



Kamu Sektöründe Bulut Hizmetleri Satın Alma

El Kitabı - Bulut Çerçeve Sözleşmesi İçin Örnek Teklif
Talebi (RFP) Metinleri Dahil

Sürüm 2: Şubat 2022

Bildirimler

Bu belge sadece bilgilendirme amacıyla hazırlanmıştır. Belirli herhangi bir bölgedeki kamu ihalesi süreçlerine ilişkin yasal gerekliliklere uygun olarak yazılmamıştır. Bulut müşterileri bu belgede yer alan bilgileri bağımsız değerlendirmelerinden geçirerek yorumlamaktan ve bir bulut sağlayıcısından aldıkları ürün veya hizmetlerin kullanımından bizzat sorumludur. Bu belge hiçbir garanti, beyan, sözleşme taahhüdü, koşul veya güvence niteliği taşımaz.

Örnek belgeler ve metinler yasal tavsiye, rehberlik veya danışmanlık olarak yorumlanmamalıdır. Bulut müşterileri faaliyet gösterdikleri ülkenin geçerli yasaları kapsamındaki sorumlulukları hakkında kendi hukuk danışmanlarının görüşüne başvurmalıdır. CISPE, bu belgede yer alan bilgilere ilişkin her türlü garantiyi veya bu bilgilerin kullanımından kaynaklanan ya da onunla bağlantılı olarak ortaya çıkan her türlü sorumluluk veya zararı açıkça reddeder.

CISPE Hakkında

CISPE (Avrupa Bulut Altyapısı Hizmetleri Sağlayıcıları, <https://cispe.cloud>) kâr amacı gütmeyen bağımsız bir sektör derneğidir. Avrupa'daki bulut altyapısı hizmet sağlayıcılarını temsil ederek bulut hizmetlerine ve bu hizmetlerin sektördeki, kamu yaşamındaki ve genel olarak toplumdaki rolüne ilişkin rehberlik ve eğitim sağlamak amacıyla sektörle ve politika yapıcılarla birlikte çalışıyoruz.

Büyüyen üye tabanımız tüm AB ülkelerinde faaliyet gösteren şirketlerden ve dünya çapında genel merkezleri bulunan 16 Avrupalı şirketten oluşmaktadır. Şirketler, hizmetlerinden en az birinin CISPE Veri Koruma Davranış Kuralları gerekliliklerini karşıladığını beyan etmeleri kaydıyla derneğe üye olabilmektedir. Dernek olarak:

- AB ve AB Üye Devletleri'nde bulut öncelikli kamu ihale politikalarının faydalarını savunuyoruz.
- Bulut altyapısı sektörünü 2030'a kadar İklim Nötr hale ulaştırmayı hedefliyoruz.
- Tüm AB genelinde tutarlı güvenlik gerekliliklerinin ve teknik standartların benimsenmesini destekliyoruz.
- Veri Koruma Davranış Kuralları ile kapsamlı gizlilik gerekliliklerini destekliyoruz.
- AB bulut altyapısı pazarını açık, rekabetçi ve bağımsız tutmaya gayret ediyoruz.
- AB mevzuat çerçevesinde haklı gerekçelere dayanmayan içerik izleme yükümlülüklerine yer verilmesini engelliyoruz.

Üyelerimiz hükümetlerin, kamu makamlarının ve işletmelerin kendi sistemlerini geliştirmesini ve milyarlarca vatandaşa temel hizmetler sunmasını mümkün kılan "BT'nin temel yapı taşlarını" sunmakta ve sürdürmektedir. Bu rolümüz gereği, yapay zekayı (AI), bağlı nesneleri, otonom taşıtları ve yeni nesil hücresel bağlantı teknolojisi olan 5G'yi bünyesinde barındıran ileri düzey teknolojilerin ve hizmetlerin geliştirilmesi için gerekli olanakların sağlanmasına yardımcı oluyoruz.

Bulut Altyapısı Hizmetleri İçin Davranış Kuralları

CISPE Veri Koruma Davranış Kuralları, Avrupa Birliği Genel Veri Koruma Yönetmeliği'nin (GDPR) yürürlüğe girmesinden daha önce, Eylül 2016'da halka açık olarak yayınlanmıştır. Bulut altyapısı sağlayıcılarının veri koruma uygunluğunu işler hale getirmesine yardımcı olmak ve müşterilerin bulut sağlayıcılarını seçmesine ve sundukları hizmetlere güvenmesine yardımcı olacak güçlü bir çerçeve ortaya koymak amacıyla katı GDPR gerekliliklerine uygun olarak hazırlanmıştır. CISPE Davranış Kuralları, Mayıs 2021'de [Avrupa Veri Koruma Kurulu \(EDPB\) tarafından doğrulanmış](#) ve Haziran 2021'de Yetkili Makam sıfatıyla hareket eden [Fransız Veri Koruma Kurumu \(CNIL\)](#) tarafından onaylanmıştır. <https://www.codeofconduct.cloud/>

İklim Nötr Veri Merkezi Paketi

CISPE, veri merkezlerini 2030'a kadar iklim nötr statüsüne kavuşturmak amacıyla bir dizi ölçüm ve bir öz düzenleyici girişim oluşturmak için 2019'un sonunda Avrupa Komisyonu ile iş birliğine girdi. EUDCA'nın (Avrupa Veri Merkezleri Birliği) yanı sıra diğer ticaret birlikleri ve veri merkezi pazarı aktörleri ile birlikte oluşturulan bu girişim Ocak 2021'de "İklim Nötr Veri Merkezi Paketi"

(<https://www.climateneutraldatacentre.net/>) ile sonuçlandı.

FAIR Yazılım Girişimi

CISPE; Fransız CIO birliği CIGREF ile birlikte Avrupa genelindeki diğer CIO ve Hizmet Sağlayıcı ticaret birliklerinin desteğiyle [Bulut Müşterileri İçin Adil Yazılım Lisanslamasının 10 İlkesi](#)'ni geliştirdi. Bu ilkeler, inovasyonla büyüme ve esneklik için bulut çözümlerine başvuran ve yazılım sağlayıcılarından adil lisanslama hükümlerinin uygulanmasını talep eden işletmelere yönelik bir dizi en iyi uygulamadan oluşmaktadır.

<https://www.fairsoftware.cloud/>

GAIA-X

CISPE; açık, şeffaf ve güvenli bir dijital ekosistem sunma amacıyla oluşturulan Avrupalı bir girişim olan GAIA-X'in yirmi iki kurucu üyesinden biridir. Dolayısıyla CISPE, GAIA-X kuruluşunun vizyonuna ve ilkelerine en baştan itibaren uygun olarak hareket etmektedir ve Genel Sekreteri Haziran 2021'de yeniden seçilerek yönetim kurulunda görev almıştır. [CISPE Veri Koruma Davranış Kuralları](#) ve [SWIPO IaaS Davranış Kuralları](#) gibi, el kitabında bahsedilen araçlardan bazıları, GAIA-X ilkelerine uygunluğun ortaya konulmasında yararlı olmaktadır. <https://www.gaia-x.eu>

CISPE ve Kamu Sektörü

CISPE, Avrupa bulut altyapısı sektörünün oynadığı rolün, yaptığı katkıların ve sahip olduğu potansiyelin daha iyi anlaşılmasını sağlamak amacıyla Avrupa kamu politikası tartışmalarına ve çalışmalarına katkıda bulunmaktadır.

Kamu satın alım modelleri bulut bilgi işlemin benimsenmesi ve kullanılması sürecine ilişkin şartları tanımlasa da bulut hizmetleri satın alma, kamu sektörünün aşına olduğu çoğu geleneksel teknoloji satın alımlarından farklılık gösterir. İhale yaklaşımlarının baştan düşünülmesi gerekiyor: CISPE, AB politika yapıcılarını, "bulut öncelikli" politika girişimlerine dayalı olarak AB ölçeğinde, Avrupa'daki tek bulut altyapısı pazarının büyümesine katkıda bulunacak ve DSM (Dijital Tek Pazar) büyüme hedeflerini destekleyecek daha iddialı ve ileriye dönük bir yaklaşım oluşturmaya teşvik etmektedir.

Bu el kitabı, bulut hizmetleri satın almada kamu makamlarına rehberlik edecek ve destek olacak yararlı bir kaynak olarak kullanılmak üzere tasarlanmıştır.

Daha fazla bilgi

CISPE üyeleri: <https://cispe.cloud/members>

Yürütme Kurulu: <https://cispe.cloud/board-of-directors>

CISPE Davranış Kuralları'na uygun olduğu beyan edilen bulut bilgi işlem hizmetleri:

<https://www.codeofconduct.cloud/public-register/>

İçindekiler

Bildirimler	2
CISPE Hakkında	3
İçindekiler	5
Bu El Kitabı'nın özeti ve amacı	1
1.0 Bulut Çerçeve Sözleşmesine Genel Bakış	4
2.0 Bulut Hizmetleri RFP'sine Genel Bakış	7
2.1 Bulut Hizmetleri RFP'sinin Oluşumu	7
2.1.1 Giriş ve Stratejik Hedefler	7
2.1.2 RFP Yanıtı Zaman Çizelgesi	10
2.1.3 Tanımlar	10
2.1.4 Satın Alma Modeline ve Çerçeve Sözleşmesi Dahilinde Rekabete İlişkin Ayrıntılı Açıklama	11
2.1.5 İsteklilerin Karşılması Gereken Asgari Gereklilikler - İdari	15
2.2 Teknik	17
2.2.1 Asgari Gereklilikler	18
2.2.2 Satıcıların Karşılaştırılması	21
2.2.3 Sözleşme yapma	22
2.3 Güvenlik	24
2.3.1 Asgari Gereklilikler	24
2.3.2 Satıcıların Karşılaştırılması	29
2.3.3 Sözleşme yapma	30
2.4 Fiyatlandırma	30
2.4.1 Asgari Gereklilikler	31
2.4.2 Satıcıların Karşılaştırılması	33
2.5 Sözleşme Yürütme Planı/Hüküm ve Koşullar	36
2.5.1 Hüküm ve Koşullar	36
2.5.2 Yazılım Hüküm ve Koşulları	38
2.5.3 Proje Bazında İstekliler Arasından Seçim Yapılması	40
2.5.4 Katılım ve Çıkış	40
3.0 En İyi Uygulamalar/Çıkarılan Dersler	41
3.1 Bulut Yönetişimi	41
3.2 Bulut için Bütçelendirme	41
3.3 Çözüm Ortağı İş Modelini Anlama	43
3.4 Bulut Aracıları	44
3.5 RFP öncesinde dış kaynak kullanımı/pazar araştırması	44
3.6 Sürdürülebilirlik	44
Ek A - İstekliler Arasında Karşılaştırmayla İlgili Teknik Gereklilikler	46
1. Bulut sağlayıcısı profili	46
2. Küresel altyapı	46
3. Altyapı	47
3.1 Bilgi İşlem	47

3.2 Ağ İletişimi	50
3.3 Depolama	54
4. İdare.....	58
5. Güvenlik.....	59
6. Uygunluk.....	61
7. Taşıma	66
8. Faturalama	68
9. Yönetim	69
10. Destek.....	71
Ek B - Canlı Teknik Değerlendirme	73
Platform - Örnek Canlı Teknik Değerlendirme	75
İş Yüğü: Web Uygulaması - Örnek Canlı Teknik Değerlendirme.....	84

Bu El Kitabı'nın özeti ve amacı

Bu **Bulut Hizmetleri Satın Alma El Kitabı**'nın amacı bir rekabetçi ihale süreci (**Bulut Hizmetleri Teklif Talebi - RFP**) yoluyla bulut hizmetleri satın almak isteyen fakat bir Bulut Çerçeve Sözleşmesi hazırlamak için gerekli uzmanlığa sahip olmayan bulut müşterilerine rehberlik sağlamaktır.

Bu belge sadece bilgilendirme amacıyla hazırlanmıştır. Belirli herhangi bir ülkedeki veya bölgedeki kamu ihalesi süreçlerine ilişkin yasal gerekliliklere uygun olarak yazılmamıştır.

El kitabı ayrıca bir Bulut Çerçeve Sözleşmesi üzerinden satın alım yapılan durumlarda **Açık Siparişler** veya **Küçük İhaleler** için ilave seçim kriterleri metnini içermektedir. El kitabının bölümleri genel bir BT RFP'sine benzer şekilde düzenlenmiştir. Örnek genel RFP ve seçim kriterleri metninin yanında açıklamalar da verilmektedir. Bu açıklamalar, bulut RFP'sinin geleneksel BT RFP'lerinden neden farklı olduğunun anlaşılmasına yardımcı olmaktadır.

Avrupalı Kurum ve Kuruluşların, bulut öncelikli bir yaklaşımla BT altyapılarını nasıl modernize edeceklerine ilişkin bilgiler içeren AB Komisyonu Bulut Stratejisi'nin yayınlanmasının ardından CISPE, el kitabını Temmuz 2019'da düzenlenen "*How to transform governments through a smart cloud policy*" adlı etkinlik sırasında AB Komisyonu'na teslim etti.



Bu el kitabının **2. sürümü**; veri koruma (bölüm 2.3.1.1), bulut sağlayıcısının değiştirilmesi ve verilerin taşınması (bölüm 2.3.1.2), yazılım hüküm ve koşulları (bölüm 2.5.2), bulutta sürdürülebilirlik (bölüm 3.6) ile ilgili yeni bilgilerin yanı sıra yenilenmiş Ek B Canlı Teknik Değerlendirme bölümünü içermektedir.

"Bulut Hizmetleri" bir son kullanıcının erişmeye gerek duyabileceği bulut teknolojilerinin ve ilişkili hizmetlerin tümünü ifade eder. Bulut hizmetleri; bulut altyapısına ek olarak, buluta geçişi destekleyip yürütmek ve buluttaki iş yüklerini desteklemek için gerekli danışmanlık hizmetlerini veya profesyonel/yönetilen hizmetleri ve Hizmet Olarak Yazılım (SaaS) ürünleri gibi bulut pazar yeri hizmetlerini içerir.

Bulut bilgi işlemin kamu sektörü BT operasyonları için varsayılan seçim olarak ortaya çıkması, mevcut ihale stratejilerinin modernleştirilmesi için fırsat sunmaktadır. Bulut odaklı satın alma süreçleri, kamu sektörü kurumlarının bir yandan verimlilikler ve maliyet tasarrufları elde ederken, diğer yandan en ileri düzey inovasyonlara erişim, daha fazla hız ve çeviklik, gelişmiş güvenlik duruşu ve uygunluk yönetimi gibi, bulutun tüm avantajlarından yararlanmasına olanak sağlamaktadır.

Donanım, yazılım ve veri merkezlerine ilişkin geleneksel BT ihale yöntemleri bulut hizmetleri satın alma için elverişsizdir. Fiyatlandırma, sözleşme yönetimi, hükümler ve koşullar, güvenlik, teknik gereklilikler, SLA'lar vb. bir bulut modelinde farklılık gösterir. Dolayısıyla mevcut ihale yöntemlerinin kullanılması, bulutun sağlayabileceği avantajları azaltır veya ortadan kaldırır.

Kamu sektörünün, bulut hizmetlerini etkili bir şekilde satın almasının en iyi yöntemlerinden biri **Bulut Çerçeve Sözleşmesi**'dir. Bulut Çerçeve Sözleşmesi kapsamında çeşitli bulut teknolojileri ve hizmetleri için birden çok ihale verilir ve alıcı kuruluşa bağlı uygun alıcılar da kendi ihtiyaçlarını karşılayan bulut teknolojilerini ve ilişkili hizmetleri satın alabilir. Bulut sözleşmelerine yönelik bir araç olarak, bu tür çerçeve sözleşmeleri, bulut hizmetlerinin verimli ve etkin bir şekilde satın alınmasını mümkün kılar. Alıcı kuruluşların ve son kullanıcıların tam kapsamlı bulut hizmetlerine erişim elde etmesini ve bulutun tüm avantajlarından yararlanmasını sağlar: çeviklik, ölçek ekonomilerinin faydaları, daha düşük maliyetle daha yüksek erişilebilirlik sağlayan ölçeklenebilirlik, geniş kapsamlı işlevler, inovasyonun hızı, ölçek artırarak yeni coğrafyalara açılma kapasitesi.

