Services die Geschäftsziele erfüllen oder verbessern, ob sie ihren Performanceanforderungen genügen oder ob sie die Fähigkeit zur Feinabstimmung von Geschäftsregeln durch Konfiguration erreichen können.

Cloud-Ausschreibungen sollten die richtigen Fragen stellen, um die besten Lösungen zu erhalten. Da in einem Cloud-Modell keine physischen Ressourcen 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 LOS 1 qualifizieren, einen hohen Standard erfüllen. Die Anforderungen sollten auch nicht zu präskriptiv sein, um den Zugang zu einer breiten Palette qualifizierter CISPs nicht zu beschneiden.

Beispielformulierungen für die Ausschreibung: Ressourcen der Cloud-Anbieter

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

Vorgeschlagene Anforderungen für CISP	*Grund*
Infrastruktur	
Die CISP-Infrastruktur sollte mindestens 2 Cluster von Rechenzentren bieten. Jedes 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 jedes 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 punktuelle Ausfälle vermieden werden können.*

Der CISP sollte logisch und geografisch isolierte Regionen bereitstellen. Kundendaten dürfen nicht außerhalb dieser Regionen durch den CISP repliziert werden.	*Die Anforderungen an die Datenaufbewahrung 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.	*Somit kann der Kunde sicherstellen, 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 die 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 DSGVO-zertifizierte Services gemäß dem CISPE-Verhaltenskodex zum Datenschutz anbieten, damit der Kunde DSGVO-konforme Anwendungen erstellen kann.	*Der Kunde muss in der Lage sein, Anwendungen in Übereinstimmung mit der DSGVO zu erstellen oder auszuführen, daher sollte das Angebot DSGVO-konformer Services und Tools eine Mindestvoraussetzung sein.*
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 transparent aufzeigen, wie die Anwendung betrieben und verwaltet wird. SOC-Berichte sind entscheidend für Vertrauen und Transparenz.*
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 Services anbieten, darunter Objektspeicher, verwaltete relationale Datenbank, verwaltete nicht relationale Datenbank, verwaltete Load Balancer, Überwachungstools und eine 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 klare 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 vollständige Kontrolle über seine Daten ermöglichen, dem Kunden die Freiheit geben, den Speicherort der Daten auszuwählen (Stadtgebiet), und	*Der Kunde muss die Kontrolle darüber haben, wo Daten gespeichert werden, wie der Zugriff auf Inhalte verwaltet*

sicherstellen, dass keine Kundendaten verschoben werden, es sei denn, eine solche Verschiebung wird vom Kunden selbst initiiert.	*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 die gesamte Zeit zu überwachen. Die Tools müssen eine grundlegende Segmentierung der Kosten basierend auf Workload, Service und Konto ermöglichen.	
Der CISP muss Tools anbieten, über die der Kunde benachrichtigt 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 vordefinierte Vorlagen und Softwarelösungen bereitstellen kann, die entweder vom CISP gehostet werden oder in diesen integriert werden, und zwar für die folgenden Lösungen:

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

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

- *Notfallwiederherstellung*
- *Entwicklung und Test*
- *Archivierung*
- *Sicherung und Wiederherstellung*
- *Big Data*
- *High Performance Computing (HPC)*
- *Internet of Things (IoT)*
- *Websites*
- *Serverlose 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 verschiedener Bewerber 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 in eine aussagekräftigere Analyse von „Optionen mit Mehrwert“ oder „bestem Wert“ einfließen.

Der öffentliche Sektor verlangt oft einen Wettbewerb zwischen Bietern, bei dem Bewertungskriterien wie Bestwert, wirtschaftlichstes Angebot oder niedrigster Preis angelegt werden. Auch bei diesem Teil einer Cloud-Services-Ausschreibung ist es 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) bewertet werden. Stattdessen empfehlen wir dringend, die Lösungen auf einer höheren Ebene zu bewerten, z. B. mit Blick auf die in Abschnitt *2.2.1* aufgeführten Punkte. Anschließend können Organisationen im öffentlichen Sektor dann die Cloud-spezifischen Anforderungen berücksichtigen, z. B. die in *Anhang A – Technische Anforderungen für den Vergleich zwischen Bietern* aufgeführten Punkte.

Ausschreibungen sollten benennen, welche Eigenschaften die Cloud erfüllen muss, um die benötigte Lösung aufbauen zu können. Dazu können Organisationen des öffentlichen Sektors die grundlegenden Cloud-Merkmale des National Institute of Standards and Technology (NIST) nutzen und zusätzlich Berichte von unabhängigen Dritten verwenden, um sicherzustellen, dass der CISP das am besten geeignete Angebot für eine „echte Cloud“ liefert und dieses auch in großem Umfang funktioniert.

Beispielformulierungen für die Ausschreibung – Vergleich zwischen Anbietern

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

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

1) ***On-Demand-Self-Service:** Der Bieter muss die Möglichkeit anbieten, Datenverarbeitungsfunktionen wie Serverzeit und Netzwerkspeicher nach Bedarf automatisch und einseitig bereitzustellen, ohne dass eine menschliche Interaktion mit einem Serviceanbieter erforderlich ist. Der Bieter stellt dem Auftraggeber die Kapazität zur Verfügung, um einseitig Dienstleistungen (d. h. ohne Prüfung oder Genehmigung durch den Bieter) bereitzustellen. Erklären Sie, wie dies mit Ihrem Angebot oder dem Angebot, das Sie vertreten, funktioniert.*

2) ***Universeller Netzwerkzugriff:** Der Bieter muss 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.*

3) ***Ressourcen-Pooling:** Der CISP des Bieters muss gebündelte Datenverarbeitungsressourcen bereitstellen, die mehrere Benutzer bedienen. Dabei wird ein Mehrmandantenmodell verwendet, in dem verschiedene virtuelle Ressourcen dynamisch zugewiesen und je nach Benutzernachfrage umverteilt werden. Der Benutzer kann den Standort auf einer höheren Abstraktionsebene angeben (z. B. Land, Region oder Rechenzentrumsstandort).*

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

Der Bieter soll die Skalierung dieser Ressourcen innerhalb von Minuten oder Stunden nach einer Bereitstellungsanfrage zur Verfügung stellen. Erklären Sie, wie dies mit Ihrem Angebot oder dem Angebot, das Sie vertreten, funktioniert.

4) ***Schnelle Anpassbarkeit:*** *Der CISP des Bieters unterstützt die Bereitstellung und Beendigung von Services (Skalierung nach oben und unten). Dadurch wird der Service innerhalb der vorgeschriebenen Mindestzeiten (maximal „x" Stunden) ab der Bereitstellungsanfrage verfügbar gemacht. Der Bieter unterstützt die Rechnungsanpassungen, die sich aus diesen Bereitstellungsanfragen ergeben, auf stündlicher oder täglicher Basis.*

5) ***Messbarer Service:*** *Der Bieter muss die Servicenutzung über ein Online-Dashboard oder einen vergleichbaren elektronischen Zugang transparent machen.*

Darüber hinaus muss der CISP:

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

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

2.2.2.1 Service-Level-Vereinbarungen (SLAs)

CISPs stellen standardisierte kommerzielle SLAs für Millionen von Kunden bereit und können daher keine kundenspezifischen SLAs, wie im Fall von lokalen Rechenzentrumsmodellen, anbieten. Kunden von CISPs können jedoch (oft mithilfe von CISP-Partnern) die Architektur ihrer Cloud-Nutzung so gestalten, dass die kommerziellen SLAs eines CISP wirksam für das Erfüllen und Übertreffen kundenspezifischer Anforderungen und individueller SLAs genutzt werden können.

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

Bespielformulierungen für die Ausschreibung: Service-Level-Vereinbarungen

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

<ORGANISATION> *wird laufend über die CISP-SLAs informiert und wichtige Workloads und Anwendungen so bereitstellen, dass sie auch bei Nichterfüllung eines SLA weiter funktionieren.*

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

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

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

2.2.3 Vertragsabschluss

Die CISP-Geschäftsbedingungen sind so konzipiert, dass sie die Funktionsweise eines Cloud-Servicemodells widerspiegeln (physische Ressourcen werden nicht erworben und CISPs arbeiten 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.

2.2.3.1 Neue und sich ändernde Services

CISPs bieten Leistung über einen Service. Im Gegensatz zu herkömmlichen Vor-Ort-Lösungen, die Upgrades und Servicewartungsverträge erfordern, stellen Cloud-Anbieter einfach den standardisierten Service bereit. Damit das Cloudmodell Größenvorteile erzielen kann, werden Upgrades und Änderungen an der zugrundeliegenden Infrastruktur für alle Kunden bereitgestellt und Kunden wählen dann die Services aus, die sie verwenden. Der Service ist somit reibungsloser als bei älteren Systemen vor Ort 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 wird, dass sie das Hinzufügen neuer CISP-Services während der Laufzeit des Rahmenvertrags ermöglichen. zwar kann das EU-Einkaufsrecht das Hinzufügung von wesentlich anderen CISP-Services zu einer bestehenden Rahmenvereinbarung einschränken, Aktualisierungen und neue Versionen von Diensten, die nicht als wesentliche Änderungen gelten, können jedoch 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 und modernste Virtualisierungstechnologien 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, Charakteristika, Eigenschaften oder andere Merkmale der Cloud-Services ändern oder löschen kann. Falls eine solche Änderung, Ergänzung oder Löschung erfolgt, werden die Vorgaben des Cloud-Service entsprechend angepasst.*

Der Umfang dieses Lieferauftrags 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 Herstellerbindung, da keine physischen Ressourcen 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 Cloud-Technologien 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 Dokumentationen darüber,

wie diese Services als vernünftige „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.

Die branchenspezifischen Verhaltenskodizes für „Data Porting“ und den „Wechsel von Cloud-Anbietern“ werden derzeit entwickelt, um die Anforderungen des Artikels 6 der EU-Verordnung über den „freien Verkehr nicht personenbezogener Daten“ zu erfüllen. Sobald sie öffentlich zugänglich sind, sollten sie als Hilfsmittel verwendet werden, um diese Art der Reversibilität zu demonstrieren. Diese Referenzen werden auf der CISPE-Website veröffentlicht.

Beispielformulierungen für die Ausschreibung: Ein- und Austritt

<ORGANISATION> sucht nach Vorschlägen, die eine angemessene Exit-Strategie enthalten, um eine Anbieterbindung zu verhindern. <ORGANISATION> kauft keine physischen Ressourcen 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 Abhängigkeit zu einem Anbieter 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 ihre Computer-Images exportieren und vor Ort oder bei einem anderen Cloud-Anbieter verwenden (vorbehaltlich der Softwarelizenzeinschränkungen).

2.3 Sicherheit

Die Verantwortlichkeiten in Bezug auf Sicherheits- und Compliance 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 ihre Verantwortlichkeiten in jedem Modell klar definieren.

Dieses Modell übergreifender Verantwortlichkeit 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 **Leistungsfähigkeit**. Organisationen im öffentlichen Sektor sollten hohe Ansprüche an die CISPs stellen und verlangen, dass CISPs die erforderlichen Sicherheitsfunktionen bieten, um sicherzustellen, dass die Kunden ihre Verantwortung im Rahmen des Modells der geteilten Verantwortlichkeit erfüllen können. Wie aus der nachstehenden, repräsentativen Liste von Anforderungen hervorgeht wird der CISP gebeten, einen standardisierten Leistungsumfang bereitzustellen, damit der Kunde über diesen Leistungsumfang seine einzigartige Cloud-Umgebung sichern kann.