Not: Bu belge bir **Bulut Altyapısı Hizmet Sağlayıcısı (CISP)** tarafından sağlanan Hizmet Olarak Altyapı (IaaS) ve Hizmet Olarak Platform (PaaS) bulut teknolojilerinin satın alınmasına odaklanmaktadır. Bu bulut teknolojileri doğrudan bir CISP'den ya da bir CISP Satıcısı aracılığıyla satın alınabilir. *Bulut pazar yeri hizmetlerinin (PaaS ve SaaS) ve bulut danışmanlık hizmetlerinin dağıtımçıları için ek RFP hususlarının dikkate alınması gerekir.*

Ayrıca bu belgede, uçtan uca bir bulut hizmeti satın alma çerçevesi oluşturulması konusunun her yönüyle ele alınmadığını unutmayın. Sektördeki kuruluşlar ve analistler tarafından hazırlanan ve bulut hizmeti satın alma en iyi uygulamaları, bulut için bütçelendirme, bulut yönetimi vb. konuların ele alındığı diğer birçok belge bulunmaktadır. Genel bir bulut hizmeti satın alma stratejisi geliştirilirken bu tür belgelerin ve tavsiyelerin dikkate alınması şiddetle önerilir.

Aşağıda **Tablo 1**'de Bulut Hizmetleri RFP'si El Kitabı'nın ana hatları sunulmaktadır ve bulut hizmetleri RFP'sinin her bileşeni için örnek RFP metninin yer aldığı bölümler belirtilmiştir.

Tablo 1 - Bulut Hizmetleri RFP'si El Kitabı'nın Bölümleri

Bölüm	Genel Bakış ve Örnek RFP Metni
0 Bulut Çerçeve Sözleşmesine Genel Bakış	Bulut çerçeve sözleşmesi modeline genel bakış (LOT'lar, rekabet etme ve sözleşme yapma)
2.0 Bulut Hizmetleri RFP'sine Genel Bakış	Kullanılan Bulut Hizmetleri RFP yapısının ve metninin altında yatan gerekçeye ilişkin açıklamalarla birlikte aşağıdaki bölümleri kapsayan örnek genel RFP metni.
2.1 Bulut Hizmetleri RFP'sinin Oluşumu	2.1.1 Giriş ve Stratejik Hedefler 2.1.2 RFP Yanıtı Zaman Çizelgesi 2.1.3 Tanımlar 2.1.4 Satın Alma Modeline ve Çerçeve Sözleşmesi Dahilinde Rekabete İlişkin Ayrıntılı Açıklama 2.1.5 İsteklilerin Karşılması Gereken Asgari Gereklilikler - İdari
2.2 Teknik	2.2.1 Asgari Gereklilikler 2.2.2 Satıcıların Karşılaştırılması 2.2.3 Sözleşme yapma
2.3 Güvenlik	2.3.1 Asgari Gereklilikler 2.3.1.1 Veri Koruma 2.3.1.2. Bulut Sağlayıcısının Değiştirilmesi ve Verilerin Taşınması 2.3.2. Satıcıların Karşılaştırılması

Bölüm	Genel Bakış ve Örnek RFP Metni
	2.3.3 Sözleşme yapma
2.4 Fiyatlandırma	2.4.1 Asgari Gereklilikler 2.4.2 Satıcıların Karşılaştırılması
2.5 Sözleşme Yürütme Planı/Hüküm ve Koşullar	2.5.1 Hüküm ve Koşullar 2.5.2 Yazılım Hüküm ve Koşulları 2.5.3 İstekliler Arasından Seçim Yapılması 2.5.4. Katılım ve Çıkış
3.0 En İyi Uygulamalar/Çıkarılan Dersler	3.1 Bulut Yönetişimi 3.2 Bulut İçin Bütçelendirme 3.3 Çözüm Ortağı İş Modelini Anlama 3.4 Bulut Aracıları 3.5 RFP öncesinde dış kaynak kullanımı/pazar araştırması 3.6 Sürdürülebilirlik
Ek A - İstekliler Arasında Karşılaştırmayla İlgili Teknik Gereklilikler	Açık Siparişlere veya Küçük İhalelere ilişkin genel bulut teknolojisi gerekliliklerinin listesi
Ek B - Canlı Teknik Değerlendirme	Bulut teknolojisi ürünü için puanlamanın gösterildiği örnek senaryo (bir Açık Sipariş veya Küçük İhale kapsamındaki bulut gösterimleri)

1.0 Bulut Çerçeve Sözleşmesine Genel Bakış

İyi tasarlanmış bir bulut çerçeve sözleşmesi, bulut hizmetlerinin hem katılımcı kamu sektörü kuruluşları hem de bulut hizmeti satıcıları açısından avantajlı bir şekilde satın alınmasını mümkün kılabilir. İyi tasarlanmış bir bulut çerçeve sözleşmesinin avantajları aşağıdakileri içerir:

- **İş Birliğine Dayalı Yapı:**
 - Birden fazla kuruluşun benzer gereklilikler için sipariş vermek üzere bir araya gelmesi kolaylık, verimlilik, daha düşük maliyet ve basitleştirilmiş sipariş verme süreci gibi avantajları beraberinde getirir. Birden fazla kamu sektörü kuruluşunun, pazar yeri çözümleri ve danışmanlık gibi, genel bulut teknolojileri ve ilişkili bulut hizmetleri talebinin birleştirilmesi açısından etkili bir yöntem sağlar.
- **Tüm Bulut Hizmetleri Yelpazesi:**
 - CISP tarafından sağlanan bulut teknolojilerine ve pazar yeri hizmetlerine ek olarak, buluta geçişi tam anlamıyla destekleyip yürütmek ve buluttaki iş yüklerini desteklemek için gerekli tüm danışmanlık hizmetlerini ve profesyonel/yönetilen hizmetleri kapsayabilir.
 - Bulut teknolojileri doğrudan bir CISP'den ya da belirlenen bir satıcı aracılığıyla satın alınabilir.
- **Sözleşme Yönetişimi:**
 - Her bir kuruluşun/alıcının farklı hüküm, koşul ve ihalelerle satın alım yapması yerine, birden fazla kuruluşun/alıcının aynı hüküm, koşul ve ihaleyle satın alım yapmasına olanak tanır.
 - Bu, satıcının her bir kamu sektörü kuruluşu için farklı satın alma süreç, hüküm, koşul ve sipariş mekanizmaları ile uğraşmak yerine standart tek bir satın alma süreci, hükmü, koşulu ve sipariş mekanizması ile ürün ve hizmet satmasına imkan tanıdığı için satıcılar açısından da avantajlıdır.
 - Esneklik sağlar. Mevcut hükümet politikaları/düzenlemeleri dahilinde etkili bir bulut sözleşmesinin oluşturulması, onaylanması ve yürütülmesi için deneme yanılma ve hızlı değişiklik yapabilme kabiliyeti gereklidir. Kamu sektörünün ve bulut hizmeti satıcılarının hep birlikte çalışarak sözleşmeleri iyileştirmelerine olanak sağlayan bir çerçeve sözleşmesi oluşturulması hem sözleşmesel hem mekanik olarak hem de verimlilik açısından çok daha yararlıdır. İşe yaramayan ve gerekli şekilde değiştirilmesi mümkün olmayan çok yıllık bir sözleşme, kamu sektörü son kullanıcıları, satın alım yapan kuruluşlar ve bulut hizmeti satıcıları açısından kötü bir deneyimle sonuçlanır.
- **Seçim:**
 - Alıcıların yeterliliğe sahip birçok CISP arasından seçim yapmasına olanak tanır ve tüm bulut hizmetlerinin yanı sıra bulut PaaS/SaaS pazar yeri ve bulut danışmanlığı gibi ilişkili hizmetler için çitayı yüksek tutar.
 - Her bir isteklinin uygun standartları karşılayıp karşılamadığının incelenmesi suretiyle çerçevedeki tedarikçi sayısı üzerinde kontrol olanağı sağlar.

Bulut hizmetleri satın almaya ilişkin bir çerçeve sözleşmesinin en çok yararlı olacağı başlıca senaryo, çerçeve sözleşmesinin bir PaaS/SaaS pazar yeri ile birlikte CISP tarafından sağlanan temel IaaS/PaaS teknolojilerini ve gerektiğinde kamu sektörü son kullanıcılarının bulutta çalışan bir iş yükünü planlamasına, taşımasına,

kullanmasına ve sürdürmesine yardımcı olması için erişebileceği danışmanlık hizmetlerini kapsadığı durumlardır. Dolayısıyla, bir Bulut Çerçeve Sözleşmesi oluşturmak için kullanılacak Bulut Hizmetleri RFP'sinin aşağıdaki gibi 3 lota ayrılması önerilir:

• **LOT 1 - BULUT TEKNOLOJİLERİ**

Doğrudan bir CISP'den ya da belirlenen bir CISP Satıcısı aracılığıyla satın alınan bulut teknolojileri.

• **LOT 2 - PAZAR YERİ**

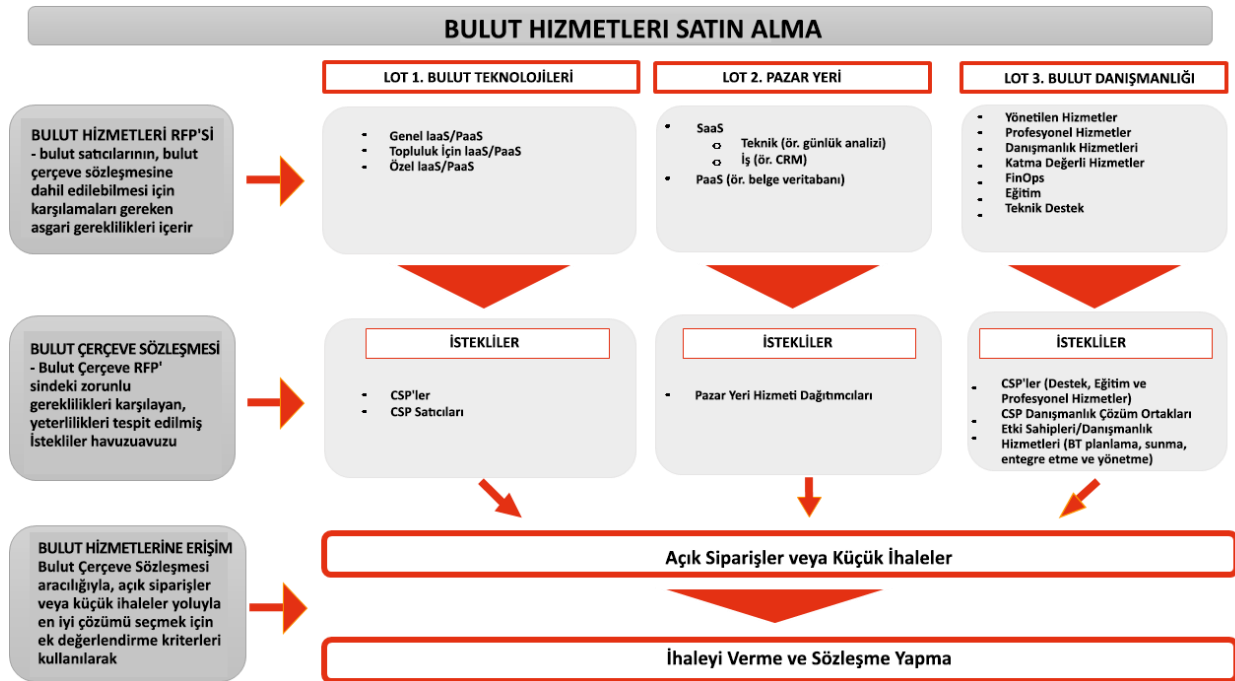
PaaS ve SaaS hizmetlerinden oluşan bir pazar yerine erişim.

• **LOT 3 - BULUT DANIŞMANLIĞI**

Bulutla ilgili danışmanlık hizmetleri (eğitim, profesyonel hizmetler, yönetilen hizmetler vb.) ve teknik destek.

Daha önce de belirtildiği gibi, bu belge bir CISP tarafından sağlanan (doğrudan bir CISP'den veya bir CISP Satıcısı aracılığıyla satın alınan) IaaS ve PaaS bulut teknolojilerinin (LOT 1) satın alınmasına odaklanmaktadır. Bir bulut hizmetleri RFP'sinin LOT 2 ve 3 kapsamına giren satıcılar için ayrı satıcı yeterlilik gerekliliklerine ihtiyaç duyulur.

Aşağıda **Şekil 1**'de, üç lota bölünen iyi yapılandırılmış bir Bulut Hizmetleri RFP'sinin, kamu sektörü kuruluşlarına çeviklik (hem teknik açıdan hem de sözleşme açısından), harcama ve bulut kullanımı üzerinde görünürlük ve kontrol olanağı sunacak ve ayrıca ihtiyaç duydukları çözümleri geliştirmek ve sürdürmek için gerekli tüm bulut hizmetlerine sahip olma imkanını verecek bir Bulut Çerçeve Sözleşmesi elde edilmesini nasıl sağlayabileceğine ilişkin bir genel bakış sunulmaktadır.



Şekil 1 - Başarılı bir Bulut Hizmetleri RFP'si 3 lota ayrılır. Her lot, Bulut Çerçeve Sözleşmesi kapsamında satın alım yapılırken son kullanıcı gerekliliklerini karşılamak amacıyla teknik ve sözleşmeden doğan uygunluğun sağlanması için farklı kategoriler veya teklif türleri içerir.

Aşağıdaki hususlara dikkat edin:

- Her lotta, ihaleyi birden çok istekli alır.
- LOT 3 başka bir RFP aracılığıyla ya da muhtemelen danışmanlık hizmetleri için zaten var olan bir sözleşme yoluyla isteklilere verilebilir.

LOT 1 Kategorileri

Başarılı bir Bulut Çerçeve Sözleşmesi, CISP'lerden her lot altında kategorilere ayrılmış şekilde, teklif ettikleri bulut modelini açıklamalarını ister. **Genel Bulut**, **Topluluk Bulutu** ve **Özel Bulut** kavramlarının tanımları için bulut bilgi işleme ilişkin sektör standardının ([Ulusal Standartlar ve Teknoloji Enstitüsü \(NIST\) Temel Bulut Özellikleri](#)) kullanılmasını öneriyoruz. Bulut çerçeve sözleşmesinin bu şekilde yapılandırılması, bu çerçeveyi kullanan satın alma kurumunun ve kamu kurumlarının kendi ihtiyaçlarına en uygun şekilde çeşitli bulut modelleri arasından seçim yapmasına olanak sağlar.

LOT 1'deki her bulut modelinin NIST tanımı için bkz. *Bölüm 2.1.3 Tanımlar* (Kamu için IaaS/PaaS, Topluluk için IaaS/PaaS ve Özel IaaS/PaaS).

Rekabet Şekli - Açık Siparişler mi, Küçük İhaleler mi?

Bir Bulut Hizmetleri RFP'sine ilişkin yeterlilik kriterleri kritik unsurları ve asgari standartları içermeli, "olsa iyi olurdu" denilebilecek standartlar içermemelidir. Çerçeveye uygunluğu kabul edilen satıcılar için başlangıç seviyesinin üzerine ilave standartlar eklenmesi, bazı satıcıların teklif yapamamasına yol açabilir ve dolayısıyla alıcıların daha az seçeneğe sahip olmasına neden olabilir.

RFP'den ve bunu müteakiben Bulut Çerçeve Sözleşmesi'nin oluşturulmasından sonra çerçeve sözleşmesine taraf olan kamu sektörü kuruluşları, ihtiyaç duydukları bulut hizmetlerini gerek olduğunda sipariş edebilir veya bunlar için "açık sipariş" verebilir. Bir çerçeve sözleşmesine bir açık sipariş sözleşmesinin dahil edilmesi, alıcıların bir yandan açık sipariş sözleşmesi için ek fonksiyonel şartname ile gereklilikleri düzeltmesine, diğer yandan çerçeve sözleşmesi altında sunulan avantajlarını elinde tutmasına olanak sağlar.

Gerekli görülmesi halinde, belirli bir iş yüküne veya projeye en uygun tedarikçiyi belirlemek için küçük bir ihale düzenlenebilir. Küçük ihalede, müşteri bir lot içindeki tüm tedarikçileri bir dizi gerekliliğe yanıt vermeye davet ederek çerçeve sözleşmesi kapsamında ek rekabet sağlayabilir. Müşteri, lot içindeki yeterliliğe sahip tüm tedarikçileri teklif vermeye davet eder ve böylece her lot altında yüksek standartta seçenekler elde edilir. Bir Bulut Hizmetleri RFP'sinde isteklilere ilişkin asgari gerekliliklerin önemi de burada yatmaktadır.

Yukarıda Şekil 1'de listelendiği gibi, lotlardan her biri için farklı sözleşme hüküm ve koşul setleri bulunmasının önemli olduğunu unutmayın. Tüm lotlarda sözleşme yapımı için "ortak" bir yaklaşım izlenmesi teknik fizibilite ve uyumluluk açısından sorunlara yol açacaktır.

2.0 Bulut Hizmetleri RFP'sine Genel Bakış

Bu bölümde, stratejik hedefler, katılımcılar, tanımlar, zaman çizelgesi ve idari asgari gereklilikler dahil olmak üzere Bulut Hizmetleri RFP modeli ve kapsamı açıklanmaktadır. Daha önce de belirtildiği gibi, bu el kitabının **LOT 1 - BULUT TEKNOLOJİLERİ**'ne odaklandığını lütfen unutmayın.

2.1 Bulut Hizmetleri RFP'sinin Oluşumu

Kamu sektörü kuruluşlarının, genel hedeflerini ve gerekliliklerini Bulut Hizmetleri RFP'sinin Giriş bölümünde net olarak tanımlamaları şiddetle önerilir.

2.1.1 Giriş ve Stratejik Hedefler

Stratejik hedeflerin net olarak ortaya konulmasını sağlamaya yönelik iyi bir uygulama olarak Bulut Hizmetleri RFP'sinin Giriş bölümünde şu hususlar tanımlanmalıdır: **(1)** kuruluşun bulutu kullanarak elde etmeyi umduğu iş hedefleri ve avantajlar; **(2)** çerçeve sözleşmesinin yapısı: satın alımı yapan taraf, işletecek olan taraf, bütçeyi hazırlayan taraf vb.; **(3)** başarılı bir bulut hizmeti satın alma ve kullanma açısından büyük önem taşıyan kamu sektörü ile bulut hizmeti satıcıları arasındaki paylaşılan sorumluluk modelinin net olarak tanımlanması ve **(4)** Bulut Hizmet Sağlayıcıları (CISP'ler), pazar yeri hizmeti dağıtımcıları, danışmanlık ortakları, devlet ihale kuruluşları/sözleşmeciler kuruluşları ve devlet son kullanıcıları arasında oluşturulan ilişkinin türü. Bu dört hususun ifade edilmesi, kuruluşların ihtiyaçlarını en iyi şekilde karşılayacak bir RFP hazırlamalarına yardımcı olur ve hem müşterilerin hem de satıcıların, RFP çıktılarına dair net bilgi sahibi olmasını sağlar.

Bulut RFP'si, amacı açısından geleneksel BT RFP'lerinden farklıdır. Bulut teknolojisi geleneksel bilgi işlem yöntemleriyle bire bir örtüşmez. Teknolojinin tüketimine ilişkin tamamen yeni bir yöntem sunmaktadır. İyi tasarlanmış Bulut Hizmetleri RFP'leri, kamu sektörü kuruluşlarının buluttan yararlanabilmek için hızla hareket etmelerine yardımcı olabilir.

Bulut hizmetleri satın almaya ilişkin tüm iyi uygulamalar arasından, paylaşılan sorumluluk modelinin net olarak anlaşılması muhtemelen en iyi başlangıç noktasıdır. Paylaşılan sorumluluk modeli¹ çoğunlukla bulutta güvenlik ve uygunluk ele alınırken kullanılır fakat bu sorumluluk tanımı bulut teknolojilerinin her alanı için geçerlidir. Bulut Hizmetleri RFP'si, CISP'nin bulut ortamındaki sorumluluklarını ve müşteri sorumluluğunda kalacak unsurları net olarak tanımlamalıdır. Örneğin CISP, bulutta çalışan kaynakları ve uygulamaları izleme yeteneği sağlar **fakat** CISP tarafından sağlanan bu tür yeteneklerin fiili olarak kullanılmasından müşteri sorumludur. Zira devasa ölçekte faaliyet gösteren bir CISP, milyonlarca müşteri için bu görevi yerine getirecek şekilde tasarlanmamıştır.

Ayrıca bulut müşterileri bir CISP'nin Çözüm Ortağı Ağı'nın, müşterilerin bulutu kullanmasına ve sorumluluklarını yönetmesine nasıl yardımcı olacağını anlamalıdır. Örneğin bulut Yönetilen Hizmet Sağlayıcıları (MSP) bir müşterinin benzersiz uygunluk ve denetim gerekliliklerini karşılamak için CISP tarafından sağlanan izleme yeteneklerini yapılandırıp kullanmasına yardımcı olabilir.

Basitçe ifade etmek gerekirse bulut modelindeki sorumluluklar aşağıdaki gibidir:

¹ CISPE Bulut Altyapısı Hizmet Sağlayıcıları İçin Davranış Kuralları, Bölüm 5'e bakın: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

CISP, bulut teknolojisini sağlar.

Müşteri, bulut teknolojisini kullanır.

Danışmanlık firmaları (varsa) müşterinin bulut teknolojisine erişmesine ve onu kullanmasına yardımcı olur.

"Danışmanlık firmaları" müşterilerin iş yüklerini ve uygulamalarını bulutta tasarlamasına, mimarisini planlamasına, geliştirmesine, yönetmesine ve buluta taşımasına yardımcı olan danışmanlık ve yönetilen/profesyonel hizmet firmalarıdır. Bu tür firmalar arasında Sistem Entegratörleri, Stratejik Danışmanlıklar, Acenteler, Yönetilen Hizmet Sağlayıcıları ve Katma Değer Sunan Satıcılar ver alır.

Bulut hizmetleri için alışveriş yapmak bir yapı markette alışveriş yapmaya benzetilebilir. Yapı marketlerde, ihtiyaç duyduğunuz şeyi inşa etmek için gerekli çok çeşitli malzeme ve aletleri bulabilirsiniz. Bir dolap, yüzme havuzu ya da baştan aşağıya bir ev yapabilirsiniz. Seçim sizin. Malzemeleri ve aletleri satın alırken yapı market personeli size rehberlik edip uzmanlık sağlayabilir fakat evinize kadar gelip inşa etmek istediğiniz şeyi yapmanıza yardımcı olmaz. Bu nedenle, birkaç seçeneğiniz bulunur:

1. Malzeme ve aletleri kendiniz satın alıp istediğiniz şeyi kendiniz inşa edebilirsiniz.
2. Malzeme ve aletleri kendiniz satın alıp istediğiniz şeyi inşa etmesi veya işletmesi için birini tutabilirsiniz.
3. İsteddiğiniz şeyi inşa etmesi/işletmesi için birini tutabilir ve gerekli tüm malzeme ve aletleri kişinin genel teklifine dahil olacak şekilde kendisinin tedarik etmesini isteyebilirsiniz.

Bir kuruluş kendi bulut ortamını ve çözümlerini kendi başına oluşturmak ve yönetmek için gerekli dahili becerilere sahipse yalnızca CISP tarafından sağlanan (doğrudan bir CISP'den ya da bir CISP Satıcısı aracılığıyla, bkz. **LOT 1**) standart bulut teknolojilerine ve araçlarına erişmesi yeterli olacaktır. Gerekli SaaS ve PaaS yazılımı bulut pazar yerinden temin edilebilecektir (**LOT 2**). Ek danışmanlık, taşıma, uygulama ve/veya yönetim alanlarında yardım gerekiyorsa işte bu noktada bir CISP'nin Çözüm Ortağı Ağı devreye girer (**LOT 3**).

Örnek RFP Metni: Giriş ve Stratejik Hedefler

Bulut bilgi işlem, kamu sektörü kuruluşlarına çok çeşitli esnek, düşük maliyetli, "kullandıkça öde" yöntemiyle ücretlendirilen BT kaynaklarına hızlı erişim imkanı vermektedir. Kuruluşlar yeni parlak fikirlerini hayata geçirmek ya da BT departmanlarını işletmek için ihtiyaç duydukları kaynakları doğru türde ve doğru boyutta temin edebilme imkanına kavuşarak, yüksek miktarda donanım yatırımı yapma ve/veya uzun süreli yazılım lisanslama sözleşmelerine duyulan ihtiyacı ortadan kaldırmaktadır.

<KURULUŞ>, çok çeşitli bağlı kuruluşlar genelinde iş ihtiyaçlarını karşılamak için Piyasada Mevcut Bulut Teknolojilerinin bu türlerine erişime gerek duymaktadır.

Bu RFP'nin ana amacı, farklı bulut teknolojilerini ve bulutla ilgili hizmetleri temsil eden en fazla <x> sağlayıcı ile münhasır olmayan bir paralel <ÇERÇEVE SÖZLEŞMESİ> akdetmektir.

1. **LOT 1.** Bulut Teknolojilerinin satın alımı için Bulut Hizmet Sağlayıcıları (CISP'ler) veya CISP Satıcıları
2. **LOT 2.** Pazar yeri hizmeti sağlayıcıları

3. **LOT 3.** Bu CISP tekliflerine geçiş yapmak ve bu teklifleri kullanabilmek için gerekli ek uzmanlığın sağlanması amacıyla Danışmanlık hizmeti sağlayıcıları

LOT 1 ile ilgili olarak, teklif veren kuruluşlar (CISP'ler veya CISP satıcıları) tekliflerinin aşağıdaki hedeflere nasıl ulaşacağını göstermelidir:

- **Çeviklik:** geleneksel yöntemlerle haftalar ve aylar süren zaman çizelgeleri yerine BT kaynaklarını dakikalar içinde son kullanıcıların kullanımına sunma.
- **İnovasyon:** piyasadaki en yeni ve en inovatif teknolojilere anında erişebilme.
- **Maliyet:** sermaye gideri yerine değişken gidere geçiş yapma (ör. CapEx'ten OpEx'e geçiş) ve yalnızca tüketim miktarı kadar ödeme yapma.
- **Bütçeleme:** faturalama ve kullanım bilgilerini hem ayrıntılı hem de özet görünümlemlerle görüntüleme, zaman içinde harcamada gözlemlenen modelleri görselleştirme ve gelecekteki harcamaları tahmin etme.
- **Esneklik:** bulutun sağladığı daha gelişmiş ölçek ekonomileri sayesinde daha düşük değişken maliyetler elde etme.
- **Kapasite:** altyapı kapasite ihtiyaçlarına ilişkin tahminlerde bulunma ihtiyacını ortadan kaldırma.
- **Veri Merkezlerine Bel Bağlamaya Son Verme:** sunucuları raflara yerleştirme, yığınlara ekleme ve çalıştırma yükünden kurtulup vatandaşların işlerine odaklanma fırsatını yakalama.
- **Güvenlik:** kaynaklara ilişkin daha fazla görünürlük ve denetlenebilirlik yoluyla hesap tasarısını resmileştirme, tesisleri ve fiziksel donanımları koruma maliyetlerini ortadan kaldırma.
- **Paylaşılan Sorumluluk:** ana sunucu işletim sisteminden ve sanallaştırma katmanından sunucuların çalıştığı tesislerin fiziksel güvenliğine kadar tüm bileşenlerin CISP tarafından işletilmesi, yönetilmesi ve kontrol edilmesi sayesinde operasyonel yüklerden kurtulma.
- **Otomasyon:** güvenli bir şekilde ölçeklendirme yeteneğini daha hızlı ve uygun maliyetli olarak geliştirmek için otomasyonu bulut mimarisine entegre etme.
- **Bulut Yönetişimi:** varlık takibi, envanter yönetimi, değişiklik yönetimi, günlük yönetimi ve analizi ile genel görünürlük ve bulut yönetişimi özellikleriyle (1) tüm BT varlıklarının tam envanterini çıkararak işe başlama; (2) bu varlıkların tamamını merkezi olarak yönetme ve (3) kullanım/faturalama/güvenlik vb. ile ilgili uyarılar oluşturma.
- **Kontrol:** BT hizmetlerinin nasıl kullanıldığına ve güvenlik, güvenilirlik, performans ve maliyet iyileştirmeleri yapılabilecek noktalara ilişkin tam görünürlük elde etme.
- **Tersine Çevrilebilirlik:** CISP altyapısına/altyapısından geçiş yapmayı kolaylaştırarak belirli bir satıcıya bağımlılığı en aza indiren ve sektör Davranış Kurallarına uygunluğun sağlanmasına yardımcı olan taşınabilirlik araç ve hizmetleri.
- **Veri Koruma:** bulut altyapısı hizmetlerine özel sektör davranış kuralları olan CISPE Veri Koruma Davranış Kuralları aracılığıyla Genel Veri Koruma Yönetmeliği'ne (GDPR) uygunluğu gösterme yeteneğini elde etme.
- **Şeffaflık:** Müşteriler verilerini işlemek ve depolamak için kullanılan altyapıların konumunu (şehir alanını) bilme hakkına sahip olmalıdır.
- **İklim Nötrlüğü:** Müşteriler, iklim nötrlüğü hedeflerine 2030'a kadar ulaşmak için kanıtlanmış, belirli adımlar atan ve İklim Nötr Veri Merkezi Paketi'nde imzası bulunan CISP'lerle etkileşim kurabiliyor olmalıdır. Bu, müşterilerin kendi iklim nötrlük hedeflerine ulaşmasına yardımcı olacaktır.

2.1.2 RFP Yanıtı Zaman Çizelgesi

Bir bulut çerçeve sözleşmesi ve ilişkili Bulut Hizmetleri RFP'si oluşturulurken iyi bir uygulama olarak, öngörülen teklif verme faaliyetinin zaman çizelgesi isteklilere sağlanmalıdır. Sektörle ne kadar fazla etkileşim kurulursa o kadar iyidir. Bu tür etkileşimler, tüm tarafların RFP gerekliliklerini ve tüm satıcı hizmetlerinin bulut hizmetleri modelinde nasıl konumlanacağını net olarak anladığından emin olunmasına yardımcı olur.

RFP zaman çizelgesinin yerel yasalara ve yasal yükümlülüklerle tabi olduğunu unutmayın. Aşağıdaki liste, faaliyetlerin ve zaman çerçevelerinin kuralcı bir listesi olmak yerine, bir en iyi uygulama kılavuzu olarak hazırlanmıştır.

Örnek RFP Metni: Yanıt Zaman Çizelgesi

Bulut Hizmetleri RFP'si için aşağıdaki RFP zaman çizelgesine bakın:

Bulut Hizmetleri RFP Zaman Çizelgesi
- Bilgi Talebinin (RFI) Sunulması: - RFI Yanıtı: - Taslak Teklif Talebinin (RFP) Sunulması: - Taslak RFP Yanıt Son Tarihi: - Sektör İstişaresi Aşaması: <zaman çizelgeleri> - Ön Yeterlilik RFP'sinin Sunulması: - Ön Yeterlilik RFP'si Yanıtı: - RFP'nin Sunulması: 1. Tur Bekleyen Sorular: 1. Tur Cevaplar: 2. Tur Bekleyen Sorular: 2. Tur Cevaplar: - RFP Yanıt Son Tarihi: - Teklif Netleştirme Dönemi: - Müzakere Dönemi: - İstekliye Bırakma Niyetinin Tarihi: - İhalenin Bırakılması: - Sözleşme Süresi (Uzatma Seçenekleri):

RFP zaman çizelgesinin yerel yasalara ve yasal yükümlülüklerle tabi olduğunu unutmayın. Aşağıdaki liste, faaliyetlerin ve zaman çerçevelerinin kuralcı bir listesi olmak yerine, bir en iyi uygulama kılavuzu olarak hazırlanmıştır.