- ***Netzwerkfirewalls und Firewallfunktionen für Webanwendungen*** *zur Erstellung privater Netzwerke und zur Steuerung des Zugriffs auf Instanzen und Anwendungen*
- ***Konnektivitätsoptionen****, die private oder dedizierte Verbindungen von Ihrem Standort oder Ihrer lokalen Umgebung ermöglichen*
- *Fähigkeit, eine tief greifende* ***Verteidigungsstrategie*** *zu implementieren und DDoS-Angriffe abzuwehren*
- ***Datenverschlüsselungsfunktionen*** *für Speicher- und Datenbankservices*
- ***Flexible Optionen für die Schlüsselverwaltung****, mit welchen Sie auswählen können, ob der CISP die Kodierungsschlüssel 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*
- ***Bereitstellungs-Tools****, um die Erstellung und Außerbetriebnahme von CISP-Ressourcen gemäß den Standards in Ihrer Organisatuib 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, sowie des Zeitpunkts und Orts des Aufrufs*
- ***Protokollzusammenführung und Optionen****, 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 Unternehmensverzeichnissen****, um die Kosten für die Administration zu verringern und das Endbenutzererlebnis zu verbessern*

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

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

Organisationen des öffentlichen Sektors sollten sich Cloud-Akkreditierungszertifizierungen und -auswertungen ansehen, um sicherzustellen, dass die erforderlichen CISP-Sicherheitskontrollen vorhanden sind. Beispiel: Stellen Sie sich einen CISP vor, der durch einen unabhängigen Auditor 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 einhalten muss. 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 gefordert werden. Aus diesem Grund ist es sinnvoll, dass ein Unternehmen 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 von unabhängigen Dritten kann auf die meisten Sicherheits- und Compliance-Kontrollen angewendet werden, z. B. DSGVO, 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 Bieter 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 Kontrollen an, über die Sie den Schutz von Inhalten von **<ORGANISATION>** gewährleisten. 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 seine Inhalte, Services und Ressourcen. Der CISP sollte erweiterte Zugriffs-, Verschlüsselungs- und Protokollierungsfunktionen bereitstellen, die **<ORGANISATION>** dabei unterstützen, dies effektiv zu tun. Der CISP greift nicht auf Inhalte von **<ORGANISATION>** zu anderen als den gesetzlich vorgeschriebenen Zwecken zu, um die CISP-Dienste zu verwalten und sie **<ORGANISATION>** und seinen Endbenutzern zur Verfügung zu stellen.*
- ***<ORGANISATION>** wählt die Region(en) aus, in 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 notwendig, um die CISP-Dienste zu verwalten und sie **<ORGANISATION>** und seinen Endbenutzern bereitzustellen.*
- ***<ORGANISATION>** legt fest, wie der Inhalt geschützt wird. Der CISP muss bei der Übertragung und im Ruhezustand eine starke Verschlüsselung für Inhalte von **<ORGANISATION>** bereitstellen und die Möglichkeit bieten, dass **<ORGANISATION>** seine eigenen Kodierungsschlüssel verwalten kann.*
- *Der CISP muss über ein Programm für die Zusicherung der Sicherheit verfügen, das bewährte globale Methoden zum Datenschutz und zur Datensicherheit verwendet. So kann er **<ORGANISATION>** dabei helfen, die CISP-Umgebung für die Sicherheitskontrolle zu erstellen, zu betreiben und nach den besten Möglichkeiten zu nutzen. Die Prozesse zum Schutz und zur Kontrolle der Sicherheit müssen mehreren unabhängigen Prüfungen durch Dritte unterzogen werden.*

Anhand von Cloud-Zertifizierungen und -Akkreditierungen sowie Bewertungen können Behörden 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 Genehmigungsworkflows vermieden, die für eine Cloud-Umgebung möglicherweise nicht erforderlich sind.

Cloud-Ausschreibungen sollten CISPs die Möglichkeit bieten, Compliance-Akkreditierungen und -Bewertungen vorzuweisen. Wie bereits erwähnt, gibt es bei diesen Akkreditierungsschemata erhebliche Überschneidungen in den Bereichen Risikoszenarien und Risikomanagementpraktiken. Da die Kontrollen und Anforderungen in solchen Akkreditierungen zusammengefasst werden, ist es einfacher, solche Akkreditierungen als Bedingung für die Berücksichtigung eines CISPs anzugeben, anstatt den bereits geleisteten Aufwand zu duplizieren und selbst einzelne Kontrollen aufzulisten. (**Häufig werden diese dann von früheren Ausschreibungen übernommen, die sich noch auf Vor-Ort-Rechenzentren beziehen und daher ohnehin nicht für Cloud-Umgebungen relevant sind.**)

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. Geheimhaltungsvereinbarungen – NDAs) und bitten Sie nicht einfach darum, dass diese Dokumente im Rahmen des Angebots eingereicht werden.

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 Beschaffung von Cloud-Technologie.

***<ORGANISATION>** bewertet die Angebote anhand der akzeptierten Sicherheits-, Compliance- und Betriebsstandards, wie unten und in **Anhang A** beschrieben. Indem sich **<ORGANISATION>** bei der Bewertung des Anbieters 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, dessen Lösung (direkt oder über einen Vertriebspartner) angeboten wird, sollte in der Lage sein, die folgenden unabhängigen Bescheinigungen, Berichte und Zertifizierungen von unabhängigen 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, den notwendigen Zugang zu erhalten):*

Zertifizierungen/Bescheinigungen	*Gesetze, Vorschriften und Datenschutz*	*Ausrichtungen/Rahmenbedingungen*
☐C5 (Deutschland)		*☐ CDSA*
☐ CISPE Data Protection Code of Conduct (CISPE-Verhaltenskodex zum Datenschutz) (DSGVO)		
☐ 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 Harbour“*
☐ *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*
	☐ *Spanische DPA-Autorisierung*	☐ *NIST*
	☐ *U.K. DPA – 1988*	☐ *Uptime Institute Tier*
	☐ *VPAT/Abschnitt 508*	☐ *UK-Cloud-Sicherheitsprinzipien*

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.

2.3.2 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 auch Kriterien anzugeben, anhand derer die CISP-Sicherheitsfunktionen und -Services im Rahmen einer kompetitiven Auswertung verglichen werden können.

Beispiele für CISP-Sicherheitsanforderungen finden Sie hier *Anhang A – Technische Anforderungen für den Vergleich zwischen Bietern*. Wir empfehlen dringend, die folgenden Leistungskriterien als wichtige Sicherheitsüberlegungen für Organisationen im öffentlichen Sektor in die Bewertung von CISPs einfließen zu lassen:

Beispielformulierungen für die Ausschreibung: Zentrale Sicherheitsüberlegungen

- *Der CISP versteht das Modell der geteilten Verantwortlichkeit und hat dieses dokumentiert, um Kunden das Verständnis für die Abgrenzung der Sicherheitsverantwortlichkeiten bei CISP-Funktionen und -Diensten zu erleichtern (z. B. im Kontext der DSGVO)*
- *Belegbare Sicherheithistorie der CISP-Infrastruktur mit öffentlich verfügbarer, nicht-proprietärer Dokumentation des Sicherheitsstatus von CISP und physischer/logischer Kontrolle*
- *CISP-Support speziell für die Cloud-Sicherheit*

- *Services, die es den Cloud-Kunden ermöglichen, das Kontodesign zu formalisieren, die Sicherheits- und Governance-Kontrollen zu automatisieren und die Überprüfung zu vereinfachen*
- *Die Möglichkeit, eine Sammlung von Ressourcen als Vorlagen zu erstellen, bereitzustellen und zu verwalten (einschließlich von CISP/CISP-Partnern erstellte Standardsicherheitsvorlagen)*
- *Möglichkeit, einen verlässlichen, wiederholbaren Einsatz der Kontrollen zu etablieren*
- *Funktionen für eine durchgehende Prüfung in Echtzeit*
- *Die Fähigkeit zur technischen Skripterstellung für Richtlinien zur Cloud-Governance*
- *Fähigkeit zum Erstellen von zwingenden Funktionen, die von Nutzern ohne entsprechende Änderungsberechtigung nicht überschrieben werden können*
- *Die 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 festzulegen, 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 arbeiten 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 Bieter nach Ablauf der Einreichfrist Produkte hinzufügen dürfen, solange sie den ursprünglichen Parametern der Ausschreibung entsprechen. Das liegt daran, dass sich Sicherheitsfunktionen und -dienste schnell entwickeln und CISPs häufig sicherheitsbezogene Dienste 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 Verantwortlichkeit ist natürlich das Herzstück des Bereichs Sicherheit in einer Cloud-Services-Ausschreibung. Jede Partei muss ihre Sicherheitsverantwortlichkeiten klar definieren und CISPs müssen die Sicherheitsverantwortlichkeiten von CISP/Kunden für von CISP bereitgestellte Cloud-Technologien dokumentieren und die 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, den Vertrag mit einem Bieter vorzeitig zu kündigen, 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 – sowie mit der erforderlichen Cloud-Governance und Transparenz hinsichtlich Nutzung und Ausgaben.

Wichtig ist dabei, dass die Ausschreibungen von Cloud-Services Wert und Gesamtbetriebskosten ("Total cost of ownership") betrachten sollten, im Gegensatz zum einfachen Vergleich der Einzelpreise. Diese traditionelle Vorgehensweise, bei der nach dem günstigsten Preis pro Einheit gesucht wird, ist nicht auf das Cloud-Modell übertragbar und führt daher nicht zur wirtschaftlichsten 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 ähnlichen Eigenschaften für die Rahmenvereinbarung ausgewählt werden können. 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 Performance und Flexibilität der von CISPs bereitgestellten Cloud-Technologieservices zu ermöglichen. In Anhang B finden Sie ein Beispieltestskript für Cloud-Technologien.*

2.4.1 Mindestvoraussetzungen

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

1. **Nutzungsbasierte Abrechnung:** Cloud-Kunden verwenden ein nutzungsabhängiges Finanzierungsmodell, bei dem sie einfach am Ende jedes Monats die genutzten Services vergüten. Dies ist optimal für die Nutzungs- und Ressourcenmetriken.
2. **Transparente Preisgestaltung:** CISP-Preise sollten öffentlich verfügbar und transparent sein.
3. **Dynamische Preisgestaltung:** Flexibles Modell, bei dem die Preise der Cloud je nach Marktpreis flexibel variieren können. Dieser Ansatz nutzt die dynamische und wettbewerbsorientierte Preisentwicklung im Cloud-Bereich und unterstützt Innovation und Preissenkungen.
4. **Kontrolle über die Ausgaben:** Die CISPs müssen Berichts-, Überwachungs- und Prognosetools bereitstellen, die es dem Auftraggeber ermöglichen, (1) Nutzung und Ausgaben in zusammenfassender und detaillierter Weise zu überwachen, (2) Benachrichtigungen zu erhalten, wenn Nutzung und Ausgaben definierte Werte überschreiten, und (3) Nutzung und Ausgaben zu prognostizieren, um künftige Cloud-Budgets planen zu können.

Beispielformulierungen für die Ausschreibung: Preise

<ORGANISATION> fordert, dass bietende 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 die Option mengenbasierter Rabatte und Tools zur Abrechnung anbieten, um den tatsächlichen Preis des gekauften Produkts und

den Gesamtwert für den Auftraggeber zu ermitteln (z. B. Dienstleistungen zur Optimierung und daraus resultierende Kostensenkungen).

Abrufberechtigte Stellen können im Rahmen der Rahmenvereinbarung mit den Anbietern sprechen, um sie zu bitten, ihre Servicebeschreibung, Geschäftsbedingungen, Preise oder Servicedefinitionsdokumente/-modelle 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 und „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?*
  - *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 CISP-Serviceeinheitenkosten niemals die auf der Cloud-Anbieter-Website veröffentlichten Einheitenpreise überschreiten, die zum Zeitpunkt der Nutzung der Serviceeinheit durch den Kunden wirksam sind.*

Budgetierung und Rechnungsbenachrichtigungen/-berichte

*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 Modells der geteilten Verantwortlichkeit für die Cloud 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>** Rechnungsinformationen sowohl auf granularer als auch auf Zusammenfassungsebene anzeigen kann, und visualisieren Sie die Ausgabenentwicklung für CISP-Ressourcen sowie die Prognose zukünftiger Ausgaben.*

- *Geben Sie an, wie **<ORGANISATION>** die Nutzungs-/Abrechnungsansicht nach Service, nach verknüpften Konten oder nach benutzerdefinierten Kriterien für Ressourcen filtern kann, und erstellen Sie Abrechnungswarnmeldungen, 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 viele Cloud-Services über einen definierten Prognosezeitraum genutzt werden. Der CISP sollte eine **Schätzung** der CISP-Rechnung an **<ORGANISATION>** vorlegen und es **<ORGANISATION>** ermöglicht , 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 den Wettbewerb zwischen den Bietern, bei dem Bewertungskriterien wie Bestwert, wirtschaftlichstes Angebot oder niedrigster Preis angelegt werden. Es ist wichtig, dass der Ansatz, den man bei der Planung für die Bepreisung 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 keine Funktionen wie Leistung, Kostenoptimierung mithilfe von Cloud-nativen Services und CISP-Überwachungstools berücksichtigt oder Services, die CISPs evtl. kostenlos anbieten, mit einbezieht. Darüber hinaus kann der Katalogpreis eines CISP Zehntausende von Einzelposten umfassen. Die Preismodelle unterscheiden sich dabei von einem Service und Anbieter zum anderen.

Analyse der TCO

Wir empfehlen Ihnen, sich auf die Gesamtbetriebskosten (Total Cost of Ownership) definierter Anwendungsbeispiele zu konzentrieren, die alle Aspekte einer Cloud-Lösung berücksichtigen (einschließlich Partnerservices, standardisierte CISP-Rabatte, technische Funktionen, die die Leistung steigern, Kosten senken/optimieren usw.).

Vergleich anhand von Szenarien

Der Bewertungsprozess kann auch typische Szenarien berücksichtigen, die auf den häufigsten Systemen oder Anwendungsbereichen basieren. Solche Szenarien (z. B. Webhosting oder die Implementierung eines Personalsystems mit x Benutzern) können Variablen wie die Geschwindigkeit und Skalierung der Ressourcen, die Performance der Anwendung oder Lösung, Speicherzugriffszeiten, komplexe Daten mit geringem Volumen im Vergleich zu einfachen Rechenaufgaben mit hohem Volumen und ähnliches beinhalten. Andere typische Szenarien für die Anwendungen oder Systeme können Dinge wie die Verarbeitung großer Datenmengen 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 müssen auch die technischen Vorteile berücksichtigt werden. Beispielsweise kann ein bestimmter CISP es Kunden ermöglichen, eine Aktiv-Aktiv-DR-Topologie (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 Disaster-Recovery-Anforderungen um x % teurer sein. Ein Beispiel dafür, warum ein ganzheitlicher Preisansatz, der technische Merkmale berücksichtigt, für die Bewertung von CISPs von entscheidender Bedeutung ist, ist die folgende Alternative zu einem direkten Vergleich einzelner Komponenten.

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

1. Wie viele redundante 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 die Nachhaltigkeit 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 Kosten für die Speicherung und Verwendung von Daten senken können (z. B. kann die Verwendung serverloser Funktionen eines CISP die Kosten um x % senken).

Dies sind nur einige von vielen technischen Aspekten, die bei der Preisgestaltung berücksichtigt werden, 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 die Anbieter etwa 3 bis 5 spezifische Szenarien (oder wie viele auch immer für den Kunden sinnvoll sind) 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 Posten-/SKU-Ebene sind für Kunden und Lieferanten eher problematisch als hilfreich. (Die Kunden müssten Zehntausende von Einzelposten über alle CISPs hinweg vergleichen und die Anbieter müssten diese Detailebene bereitstellen und verwalten, obwohl der Preis später nur anhand der Servicenutzung bestimmt wird.)

Die Bewertung der übergreifenden Fähigkeiten eines CISP ist ein Muss für Cloud-Kunden, die den besten Wert erzielen 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/Spot-Instances berücksichtigen. Beispiel:

- Einsparungen von x %, wenn Kunden reservierte Rechenkapazität kaufen (1 Jahr, 3 Jahre usw.)
- X % Rabatt auf gestaffelte Preise/Mengenrabatte
- Einsparungen von x % basierend auf Architekturprüfungen und der Optimierung der Infrastruktur, wie z. B. dem Wechsel auf eine Option für bessere Datenverarbeitung.
- Berücksichtigen Sie wie oben angegeben die Kosten für die gesamte Lebensdauer und wie Sie mit Funktionen zur Kostenoptimierung Kosten 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 On-Demand-Pay-per-Use-Modell.

Im Folgenden finden Sie repräsentative Anforderungen für die 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 nach Bedarf 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*
- *99,95 % Serviceverfügbarkeit*

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 nativen Cloud-Lösungen und CISP-Preissenkungen.

2.5 Vertragsausführung/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 Bietern verlangen, viele oder alle angegebenen Anforderungen zu erfüllen, um nicht ausgeschlossen zu werden. Oder wenn schon nicht alle Anforderungen erfüllt werden müssen, dann auf jeden Fall eine bestimmte Teilmenge. Wird diese Vorgehensweise auf Cloud-Technologien übertragen, bei denen es sich tatsächlich 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 CISP-Geschäftsbedingungen zu überprüfen und zu verstehen. In vielen Fällen sind diese öffentlich auf den CISP-Websites zu finden. Organisationen im öffentlichen Sektor akzeptieren immer vorbehaltloser die Geschäftsbedingungen von CISPs. Ein Teil dieses Prozesses 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 herkömmlicher IT-Bedingungen zu unterscheiden, aber es gibt sehr spezifische Gründe, warum sie Teil eines Cloud-Vertrags sind. Wenn die öffentlich verfügbaren Bedingungen nicht akzeptabel sind, haben CISPs häufig leicht veränderbare Vereinbarungen für Unternehmenskunden, die in Betracht gezogen werden können.

Neben der Überprüfung der Geschäftsbedingungen des CISP ist es wichtig, die bestehenden Richtlinien, Vorschriften und/oder Gesetze (z. B. 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. Ist dies der Fall, 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 existieren. Die Geschäftsbedingungen für die Cloud unterscheiden sich beispielsweise von den Bedingungen für herkömmliche Rechenzentren, Managed Services, Hardware, 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 auszuschließen. Ein typischer Prozess besteht darin, dass die Organisation bestimmte Bedingungen im Voraus benennt, 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 vorteilhaften Angebots führen könnten. Organisationen des öffentlichen Sektors können auch ihre Richtlinien, Vorschriften und Gesetze überprüfen 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, wird empfohlen, trotz der Akzeptanz der Geschäftsbedingungen der CISPs, (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 Angebote zu bieten, die zu der Rahmenvereinbarung führen werden (mit Ausnahme der obligatorischen, gesetzlich vorgeschriebenen Klauseln).

Hinweis: Das Ausmaß der geteilten Verantwortlichkeit ist im Cloud-Modell inhärent 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 jedes der Loseeiner Cloud-Rahmenvereinbarung ***unterschiedliche Vertragsbedingungen*** *gelten. Eine „*Einheitslösung*" für die Verträge aller Lose führt zu Problemen in Bezug auf technische Machbarkeit und Kompatibilität.*

Wie bereits erwähnt, führen Ausschreibungen mit nicht verhandelbaren Bedingungen dazu, dass 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 CISP-Cloud-Technologien vollständig standardisiert und automatisiert bereitgestellt werden. Daher ist ein CISP nicht in der Lage, Änderungen an den Geschäftsbedingungen vorzunehmen, wenn dies eine grundlegende Veränderung des Diensts 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. Der Bieter sollte **<ORGANISATION>** seine Vertragsbedingungen mit dem besten kommerziellen und rechtlichen Angebot zur Überprüfung vorlegen. Die Bieter und <ORGANISATION> können beide Sätze von Bedingungen während der Phase <GESPRÄCH/VERHANDLUNG> besprechen.*

- *Allgemeine Bedingungen für die Rahmenvereinbarung bestehen höchstens aus den folgenden Komponenten:*
  - *Laufzeit der Rahmenvereinbarung*
  - *Governance Rahmenvereinbarung*
  - *Performance Rahmenvereinbarung*
  - *Kündigung der Rahmenvereinbarung*
  - *Umfang der Rahmenvereinbarung*
  - *Bestellvorgang (Abruf aus der Rahmenvereinbarung)*
  - *Vertraulichkeitsbestimmungen*
  - *Kategorie-spezifische 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 Auftraggeber und Bieter nicht davon abhalten, sich auf Vertragsänderungen zu einigen und 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 Auftraggeber festgelegt werden. Die Geschäftsbedingungen des Auftraggebers sollten keine provisionsspezifischen, 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 dies an die Kunden weitergeben, während diese sich darauf verlassen können, dass der CISP die SLA einhalten kann.*
- *Die Haftungsobergrenzen sollten anteilig 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 jedoch oft ein nützliches Einführungs- und Testszenario 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 So wählen Sie zwischen Teilnehmern pro Projekt aus

Öffentliche Einrichtungen, die Teil der Rahmenvereinbarung sind, können die benötigten Dienstleistungen bei Bedarf bestellen oder „abrufen“. Ein Abrufvertrag im Rahmen einer Rahmenvereinbarung ermöglicht es Käufern, 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 Lieferanten für eine bestimmte Workload oder ein bestimmtes Projekt zu ermitteln. Ein Mini-Wettbewerb bedeutet, dass ein Kunde im Rahmen der Rahmenvereinbarung einen weiteren Wettbewerb ausruft, indem er alle Lieferanten innerhalt eines Loses dazu einlädt, auf eine Reihe von Anforderungen zu reagieren. Der Kunde lädt dann alle infrage kommenden Lieferanten innerhalb des Loses ein, ein Angebot abzugeben. Daher ist es wichtig, bei einer Cloud-Services-Ausschreibung die Mindestanforderungen für die Teilnehmer zu definieren: So wird für jedes Los eine qualitativ hochwertige Auswahl an Optionen gewährleistet.

Bitte beachten Sie, dass es für jede der Loskategorien von Angebotstypen (z. B. Public IaaS/PaaS, Community IaaS/PaaS, Private IaaS/PaaS) unterschiedliche Geschäftsbedingungen gibt, 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 der Ausschreibung bei der Auswahl zwischen Teilnehmern.

2.5.3 On-Boarding und Off-Boarding

Bei der Erstellung einer Cloud-Rahmenvereinbarung ist die Option eines dynamischen Einkaufssystems (Dynamic Purchasing System, DPS) zu beachten. Bei einem DPS-Modell werden alle Anbieter, die die Mindestanforderungen für die Rahmenvereinbarung erfüllen, in die Rahmenvereinbarung aufgenommen. Die Anzahl der Anbieter, die der Rahmenvereinbarung beitreten können, ist unbegrenzt. Im Gegensatz zum herkömmlichen Rahmenvereinbarungs-Modell 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 Sicherheit des Service 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 Cloud-Technologien hoch zu halten.

3.0 Best Practices/Erkenntnisse

Im Folgenden werden wir einige unserer 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 Cloud-Governance in jeden Aspekt einer Cloud-Umgebung zu integrieren, während Kunden ihre bestehenden Cloud-Governance-Standards mitbringen und lernen, wie die Cloud die Cloud-Governance ermöglicht.

In der Cloud haben Kunden 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 Cloud-Serviceanbieter übernommen, sodass Kunden ihren eigenen Schwerpunkt von einer undifferenzierten Infrastrukturverwaltung auf die geschäftskritische Betriebstätigkeit verlagern können.