2.1.3 Tanımlar

Bulut Hizmetleri RFP'si, tanımların ayrıntılı bir listesini içermelidir. Bu liste satıcı rollerini (ör. bulut hizmeti sağlayıcısı, bulut hizmeti satıcısı, satıcı çözüm ortağı), genel teknoloji kavramlarını (bilgi işlem, depolama, IaaS/PaaS, SaaS) ve sözleşmenin diğer önemli parçalarını içerir. Aşağıda bir örnek tanım listesi verilmiştir:

Örnek RFP Metni: Tanımlar

Aşağıdaki tanımlar, bulut bilgi işlem terimleri için Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından hazırlanmıştır.²

- **Hizmet Olarak Altyapı (IaaS).** Tüketicie sağlanan olanak, tüketicinin işletim sistemleri ve uygulamalar dahil olmak üzere istediği yazılımları dağıtıp çalıştırabileceği işleme, depolama, ağ ve diğer temel bilgi işlem kaynaklarının tedarik edilmesidir. Tüketici temel bulut altyapısını yönetmez veya kontrol etmez ancak işletim sistemleri, depolama ve dağıtılmış uygulamalar üzerinde kontrole sahip olur. Muhtemelen, seçili ağ iletişimi bileşenleri (ör. ana sunucu güvenlik duvarları) üzerinde de sınırlı kontrole sahip olur.
- **Hizmet Olarak Platform (PaaS).** Tüketicie sunulan olanak, sağlayıcı tarafından desteklenen programlama dilleri, kitaplıkları, hizmetleri ve araçları kullanılarak tüketici tarafından oluşturulan veya satın alınan uygulamaları bulut altyapısına dağıtmaktır.³ Tüketici; ağlar, sunucular, işletim sistemleri ve depolama dahil olmak üzere temel bulut altyapısını yönetmez veya kontrol etmez ancak dağıtılan uygulamalar üzerinde ve ayrıca muhtemelen uygulama barındırma ortamının yapılandırma ayarları üzerinde kontrole sahip olur.
- **Hizmet Olarak Yazılım (SaaS).** Tüketicie sağlanan olanak, bir bulut altyapısı üzerinde çalışan sağlayıcının uygulamalarını kullanmaktır. Uygulamalara web tarayıcısı gibi bir ince istemci arabirimi (ör. web tabanlı e-posta) veya bir program arabirimi yoluyla çeşitli istemci cihazlardan erişilebilir. Tüketici, muhtemelen sınırlı kullanıcıya özel uygulama yapılandırma ayarları hariç olmak üzere ağlar, sunucular, işletim sistemleri, depolama veya hatta ayrı ayrı uygulama özelliklerini yönetmez veya kontrol etmez.
- **Genel bulut.** Bulut altyapısı genel halkın açık kullanımı için tedarik edilir. Bir işletme, akademik kuruluş, devlet kuruluşu veya bunların herhangi bir birleşimi tarafından yönetilebilir, işletilebilir veya bunlara ait olabilir. Bulut sağlayıcısının tesislerinde barındırılır.
- **Topluluk bulutu.** Bulut altyapısı ortak görev, amaç veya kaygıları (ör. görev, güvenlik gereklilikleri, politika ve uygunluk gereklilikleri) bulunan kuruluşlar bünyesindeki belirli bir tüketici topluluğunun münhasır kullanımı için tedarik edilir. Bulut altyapısı topluluktaki bir veya daha fazla kuruluş, bir üçüncü taraf veya bunların herhangi bir birleşimi tarafından yönetilebilir, işletilebilir veya bunlara ait olabilir ve sağlayıcının tesislerinde ya da başka bir yerde barındırılabilir.
- **Hibrit bulut.** Bulut altyapısı, veri ve uygulama taşınabilirliğine imkan veren standart veya müseccel teknoloji (ör. bulutlar arasında yük dengeleme için bulutta ani işlem artışı) ile birbirine bağlanan fakat benzersiz varlıklar olarak varlığını sürdüren iki veya daha fazla farklı bulut altyapısının (özel, topluluk veya genel) bir birleşimidir.
- **Özel bulut.** Bulut altyapısı birden çok tüketiciden (ör. iş birimleri) oluşan tek bir kuruluşun münhasır kullanımı için tedarik edilir. Bulut altyapısı söz konusu kuruluş, bir üçüncü taraf veya bunların herhangi bir birleşimi tarafından yönetilebilir, işletilebilir veya bunlara ait olabilir ve şirket içinde ya da şirket dışında barındırılabilir.

2.1.4 Satın Alma Modeline ve Çerçeve Sözleşmesi Dahilinde Rekabete İlişkin Ayrıntılı Açıklama

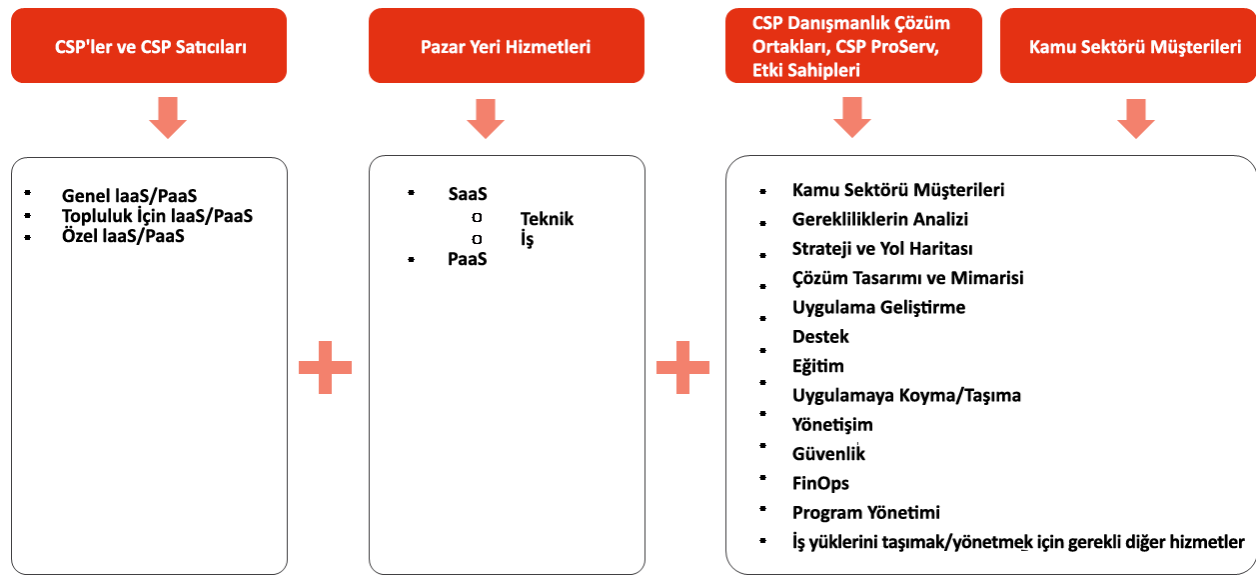
Yukarıda belirtildiği gibi, kamu sektörü kuruluşları bir çerçeve sözleşmesinin bulut teknolojilerine ve ilgili uygulama ve yönetim hizmetlerine yönelik bir satın alma mekanizması olarak nasıl kullanılacağını belirleyen modeli tanımlamalıdır. Bulut teknolojisi satıcılarının, ilgili danışmanlık hizmeti kuruluşlarının, pazar yeri dağıtıcılarının ve alıcı kurumların kendi özel rollerini anlayabilmeleri için bu model, Bulut Hizmetleri RFP'sinde net olarak tanımlanmalıdır.

² <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

Kuruluşlar, çerçeve sözleşmesinin ve bunu takip eden açık siparişlerin veya küçük ihalelerin kapsamına ilişkin olarak aşağıdaki hususları göz önünde bulundurmalıdır:

- Sözleşme kapsamındaki bulut teknolojilerinin kullanımını içeren entegrasyon ve yönetilen hizmetlerden kim sorumlu olacak?
- CISP Satıcısının/Çözüm Ortağının CISP ile bir sözleşmesel ilişkiyi sürdürmek, birleştirilmiş faturalama hizmetleri sağlamak ve bulut sağlayıcısı hizmetlerinin kullanımıyla ilişkili kullanım ve faturalama verilerine zamanında ve doğrudan erişim sağlamak dışında katma değerli hizmetler sunmasını öngören bir gereklilik var mı?
- Tam hizmet sağlayan ve katma değer sunan bir satıcı, sistem entegratörü ya da yönetilen hizmet sağlayıcısı veya herhangi bir biçimde BT iş gücü hizmeti gerekiyor mu?

CISP'nin Sistem Entegratörü (SI) veya Yönetilen Hizmet Sağlayıcısı (MSP) olmadığına bilinmesi önemlidir. Birçok kamu sektörü müşterisi IaaS/PaaS'leri için bir CISP'ye gerek duyar ve danışmanlık, "klavye başında" planlama, taşıma ve yönetim işlerini dış kaynak olarak bir SI veya MSP'ye devreder. Şekil 2'de, bir bulut hizmetleri modelinde rol ve sorumluluklarının nasıl ayrıldığı gösterilmektedir.



Şekil 2 - Bir Bulut Hizmetleri RFP'si son kullanıcılara ihtiyaç duydukları tüm bulut hizmetlerini kapsayan bir menü sunmalıdır. Kamu sektörü müşterileri bulut teknolojileri için bir CISP'ye ve gerekirse PaaS ve SaaS ürünleri için bir pazar yerine ihtiyaç duyacaktır. Müşteriler daha sonra bulut hizmetlerinin sunumunda ne kadar büyük bir rol almak istediklerine ve sorumluluklarını yerine getirmek için işlerinin ne kadar büyük bir kısmını dış kaynak olarak bir Danışmanlık Firmasına/Sistem Entegratörüne/Yönetilen Hizmet Sağlayıcısına vb. devretmek istediklerine karar verebilir.

Aşağıdaki örnek metin, yukarıda Şekil 2'de gösterilen rol ve sorumluluklar temelinde hazırlanmıştır. Bir Bulut Çerçeve Sözleşmesi ve ilişkili Bulut Hizmetleri RFP'si, alıcılara her bir satıcının teklifini yeterli bir şekilde değerlendirme olanağını sağlamalı, iş yükü/proje için ihtiyaç duyulan hizmetler arasından seçim yapma imkanını vermelidir. Bunu sağlamanın en iyi yolu, daha önce de belirtildiği gibi hizmetleri lotlara ayırmak ve açık siparişlerin ve küçük ihalelerin çerçeve sözleşmesi kapsamında nasıl yürütüleceğini net olarak tanımlamaktır.

Örnek RFP Metni: Satın Alma Modeli

Bu Sözleşme bir **Çerçeve** satın alma aracı görevi görecektir. Bu bulut Çerçeve Sözleşmesi, **<KURULUŞ>** tarafından tanımlanan Bulut Teknolojileri ve ilgili pazar yeri hizmetleri/ürünleri, danışmanlık hizmetleri, profesyonel hizmet/sistem entegrasyonu/yönetilen hizmet/profesyonel taşıma hizmetleri, eğitim ve destek için **<KURULUŞ>** tarafından tanımlanan birden çok **lot** içerecek ve **<KURULUŞ>** bağlı birden fazla uygun alıcı tarafından kullanılacaktır. Bu sözleşme, ihale sürecini basitleştirmenin yanı sıra ölçek ekonomilerinin optimize edilmesini sağlayacaktır.

Bu çerçeve sözleşmesi bir kuruluşun istediği belirli bulut teknolojilerini ve bulutla ilgili hizmetleri, ayrı ayrı ihaleler düzenlemek suretiyle satın almak yerine, ihtiyaç duyduğu zaman satın almasına olanak sağlayacaktır. Bu yaklaşım, idari gereklilikleri azaltmanın yanı sıra ihale karmaşıklığını ve döngü süresini önemli ölçüde azaltacaktır.

Çerçeve Sözleşmesi'nin süresi, tüm yenileme dönemleri dahil olmak üzere **<X>** yıldır. Bir Çerçeve açık sipariş sözleşmesinin maksimum uzunluğu normal şartlarda **<X>** aydır ancak sözleşmeyi uzatmak için gerekli olması halinde dahili onaylar alınmak suretiyle, bu süre **<X>** ay ve daha sonra ilave **<X>** ay uzatılabilir. Bu durum, her bir özel **Açık Siparişte** belirtilecektir.

ÇERÇEVE 3 (üç) lota bölünmüştür.

1. **LOT 1: BULUT TEKNOLOJİLERİ:** bulut sağlayıcı teknolojilerinin tam kapsamı (doğrudan CISP'den, Satıcıdan ya da katma değerli hizmetler/destek sağlayan bir Satıcıdan).
 - i. **IaaS ve PaaS hizmetleri:** çeşitli bulut teknolojilerini (ör. bilgi işlem, depolama, ağ iletişimi, veritabanı, analiz, uygulama hizmetleri, dağıtım, yönetim, geliştirici, Nesnelerin İnterneti (IoT) vb.) içeren bir menü. DR/COOP, Arşiv, Büyük Veri ve Analiz, DevOps vb. paketlenmiş bulut teknolojisi çözümlerini de kapsar.
2. **LOT 2: PAZAR YERİ:** Muhasebe, CRM, Tasarım, İK, GIS ve Eşleme, HPC, BI, İçerik Yönetimi, günlük analizi vb. PaaS ve SaaS hizmet/ürünlerinin tam kapsamı.
3. **LOT 3: BULUT DANIŞMANLIĞI:** buluta taşıma ve kullanım ile ilgili danışmanlık hizmetlerinin tam kapsamı (yönetilen hizmetler, profesyonel hizmetler, müşavirlik/danışmanlık hizmetleri, katma değerli hizmetler, FinOps, teknik destek). Bu hizmetler şunları içerebilir: Planlama, Tasarım, Taşıma, Yönetim, Destek, Kalite Güvencesi, Güvenlik, Eğitim vb.

Satıcılar birden fazla lot için teklif verebilir.

Satıcılar tekliflerini ve ilgili fiyatlandırmaları kendi seçtikleri formatta sunabilir.

ÇERÇEVE DAHİLİNDE REKABET VE SÖZLEŞME YAPILMASI**AÇIK SİPARİŞLER**

Çerçeve sözleşmesine taraf olan kamu sektörü kurumları, ihtiyaç duydukları hizmetleri istedikleri zaman sipariş edebilir veya bunlar için "açık sipariş" verebilir. Çerçeve sözleşmesine bir açık sipariş sözleşmesinin dahil edilmesi, alıcıların bir yandan açık sipariş sözleşmesi için ek fonksiyonel şartname ile gereklilikleri düzeltmesine, diğer yandan çerçeve sözleşmesi altında sunulan avantajları elinde tutmasına olanak sağlar.

Çerçeve sözleşmesi yoluyla verilen sözleşmeler, her lotta tedarikçiyi seçmek için kullanılan gereklilikler açısından net bir denetim kaydının gösterilmesini sağlayacaktır. Son alıcılar, potansiyel satıcılarla yapılan tüm ön görüşmeler, netleştirme amacıyla sorulan sorular, e-postalar ve yüz yüze görüşmeler dahil satıcılarla kurulan iletişimlerin kaydını tutacaktır.

1. AÇIK SİPARİŞ GEREKLİLİKLERİNİN YAZILMASI VE DAHİLİ SATIN ALMA ONAYININ ALINMASI

Çerçeve Sözleşmesi'ni kullanma hakkına sahip tüm son alıcılar, "mutlak gereklilikler" ve "isteklerden" oluşan gereklilikler listesini hazırlamak üzere işletme son kullanıcıları, satın alma uzmanları ve teknik uzmanlardan oluşan ortak ekipler kuracaktır. Bu gereklilikler hangi lotlar kapsamında çalışılması gerektiğinin ve gereklilikleri karşılamaya en uygun yeterlilikteki satıcının belirlenmesine yardımcı olur. Alıcılar gereklilikleri yazarken aşağıdakileri göz önünde bulundurmalıdır:

- hizmeti kullanmak için mevcut fonlar
- projenin teknik ve ihale gereklilikleri
- seçim için temel alınacak kriterler

2. HİZMETLERİN ARANMASI

Çerçeve Sözleşmesi'ne taraf alıcılar, tanımlanan ihtiyaçlarını karşılayan ürün/hizmetleri bulmak için bir çevrimiçi Çerçeve Kataloğu (Uygun Yeterliliklere Sahip Çerçeve Sözleşmesi İsteklilerinin ve sundukları hizmetlerin listeleneceği bir portaldır) kullanacaktır. Uygun lotları seçecek ve ardından hizmetleri arayacaklardır.

3. HİZMETLERİN İNCELENMESİ VE DEĞERLENDİRİLMESİ

Çerçeve Sözleşmesi'ne taraf olan alıcılar, hizmet açıklamalarını inceleyerek hem gereklilikler hem de bütçe doğrultusunda ihtiyaçlarını en iyi karşılayan hizmetleri tespit edecektir. Her hizmet açıklaması aşağıdakileri içermelidir:

- Hizmet tanımı belgesi veya hizmet tanımlarına ilişkin bağlantılar
- Hüküm ve koşullar belgesi
- Fiyatlandırma belgesi (tam fiyat listesinin/fiyat belgesinin talep üzerine temin edilebilir olacağı varsayımıyla halka açık fiyatlandırmaya ilişkin bağlantılar kabul edilebilir)

Fiyat, hizmetin en yaygın yapılandırmasının maliyeti olacaktır. Bununla birlikte, fiyatlandırma normalde hacme dayalıdır. Dolayısıyla, alıcılar satın alınan hizmetlerin gerçek fiyatını ve alıcıya sağlanacak toplam değeri (örneğin optimizasyon hizmetleri ve sonuç olarak ortaya çıkacak maliyet azalması) belirlemek için her zaman tedarikçinin fiyatlandırma belgesine veya genel erişime açık fiyatlandırmasına ve fiyat hesaplama araçlarına başvurmalıdır.

Çerçeve Sözleşmesi'ne taraf olan alıcılar, hizmet açıklamalarını, hüküm ve koşullarını, fiyatlandırmalarını veya hizmet tanımı belgelerini/modellerini açıklamaları için tedarikçilerle konuşabilir. Tedarikçilerle yapılan tüm görüşmelerin kaydı tutulacaktır.