Im Grunde genommen können Sie sich eine CISP-Cloud als sehr große API vorstellen: 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 erfolgt ist). 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 die Zeitpläne für die Erstellung einer Entwicklungs- oder Testumgebung in der Cloud deutlich überschätzen (denn dies dauert mit der Cloud unter Umständen nur wenige Minuten). Sich an diese neue Flexibilität zu gewöhnen wird ein evolutionärer Prozess sein und passiert von Projekt zu Projekt. Diese Erkenntnisse sollten weitergegeben werden, damit eine Cloud-Rahmenvereinbarung so weiterentwickelt werden kann, dass die Anforderungen auf diese neuen Prozesse und diese neue Flexibilität abgestimmt sind.

3.2 Budgetierung für die Cloud

Wenn es um die passende Strukturierung der nutzungsabhängigen Cloud-Preise für Akquise und Budgetierung im öffentlichen Sektor geht, haben wir festgestellt, dass es hilft, CISP-Services in einem einzigen Posten (Datenverarbeitung, Speicher, Netzwerk, Datenbank, IoT usw.) zu bündeln, und zwar alles unter dem Begriff **Cloud-Technologien**. Dies garantiert die Flexibilität, den Benutzern alle aktuellen und neuen CISP-Technologien in Echtzeit anzubieten und ermöglicht ihnen schnellen Zugriff auf die benötigten

Ressourcen, wann immer sie benötigen werden. Dieser Ansatz berücksichtigt auch eine schwankende Nachfrage und sorgt so für eine optimierte Auslastung und niedrige Kosten.

Organisationen des öffentlichen Sektors können zusätzliche Posten für Aufträge aus anderen Losen zu einer Cloud-Rahmenvereinbarung hinzufügen, wenn sie Beratungsleistungen, 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 Beratungsleistungen/ Professional Services/Managed Services in einem Posten bündeln möchte, kann dies auch unter einem Oberbegriff wie „Cloud-Technologien und optionale Leistungen“ erfolgen.

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

Tabelle 3 – Beispiel für eine Preisstruktur für Einzelposten

ARTIKELNR.	LIEFERUNGEN/SERVICES	STÜCKZAHL	EINHEIT	PREIS PRO EINHEIT	BETRAG
1001	Cloud-Technologien	1 000	Jede Einheit	1 €	1 000 €
1002	Beratungsleistungen	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 €

Diese Struktur kann beispielsweise wie folgt funktionieren: Eine Organisation des öffentlichen Sektors kontaktiert einen CISP, um einzuschätzen, wie viele Cloud-Technologieservices das Unternehmen 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 erhält es eine Rechnung und das Geld wird aus dem Fonds zur Zahlung genommen. Dieses Konto wird stark belastet. Die verbleibenden Mittel werden mithilfe von CISP-Überwachungs- und Prognosetools auf die Burn-Rate 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 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 Artikels für „Cloud-Technologien" angegeben.*

*Jede Einheit des bestellten Artikels 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 unterschiedliche Anforderungen 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.*

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

MINDESTBESTELLUNG/INKREMENTELLE BESTELLUNG

*Bestellungen werden in regelmäßigen Abständen für verschiedene Mengen von weniger als <10.000> Artikeln 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 „Pay-as-you-go"-Praktiken von Cloud-Computing zu operieren.*

*Bei der Aufgabe des Abrufs wird eine anfängliche Stückzahl von **<100.000>** Einheiten zu Kosten von **<100 000 €>** bestellt. Die Mindestanzahl der gesamten Einzelposteneinheiten, 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 Lieferauftrags bestellt werden, darf **<x>** nicht überschreiten. Gleichzeitig darf dabeider Abrufwert der Rahmenvereinbarung nicht überschritten werden, wenn sie mit allen zuvor bestellten Einheiten kombiniert wird. **<ORGANISATION>** ist dafür verantwortlich, dass alle Aufträge innerhalb der in diesem Abschnitt festgelegten Grenzen liegen.*

MAXIMALE BESTELLUNG

*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 Verstehen 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 an einen System-Integrator (SI) oder Managed Services Provider abgegeben. 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 Vertriebsparter mit CISPs zusammenarbeiten. In manchen Beschaffungsfällen gibt es Klauseln die vorsehen, dass der Hauptauftragnehmer einige erforderliche Klauseln an Partner/Subauftragnehmer weitergibt. In der Regel liefern CISPs ihre Services nicht wie formelle Subunternehmer, sondern bieten einen

standardisierten Service in großem Umfang an, der nicht auf die individuellen Anforderungen eines bestimmten Endkunden ausgerichtet ist (die Anforderungen von Kunden des öffentlichen Sektors mit einem 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 „Second-Tier"-Anbieter von kommerziellen Services nicht anwendbar sind. In einem solchen Fall führt der CISP die vertraglich vereinbarten Leistungen nicht selbst aus, sondern ein CISP-Partner nutzt die Infrastruktur eines CISP. Daher gilt der CISP als kommerzieller Anbieter (und nicht als Subunternehmer) für die Leistungen des Partners. In einem direkten Beschaffungsmodell (Cloud-Services werden direkt von einem CISP erworben) lehnt der CISP diese „erforderlichen" Vertragsklauseln, die für einen normalen Subunternehmer von Massenware typisch sind, in der Regel mit einem Verweis auf die kommerzielle Natur der vertraglich vereinbarten Services und die Tatsache ab, 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 der 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 – die Führungskräfte, die Stakeholder der Organisation, Technologie, Finanzen, Beschaffung, Recht und Verträge – einbeziehen. Dadurch wird sichergestellt, dass sich alle Beteiligten mit dem Cloud-Modell vertraut machen und folglich eine fundierte Einschätzung zur Neubewertung herkömmlicher IT-Beschaffungsmethoden abgeben 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 tiefgehendes Verständnis für die Cloud-Beschaffung zu erlangen, ist die Durchführung einer Markterkundung oder idealerweise der Entwurf eines Ausschreibungsdokuments. Häufig enthalten diese Entwürfe potenzielle Probleme, die im Vorfeld identifiziert, diskutiert und angepasst werden können, bevor die endgültige Ausschreibung für Cloud-Services veröffentlicht wird.

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-Bereich 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 Präsenz in den benötigten Regionen?*
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 entfernten Rechenzentren auf, um Redundanz, hohe Verfügbarkeit und geringe Latenz zu unterstützen?*
5.	***AUSFALLSICHERHEIT DER RECHENZENTREN:*** *Bietet der Cloud-Anbieter Rechenzentren, die vor Ausfällen in anderen Rechenzentren durch doppelte Stromversorgung, Kühlung und Netzwerke geschützt sind?*
6.	***RECHENZENTRUMSREPLIKATION:*** *Bietet der Cloud-Anbieter Datenreplikation über Rechenzentren innerhalb einer Domäne oder Zone mit automatischem Failover an?*
7.	***DOMÄNEN-/ZONENREPLIKATION:*** *Bietet der Cloud-Anbieter eine Datenreplikation über Domänen oder Zonen innerhalb einer Region hinweg an?*

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 allgemeine Anwendungen und bietet ein ausgewogenes Verhältnis von Rechen-, Arbeitsspeicher- und Netzwerkressourcen.* o *Wenn ja, welches ist die größte Instance, die angeboten wird?*
2.	***DATENVERARBEITUN – NORMALE INSTANCE – ARBEITSSPEICHEROPTIMIERT:*** *Bietet der Cloud-Anbieter die folgenden Instance-Typen an?* • *Arbeitsspeicheroptimiert – optimiert für arbeitsspeicherintensive Anwendungen* o *Wenn ja, welches ist die größte Instance, die angeboten wird?*
3.	***DATENVERARBEITUNG – NORMALE INSTANCE – DATENVERARBEITUNGSOPTIMIERT:*** *Bietet der Cloud-Anbieter die folgenden Instance-Typen an?* • *Datenverarbeitungsoptimiert – optimiert für rechenintensive Anwendungen* o *Wenn ja, welches ist die größte Instance, die angeboten wird?*
4.	***DATENVERARBEITUNG – NORMALE INSTANCE – SPEICHEROPTIMIERT:*** *Bietet der Cloud-Anbieter die folgenden Instance-Typen an?* • *Speicheroptimiert – bietet 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 angeschlossen 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, die angeboten wird?*
6.	***DATENVERARBEITUNG – NORMALE INSTANCE – GPU-OPTIMIERT:*** *Bietet der Cloud-Anbieter die folgenden Instance-Typen an?* • *GPU – bietet 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 – bietet vor Ort programmierbare Gate-Arrays (Field Programmable Gate Arrays, FPGA) für die Entwicklung und Bereitstellung benutzerdefinierter Hardwarebeschleunigung für Anwendungen.* o *Wenn ja, wie viele FPGAs kann der Cloud-Anbieter pro Instance anbieten?*
8.	***DATENVERARBEITUNG – BURSTABLE-INSTANCE:*** *Bietet der Cloud-Anbieter Burstable-Instances, die ein Baseline-Level der CPU-Leistung (Central Processing Unit) mit der Möglichkeit bieten, über die Baseline zu bursten?* • *Wenn ja, welche ist die größte Burstable-Instance?*

9.	*DATENVERARBEITUNG – E/A-INTENSIVE INSTANCE:* *Bietet der Cloud-Anbieter Instances an, die Non-Volatile-Memory-Express-Solid-State-Laufwerke (NVMe-SSDs) verwenden, die für eine geringe Latenz, eine sehr hohe zufällige 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, der 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) Netzwerkschnittstellenkarten (Network Interfaces Cards, NICs), die einer bestimmten Instance zugewiesen 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 in einer Region zu platzieren?*
14.	*DATENVERARBEITUNG – SELF-SERVICE-BEREITSTELLUNG:* *Bietet der Cloud-Anbieter gleichzeitig Self-Service-Bereitstellung für mehrere Instances über eine Programmschnittstelle, eine Verwaltungskonsole oder ein Webportal?*
15.	*SELF-SERVICE PROVISIONING – ANPASSUNG:* *Bietet der Cloud-Anbieter anpassbare Instance, d. h. die Möglichkeit, Konfigurationseinstellungen wie virtuelle Zentralprozessoren (vCPUs) und Arbeitsspeicher (RAM) zu ändern?*
16.	*DATENVERARBEITUNG – TENANCY:* *Bietet der Cloud-Anbieter Single-Tenant-Instances, die auf Hardware ausgeführt werden, die einem einzelnen Benutzer zugewiesen ist?* • *Wenn ja, wie groß ist die größte verfügbare Single-Tenant-Instance?*
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 dort zu hosten?*
19.	*DATENVERARBEITUNG – AUTO-SCALING:* *Bietet der Cloud-Anbieter die Möglichkeit, die Anzahl der Instances automatisch während Bedarfsspitzen zu erhöhen, um die Performance aufrechtzuerhalten (d. h. zu „skalieren“)?*
20.	*DATENVERARBEITUNG – MÖGLICHKEIT 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 in Zukunft für die Bereitstellung von Instances verwendet werden können?* • *Wenn ja, welche Formate werden unterstützt?*