4. HİZMETİN SEÇİLMESİ VE İHALENİN VERİLMESİ**Tek Satıcı**

Sadece bir satıcı gereklilikleri karşılıyorsa ihale bu satıcıya verilebilir.

Birden Fazla Satıcı

Nihai listede birden fazla hizmet bulunuyorsa alıcı, Ekonomik Açıdan En Avantajlı Teklifi (EAEAT) içeren hizmeti seçecektir. EAEAT temelli değerlendirme için aşağıdaki tabloda yer alan kriterlere bakın. Alıcılar kullanacakları ayrıntılı özelliklere ve bunların nasıl ağırlıklandırılacağına karar verebilir.

Alıcıların aşağıdakileri yapması gerekebileceğini unutmayın:

- farklı tedarikçilerin birleşimlerine bakma

- hacim indirimleri veya kurumsal indirimler hakkında ve satıcının maliyet optimizasyonu hizmetleri hakkında özel bilgi edinme

Tedarikçiler her zaman adil ve şeffaf bir şekilde değerlendirilmelidir. Seçim, en uygun teklife dayalı olarak yapılacaktır. Satıcılar/hizmetler proje gerekliliklerine dayalı olmayan nedenlerle dışarıda bırakılmayacaktır.

Tablo 2 - EAEAT Temelli Değerlendirme

<i>İhaleyi verme kriterleri</i>
<i>Yaşam boyu maliyet: maliyet etkinliği, fiyat ve işletme maliyetleri</i>
<i>Teknik liyakat ve fonksiyonel uygunluk: ilgili hizmet düzeylerinde belirtildiği gibi kapsam, ağ kapasitesi ve performans</i>
<i>Satış sonrası hizmet yönetimi: yardım masası, dokümantasyon, hesap yönetim fonksiyonu ve çeşitli hizmetleri tedarik etme güvencesi</i>
<i>Fonksiyonel olmayan özellikler</i>

KÜÇÜK İHALELER

Gerekli görülmesi halinde, belirli bir iş yüküne veya projeye en uygun tedarikçiyi belirlemek için küçük bir ihale düzenlenebilir. Küçük ihalede, müşteri bir lot içindeki tüm tedarikçileri bir dizi gerekliliğe yanıt vermeye davet ederek çerçeve sözleşmesi kapsamında ek rekabet sağlayabilir. Müşteri, lot içindeki tüm yetkin tedarikçileri teklif vermeye davet edecektir. Aşağıdaki bölümlerde verilen teknik, güvenlik ve fiyatlandırma/değer ile ilgili ek karşılaştırma bilgilerine bakın.

SÖZLEŞME

Hizmetin kullanılabilmesi için alıcı ve Satıcı sözleşmenin bir nüshasını imzalayacaktır. Bir Çerçeve sözleşmesinin maksimum uzunluğu normal şartlarda <x> aydır ancak sözleşmeyi uzatmak için gerekli olması halinde dahili onaylar alınmak suretiyle, bu süre <x> ay ve daha sonra ilave <x> ay uzatılabilir.

Hizmetin kullanılabilmesi için sözleşmenin bir nüshası ilgili tüm taraflarca (alıcı ve tedarikçi) imzalanmalıdır.

2.1.5 İsteklilerin Karşılması Gereken Asgari Gereklilikler - İdari

Çerçeve sözleşmesi yeterlilik kriterlerinin basit ve net bir dil kullanılarak hazırlanması, geleneksel bir çözümü "bulut" etiketi altında paketleyerek sunan geleneksel veri merkezi veya donanım sağlayıcılarının teklifte bulunmasını önleyecektir. RFP katılımcıları, isteklilerin karşılması gereken aşağıdaki asgari idari gereklilikleri nasıl karşıladıklarını göstermelidir.

Tekrar belirtmek gerekirse bu belge **LOT 1 - BULUT TEKNOLOJİLERİ**'ne odaklanılarak hazırlanmıştır. Bununla birlikte, gereklilikler ve RFP kapsamı açısından genel bağlamın sağlanması için faydalı olacağı yerlere **LOT 2 - PAZAR YERİ** ve **LOT 3 - BULUT DANIŞMANLIĞI** hakkında ilave bilgiler içerir. Örneğin bir CISP Satıcısı/MSP/SI/Danışmanlık Firması vb. için asgari yeterlilik kriterlerinin dahil edilmesi önemlidir ve bu tür sağlayıcıların (1) bir satıcı veya kanal çözüm ortağı olarak CISP'ye doğrudan bağlı olduğundan, (2) üçüncü taraf kurumlara CISP'nin tekliflerine doğrudan erişimi satmak için ilgili CISP tarafından yetkilendirilmiş olduğundan ve (3) yeterliliklerini ve uzmanlıklarını tasdik eden, CISP'ler tarafından verilmiş sertifikalara sahip olduğundan emin olunmasını sağlar.

Örnek RFP Metni: İsteklilerin Karşılması Gereken Asgari Gereklilikler - İdari

Bu çerçeve sözleşmesi ile aşağıdaki kategoriler altında birden fazla satıcıya ihale verilecektir. Satıcılar bir Ticari CISP, bir CISP'nin üçüncü taraf satıcısı, bir pazar yeri hizmetleri dağıtıcısı ve/veya bir CISP'nin kullanılması için gerekli hizmetlerin (ör. danışmanlık, taşıma hizmetleri, yönetilen hizmetler, FinOps vb.) sağlayıcısı olmalıdır. Lütfen hangi rollerde teklif verdiğinizi belirtin:

LOT 1

- _____ - Genel Bulut Hizmeti (IaaS VE PaaS) doğrudan sağlayıcısı (CISP)
- _____ - Topluluk Bulut Hizmeti (IaaS VE PaaS) doğrudan sağlayıcısı (CISP)
- _____ - Özel Bulut Hizmeti (IaaS VE PaaS) doğrudan sağlayıcısı (CISP)
- _____ - CISP Üçüncü Taraf Satıcısı (bir CISP'nin çevrimiçi bulut tekliflerine doğrudan erişim sağlama yeteneğine sahip)

- Hizmetlerine doğrudan erişimi satabilme yetkisine sahip olduğunuz CISP tekliflerini belirtin: _____
- CISP'nin tekliflerinin yetkili bir satıcısı olduğunuza dair CISP tarafından düzenlenmiş bir belge sağlayın: _____

LOT 2

- _____ - Bir CISP üzerinde çalışan Pazar Yeri Hizmetlerinin doğrudan sağlayıcısı (PaaS ve/veya SaaS)
- _____ - Bir CISP üzerinde çalışan Pazar Yeri Hizmetlerinin dağıtıcısı (PaaS ve/veya SaaS)

LOT 3

- _____ - Profesyonel Hizmetler sağlayan CISP
- _____ - CISP Teknik Desteği sağlayıcısı
- _____ - Bir CISP üzerinde kullanılan veya çalıştırılan hizmetler sağlayan CISP Çözüm Ortağı
- _____ - Bir CISP üzerinde kullanılan veya çalıştırılan hizmetler sağlayan Etki Sahibi/Danışman

Teklif türünü belirtin:

- Bir CISP üzerindeki iş yükleriyle ilgili Yönetilen Hizmetler (E/H): _____
 - Uzmanlık Alanlarını (varsa) belirtin: _____
- Profesyonel Hizmetler (E/H): _____
- Danışmanlık - Eğitim (E/H): _____
- Danışmanlık - Strateji (E/H): _____
- Danışmanlık - Taşıma (E/H): _____
- Danışmanlık - Bulut Yönetişimi (E/H): _____
- Danışmanlık - FinOps (E/H): _____
- Danışmanlık - Diğer (lütfen belirtin): _____

Hizmetlerini sağladığınız CISP'yi/CISP'leri belirtin: _____

CISP'nin modeli kapsamında çözüm ortağı statünüzü doğrulayan, CISP'den alınmış bir belge sağlayın: _____

LOT 1 ASGARİ İDARİ GEREKLİLİKLER**Bulut Hizmeti Sağlayıcıları (CISP'ler)**

Satıcıların bir CISP olarak kabul edilebilmesi için aşağıdaki gereklilikleri karşılaması gerekir:

<i>CISP İçin Önerilen Yeterlilik Kriterleri</i>	<i>Nedeni</i>
<i>Kuruluşla ilgili ayrıntılar: ad, yasal yapı, sicil/DUNS numarası, vergi kimlik numarası vb.</i>	
<i>Şirket büyüklüğü, ekonomik ve mali durum³.</i>	<i>Müşteri, CISP'nin sözleşmeyi ifa edip edemeyeceğini belirleyebilir.</i>
<i>Değerlendirme dışı bırakma gerekçeleri, ör. suç kaydı/dolandırıcılık faaliyetleri vb.</i>	
<i>Örnek Olay İncelemeleri/Müşteri Referansları (talep numarasını/türünü belirtin).</i>	<i>Müşteri, CISP'nin talep edilen hizmetleri sunmak için gerekli deneyime sahip olup olmadığını ölçme yeteneğine sahiptir.</i>
<i>Kurumsal Sosyal Sorumluluklar.</i>	<i>CISP'nin sağladıkları için genel erişime açık sürümler bulunmalıdır.</i>
<i>Genel erişime açık sürdürülebilirlik taahhütleri ve uygulamaları.</i>	<i>Müşteri bir CISP'nin işlerini mümkün olan en çevre dostu şekilde yürütmeyi taahhüt edip etmediğini görebilir.</i>
<i>CISP son 5 yıl içinde özellikle PaaS, makine öğrenimi ve analiz, büyük veri, yönetilen hizmetler ve bulut kullanımı optimizasyon özellikleri alanlarında yeni faydalı hizmetler ve özellikler geliştirme ve sunma konusunda kanıtlanmış bir başarı geçmişine sahip olmalıdır. Bu hususu kanıtlamak için genel erişime açık değişiklik günlükleri veya haber akışları kullanılabilir.</i>	<i>CISP'nin müşterilere hızla yeni ürünler ulaştırmak için çalıştığını ve ardından ürünlerde değişiklikler yaparak gelişmiş ürünleri sunduğunu gösterir. Bu, müşterilerin yeniden sermayelendirme yatırımları yapmak zorunda kalmadan son teknoloji BT altyapısını sürdürmelerine yardımcı olur.</i>

CISP ile Satıcı/Çözüm Ortağı İlişkisi

<KURULUŞ>, ana yüklenicinin bir satıcı veya kanal çözüm ortağı olarak CISP'ye doğrudan bağlı olmasını, üçüncü taraf kurumlara CISP'nin tekliflerine doğrudan erişimi satmak için ilgili CISP tarafından yetkilendirilmiş olmasını, yeterliklerini ve uzmanlıklarını tasdik eden ilgili CISP'ler tarafından verilmiş sertifikalara sahip olmasını zorunlu kılmaktadır. Bu, **<KURULUŞUN>**, **Çerçeve Sözleşmesi'nin** ana yüklenicisi ile CISP arasındaki ilave alt yüklenicilik katmanıyla ilişkili Hükümleri ve Hizmetleri inceleme ihtiyacını ortadan kaldırır. Bu gereklilik aynı zamanda (1) **<KURULUŞUN>** sağlanacak hizmetlerle ilgili sorumlulukların net olarak atandığından emin olmak için kendi durum tespitini yaparken ve (2) **<KURULUŞUN>**, bulut hizmetlerinin kullanımını içeren ilgili günlük faaliyetlerini yürütürken ilave satıcı katmanlarının doğuracağı karmaşıklığı azaltır.

2.2 Teknik

Bulut Hizmetleri RFP'si, CISP'lerin bir müşterinin kendi özelleştirilmiş çözümünü oluşturması için gerekli standart bulut teknolojilerini sağlamalarını zorunlu kılarak CISP'ler için çitayı yükseltmelidir. Daha önce de bahsedildiği gibi, bir Bulut Hizmetleri RFP'si ele alınırken standart ve özelleştirilmiş çözümler arasındaki bu fark büyük önem taşımaktadır. CISP'ler milyonlarca müşteriye standart hizmetler sunmaktadır. Bu nedenle, bir Bulut Hizmetleri RFP'sindeki özelleştirmelerde, çözüm sonuçlarını elde etmede kullanılan bulut hizmetlerini sunmak için kullanılan altta yatan yöntemler, altyapı veya donanımın yerine, yığının en üst dilimindeki çözümlere ve sonuçlara odaklanılır.

³ Bir Bulut Hizmetleri RFP'sinde, şirketlerin çalışan sayısı ve dahili çalışan ekiplerinin yapısı gibi ayrıntılar yerine genel şirket bilgilerine bakılacağını unutmayın. Bulut teknolojisi söz konusu olduğunda, hizmet performansı garantisi ile çalışan sayısı arasında bir ilişki bulunmaz. Bulut RFP'lerinde, bunun yerine, şirketin gereklilikleri karşılamak için gerekli büyüklükte olup olmadığına (yeterli ölçek) ve kanıtlanmış deneyimine/performansına bakılır.

2.2.1 Asgari Gereklilikler

Geleneksel BT satın alımlarında genellikle, kuruluşun halihazırda işlerini nasıl yürüttüğünü belgeleyen bir dizi çalışma oturumu düzenlenerek hazırlanmış iş gerekliliklerine odaklanılır. Bu gerekliliklerin tam olarak doğru bir şekilde oluşturulması en iyi koşullarda bile zor bir süreçtir. Başarılı olunması halinde, bu gereklilik oturumları eskimiş ve verimsiz kalmış olabilecek geçmişteki iş sürecini belgeler. Daha sonra bu gereklilikler CISP tarafından karşılanmak üzere bir RFP'ye dahil edildiğinde bulunabilecek tek çözüm, özel geliştirilmiş bir çözüm olabilir. Bu model, bulut hizmeti satın alma yöntemleri için uygun değildir.

Kamu sektörü kuruluşları, iş hedeflerini ve performans ihtiyaçlarını anlamalıdır fakat RFP'de, sistem tasarımı ve fonksiyonelliğini dikte ederek kuralcı bir yaklaşım izlememelidir. Kuruluş, bunun yerine, işe en uygun çözüm için alışveriş yapmalıdır. Kuruluşlar, başarılı hizmetler ortaya çıkarmayabilecek yüzlerce veya hatta binlerce kuralcı gerekliliğe ilişkin teklifleri değerlendirmek yerine, teknolojinin ve ilişkili hizmetlerin iş hedeflerini ne derece iyi karşılayacağına veya geliştireceğine, kendi performans ihtiyaçlarını karşılayıp karşılamayacağına ve yapılandırma yoluyla iş kurallarında ince ayar yapma yeteneği sunup sunmayacağına dayalı değerlendirme kriterleri dahil etmelidir.

*En iyi çözümlerin elde edilebilmesi için Bulut RFP'lerinde doğru soruların sorulması gerekir. Bir bulut modelinde fiziksel varlıklar satın alınmadığından, geleneksel veri merkezi satın alımlarında kullanılan birçok gereklilik uygulanamaz. **Veri merkezleriyle ilgili soruları sormaya devam etmeniz, alacağınız cevapların da veri merkezleriyle ilgili olmasına yol açacaktır.** Bu da CISP'lerin teklif verememesine ya da bir kamu sektörü müşterisi olarak bulutun özellik ve avantajlarından tam olarak yararlanmanızı engelleyen, kötü tasarlanmış sözleşmeler yapmanıza neden olabilir.*

Bir Bulut Hizmetleri RFP'sinde, CISP'ler ve bulut hizmetleri tarafından karşılanması istenen temel gerekliliklere odaklanılır. Bu da LOT 1'de yer almaya hak kazanan satıcıların yüksek çıtaya uygun olmalarını sağlar. Gereklilikler ayrıca, yeterliliğe sahip çok çeşitli CISP'lere kamu sektörünün erişimini sınırlandırmamak için çok kuralcı olmamalıdır.

Örnek RFP Metni: Bulut Sağlayıcısı Özellikleri

LOT 1 için yukarıdaki asgari CISP idari gerekliliklerine de bakın

CISP için Önerilen Yeterlilik Kriterleri	Nedeni
Altyapı	
CISP altyapısı en az 2 veri merkezi kümesi sunmalıdır. Yüksek Erişilebilirliğe Sahip Aktif-Aktif dağıtımlara ve DR-BC senaryolarının uygulamalarına olanak sağlamak için her küme, düşük gecikmeli bağlantı ile birbirine bağlı olan en az 2 veri merkezinden oluşmalıdır. Her kümeyi meydana getiren veri merkezleri birbirinden fiziksel olarak yalıtılmış olmalıdır ve bir veri merkezinde hata meydana gelmesi durumunda diğer veri merkezleri bundan etkilenmeden çalışmaya devam edebilmelidir.	CISP, tek hata noktasından kaçınılabilecek yüksek erişilebilirliğe sahip uygulamalar oluşturulmasına elverişli bir altyapı sunabilecek yeterlilikte olmalıdır.
CISP, mantıksal ve coğrafi olarak yalıtılmış bölgeler sağlamalıdır. Müşteri Verileri, CISP tarafından bu bölgelerin dışında çoğaltılmamalıdır.	Veri yerleşimi gereklilikleri, müşterinin, verilerinin tutulduğu konum üzerinde tam kontrole sahip olmasını zorunlu kılar.