21.	***DATENVERARBEITUNG – MÖGLICHKEIT 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 an, wenn der Anbieter Hardware- oder Servicewartung auf Hostebene durchführt?*
23.	***DATENVERARBEITUNG– INSTANCE-NEUSTART:*** *Bietet der Cloud-Anbieter Mechanismen für den automatischen Neustart von Instances auf einem funktionstüchtigen Host an, wenn der ursprüngliche physische Host ausfällt?*
24.	***DATENVERARBEITUNG – BENACHRICHTIGUNGEN:*** *Ist der Cloud-Anbieter im Fall eines datenverarbeitungsresistenten Ereignisses in der Lage, den Benutzer über ein solches Ereignis zu informieren und kann der Benutzer diese Kommunikation über Self-Service-Methoden aktivieren oder deaktivieren?*
25.	***DATENVERARBEITUNG – EREIGNIS-ZEITPLAN:*** *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 – BACKUP- UND WIEDERHERSTELLUNGSMECHANISMUS:*** *Bietet der Cloud-Anbieter einen integrierten Backup- und Recovery-Mechanismus an?*
27.	***DATENVERARBEITUNG – SNAPSHOT-MECHANISMUS:*** *Bietet der Cloud-Anbieter einen manuellen On-Demand-Snapshot-Mechanismus an?*
28.	***DATENVERARBEITUNG – METADATEN:*** *Bietet der Cloud-Anbieter einen Instance-Metadatendienst, mit dem Benutzer beliebige Schlüsselwertpaare für die Instance festlegen können?*
29.	***DATENVERARBEITUNG – METADATENABRUF:*** *Bietet der Cloud-Anbieter einen Instance-Metadatendienst, der eine Anwendungsprogrammierschnittstelle (API) bereitstellt, die 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. 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 Softwarehersteller, die Softwarenamen, die Editionen und die zugehörigen Versionen an.*
36.	***DATENVERARBEITUNG – SERVICE LIMITS:*** *Hat der Cloud-Anbieter Einschränkungen (d. h. Service Limits) in Bezug auf den oben genannten 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, dass das organisationseigene Netzwerk in der Cloud repräsentiert?*
2.	***NETZWERK – KONNEKTIVITÄT IN DER GLEICHEN REGION:*** *Unterstützt der Cloud-Anbieter die Verbindung von zwei virtuellen Netzwerken innerhalb derselben Region, um Datenverkehr mithilfe von IP-Adressen (Private Internet Protocol) 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 – BEREICHE VIRTUELLE NETZWERKADRESSEN:*** *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) 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 Netzwerkschnittstellenkarte (NIC), die mit einer bestimmten Instance verbunden ist?*
11.	***NETZWERK – MEHRERE NICS:*** *Unterstützt der Cloud-Anbieter die Möglichkeit einer bestimmten Instance mehrere Netzwerkschnittstellenkarten (Network Interfaces Cards, NICs) zuzuweisen?*
12.	***NETZWERK – NIC- UND IP-MOBILITÄT:*** *Unterstützt der Cloud-Anbieter die Möglichkeit Netzwerkschnittstellenkarten (Network Interfaces Cards, NICs) und IP-Adressen zwischen Instances zu verschieben?*
13.	***NETZWERK – SR-IOV-SUPPORT:*** *Unterstützt der Cloud-Anbieter Funktionen wie SR-IOV (Single Root Input/Output Virtualization) für höhere Leistung (z. B. Pakete pro Sekunde - PPS), 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 (Access Control Lists, ACLs) zur Steuerung des ein- und ausgehenden Datenverkehrs zu Subnetzen?*
17.	***NETZWERK – UNTERSTÜTZUNG VON FLUSSPROTOKOLLEN:*** *Bietet der Cloud-Anbieter die Möglichkeit Datenflussprotokolle für den Netzwerkverkehr zu erfassen?*
18.	***NETZWERK – NAT:*** *Stellt der Cloud-Anbieter einen verwalteten Gateway-Service für Netzwerkadressübersetzungen (Network Address Translation, NAT) 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 – QUELLE-/ZIELORTPRÜFUNG:*** *Kann der Cloud-Anbieter die Quell-/Zielprüfung auf Netzwerkschnittstellenkarten (Network Interfaces Cards, NICs) deaktivieren?*
20.	***NETZWERK – VPN-SUPPORT:*** *Unterstützt der Cloud-Anbieter VPN-Verbindungen (Virtual Private Network) zwischen dem Cloud-Anbieter und dem Rechenzentrum des Benutzers?*
21.	***NETZWERK – VPN-TUNNEL:*** *Unterstützt der Cloud-Anbieter mehrere VPN-Verbindungen (Virtual Private Network) 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 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 – FRONTEND-LOAD-BALANCER:* *Bietet der Cloud-Anbieter einen Frontend-Lastenausgleichsdienst (für das Internet), der Anforderungen von Clients über das Internet annimmt und diese Anfragen auf Instances verteilt, die beim Load Balancer registriert sind?*
26.	*NETZWERK – BACKEND-LOAD-BALANCER:* *Bietet der Cloud-Anbieter einen Backend- (privaten) Lastenausgleichsdienst, 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- (Hypertext Transfer Protocol – HTTP) Lastenausgleichsdienst, der den Netzwerkdatenverkehr über mehrere Instances hinweg lastenausgleichfähig macht?*
28.	*NETZWERK – LAYER 4-LOAD BALANCER:* *Bietet der Cloud-Anbieter einen Layer 4- (Transmission Control Protocol – TCP) Lastenausgleichsdienst, der den Netzwerkdatenverkehr über mehrere Instances hinweg lastenausgleichfähig macht?*
29.	*NETZWERK – SITZUNGSAFFINITÄT FÜR LOAD BALANCER:* *Bietet der Cloud-Anbieter einen Lastenausgleichsdienst, der Sitzungsaffinität unterstützt?*
30.	*NETZWERK – DNS-BASIERTES LOAD BALANCING:* *Bietet der Cloud-Anbieter einen Lastenausgleichsdienst, der den Lastenausgleich des Datenverkehrs auf Instances ermöglicht, die auf mehreren Hosts gehostet werden, die 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 hoch verfügbaren und skalierbaren DNS-Service (Domain Name System)?*
33.	*NETZWERK – LATENZBASIERTES DNS-ROUTING:* *Bietet der Cloud-Anbieter einen DNS-Service (Domain Name System) 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 (Domain Name System) an, der geo-basiertes Routing unterstützt (d. h. der DNS-Service antwortet auf DNS-Abfragen basierend auf der geografischen Position der Nutzer)?*
35.	*NETZWERK – FAILOVER-BASIERTES DNS-ROUTING:* *Bietet der Cloud-Anbieter einen DNS-Service (Domain Name System) 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 – DOMÄNENREGISTRIERUNGSSERVICE:* *Bietet der Cloud-Anbieter Services zur Registrierung von Domänennamen an (d. h. Benutzer können nach verfügbaren Domänennamen suchen und diese registrieren)?*
37.	*NETZWERK – DNS-INTEGRITÄTSPRÜFUNGEN:*

	Bietet der Cloud-Anbieter einen DNS-Service (Domain Name System) an, der mithilfe von Integritätsprüfungen Zustand und Leistung von Ressourcen überwacht?
38.	*NETZWERK – DNS- UND LOAD-BALANCER-INTEGRATION:* *Bietet der Cloud-Anbieter einen DNS-Service (Domain Name System), der in den Load Balancer des Cloud-Anbieters integriert werden kann?*
39.	*NETZWERK – VISUAL EDITOR:* *Bietet der Cloud-Anbieter ein Tool, mit dem Benutzer Richtlinien für die Datenverkehrsverwaltung 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 (Content Delivery Network), mit dem ein Objekt vor dem Ablauf aus dem Edge-Cache entfernt werden kann, einschließlich Funktionen wie das Ungültigmachen von Objekten und die Objektversionierung?*
42.	*NETZWERK – EXTERNE CDN-URSPRÜNGE:* *Bietet der Cloud-Anbieter einen CDN-Dienst (Content Delivery Network) an, der einen benutzerdefinierten Ursprung, d. h. einen HTTP-Server (Hypertext Transfer Protocol), unterstützt?*
43.	*NETZWERK – CDN-OPTIMIERUNG:* *Bietet der Cloud-Anbieter einen CDN-Service (Content Delivery Network) mit detaillierter Kontrolle für die Konfiguration mehrerer Ursprungsserver und Caching-Eigenschaften für verschiedene URLs?*
44.	*NETZWERK – CDN GEO-BESCHRÄNKT:* *Bietet der Cloud-Anbieter einen CDN-Service (Content Delivery Network), der geografische Beschränkungen unterstützt, d. h. Benutzer in bestimmten Regionen daran hindert, auf Inhalte zuzugreifen?*
45.	*NETZWERK – CDN-TOKEN:* *Bietet der Cloud-Anbieter einen CDN-Service (Content Delivery Network) 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 (Content Delivery Network), der benutzerdefinierte SSL-Zertifikate (Secure Sockets Layer) unterstützt, um Inhalte sicher über HTTPS (Hypertext Transfer Protocol Secure) von Edge-Standorten bereitzustellen?*
47.	*NETZWERK – CDN MULTI-TIER-CACHE:* *Bietet der Cloud-Anbieter einen CDN-Service (Content Delivery Network), der einen Multi-Tier-Cache-Ansatz mit regionalen Edge-Caches nutzt, um die Latenz zu reduzieren?*
48.	*NETZWERK – CDN-KOMPRIMIERUNG:* *Bietet der Cloud-Anbieter einen CDN-Service (Content Delivery Network), der die Dateikomprimierung unterstützt?*
49.	*NETZWERK – CDN-VERSCHLÜSSELTE UPLOADS:* *Bietet der Cloud-Anbieter ein CDN-Service (Content Delivery Network), 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 Netzwerkdienst 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 Einschränkungen (d. h. Service Limits) in Bezug auf den oben genannten 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 (Access Control List, Zugriffskontrollliste)* *Maximale Anzahl von VPN-Tunneln* *Maximale Anzahl von Ursprüngen pro Distribution* *Maximale Anzahl von Zertifikaten pro Load Balancer*

3.3 Speicherung

	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 -Tiers 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-LAUFWERKE:*** *Unterstützt der Cloud-Anbieter SSD-gestützte Speichermedien (Solid-State-Laufwerk), die Latenzen im Millisekundenbereich bieten?* • *Wenn ja, wie viele SSDs können pro Instance maximal angeschlossen werden?*
4.	***BLOCKSPEICHER – SKALIERUNG:*** *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, die Größe eines vorhandenen Blockspeicher-Volume 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 ruhenden Daten für 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 – SELTENER ZUGRIFF:*** *Bietet der Cloud-Anbieter einen kostengünstigeren Speicher-Service-Tier, der darauf abzielt, weniger häufig genutzte Objekte und Dateien zu speichern?*
10.	***OBJEKTSPEICHER – GERINGERE BESTÄNDIGKEIT:*** *Bietet der Cloud-Anbieter einen Tier mit reduzierter Redundanzebene, in der ein Benutzer nicht kritische, einfach reproduzierbare Objekte zu einem niedrigeren Preis speichern kann?*
11.	***OBJEKTSPEICHER – WENIGER HÄUFIGER ZUGRIFF:*** *Bietet der Cloud-Anbieter einen Tier für Daten, auf die seltener zugegriffen wird, die aber dennoch einen schnellen Zugriff erfordern?*
12.	***OBJEKTSPEICHER – OBJEKT-TIERING:*** *Bietet der Cloud-Anbieter Objektspeicher-Tiering-Funktionen, d. h. die Möglichkeit, ein Objekt basierend auf seiner Zugriffshäufigkeit zwischen Objektspeicherklassen oder Tiers 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 Tiering-Einstellungen 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) von ruhenden Daten, wobei er die Kodierungsschlüssel verwaltet?* • *Wenn ja, welcher kryptografische Algorithmus wird eingesetzt?*
18.	***OBJEKTSPEICHER – VERSCHLÜSSELUNG MIT BENUTZERSCHLÜSSELN:*** *Bietet der Cloud-Anbieter serverseitige Verschlüsselungsfunktionen (SSE) mit vom Kunden bereitgestellten kryptografischen Schlüsseln an?*
19.	***OBJEKTSPEICHER – SCHLÜSSELVERWALTETER SERVICE:*** *Unterstützt der Cloud-Anbieter die serverseitige Verschlüsselung (SSE) mithilfe eines Schlüsselverwaltungsservices, der Kodierungsschlüssel erstellt und Richtlinien definiert, die steuern, wie Schlüssel verwendet werden können und die Schlüsselverwendung prüft, um nachzuweisen, dass sie korrekt verwendet werden?*
20.	***OBJEKTSPEICHER – CLIENTSEITIGER MASTERSCHLÜSSSEL:*** *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, die Kontrolle über die Kodierungsschlüssel zu behalten und die Verschlüsselung/Entschlüsselung von Objekten auf Clientseite abzuschließen?*