<i>CISP, CISP veri merkezleri arasında doğrudan, tahsis edilmiş ve özel bağlantı sağlama yeteneğine sahip olmalıdır.</i>	<i>Özel bağlantı, güvenli bir hibrit altyapı oluşturulabilmesi için karşılanması gereken temel bir gerekliliktir.</i>
<i>CISP, taşınan veriler için şifreleme içeren yeterli mekanizmalar sağlamalıdır.</i>	<i>Müşteri, verilerin şifrelenmemiş halde taşınamamasını sağlayan bir özellik talep edebilir.</i>
Asgari CISP sertifikaları	
<i>CISP, ISO 27001 sertifikasına sahip olmalıdır.</i>	<i>Üçüncü taraf denetimi, sertifikasyon ve akreditasyon, müşterilerin hizmetleri (ve özellikle platformu) kalite, güvenilirlik ve güvenilirlik açısından karşılaştırılabilmesini sağlar. Asgari sertifika gerekliliklerinin yerine getirilmesi önemlidir.</i>
<i>CISP, GDPR'ye uygun olarak kullanılabilen ve müşterilerin de GDPR'ye uygun uygulamalar geliştirmesine imkan veren özellikler ve hizmetler sağlamak için CISPE Veri Koruma Davranış Kuralları'na uymalıdır.</i>	<i>Müşteri, GDPR'ye uygun olarak uygulamalar geliştirebilmeli veya çalıştırabilmelidir.</i>
<i>CISP, CISP kontrol ve prosedürlerine ilişkin şeffaflığı sağlamak için Sistem ve Organizasyon Kontrolleri 1 ve 2 Raporları (SOC Raporları) gibi 3. taraf denetiminden geçmiş raporları (EC tarafından kullanılan konumları ve hizmetleri kapsayan) sunmalıdır.</i>	<i>CISP, uygulamanın nasıl kullanıldığı ve yönetildiği konusunda şeffaf olmalıdır. SOC raporları, güven ve şeffaflığın tesis edilmesine yardımcı olur.</i>
<i>CISP, İklim Nötr Veri Merkezi Paketi'ne uymalıdır .</i>	<i>İklim Nötr Veri Merkezi Paketi, CISP'nin 2030'a kadar İklim Nötrlüğü hedefine ulaşmasını gerektirir ve dolayısıyla kullanıcının kendi sürdürülebilirlik hedeflerini desteklemesine olanak sağlar. Tam zaman eş değeri (FTE) cinsinden çalışan sayısı 250'den fazla olan (KOBİ olmayan) sağlayıcılar için üçüncü taraf denetçiler zorunludur</i>
<i>CISP, SWIPO IaaS Taşınabilirlik Davranış Kuralları'na uymalıdır .</i>	<i>SWIPO IaaS Taşınabilirlik Davranış Kuralları, hizmetlerin, Kişisel Olmayan Verilerin Serbest Dolaşımına İlişkin Yönetmeliğin 6. Maddesi olan "Verilerin Taşınması" altında belirlenen gereklilikleri karşılamasını sağlar.</i>
Hizmet Özellikleri	
<i>CISP altyapısı, uygulama programlama arabirimleri (API'ler) ve web tabanlı yönetim konsolu yoluyla erişilebilir olmalıdır.</i>	<i>Self servis erişim ve uygulama programlama arabirimleri, kullanıcı erişiminin ve sağlayıcının mümkün olduğunca aracısızlaştırılması için CISP sağlayıcılarının karşılaması gereken zorunlu bir standarttır.</i>
<i>CISP şu Hizmetleri içeren bir temel hizmet seti sunmalıdır: Nesne Depolama, Yönetilen İlişkisel Veritabanı, Yönetilen İlişkisel Olmayan Veritabanı, Yönetilen Yük Dengeleyiciler, İzleme ve entegre Otomatik Ölçeklendirme.</i>	<i>Tek başına sanal makineler sunulması, bulut sağlayıcısı olarak değerlendirilmek için yeterli değildir. Bulut sağlayıcıları, müşterinin uygulamalarını hızlandırmak ve geliştirmek için bir dizi PaaS ve IaaS hizmeti sunmalıdır.</i>
<i>CISP, Müşterinin hizmet kullanımını ve yapılandırmasını serbestçe değiştirmesine veya verileri CISP içinde ve dışına taşımaya izin vermelidir (self servis teklif).</i>	<i>Hizmetlere ve verilere self servis erişim, müşterinin tamamen bağımsız olmasına olanak sağlayan mutlak bir gerekliliktir.</i>
<i>CISP, hizmetlerinin "kullandığın kadar öde" yöntemine göre faturalandırılmasına olanak sağlamalıdır.</i>	<i>Kullandığın kadar öde yöntemi, müşterinin iş yüklerini optimize etmesine, riski en aza indirmesine ve kısa ömürlü uygulamalar ve PoC'ler için CISP'den yararlanmasına olanak sağlar.</i>

Veri ve Sistemlerin Güvenliği	
CISP, Müşterinin, verilerinin tam kontrolünü elinde tutmasına izin vermeli, Müşteriye verilerin depolanacağı yeri (şehir kentsel alanı) seçme özgürlüğünü sunmalı ve taşıma işlemi bizzat Müşteri tarafından başlatılmadığı sürece hiçbir müşteri verisinin taşınmayacağını garanti etmelidir.	Müşteri, verilerin depolanacağı yer, içeriğe erişimin nasıl yönetileceği ve hizmetler ile kaynaklara kullanıcı erişimi üzerinde kontrole sahip olmalıdır.
CISP özellikleri Müşteriye kendi güvenlik politikaları üzerinde, Müşteri veri ve sistemlerinin Gizliliği, Bütünlüğü ve Erişilebilirliği dahil olmak üzere, tam kontrol olanağı sunmalıdır.	Müşteri, kendi iş yükleri genelinde kendi güvenlik standartlarını tanımlayabilmeli ve uygulayabilmelidir. Sağlayıcının müşteri verileriyle "doğru olanı yapacağına" güvenilmesi yeterli değildir.
Maliyet Kontrolü	
CISP, müşterinin zaman içindeki harcamalarını izlemesine olanak sağlayan mekanizma ve araçlara sahip olmalıdır. Araçlar maliyetin iş yükü, hizmet ve hesap bazında dökümüne olanak sağlamalıdır.	
CISP, müşterinin bir maliyet eşiği aşıldığında her defasında uyarılmasını sağlayan araçlar sunmalıdır.	
CISP, müşteriye ayrıntılı faturalar vermelidir. Faturanın; iş yükü, ortam ve hesap bazında maliyetin dökümünün alınmasına izin verecek şekilde yapılandırılması mümkün olmalıdır.	

CISP'ler ayrıca aşağıdaki teknik gereklilik sorularına yanıt vermelidir.

ÇÖZÜMLER

CISP, aşağıdaki çözümler için CISP'de barındırılan veya CISP ile entegre edilen önceden oluşturulmuş şablonlar ve yazılım çözümlerini nasıl sağlayacağını göstermelidir:

- Depolama
- DevOps
- Güvenlik/Uygunluk
- Büyük Veri/Analiz
- İş Uygulamaları
- Telekomünikasyon ve Ağ İletişimi
- Geo-uzamsal
- IoT
- [Diğer]

CISP'nin aşağıdaki iş yükleri için nasıl kullanıldığına dair bir genel bakış sağlayın:

- Olağanüstü Durum Kurtarma
- Geliştirme ve Test
- Arşivleme
- Yedekleme ve Kurtarma
- Büyük Veri
- Yüksek Performanslı Bilgi İşlem (HPC)
- Nesnelerin İnterneti (IoT)
- Web Siteleri
- Sunucusuz Bilgi İşlem

- DevOps
- İçerik Teslimi
- [Diğer]

2.2.2 Satıcıların Karşılaştırılması

Bir Bulut Hizmetleri RFP'sindeki asgari gerekliliklere ek olarak, bir rekabetçi değerlendirme sırasında CISP teknolojilerinin karşılaştırılmasında esas alınacak kriterlerin belirtilmesi önemlidir.

Bulut Hizmetleri RFP'lerinde, bir kuruluşun ihtiyaç duyduğu bulut özellikleri istenilmelidir ve müşterinin bu özellikleri kendi çözümünü oluşturmak için kullanacağı dikkate alınmalıdır. Bir CISP'nin standart ötesinde sağlayabileceği işlevsellikler (CISP'nin sağladığı önceden oluşturulmuş çözümler veya otomasyon özellikleri gibi), Bulut Hizmetleri RFP'sinde "katma değer sunan seçenekler" veya "en iyi değer" kriterlerini daha anlamlı bir şekilde analiz etmek amacıyla kullanılabilir.

Kamu sektörü genellikle en iyi değer, ekonomik açıdan en avantajlı teklif (EAEAT) veya en düşük fiyat gibi değerlendirme kriterlerini kullanarak istekliler arasında rekabet oluşmasını zorunlu kılar. Kamu sektörü kurumları bir Bulut Hizmetleri RFP'sinin bu bölümünü planlarken, bulutun benzersiz özelliklerini dikkate alan bir yaklaşım geliştirilmesi önemlidir. Örneğin bulut sağlayıcılarının tekliflerini sadece ürün kalemleri (ör. bilgi işlem veya depolama) açısından karşılaştırmanın, tekliflerin karşılaştırılması için etkin bir yöntem olmadığı bilinmelidir. Bunun yerine, yukarıda bölüm 2.2.1 altında listelenenler gibi daha üst düzey çözümlere odaklanılması şiddetle önerilir. Kamu sektörü kurumları daha sonra, *Ek A - İstekliler Arasında Karşılaştırmayla İlgili Teknik Gereklilikler* bölümünde listelenenler gibi buluta özel gerekliliklere bakabilir.

RFP'lerde müşterinin kendi bulut çözümünü oluşturabilmesi için gerekli temel bulut özellikleri belirtilmelidir. Kamu sektörü kuruluşları CISP'nin devasa bir ölçekte çalışan en uygun "gerçek bulut" teklifine sahip olduğundan emin olmak için üçüncü taraf analist raporlarını kullanmanın yanı sıra Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Temel Bulut Özellikleri'nden yararlanabilir.

Örnek RFP Metni - Satıcıların Karşılaştırılması

CISP'ler **Ek A**'daki TÜM teknik gereklilik sorularına yanıt vermelidir.

Katılımcılar aşağıdaki özniteliklere sahip olmalı ve bulut hizmetleri tekliflerinin bulut bilgi işleme ilişkin beş temel özelliği nasıl işleyeceğini açıklamalıdır⁴.

- 1) **İstek Üzerine Self Servis:** Katılımcı, sunucu zamanı ve ağ depolaması gibi bilgi işlem özelliklerini, ihtiyaç duyulduğunda her hizmet sağlayıcısıyla insan etkileşimini gerektirmeden otomatik bir şekilde tek taraflı olarak tedarik etme özelliğini sağlamalıdır. Katılımcı, sipariş faaliyetiyle tek taraflı olarak (satıcı incelemesi veya onayı olmaksızın) hizmet tedarik edilmesi özelliğini sağlayacaktır. Bunun teklifinizde veya temsil ettiğiniz teklifte nasıl işleyeceğini açıklayın.
- 2) **Her Yerden Ağ Erişimi:** Katılımcı, biri internet tabanlı olmak üzere birden çok ağ bağlantısı seçeneği sağlamalıdır. Bunun teklifinizde veya temsil ettiğiniz teklifte nasıl işleyeceğini açıklayın.
- 3) **Kaynak Havuzu:** Katılımcının CISP'si, tüketici talebine göre dinamik olarak atanan ve yeniden atanan farklı sanal kaynaklar içeren bir çoklu kiracı modeli kullanarak birden fazla tüketiciye hizmet veren, havuza alınmış bilgi işlem kaynakları sağlamalıdır. Kullanıcı, üst düzey bir soyutlama ile konumu belirtebilir (ör. ülke, bölge veya veri merkezi konumu). Katılımcı, tedarik isteğinin ardından dakikalar veya saatler içinde bu kaynakların ölçeklendirilmesini desteklemelidir. Bunun teklifinizde veya temsil ettiğiniz teklifte nasıl işleyeceğini açıklayın.

⁴ <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

4) **Hızlı Esneklik:** Katılımcının CISP'si hizmet tedarik etme ve devreden çıkarma (ölçek artırma ve azaltma) özelliklerini desteklemelidir. Hizmeti, tedarik isteğinden sonra belirtilen minimum süreler (maksimum "x" saat) içinde kullanılabilir hale getirmelidir. Katılımcı, bu tedarik isteklerinden kaynaklanan günlük veya saatlik bazda faturalama ayarlamalarını desteklemelidir.

5) **Ölçülen Hizmet:** Katılımcı bir çevrimiçi pano veya benzeri bir elektronik araçla hizmet kullanımına dair görünürlük sunmalıdır.

Ek olarak, CISP:

- Gartner Magic Quadrant for IaaS⁵ ile gösterildiği gibi bulut hizmetleri sağlama konusunda tanınan bir lider olmalıdır.
- CISP'nin kanıtlanmış özelliklerini ve güvenilirliğini gösteren, sektör tarafından kabul gören üçüncü taraf analist raporlarını sağlamalıdır.

Son olarak, CISP'ler Ek B'de verilen senaryolar kullanılarak karşılaştırılacaktır.

2.2.2.1 Hizmet Düzeyi Sözleşmeleri (SLA'lar)

CISP'ler milyonlarca müşteriye standart ticari SLA'lar sunmaktadır. Bu nedenle, tıpkı şirket içi veri merkezi modelinde olduğu gibi, özelleştirilmiş SLA'lar sunamamaktadır. Bununla birlikte, CISP müşterileri (genellikle CISP Çözüm Ortaklarının desteğiyle), müşteriye özel gereklilikleri karşılayıp aşmak için kendi bulut kullanımlarını bir CISP'nin ticari SLA'larından ve benzersiz SLA'lardan yararlanacak şekilde tasarlayabilir.

Bireysel son kullanıcıların performans ve erişilebilirlik gerekliliklerini karşılayabilmesi için Bulut Hizmetleri RFP'leri, CISP'lerin kendi hizmetlerinden ve ticari SLA'larından yararlanılabilmesi amacıyla gerekli özellikleri ve rehberliği sunmasını sağlamalıdır.

Örnek RFP Metni: Hizmet Düzeyi Sözleşmeleri

CISP'nin Hizmet Düzeyi Sözleşmelerine (SLA'lar) yaklaşımıyla ilgili bilgi ve bağlantıları sağlayın.

<KURULUŞ>, CISP SLA'ları ile ilgili farkındalığı sürdürecektir ve önemli iş yükleri ile uygulamaları, bir SLA'nın karşılanmaması halinde bile çalışmaya devam edecek şekilde dağıtacaktır.

<KURULUŞ>, kendisine ait tüm ekipmanlarla veya CISP ile kullanılan ve **<KURULUŞ>** tarafından işletilen hizmetlerle ilişkili uygun SLA'ları sürdürmekten sorumlu olacaktır.

CISP, **<KURULUŞ>** operasyonel SLA performansına ilişkin sürekli görünürlük ve raporlama edinmesi için gerekli özellikleri sağlayacak ve hizmetlerin performans, dayanıklılık ve güvenilirlik odaklı tasarlanması için CISP altyapısından yararlanılmasına ilişkin belgelenmiş en iyi uygulamaları sunacaktır.

2.2.3 Sözleşme yapma

CISP hüküm ve koşulları, bir bulut hizmetleri modelinin nasıl işleyeceğini yansıtacak şekilde tasarlanır (fiziksel varlıklar satın alınmamaktadır, CISP'ler devasa bir ölçekte faaliyet göstererek standart hizmetler sunar). Dolayısıyla, CISP'nin hüküm ve koşullarının mümkün olan azami ölçüde entegre edilmesi ve kullanılması kritik önem taşır. Hüküm ve koşulların yanı sıra sözleşme yapma konusunda daha fazla bilgi için bkz. bölüm 2.5.

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

2.2.3.1 Yeni ve Değişen Hizmetler

CISP'ler bir hizmet üzerinden performans sağlar. Yükseltmeler ve süresi dolan servis bakım sözleşmeleri gerektiren geleneksel şirket içi çözümlerin aksine, bulut sağlayıcıları sadece standart hizmeti sağlar. Bulut modelinin ölçek ekonomilerinden yararlanabilmesi için temel altyapıdaki yükseltmeler ve değişiklikler, tek tek değil, tüm kullanıcılar için yapılır ve müşteriler daha sonra kullandıkları hizmetleri seçer. Hizmet geçmişe ait şirket içi sistemlerden daha sorunsuz olarak sağlanır ve bulut sağlayıcıları, müşterilerin diledikleri şekilde kullanmaları için sürekli olarak yeni ve geliştirilmiş hizmetler ekler.

Bir RFP'nin başvuru bitiş tarihinden sonra yeni veya geliştirilmiş CISP hizmetlerinin eklenmesine izin verilmemesi halinde, kamu sektörü kuruluşları, kendilerini Çerçeve Sözleşmesi'nin bir sonraki sürümü yayınlanana kadar bu tür yeni hizmetlerden ve gelişmiş özelliklerden mahrum bırakmış olacaktır. Bu nedenle, Çerçeve Sözleşmesi'nde açıklanan hizmet tedarikinin, başvuru bitiş tarihinden sonra da yeni CISP hizmetlerinin eklenmesine geniş bağlamda izin vermesi şiddetle önerilir. AB ihale kanunu, maddi açıdan farklı yeni CISP Hizmetlerinin Çerçeve Sözleşmesi'ne eklenmesini kısıtlayabilir fakat maddi değişiklik sayılmayan hizmet güncellemeleri ve yeni sürümleri ihale açısından herhangi bir zorluk olmadan eklenebilir.

Örnek RFP Metni: Yeni ve Değişen Hizmetler

CISP, kanıtlanmış ve kararlı sanallaştırma teknolojilerini kullanan, uygun maliyetli bir çözüm sağlayacak ve ileri düzey teknolojiler sürekli olarak yenilenecektir. <KURULUŞ>, Bulut Teknolojilerinin <KURULUŞA> ve CISP'nin diğer müşterilerine, paylaşılan hizmet esasına göre ortak bir kod tabanından ve/veya ortak bir Ortamdan sağlanabileceğini ve CISP'nin Bulut Hizmetlerinin fonksiyonları, özellikleri, performansı veya diğer özelliklerinde zaman zaman değişiklik, ekleme veya silme yapabileceğini ve bu tür bir değişiklik, ekleme veya silme yapıldığında Bulut Hizmeti şartnamesinin uygun şekilde tadil edileceğini kabul eder.

Bu teslimat siparişinin kapsamı, ÇERÇEVENİN KAPSAMI DAHİLİNDEKİ halihazırda mevcut olan ve yeni veya geliştirilmiş CISP Hizmetlerini kapsar. CISP tarafından ticari müşterilere sunulan bulut hizmetleri, <KURULUŞUN> kullanımına sunulacaktır.

2.2.3.2 Satıcıya Bağımlılık/Tersine Çevrilebilirlik

Bulut teknolojisi, fiziksel varlıklar satın alınmasını gerektirmediği için satıcıya bağımlılığı azaltır ve müşteriler verilerini istedikleri zaman bir bulut sağlayıcısından diğerine taşıyabilir.

Ancak, bulut hizmetleri satın alındığında, tüm bulut hizmetleri eşit olmadığı için bir miktar satıcıya bağımlılık kaçınılmazdır. Bu nedenle, bir CISP başka bir CISP'nin sağlayamayacağı hizmetler ve özellikler sunabilir ve bu da söz konusu hizmetleri başka bir sağlayıcıda kullanma yeteneğini kısıtlar. Bir CISP'nin; bir müşterinin, standart hizmetlerini kullandığı benzersiz yapılandırmayı bilmesi ve dolayısıyla özelleştirilmiş bir çıkış planı sağlaması mümkün değildir. Bu nedenle, ihtiyatlı bir yaklaşım olarak, CISP'lerden elzem özellik ve hizmetlerini, bu hizmetlerin kullanımına ilişkin belgelerle birlikte bulutlarının dışına çıkarılabilir kılması talep edilebilir. Bu, makul bir "çıkış stratejisi" görevi görebilir.

AB "Kişisel Olmayan Verilerin Serbest Dolaşımına İlişkin Yönetmelik" in 6. Maddesi altında belirtilen gereklilikleri yerine getirmek üzere "Verilerin Taşınması" ve "Bulut Sağlayıcısının Değiştirilmesi" konularını ele almak için Sektör Davranış Kuralları hakkında bilgi için bkz. bölüm 2.3.1.2.

Örnek RFP Metni: Katılım ve Çıkış

<KURULUŞ>, belirli bir satıcıya bağımlılığı önlemek için makul bir çıkış stratejisi sağlayan teklifler aramaktadır. **<KURULUŞ>**, fiziksel varlıklar satın almamaktadır ve CISP, BT yığınına yükseltme ve tekrar düşürme yeteneğini sağlayacaktır. CISP, bağımlılığı en aza indirmek için CISP'nin platformuna taşımaya/platformundan taşınmaya yardımcı olmak için taşınabilirlik araç ve hizmetleri sağlayacaktır. CISP tarafından sağlanan taşınabilirlik araç ve hizmetlerinin kullanımına ilişkin ayrıntılı belgeler makul bir çıkış planı görevi göreceklerdir.

CISP, asgari taahhütler veya uzun vadeli sözleşmeler **talep etmemelidir**.

Bir hizmet sağlayıcısında depolanan veriler müşteri tarafından istenildiği zaman dışarı aktarılabilir. CISP, **<KURULUŞUN>** verileri gerektiği şekilde CISP depolama alanına/alanından taşınmasına izin verecektir. CISP ayrıca sanal makine görüntülerinin indirilmesine ve yeni bir bulut sağlayıcısına taşınmasına izin verecektir. **<KURULUŞ>**, kendi makine görüntülerini dışarı aktarabilir ve bunları şirket içinde veya başka bir sağlayıcıda kullanabilir (yazılım lisanslama kısıtlamalarına tabi olarak).

2.3 Güvenlik

Güvenlik ve uygunluk sorumlulukları, CISP ile bulut müşterileri arasında paylaşılır. Bu modelde, bulut müşterilerinin, uygulamalarının ve altyapıya konulan verilerinin mimarisi ve güvenliği bulut müşterilerinin kontrolünderken, CISP'ler ise son derece güvenli ve kontrollü bir altyapı üzerinde hizmet sunmaktan ve çeşitli ek güvenlik özellikleri sağlamaktan sorumludur. Bu modelde CISP ve müşteri sorumluluklarının düzeyi, bulut dağıtım modeline (IaaS/PaaS/SaaS) bağlıdır. Müşteriler her modelde kendi sorumlulukları konusunda net olmalıdır.

Bu paylaşılan sorumluluk modelinin anlaşılması başarılı bir Bulut Hizmetleri RFP'si formüle edilmesinde önemli bir rol oynar. Kamu sektörü kuruluşları; CISP sorumluluklarını, kendi sorumluluklarını ve danışmanlık/ISV çözüm ortaklarının ve bunların çözümlerinin hangi noktalarda yardımcı olmak üzere devreye girebileceğini bildiklerinden emin olmalıdır.

2.3.1 Asgari Gereklilikler

Bulutta güvenlik denildiğinde anahtar sözcük **Özelliktir**. Kamu sektörü kuruluşları, CISP'ler karşısında talepkâr bir yaklaşım izleyerek CISP'lerin, müşterilerin paylaşılan sorumluluk modelinde kendi sorumluluklarını yerine getirebilmesine imkan tanımak için gerekli güvenlik özelliklerini sağlamalarını zorunlu kılmalıdır. Aşağıdaki temsili gereklilik listesinde görüldüğü üzere, müşterinin kendi benzersiz bulut ortamını güvenli kılmak amacıyla kullanabilmesi için CISP'den standart özellik sağlaması istenmektedir.

- Özel ağlar oluşturmak, ayrıca bulut sunucularına ve uygulamalara erişimi kontrol etmek için ağ güvenlik duvarları ve web uygulaması güvenlik duvarı **özellikleri sağlama**.
- Ofisinizden veya şirket içi ortamınızdan özel veya tahsis edilmiş bağlantılara olanak tanıyan bağlantı **seçenekleri sağlama**.
- Derinlemesine bir savunma stratejisi uygulama ve DDoS saldırılarını püskürtme **özellikliğini sağlama**.
- Depolama ve veritabanı hizmetlerinde veri şifreleme **özellikleri bulundurma**.
- Şifreleme anahtarlarını CISP'ye yönetirmeyi ya da müşterinin anahtarlar üzerinde tam kontrolü elinde bulundurmasını seçmenize olanak tanıyan esnek anahtar yönetimi **seçenekleri sağlama**.
- Müşterilerin şifreleme ve veri korumayı bir CISP ortamında geliştirilen veya dağıtılan tüm hizmetlere entegre etmesi için **API'ler sağlama**.
- CISP kaynaklarının kuruluş standartlarına göre oluşturulmasını ve kullanımdan çıkarılmasını yönetmek için dağıtım **araçları sağlama**.

- CISP kaynaklarını tanımlayan ve zaman içinde bu kaynaklardaki değişiklikleri izleyip yöneten envanter ve yapılandırma yönetim **araçları sağlama**.
- Müşterilerin, CISP ortamlarında tam olarak neler olduğunu görmesine olanak tanıyan **araçlar ve özellikler sağlama**.
- API çağrılarına ilişkin derin **görünürlük** (çağrılar kimin ve neyin yaptığı, ayrıca çağrılar kimden ve nereden geldiği dahil) **sağlama**.
- Araştırmaları ve uygunluk raporlamalarını hızlandıracak günlük birleştirme **seçenekleri sağlama**.
- Belirli olaylar meydana geldiğinde veya eşikler aşıldığında tetiklenecek uyarı bildirimlerini **yapılandırma özelliğini sağlama**.
- CISP hizmetleri genelinde kullanıcı erişim politikalarını tanımlama, uygulama ve yönetme **özellikleri sağlama**.
- CISP kaynakları genelinde izinlere sahip bireysel kullanıcı hesapları tanımlama **özelliğini sağlama**.
- Yönetim yükünü azaltmak ve son kullanıcı deneyimini iyileştirmek için kurumsal dizinlerle entegre etme ve birleştirme **özelliğini sağlama**.

Bunun gibi daha fazla gereklilik için bkz. Ek A - İstekliler Arasında Karşılaştırmayla İlgili Teknik Gereklilikler.

Güvenlik için asgari standardın ötesinde işlevsellikler, RFP'de "katma değer sunan seçenekler" veya "en iyi değer" kriterlerini daha anlamlı bir şekilde analiz etmek amacıyla kullanılabilir. Üstelik, söz konusu güvenlik olduğunda yerleşik veya otomatik ne kadar fazla işlevsellik olursa o kadar iyidir. İstekliler arasında karşılaştırmayla ilgili olarak gereklilikler için bkz. Ek A - İstekliler Arasında Karşılaştırmayla İlgili Teknik Gereklilikler.

Kamu sektörü kuruluşları gerekli CISP güvenlik kontrollerinin mevcut olduğuna dair güvence için akreditasyon sertifikalarına ve değerlendirmelerine bakmalıdır. Örneğin ISO 27001 sertifika standardıyla uyumluluğu onaylamak için bağımsız bir denetçi tarafından doğrulanmış ve sertifikalandırılmış bir CISP'yi düşünün. ISO 27001 Ek A'da düzenlenen 14. alan, bir CISP'nin ISO gereklilikleri uyarınca sistem edinme, geliştirme ve bakım faaliyetleriyle ilgili olarak uyguladığı belirli kontrollerin ayrıntılı bir incelemesini sunmaktadır. Bu kontroller, BT ile ilgili bir RFP'de bir kuruluştan istenebilecek sistem edinme, geliştirme ve bakım faaliyetleriyle ilgili kontrollerin tümünü olmasa bile çoğunu kapsamaktadır. Bu nedenle, bir kuruluşun sistem edinme, geliştirme ve bakım faaliyetleri ile ilgili kontrol gerekliliklerini yeni baştan formüle edip Bulut Hizmetleri RFP'sine eklemeye çalışmak yerine, CISP'ler için ISO 27001 sertifikası şartını araması yerinde bir uygulama olacaktır.

Üçüncü taraf uygunluk raporlarından yararlanılmasını öngören bu yaklaşım, çoğu güvenlik ve uygunluk kontrolüne (CISPE GDPR Davranış Kuralları, ISO, SOC vb.) uygulanabilir.

Örnek RFP Metni: Güvenlik

CISP, <KURULUŞ> ile hizmet sağlayıcısı arasında yeterli korumanın ve esnekliğin elde edilebilmesi için müseccel olmayan güvenlik süreçlerini ve teknik sınırlamalarını <KURULUŞ> açıklayacaktır.

CISP, güvenlik ve uygunluk ile ilgili görev ve sorumluluklarını tanımlayacaktır:

- Önerilen teklifte CISP'nin ve <KURULUŞUN> güvenlikle ilgili rollerini ve sorumluluklarını açıklayın. Sorumluluk ayrımı konusunda net olun ve <KURULUŞUN>, bulut ortamında güvenlik işlevlerini oluşturmaya ve otomatik hale getirmesine yardımcı olacak CISP hizmetlerini belirtin.
- EK A'da yer alan, <KURULUŞUN> güvenlik gereklilikleriyle ilgili teknik şartnameleri yanıtlayın.

<KURULUŞ> İÇERİKLERİNİN MÜLKİYETİ VE KONTROLÜ

CISP özelliklerinin, <KURULUŞUN> veri gizliliğini nasıl koruyabileceğini açıklayın. <KURULUŞUN> içeriklerinin korunmasını sağlamak için uygulanan kontrolleri dahil edin. CISP bir bölgede depolanan nesnelerin, <KURULUŞUN> tarafından başka bir bölgeye açıkça aktarılmadığı sürece, bölgeden asla ayrılması için güçlü bölgesel izolasyon sağlamalıdır.

- <KURULUŞUN> kendi içerik, hizmet ve kaynaklarına erişimi yönetecektir. CISP, <KURULUŞUN> bunu etkin bir şekilde gerçekleştirmesine yardımcı olmak için gelişmiş erişim, şifreleme ve günlüğe kaydetme özellikleri sağlamalıdır. CISP, yasalar uyarınca gerekli olduğu haller dışında ve CISP hizmetlerini sürdürmek ve hem <KURULUŞUN> hem de son kullanıcılarına sunmak amacı dışında başka hiçbir amaçla <KURULUŞUN> içeriklerine erişmeyecek veya bunları kullanmayacaktır.
- <KURULUŞUN>, içeriklerinin depolanacağı bölgeyi kendisi seçecektir. CISP, yasalar uyarınca gerekli olduğu haller dışında ve CISP hizmetlerini sürdürmek ve hem <KURULUŞUN> hem de son kullanıcılarına sunmak amacı dışında başka hiçbir amaçla <KURULUŞUN> içeriklerini onun seçtiği bölgelerin dışına taşımayacak veya çoğaltmayacaktır.
- <KURULUŞUN>, içeriklerinin güvenliğini nasıl sağlanacağını kendisi seçecektir. CISP, <KURULUŞUN>, taşınma veya bekleme halindeki içerikleri için güçlü şifreleme sağlamalı ve <KURULUŞUN> kendi şifreleme anahtarlarını yönetme seçeneğini sunmalıdır.
- CISP; <KURULUŞUN>, CISP'nin güvenlik kontrolü ortamını kurmasına, işletmesine ve kullanmasına yardımcı olmak için küresel gizlilik ve veri koruma en iyi uygulamalarının kullanıldığı bir güvenlik teminatı programına sahip olmalıdır. Güvenlik korumaları ve kontrol süreçleri, birden çok üçüncü tarafın bağımsız değerlendirmeleriyle bağımsız olarak doğrulanmalıdır.

Bulut akreditasyon sertifikaları ve değerlendirmeleri, kamu sektörü kuruluşlarına CISP'lerin etkin fiziksel ve mantıksal güvenlik kontrollerine sahip olduğuna dair güvence sağlar. RFP'lerde bu akreditasyonlardan yararlanılması, ihale sürecini hızlandırır ve bulut ortamı için gerekli olmayabilecek yinelenen, son derece zahmetli süreçlerden veya onay iş akışlarından kaçınılmasına yardımcı olur.