21.	***OBJEKTSPEICHER – HOHE KONSISTENZ:*** *Unterstützt der Cloud-Anbieter Konsistenz durch Kontrolllesen für PUT-Vorgänge für neue Objekte?*
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 – VERSIONIERUNG:*** *Unterstützt der Cloud-Anbieter die Versionierung, d. h. die Möglichkeit, mehrere Versionen eines Objekts zu speichern und zu verwalten?*
25.	***OBJEKTSPEICHER – MARKIERUNG VON ELEMENTEN ALS NICHT LÖSCHBAR:*** *Erlaubt der Cloud-Anbieter einem Benutzer, ein Element als nicht löschbar zu markieren?*
26.	***OBJEKTSPEICHER – LÖSCHEN MIT MFA:*** *Unterstützt der Cloud-Anbieter als zusätzliche Sicherheitsoption die Multi-Factor Authentication (MFA) für Löschvorgänge?*
27.	***OBJEKTSPEICHER – MEHRTEILIGE UPLOADS:*** *Ermöglicht der Cloud-Anbieter das Hochladen eines Objekts in mehreren Teilen, wobei jedes 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, Auditprotokolle zu erstellen, die Details zu einer einzelnen Zugriffsanforderung enthalten, z. B. den Anforderer, die Anforderungszeit, die Anforderungsaktion, den Antwortstatus und den Fehlercode?*
31.	***OBJEKTSPEICHER – INVENTARISIERUNG VON OBJEKTEN:*** *Bietet der Cloud-Anbieter Bestandsaufnahmefunktionen, mit denen Benutzer Objekte und deren Status schnell visualisieren können, sodass die Benutzer Objekte mit öffentlichem Zugriff schnell erkennen können?*
32.	***OBJEKTSPEICHER – INVENTARISIERUNG VON METADATEN:*** *Bietet der Cloud-Anbieter Bestandsaufnahmefunktionen, 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 UNTERGRUPPEN:*** *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, mithilfe einfacher SQL-Befehle (Structured Query Language) 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 gemanagte Dateisystem eine hohe Verfügbarkeit?*
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 Cloud-basierte Dateisystem verschieben können?*
45.	***ARCHIVSPEICHERSERVICE:*** *Bietet der Cloud-Anbieter einen sehr kostengünstigen Speicherservice an, der auf die Archivierung von weniger häufig genutzten und nahezu unveränderlichen 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 UNTERGRUPPEN:*** *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, mithilfe einfacher SQL-Befehle (Structured Query Language) 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:*** *Hat der Cloud-Anbieter Einschränkungen (d. h. Service Limits) in Bezug auf den oben genannten Abschnitt zum Thema Speicher?* *Beispiel:* *Maximale Volume-Größe* *Maximale Anzahl an Laufwerken, die mit einer Instance verbunden werden können* *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 ZURÜCKSEZTEN:*** *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 nur für einen bestimmten Zeitraum 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 Steuerelementen 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 von Multi-Factor Authentication (MFA) als zusätzliche Ebene der Zugriffskontrolle und Authentifizierung für seine Infrastruktur?*
11.	***ADMINISTRATION – SERVICE LIMITS:*** *Hat der Cloud-Anbieter Einschränkungen (d. h. Service Limits) in Bezug auf den oben genannten 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 Service-Infrastruktur 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 Änderungsanforderung oder eine ähnliche formale Autorisierung?*
3.	***SICHERHEIT – ZUGRIFFSPROTOKOLLE:*** *Protokolliert der Cloud-Anbieter Personalzugriff auf seine Infrastrukturund wird dieser Zugriff immer protokolliert und die Protokolle mindestens 90 Tage aufbewahrt?*
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 – ZUGRIFFSSCHLÜSSELVERWALTUNG:* *Bietet der Cloud-Anbieter die Möglichkeit, zu erkennen, 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 ruhende Daten bereitzustellen?*
9.	*SICHERHEIT – HSM:* *Bietet der Cloud-Anbieter dedizierte Hardwaresicherheitsmodule (HSM), d. h. Hardwareanwendungen, 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" bzw. „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)?*
16.	*SICHERHEIT – ACTIVE DIRECTORY:* *Bietet der Cloud-Anbieter einen verwalteten Microsoft Active Directory-Service (AD-Service) in der Cloud an?*
17.	*SICHERHEIT – ATIVES VERZEICHNIS VOR ORT:* *Unterstützt der verwaltete Microsoft Active Directory-Service (AD-Service) des Cloud-Anbieters die Integration in ein Microsoft Active Directory (AD) vor Ort?*
18.	*SICHERHEIT – LADP:* *Unterstützt der verwaltete Microsoft Active Directory-Service (AD-Service) des Cloud-Anbieters das Lightweight Directory Access Protocol (LDAP)?*
19.	*SICHERHEIT – ACTIVE DIRECTORY:* *Unterstützt der verwaltete Microsoft Active Directory-Service (AD-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 (Application Programming Interface), Datenbankanmeldedaten und andere Geheimnisse einfach rotieren, verwalten und abrufen können?
21.	***SICHERHEIT – WAF:*** *Bietet der Cloud-Anbieter eine Web-Application-Firewall (WAF), die Web-Anwendungen vor gängigen Web-Exploits 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 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?*
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 Managed Service zur Erkennung von Bedrohungen?*
25.	***SICHERHEIT – SERVICE LIMITS:*** *Hat der Cloud-Anbieter Einschränkungen (d. h. Service Limits) in Bezug auf den oben genannten 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:

Zertifizierungen/Bescheinigungen	***Gesetze, Vorschriften und Datenschutz***	***Ausrichtungen/Rahmenbedingungen***
☐ C5 [Deutschland]	*☐ EU-Datenschutzrichtlinie*	*☐ CDSA*
☐ CISPE Data Protection Code of Conduct (CISPE-Verhaltenskodex zum Datenschutz)	*☐ EU-Modellklauseln*	
☐ 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 Harbour“
☐ 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
		☐ Uptime Institute Tier
		☐ UK-Cloud-Sicherheitsprinzipien

Durch die Nutzung der oben genannten Compliance-Berichte können Organisationen des öffentlichen Sektors Angebote im Hinblick auf Sicherheits-, Compliance- und Betriebsstandards auswerten. Solche Berichte können zeigen, dass der CISP aufgrund seiner Konformität mit ihnen die unten aufgeführten Rechenzentren-Betriebskontrollen erfüllt, die von einem Public-Cloud-Service-Anbieter gefordert werden. Indem Konformität mit solchen Berichten gefordert wird, können öffentliche Einrichtungen 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 phyischen Rechenzentrums sollte ein kontrollierter Prozess sein. Der CISP sollte an den Zugangstoren Sicherheitskräfte einsetzen, die ebenso wie die Besucher von Vorgesetzten über Sicherheitskameras überwacht werden. Wenn genehmigte Personen vor Ort sind, sollten sie einen Ausweis erhalten, der eine mehrstufige Authentifizierung erfordert und den Zugriff 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 überprüft wird. Mitarbeiterlisten sollten regelmäßig von einem zuständigen Bereichsleiter überprüft werden, um sicherzustellen, dass die Autorisierung jedes Mitarbeiters weiterhin erforderlich ist. Wenn ein Mitarbeiter keine berechtigten geschäftlichen Gründe hat, sich in einem Rechenzentrum aufzuhalten, sollte er den Besucherprozess durchlaufen.*
- ***Überwachung auf unberechtigten Zutritt:*** *CISPs sollten die Standorte kontinuierlich auf unberechtigten Zugang zu Rechenzentrumseigentum überwachen. Dazu werden Videoüberwachungs-, Einbruchmelde- und Zugriffsprotokollüberwachungssysteme verwendet. Eingänge sollten mit Vorrichtungen gesichert werden, die Alarme auslösen, wenn eine Tür zwangsweise geöffnet oder offengehalten wird.*

- ***CISP Security Operations Center überwachen die globale Sicherheit:*** *CISP Security Operations Center sollten sich auf der ganzen Welt befinden und für die Überwachung, das Triaging und die Ausführung von Sicherheitsprogrammen für CISP-Rechenzentren verantwortlich sein. Die Center sollten die Verwaltung des physischen Zugriffs und die Reaktion auf Eindringversuche 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 für jede Ebene 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 Unterbrechung 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 Personen. 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 physischem und technologischem Eindringen:*** *Zugangspunkte zu Serverräumen sollten mit elektronischen Steuergeräten gesichert werden, die eine mehrstufige Autorisierung erfordern. Der CISP sollte auch darauf vorbereitet sein, ein technologisches Eindringen zu verhindern. CISP-Server sollten Mitarbeiter vor allen Versuchen warnen können, Daten zu entfernen. Im unwahrscheinlichen Fall eines Verstoßes sollte der Server automatisch deaktiviert werden.*

- ***Server und Medien werden mit höchster Aufmerksamkeit behandelt:*** *Medienspeichergeräte, die zum Speichern von Kundendaten verwendet werden, sollten vom CISP als kritisch eingestuft und während ihres gesamten Lebenszyklus entsprechend als extrem wichtig behandelt werden. Der CISP sollte genaue Standards für die Installation, Wartung und endgültige 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 durch den CISP entfernt, wenn sie sicher stillgelegt wurden.*

- ***Unabhängige Auditoren überprüfen die CISP-Verfahren und -Systeme:*** *CISPs sollten von externen Auditoren geprüft 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. Auditoren können auch Feeds von Überwachungskameras überwachen und Eingänge und Gänge im gesamten Rechenzentrum beobachten. Und sie können Geräte wie elektronische Zutrittskontrollgeräte und Überwachungskameras von CISPs analysieren.*

- ***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, während automatische Pumpen eingesetzt werden, um Flüssigkeiten zu entfernen und Schäden zu verhindern. Ebenso reduzieren automatische Brandmelde- und -verhinderungsvorrichtungen das Risiko und können CISP-Mitarbeiter und Feuerwehrleute über ein Problem informieren.*

- ***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 durchführen.*

- ***Simulieren von Unterbrechungen und Messen der Reaktion****: Der CISP sollte einen Betriebskontinuitätsplan als Prozessleitfaden haben, in dem erläutert wird, wie Störungen aufgrund von Naturkatastrophen vermieden und reduziert werden können. Darin sollten die detaillierten Schritte ausgeführt werden, die vor, während und nach einem Ereignis durchgeführt 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 Reaktionsfähigkeit 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.*

- ***Das Erreichen von Effizienzzielen unterstützen:*** *Neben dem Umgang mit Umweltrisiken sollte der CISP auch Überlegungen zur Nachhaltigkeit in das Design 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 Umgebungs- und geografische Bewertungen durchführen. Rechenzentrumsstandorte sollten sorgfältig ausgewählt werden, um Umweltrisiken wie Überschwemmungen, Risiken durch extreme Wetterbedingungen und seismische Aktivitäten gering zu halten. CISP Availability Zones sollten unabhängig voneinander und physisch voneinander getrennt sein.*

- ***Redundanz:*** *Rechenzentren sollten so ausgelegt sein, dass Ausfälle vorhergesehen und toleriert werden können, während die Service-Level aufrechterhalten werden. Bei einem Ausfall sollten automatisierte Prozesse den Datenverkehr aus dem betroffenen Bereich entfernen. Die Kernanwendungen sollten in einem N+1-Standard bereitgestellt werden, sodass im Falle eines Rechenzentrumsausfalls ausreichend Kapazität vorhanden ist, um den Datenverkehr lastenverteilt an die verbleibenden Standorte zu verteilen.*

- ***Verfügbarkeit:*** *Der CISP sollte kritische Systemkomponenten identifizieren, die zur Aufrechterhaltung der Verfügbarkeit des Systems und, im Falle eines Ausfalls, zur Wiederherstellung des Service erforderlich sind. Kritische Systemkomponenten sollten über mehrere isolierte Standorte 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. Hochausfallsichere Systeme und damit die Serviceverfügbarkeit sollten eine Funktion des Systemdesigns sein. Das Rechenzentrumsdesign mit Availability Zones und Datenreplikation, sollte es CISP-Kunden ermöglichen, extrem kurze Recovery-Zeiten- und Recovery-Point-Ziele sowie ein Höchstmaß an Serviceverfügbarkeit zu erreichen.*

- ***Kapazitätsplanung****: Der CISP sollte die Servicenutzung kontinuierlich überwachen, um die notwendige Infrastruktur bereitzustellen und so die Verfügbarkeitsverpflichtungen und -anforderungen zu erreichen. Der CISP sollte ein Kapazitätsplanungsmodell pflegen, 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 Überwachungsprotokollspeicherung umfassen.*

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 zu ergreifenden Schritten enthalten. Der Betriebskontinuitätsplan sollte durch Tests unterstützt werden, die Simulationen verschiedener Szenarien umfassen. 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 Notfallswiederherstellungsplanung integrieren, um schnell auf Bedrohungen durch Infektionskrankheiten zu reagieren. Strategien zur Risikominderung umfassen alternative Personalmodelle zur Übertragung kritischer Prozesse auf Ressourcen außerhalb der Region sowie die Aktivierung eines Krisenmanagementplans zur Unterstützung wichtiger*

Geschäftsabläufe. Pandemiepläne sollten auf internationale Gesundheitsbehörden und Vorschriften, einschließlich Kontaktstellen für internationale Behörden, verweisen.

ÜBERWACHUNG und PROTOKOLLIERUNG

- ***Überprüfung des Zugangs zu Rechenzentren:*** *Der Zugang zu Rechenzentren sollte regelmäßig überprüft 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 Anfragedauer 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 korrelieren, um die Sicherheit nach Bedarf zu erhöhen.*

- ***Zugangsüberwachung für Rechenzentren:*** *Der CISP sollte Rechenzentren über globale Security Operations Center überwachen, die für die Überwachung, das Triaging und die Ausführung von Sicherheitsprogrammen zuständig sind. Die Center sollten einen weltweiten Support rund um die Uhr bereitstellen, indem sie die Zugriffsaktivitäten im Rechenzentrum verwalten und überwachen sowie lokale Teams und andere Supportteams so ausstatten, dass sie auf Sicherheitsvorfälle durch Triaging, Beratung, Analyse und aktives Handeln reagieren können.*

ÜBERWACHUNG und ERKENNUNG

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

- ***Zugangspunkt zu Rechenzentren:*** *Der physische Zugang an den Zugangspunkten zum Gebäude sollte von professionellem Sicherheitspersonal mithilfe von Videoüberwachung, Angriffserkennungssystemen und anderen elektronischen Mitteln überwacht werden. Autorisierte Mitarbeiter sollten für den Zugriff auf Rechenzentren mehrstufige Authentifizierungsmechanismen einsetzen. Eingänge zu Serverräumen sollten mit Geräten gesichert werden, die Alarme auslösen, um bei gewaltsam geöffneter oder offen gehaltener Tür eine Reaktion auf einen Vorfall auszulösen.*

- ***Eindringungserkennung:*** *In der Datenschicht sollten elektronische Meldesysteme zur Erkennung von Eindringversuchen installiert werden, um Sicherheitsvorfälle zu überwachen, diese zu erkennen und das entsprechende Personal zu alarmieren. Eingangs- und Ausgangspunkte zu Serverräumen sollten mit Geräten gesichert werden, bei denen jede Person vor dem Betreten oder Verlassen eine mehrstufige Authentifizierung durchführen muss. Diese Geräte lösen Alarme aus, wenn die Tür ohne Authentifizierung zwangsweise geöffnet oder offen gehalten 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 mehrstufige Authentifizierung erfolgt. Alarme sollten sofort an rund um die Uhr verfügbare CISP Security Operations Center weitergeleitet werden, wo sie sofort protokolliert, analysiert und beantwortet werden können.*

GERÄTEMANAGEMENT

- ***Asset-Management:*** *CISP-Assets sollten zentral über ein Bestandsverwaltungssystem verwaltet werden, das Eigentümer-, Standort-, Status-, Wartungs- und beschreibende Informationen für CISP-eigene Assets speichert und verfolgt. Nach der Beschaffung sollten die Ressourcen gescannt und nachverfolgt werden und Assets, die einer Wartung unterzogen werden, auf Eigentümerschaft, Status und Auflösung 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 als extrem wichtig behandelt werden. Der CISP sollte exakte Standards zur Installation, Wartung und endgültigen Zerstörung 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, werden erst aus der Kontrolle durch den CISP entfernt, wenn sie sicher stillgelegt wurden.*

BETRIEBLICHE SUPPORT-SYSTEME

- ***Stromversorgung:*** *Die elektrischen Stromversorgungssysteme des CISP-Rechenzentrums sollten so ausgelegt sein, dass sie rund um die Uhr vollständig redundant und wartungsfrei sind. Der CISP sollte dafür sorgen, dass Rechenzentren mit einer Notstromversorgung ausgestattet sind, um sicherzustellen, dass bei einem Ausfall die Stromversorgung für den Betrieb kritischer und wichtiger Lasten im Rechenzentrum verfügbar ist*

- ***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 Möglichkeit von Serviceausfällen verringert. Temperatur und Luftfeuchtigkeit müssen in angemessener Weise vom Personal und den technischen Systemen überwacht und geregelt werden.*

- ***Branderkennung und -unterdrückung****: CISP-Rechenzentren sollten mit automatischen Brandmelde- und -unterdrückungsanlagen ausgestattet werden. Brandmeldeanlagen sollten Rauchmelder in Netzwerk-, Mechanik- und Infrastrukturbereichen verwenden. Diese Bereiche müssen zusätzlich durch Unterdrückungssysteme geschützt werden.*

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

INFRASTRUKTURWARTUNG

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

- ***Umgebungsmanagement:*** *Der CISP sollte elektrische und mechanische Systeme und Geräte überwachen, um Probleme sofort erkennen zu können. Dies sollte mithilfe von kontinuierlichen Audit-Tools und Informationen erfolgen, die über CISP-Systeme zum Gebäudemanagement und zur elektrischen Kontrolle bereitgestellt werden. Es sollten vorbeugende Wartungen vorgenommen werden, um eine kontinuierliche Funktionsfähigkeit der Anlagen sicherzustellen.*

GOVERNANCE UND RISIKO

- ***Fortlaufendes Risikomanagement für Rechenzentren:*** *Das CISP Security Operations Center sollte regelmäßige Überprüfungen von Bedrohungen und Schwachstellen in Rechenzentren durchführen. Eine laufende Bewertung und Minderung potenzieller Schwachstellen sollte über Risikobewertungaktivitäten im Rechenzentrum durchgeführt werden. Diese Bewertung sollte zusätzlich zum Risikobewertungsprozess auf Unternehmensebene durchgeführt werden, der zur Identifizierung und Verwaltung 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 durch Dritte, wie in den Berichten von unabhängigen Dritten dokumentiert, 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 Gänge 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 – ZENTRALES MONITORING:*** *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 Kennzahlen 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 DRITTANBIETERN:* *Ermöglicht das Migrationstool des Cloud-Anbieters die Integration von Migrationstools von Drittanbietern?* • *Wenn ja, welche Migrations-Tools von Drittanbietern werden unterstützt?*
6.	*MIGRATIONEN – ÜBERREGIONALE 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, vor Ort 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 virtuelle Server vor Ort automatisch zu suchen, 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 (Central Processing Unit) und RAM (Random Access Memory) zu erfassen und anzuzeigen?*
10.	*MIGRATIONEN – ERKENNUNGSDATENBANK:* *Kann das Migrationstool des Cloud-Anbieters alle erfassten Daten in einer zentralen Datenbank speichern?* • *Wenn ja, können Kunden diese Daten exportieren? Welche Formate werden unterstützt?*
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 virtuellen Maschinen -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 virtuellen Maschinen-Migrationen von lokalen zu virtuellen VMware-Maschinen?*
14.	*MIGRATIONEN – HYPER-V:* *Unterstützt das Migrationstool des Cloud-Anbieters Migrationen virtueller Hyper-V-Maschinen von vor Ort 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 VON 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 wie Oracle zu SQL Server?* • *Wenn ja, listen Sie bitte alle möglichen Kombinationen aus heterogenen Datenbankmigrationen auf.*
21.	*MIGRATIONEN – DATENMIGRATION AUF PETABYTEEBENE:* *Bietet der Cloud-Anbieter eine Datentransportlösung in Petabytegröße, die sichere Geräte verwendet, um große Datenmengen in die und aus der Cloud zu übertragen?*
22.	*MIGRATIONEN – DATENMIGRATION AUF EXABYTEEBENE:* *Bietet der Cloud-Anbieter eine Datentransportlösung in Exabytegröße, um extrem große Datenmengen in die Cloud zu verschieben?*
23.	*MIGRATIONEN – ENTERPRISE-BACKUPS:* *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 gespeichert werden können?*
24.	*MIGRATIONEN – ENTERPRISE BACKUPS – OBJEKTSPEICHER:* *Bietet der Enterprise-Backup-Service des Cloud-Anbieters die Integration in den Cloud-Objekt-Speicherservice des Anbieters?*
25.	*MIGRATIONEN – ENTERPRISE-BACKUPS – DATEIZUGRIFF:* *Ermöglicht der Enterprise-Backup-Service des Cloud-Anbieters Benutzern das Speichern und Abrufen von Objekten mithilfe von Dateiprotokollen wie dem NFS-Protokoll (Network File System)?*
26.	*MIGRATIONEN – ENTERPRISE-BACKUPS – BLOCKZUGRIFF:* *Ermöglicht der Enterprise-Backup-Service 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-BACKUPS – BANDZUGRIFF:* *Ermöglicht der Enterprise-Backup-Service des Cloud-Anbieters Benutzern, ihre Daten über eine virtuelle Bandbibliothek zu sichern und diese Band-Backups in der Cloud des Anbieters zu speichern?*
28.	*MIGRATIONEN – ENTERPRISE-BACKUPS – VERSCHLÜSSELUNG:* *Bietet der Enterprise-Backup-Service des Cloud-Anbieters die Verschlüsselung von Daten im Ruhezustand und während der Übertragung?*
29.	*MIGRATIONEN – ENTERPRISE-BACKUPS – INTEGRATION IN DRITTANBIETER-SOFTWARE:*

	Lässt sich der Enterprise-Backup-Service des Cloud-Anbieters in gängige Backup-Software von Drittanbietern integrieren?
30.	***MIGRATIONEN – SERVICE LIMITS:*** *Hat der Cloud-Anbieter Einschränkungen (d. h. Service Limits) in Bezug auf den oben genannten Abschnitt zum Thema Migrationen?* *Beispiel:* *Maximale Anzahl gleichzeitiger Migrationen virtueller Maschinen* *Maximal bestellbare Anzahl an Datentransportlösungen*

8. Rechnungsstellung

	Anforderung
1.	***RECHNUNGSSTELLUNG – NACHVERFOLGUNG UND REPORTING:*** *Bietet der Cloud-Anbieter einen Service für Nachverfolgung und Reporting 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 benachrichtigen, 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 mehrerer Konten unter einem einzigen primären Zahlungskonto?*
6.	***RECHNUNGSSTELLUNG – SERVICE LIMITS:*** *Hat der Cloud-Anbieter Einschränkungen (d. h. Service Limits) in Bezug auf den oben genannten 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 erfasst, überwacht und Berichte erstellt?*

2.	***VERWALTUNG – ALARME:*** *Ermöglicht der Überwachungsservice des Cloud-Anbieters Benutzern die Einrichtung von Alarmen?*
3.	***VERWALTUNG – BENUTZERDEFINIERTE KENNZAHLEN:*** *Ermöglicht der Überwachungsservice des Cloud-Anbieters Benutzern die Erstellung und Überwachung benutzerdefinierter Kennzahlen?*
4.	***VERWALTUNG – ÜBERWACHUNG DER GRANULARITÄT:*** *Bietet der Überwachungsservice des Cloud-Anbieters bis hinunter zur 1-Minuten-Ebene verschiedene Ebenen der Überwachung von Granularität?*
5.	***VERWALTUNG – API-NACHVERFOLGUNGSSERVICE:*** *Bietet der Cloud-Anbieter einen Service, der Aktivitäten sowohl auf Konsolen- als auch auf API-Ebene (Application Programming Interface) protokolliert, überwacht und auf Cloud-Ressourcen speichert, um die Transparenz zu verbessern?* • *Wenn ja, welche Services lassen sich mit diesem Nachverfolgungsservice integrieren?*
6.	***VERWALTUNG – BENACHRICHTIGUNGEN:*** *Ermöglicht der Cloud-Anbieter das Senden von Benachrichtigungen basierend auf den Aktivitätsleveln der API (Application Programming Interface)?*
7.	***VERWALTUNG – KOMPRIMIERUNG:*** *Bietet der Cloud-Anbieter einen Mechanismus zur Komprimierung von Protokollen, die vom API-Nachverfolgungssystem (Application Programming Interface) generiert werden, um die mit diesem Service verbundenen Speicherkosten zu senken?*
8.	***VERWALTUNG – ZUSAMMENFASSUNG VON REGIONEN:*** *Bietet der Cloud-Anbieter die Möglichkeit, API-Aktivitäten (Application Programming Interface) eines Kontos in allen Regionen aufzuzeichnen und diese Informationen für eine einfache Nutzung aggregiert bereitzustellen?*
9.	***VERWALTUNG – RESSOURCENBESTAND:*** *Bietet der Cloud-Anbieter einen Service zur Bewertung, Prüfung und Evaluierung 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 Punkt in der Vergangenheit zu untersuchen?*
12.	***VERWALTUNG – KONFIGURATIONSREGELN:*** *Bietet der Cloud-Anbieter Richtlinien und Empfehlungen für Bereitstellung, Konfiguration und kontinuierliche Überwachung der Compliance?*
13.	***VERWALTUNG – RESSOURCENVORLAGEN:*** *Bietet der Cloud-Anbieter Benutzern die Möglichkeit, eine Sammlung von Ressourcen auf Vorlagenebene 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. bei Notfallwiederherstellungen (DRs) 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) und ermöglicht die Automatisierung von Verwaltungsaufgaben mithilfe 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:*** *Hat der Cloud-Anbieter Einschränkungen (d. h. Service Limits) in Bezug auf den oben genannten 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 – SUPPORT-TIER:*** *Bietet der Cloud-Anbieter verschiedene Support-Tier-Stufen?*
3.	***SUPPORT – TIER-VERTEILUNG:*** *Ermöglicht der Cloud-Anbieter Benutzern die Selbstzuweisung der verwendeten Ressourcen/Services zu verschiedenen Supportstufen auf der Grundlage einer granularen Klassifizierung und nicht durch die 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 aktuelle 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-HISTORIE:*** *Bietet der Cloud-Anbieter eine 365-Tage-Dashboard-Historie 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 (Application Programming Interface), die programmatisch mit Support-Fällen 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 sichtbare technische Dokumentation für seine Befehlszeilenschnittstelle (CLI)?*
14.	***SUPPORT – REFERENZARCHITEKTUREN:*** *Bietet der Cloud-Anbieter eine kostenlose Online-Sammlung von Referenzarchitekturdokumenten an, um Kunden beim Aufbau spezifischer Lösungen zu unterstützen, die viele Cloud-Services von Cloud-Anbietern kombinieren?*
15.	***SUPPORT – REFERENZBEREITSTELLUNGEN:*** *Bietet der Cloud-Anbieter eine kostenlose Online-Sammlung von Dokumenten mit detaillierten, getesteten und validierten Verfahren, einschließlich Best Practices, zur Implementierung allgemeiner Lösungen (d. h. DevOps, Big Data, Data Warehouse, Microsoft-Workloads, SAP-Workloads usw.) in seinen Cloud-Angeboten?*

Anhang B – Demo

Anhand von Demos können Endbenutzer Cloud-Angebote effektiv testen und entscheiden, ob sie den Geschäftsanforderungen der Organisation am besten entsprechen. Im Folgenden finden Sie ein Beispieltestskript für Cloud-Technologien.

1. *Demonstrieren Sie auf hoher Ebene die CISP-Konsole und die öffentlich verfügbaren Angebote/Ressourcen:*
    - *Speicherfunktionen*
    - *Datenverarbeitungsfunktionen*
    - *Datenbankfunktionen und -typen*
    - *Netzwerk*
    - *Management- und Analysetools*
    - *Sicherheit*
    - *Weitere Funktionen*
2. *Beschreiben Sie, wie Sie Ihre in der Demoversion verwendeten Cloud-Technologien betreiben.*
3. *Demonstrieren Sie, wie Sie diese Demos in Echtzeit mit dem Cloud-Angebot durchführen.*
4. *Konten:*
    - *Beschreiben Sie das Kontoschlüsselsystem (Root und Benutzer), dass in der Demoversion verwendet wird.*
    - *Demonstrieren Sie, wie Sie Ihre Kontoschlüssel verwalten und schützen.*
5. *Demonstrieren Sie, wie Sie den physischen Speicherort für Ihre Workloads/Daten auswählen können.*
6. *Demonstrieren Sie die Skalierung Ihres Angebots, indem Sie umfangreiche Datenverarbeitungs- und Speicherlösungen einrichten.*
7. *Veranschaulichen Sie, wie ein Endbenutzer verschiedene Services von Cloud-Angeboten anfordert. Demonstrieren Sie Folgendes:*
    - *Wie Konten eingerichtet werden*
    - *Wie Sicherheitsmaßnahmen aktiviert werden*
    - *Wie Hauptkonten in Unterkonten unterteilt werden können*
    - *Wie Ihr Identitäts- und Zugriffsmanagement (IAM) den Zugriff auf verschiedene Ressourcen trennen kann:*
        - *Wie Konten gesichert werden*
        - *Wie Benutzer und Gruppen erstellt werden*
        - *Richtlinie anhängen*
        - *Passwörter einrichten*
8. *Demonstrieren Sie, wie virtuelle Umgebungen aus Sicherheits- und Netzwerkperspektive isoliert werden können:*
    - *Erstellen von Subnetzen*
    - *Internet-Routing*
9. *Demonstrieren Sie, wie Sie eine Umgebung an zwei oder mehr getrennten Standorten erstellen können.*
    - *Demonstrieren Sie den Lastenausgleich zwischen den Umgebungen.*
10. *Demonstrieren Sie die Fähigkeit, mehrere Methoden für die Interaktion mit den Cloud-Computing-Services zu verwenden (z. B. Anwendungsprogramm-Schnittstelle (API), Webkonsole, Befehlszeile).*
11. *Speicherung:*
    - *Beschreiben der Speicheroptionen*
    - *Demonstrieren Sie die verfügbaren Speichertypen (z. B. Block, Objekt) und Datenlebenszyklusprozesse.*
    - *Erstellen Sie ein Speicher-Volume und demonstrieren Sie, wie Daten geladen und abgerufen werden.*

- *Erstellen Sie ein XGB-Speicher-Volume mit und ohne Datenverarbeitungsoption.*
- *Demonstrieren und validieren Sie die Berechtigungen für den Zugriff auf diese Volume.*

12. *Datenverarbeitung:*
    - *Beschreiben Sie die Datenverarbeitungsoptionen – Größe und Funktionen von Datenverarbeitungsressourcen.*
    - *Demonstrieren Sie die Aktivierung und Deaktivierung einer Datenverarbeitungsressource.*
    - *Demonstrieren Sie die Eigenschaften (Fähigkeit, x Instances gleichzeitig zu starten, Netzwerkauswahl, Schutz vor versehentlicher Beendigung, Mandantenfähigkeit usw.)*
    - *Demonstrieren Sie eine Datenverarbeitungsoption mit dem Äquivalent von x Cores und x GB RAM.*
    - *Demonstrieren Sie die lastbasierte Skalierung von Ressourcen durch Ausführung einer Workload.*
    - *Demonstrieren Sie die automatischen Skalierungsfunktionen.*
    - *Demonstrieren Sie, wie die Datenverarbeitung gestoppt und später neu gestartet werden kann.*
    - *Demonstrieren Sie, wie eine Datenverarbeitungsoption die Größe nach oben oder unten ändern und Konfigurationen beibehalten kann.*
    - *Demonstrieren Sie, wie eine Datenverarbeitungsoption kopiert werden kann.*
    - *Demonstrieren Sie die Konfiguration von Sicherheitsgruppen.*
    - *Beschreiben Sie, welche Betriebssysteme im CISP-Angebot verfügbar sind.*
    - *Demonstrieren Sie ein Beispiel für die Installation eines Linux-Betriebssystems.*
    - *Beschreiben Sie Ihre Möglichkeiten zur Bereitstellung von Images für Datenverarbeitungsangebote.*
    - *Welche Bildformate unterstützen Sie?*
    - *Demonstrieren Sie, wie Sie ein Image laden und betreiben würden.*
    - *Demonstrieren Sie serverlose Datenverarbeitung.*
    - *Demonstrieren Sie die Fähigkeit, ein Cluster von Server-Instances mit variablen Preisen auf Basis eines Spotmarkts zu starten.*
13. *Datenbank:*
    - *Beschreiben Sie Ihre Datenbankfunktionen.*
    - *Demonstrieren Sie die Funktionen von MySQL, MS SQL Server, Oracle und Postgres.*
    - *Demonstrieren Sie alle Data-Warehousing-Funktionen.*
    - *Demonstrieren Sie die Möglichkeiten, diese Ressourcen zu sichern.*
14. *Netzwerke:*
    - *Demonstrieren Sie softwaredefinierte Netzwerkoptionen und Netzwerkverwaltungs-funktionen.*
15. *Verwaltung und Analyse*
    - *Beschreiben Sie Ihre Cloudmanagement- und Analysefunktionen.*
    - *Demonstrieren Sie die Überwachungsoptionen.*
    - *Demonstrieren Sie Ihre Fähigkeiten mit Hadoop-Frameworks.*
16. *Sicherheit: Demonstrieren Sie die Netzwerksicherheit.*
    - *Beschreiben Sie Ihren Sicherheitsansatz.*
    - *Firewalls*
    - *Sicherheitsgruppen*
    - *Gateways*
    - *NACLs*
    - *Systemprotokolle*
    - *Verschlüsselung*
    - *Verfügbare Compliance-Akkreditierungen*

- *Schlüsselspeicher*
- *Weitere Funktionen*

17. *Bereitstellung: Demonstrieren Sie, wie Sie eine Sammlung verwandter Cloud-Ressourcen erstellen und diese mithilfe einer wiederverwendbaren Vorlage geordnet und vorhersagbar bereitstellen können.*
18. *Software: Demonstrieren Sie Ihre Fähigkeiten, Zugriff auf häufig verwendete Software und deren Nutzung zu ermöglichen.*
19. *Demonstrieren Sie, wie Sie umfangreiche Datenübertragungen durchführen können.*
20. *Demonstrieren Sie Abrechnungsoptionen, darunter:*
    - *Zusammenfassungsansicht, granulare Ansicht, Ansicht nach markierten Ressourcen*
    - *Prognostizierte Ausgaben/Nutzung basierend auf aktuellen Ausgaben/aktueller Nutzung*
21. *Demonstrieren Sie die verfügbaren Support- und Beratungsmöglichkeiten*
    - *Welche Support-Optionen sind verfügbar?*
    - *Gibt es Funktionen, die Überprüfungen und Ratschläge zur Nutzung der Services bieten?*

Demonstrieren Sie alle anderen Merkmale des Angebots, von denen Sie glauben, dass sie das Angebot von anderen abgrenzen.