Bulut RFP'leri, CISP'lere uygunluk akreditasyonlarını ve değerlendirmelerini benimsediklerini kanıtlama fırsatını tanır. Daha önce de bahsedildiği gibi, bu akreditasyon şemaları genelinde risk senaryoları ve risk yönetim uygulamaları önemli ölçüde birbiriyle örtüşmektedir ve bu akreditasyonlarda kontroller ile gereklilikler aynı pakette bir araya getirildiklerinden, bu tür ayrı ayrı kontrolleri (bu kontrollerden birçoğu doğrudan şirket içi veri merkezlerinde yer alan önceki RFP'lerden alınabilir ve dolayısıyla bulut bilgi işlem için geçerli olmayabilir) açıklama uğraşına girmek yerine CISP'lerin akreditasyonlara uymalarını talep etmek, RFP'de uyum konusunu ele almanın daha hızlı bir yoludur.

NOT: Aşağıda listelenen raporlara nasıl erişilebileceğinin anlaşılması da çok önemlidir. Örneğin SOC 1 ve SOC 2 raporları genellikle hassas belgelerdir. Bunlara erişebilmek için gerekli sözleşmelerin (ör. gizlilik sözleşmesi, NDA) bilincinde olun ve bu belgelerin RFP'ye verilen yanıtın bir parçası olarak sunulmasını istemeyin (bu belgeler Kayıtların Açıklığı kanunları veya benzer mevzuat uyarınca kamu oyuna açık hale getirilebilir ve bu da bulut güvenliğini tehlikeye atabilir).

Örnek RFP Metni: Uygunluk

Veri işleme, veri güvenliği, gizlilik, erişilebilirlik vb. konular dahil olmak üzere bulut hizmeti operasyonlarındaki en iyi uygulamalardan türetilmiş kabul gören güvenlik, uygunluk ve operasyon standartlarının kullanılması, bulut teknolojilerinin satın alınmasını hızlandırır.

<KURULUŞ>, benzersiz teklifleri aşağıda ve **Ek A**'da açıklanan, kabul gören güvenlik, uygunluk ve operasyon standartlarına göre değerlendirecektir. **<KURULUŞ>**, satıcının her standarda ilişkin uygunluk sertifikasına güvenerek, standarda asgari uygunluğu, teklifin değerlendirilmesinde başlangıç düzeyi olarak kullanabilir.

CISP'den sözleşme süresi boyunca asgari standarda uygunluğu sürdürmesini talep etmek, hizmet uygunluğunu güncel tutma avantajını beraberinde getirir.

Teklif veren (doğrudan veya bir satıcı yoluyla) CISP aşağıdaki bağımsız üçüncü taraf tasdik belgelerini, raporlarını ve sertifikalarını karşılama yeteneğini gösterebilmelidir (Not: Bu tasdik, rapor ve sertifikalardan bazıları güvenlik sorunları nedeniyle gizlilik kısıtlamalarına tabiyse **<KURULUŞ>**, müşterek olarak üzerinde mutabakata varılan erişimi edinmek için CISP ile iş birliği yapacaktır):

Sertifikalar/Tasdikler	Yasalar, Düzenlemeler ve Gizlilik	Uyumlaştırmalar/Çerçeveler
☐ C5 (Almanya)		☐ CDSA
☐ CISPE Veri Koruma Davranış Kuralları (GDPR)		
☐ CNDPCP (İklim Nötr Veri Merkezi Paketi)		
☐ DIACAP	☐ AB Veri Koruma Direktifi	☐ CIS
☐ DoD SRG Düzey 2 ve 4	☐ AB Model Maddeleri	☐ Criminal Justice Info. Service (CJIS)
☐ HDS (Fransa, Sağlık)		
☐ FedRAMP	☐ FERPA	☐ CSA
☐ FIPS 140-2	☐ GDPR	☐ AB-ABD Gizlilik Kalkanı
☐ ISO 9001	☐ GLBA	☐ AB Güvenli Liman
☐ ISO 27001	☐ HIPAA	☐ FISC
☐ ISO 27017	☐ HITECH	☐ FISMA
☐ ISO 27018	☐ IRS 1075	☐ G-Cloud [Birleşik Krallık]
☐ IRAP [Avustralya]	☐ ITAR	☐ GxP (FDA CFR 21 Bölüm 11)
☐ MTCS Katman 3 [Singapur]	☐ PDPA - 2010 [Malezya]	☐ ICREA
☐ PCI DSS Düzey 1	☐ PDPA - 2012 [Singapur]	☐ I T Grundschutz [Almanya]
☐ SEC Kural 17-a-4(f)	☐ PIPEDA [Kanada]	☐ MARS - E
☐ SecNumCloud (Fransa)		
☐ SOC1 / ISAE 3402	☐ Gizlilik Kanunu [Avustralya]	☐ MITA 3.0
☐ SOC2/SOC3	☐ Gizlilik Kanunu [Yeni Zelanda]	☐ MPAA
☐ SWIPO IaaS Davranış Kuralları		

☐ İspanya DPA Yetkisi	☐ NIST
☐ Birleşik Krallık DPA - 1988	☐ Uptime Institute Katmanları
☐ VPAT/Bölüm 508	☐ Birleşik Krallık Bulut Güvenliği İlkeleri

Yukarıdaki liste yalnızca örnek olarak verilmiştir. Bulut hizmetleri için geçerli olabilecek sertifika ve standartların tam kapsamlı listesi olarak kabul edilmemelidir.

2.3.1.1 Veri Koruma

Kişisel verilerin, Genel Veri Koruma Yönetmeliği (GDPR) dahil olmak üzere geçerli AB veri koruma yasalarına uygun olarak işlenmesi, bulut hizmetleri kullanılırken dikkat edilmesi gereken önemli bir husustur. GDPR, ilkelere dayalı bir yönetmeliktir ve bu nedenle uygunluğun sağlanmasına yardımcı olacak, sektöre özel rehberlik sağlamaz. Bununla birlikte, GDPR'de, bu tür rehberlik için davranış kuralları gibi uygunluk araçlarının benimsenmesi teşvik edilmektedir. CISPE, Fransa Veri Koruma Kurumu (CNIL) ile birlikte çalışarak, Avrupa Veri Koruma Kurulu tarafından onaylanan ve Avrupa'da genel geçerliliğe sahip veri koruma davranış kuralları (CISPE Davranış Kuralları⁶) oluşturmuştur. Bu Davranış Kurallarının amacı, CISP'lerin GDPR'ye uygunluğu sağlamasına yardımcı olmak ve CISP'lerin müşteri tarafından gerçekleştirilmek istenen kişisel verileri işleme faaliyeti için uygun olup olmadığını değerlendirme konusunda müşterilere rehberlik etmektir.

- Davranış Kuralları münhasıran IaaS sektörüne odaklı olup IaaS sağlayıcılarının özel rol ve sorumluluklarını ele almaktadır.
- Bulut altyapı hizmetleri bağlamında, adil ve şeffaf işleme ile ilgili hususların ve uygun güvenlik önlemlerinin netleştirilmesine yardımcı olmaktadır (GDPR, Madde 40 [2]).
- Müşterilerin, verilerinin AB sınırları içinde kaldığından emin olarak verileri üzerindeki kontrolü nasıl ellerinde tutabilecekleri hakkında bilgi sağlamaktadır.
- Avrupa'da bulut veri hizmetlerinin geliştirilmesini amaçlayan AB GAIA-X girişimini destekleyen veri koruma en iyi uygulamalarını teşvik etmektedir.

CISP'nin, CISPE Davranış Kuralları gibi veri koruma davranış kurallarına uygunluğu, kişisel verilerin GDPR'ye tamamen uygun olarak işleneceğine dair güvence sağlar.

Örnek RFP Metni: Veri Koruma

Teklif veren (doğrudan veya bir satıcı yoluyla) CISP, CISPE Davranış Kuralları gibi veri koruma davranış kurallarına uyma yeteneğini göstermelidir. Veri koruma davranış kuralları, GDPR çerçevesinde belirlenen gerekliliklerle uyumlu olmalıdır. Davranış kuralları asgari olarak şunları içermelidir: (1) CISP'nin net olarak tanımlanmış rol ve sorumlulukları, (2) CISP'nin müşteri verilerini pazarlama veya reklam amaçlarıyla kullanmaması gerekliliği ve (3) müşterilerin, verilerin tamamen Avrupa Ekonomik Alanı sınırları içinde işlenmesine olanak sağlayan CISP hizmetlerini seçme yeteneği. Davranış kurallarına uygunluk, Avrupa Veri Koruma Kurumu tarafından akredite edilmiş bağımsız dış denetçiler (izleme kurumları) tarafından doğrulanmalıdır.

⁶ <https://cispe.cloud/code-of-conduct/>

2.3.1.2 Bulut Sağlayıcısının Değiştirilmesi ve Verilerin Taşınması

Müşteriler kullanmak istedikleri bulut hizmetlerini seçme özgürlüğüne sahip olmalı, belirli bir CISP'ye veya PaaS/SaaS sağlayıcısına "bağımlı" olmamalıdır.

CISP tarafından sağlanan bulut hizmetleri, standarttır ve "birden çoğa" esasına göre sunulur ve hizmetler müşteri tarafından yapılandırılır, tedarik edilir ve kontrol edilir. Bulut bilgi işlemin bir avantajı da müşterilerin kendi benzersiz uygulama ve çözümlerini geliştirmek için ihtiyaç duydukları standart hizmetleri seçme yeteneğine sahip olmasıdır. Bu avantaj, belirli bir zamanda ihtiyaçları en iyi karşılayan yeni veya farklı hizmetlere geçiş yapabilme özgürlüğüne kadar uzanır.

Veri koruma konusunda olduğu gibi, davranış kuralları, şirket içi altyapıdan buluta geçiş yapma ya da CISP'ler arasında geçiş yapma konusunda müşterilere güvence ve güven sağlanmasına yardımcı olur. CISPE, EuroCIO (Avrupa CIO Birliği) ile birlikte çalışıp IaaS bulut hizmetleriyle ilgili olarak veri taşınabilirliği ve bulut hizmetlerinin değiştirilmesi konusunda davranış kuralları (SWIPO IaaS Davranış Kuralları^{7,8}) geliştirmiştir. Davranış kurallarının ilk sürümü, AB'nin Verilerin Serbest Dolaşımına İlişkin Yönetmeliğine uygun olarak geliştirilmiş, Finlandiya'nın AB Başkanlığı döneminde Kasım 2019'da Avrupa Komisyonu'na sunulmuş ve Mayıs 2020'de SWIPO AISBL birliği tarafından yayınlanmıştır. Nisan 2021'de, SWIPO AISBL tarafından davranış kurallarına uygun ilk hizmetler, Mayıs 2021'de de ilk CISPE üyesi hizmetlerinin davranış kurallarına uygun olduğu duyurulmuştur.

Örnek RFP Metni: Bulut Sağlayıcısının Değiştirilmesi ve Verilerin Taşınması

Teklif veren (doğrudan veya bir satıcı yoluyla) CISP, SWIPO IaaS Davranış Kuralları gibi, "bulut sağlayıcısını değiştirme ve verilerin taşınması" ile ilgili davranış kurallarına uyma yeteneğini göstermelidir. Davranış kurallarında, müşterilerin bir CISP'den bir başkasına geçiş yapmaya karar vermesi halinde CISP'nin müşteriler için iş verilerinin güvenli aktarımı olanağını nasıl sağlayacağı ayrıntılı olarak belirtilmelidir.

2.3.2 Satıcıların Karşılaştırılması

Yukarıdaki bölümlerde açıklanan teknik kriterlerde olduğu gibi, bir rekabetçi değerlendirme sırasında bir Bulut Hizmetleri RFP'sindeki asgari güvenlik gerekliliklerine ek olarak, CISP güvenlik özelliklerinin ve hizmetlerinin karşılaştırılmasında esas alınacak kriterlerin sağlanması önemlidir.

Örnek CISP güvenlik gereklilikleri için bkz. *Ek A - İstekliler Arasında Karşılaştırmayla İlgili Teknik Gereklilikler*. Kamu sektörü kurumlarının CISP'leri değerlendirirken aşağıdaki özellikleri temel güvenlik hususları olarak dikkate almaları şiddetle önerilir:

Örnek RFP Metni: Temel Güvenlik Hususları

- CISP'nin, paylaşılan sorumluluk modelini anlaması ve müşterilerin, CISP özelliklerine ve hizmetlerine ilişkin güvenlik sorumluluklarının (örneğin GDPR bağlamında) ayrımını anlamasına yardımcı olacak belgeler
- CISP altyapısının güvenliğini kanıtlanmış başarı geçmişi, CISP güvenlik durumu ve fiziksel/mantıksal kontroller ile ilgili müseccel olmayan, genel erişime açık belgeler
- Bulut güvenliğine özel CISP desteği

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

⁸ <https://swipo.eu/>

- Müşterilerin hesap tasarısını resmîleştirmesine, güvenlik ve bulut yönetişimi kontrollerini otomatik hale getirmesine ve denetimi kolaylaştırmasına olanak sağlayan hizmetler
- Çeşitli kaynakları şablon benzeri bir biçimde oluşturma, tedarik etme ve yönetme özelliği (CISP/CISP-Çözüm Ortağı tarafından oluşturulan altın standart güvenlik şablonları dahil)
- Kontrollerin güvenilir ve tekrarlanabilir şekilde yürütülmesini tesis etme özelliği
- Sürekli ve gerçek zamanlı denetim özellikleri
- Bulut yönetim politikaları için teknik betik oluşturma özelliği
- Değişirme izni verilmeyen kullanıcılar tarafından geçersiz bırakılamayan zorlayıcı fonksiyonlar oluşturma özelliği
- Politikalar, standartlar ve düzenlemelerde daha önce yazılanların güvenilir şekilde uygulanmasını yürütme ve BT ortamları için fonksiyonel ve güvenilir bir bulut yönetim modeli ortaya çıkaran uygulanabilir güvenlik ve uygunluk oluşturma yeteneği
- Yaygın, sık karşılaşılan ağ ve aktarım katmanı dağıtılmış hizmet reddi (DDoS) saldırılarına karşı koruma sağlayan hizmetler ve gelişmiş uygulama katmanı saldırılarını hafifletmek için özelleştirilmiş kurallar yazma yeteneği
- Yönetilen tehdit algılama hizmeti

2.3.3 Sözleşme yapma

Yukarıda belirtildiği gibi, CISP hüküm ve koşulları, bir bulut hizmetleri modelinin nasıl işleyeceğini yansıtacak şekilde tasarlanır (fiziksel varlıklar satın alınmamaktadır, CISP'ler devasa bir ölçekte faaliyet göstererek standart hizmetler sunar). Dolayısıyla, CISP'nin hüküm ve koşullarının mümkün olan azami ölçüde entegre edilmesi ve kullanılması kritik önem taşır. Hüküm ve koşulların yanı sıra sözleşme yapma konusunda daha fazla bilgi için bkz. bölüm 2.5.

Güvenlik söz konusu olduğunda, RFP'nin orijinal parametrelerine uymaları kaydıyla CISP'lerin tekliflerini sürekli olarak güncellemesine ya da tedarikçilerin başvuru bitiş tarihinden sonra ürün eklemesine izin verilmesi şiddetle önerilir. Bu, güvenlik özelliklerinin ve hizmetlerinin hızlı değişim gösterdiği ve CISP'lerin sık sık, çoğu durumda ücretsiz olarak kullanıma sunulan güvenlik odaklı hizmetler yayınlıyor olduğu gerçeğiyle örtüşen bir uygulama olacaktır. Güvenlik tekliflerinde yapılan değişikliklerin güvenliği zedelediğinden emin olmak için bir başlangıç seviyesi güvenlik düzeyinin (yukarıdaki asgari gerekliliklere bakın) tespit edilmesi önemlidir.

Paylaşılan sorumluluk modeli, Bulut Hizmetleri RFP'lerinde doğal olarak güvenliğin ana unsurlarından biridir. Taraflardan her biri kendi güvenlik sorumluluklarını net olarak bilmelidir. Ayrıca CISP'lerden, müşterilerin güvenlik en iyi uygulamalarını geliştirmelerine ve otomatik hale getirmelerine yardımcı olacak belgelerin yanı sıra CISP tarafından sağlanan bulut teknolojileri için CISP/Müşteri güvenlik gerekliliklerini belgelemeleri talep edilmelidir.

Bir Bulut Çerçeve Sözleşmesi, bir satıcının Bulut Hizmetleri RFP'sinde belirlenen asgari güvenlik ve uygunluk gerekliliklerini artık yerine getirmemesi halinde bu satıcıyı çerçeveden çıkarma esnekliğini sağlamalıdır.

2.4 Fiyatlandırma

Kamu sektörü kuruluşları, bulut teknolojisi için dalgalanan talebi dikkate alan bir şekilde sözleşme yapabilmek için, gerekli bulut yönetişimi ve kullanım ile harcamalar üzerinde görünürlük ile birlikte, hizmetleri kullandıkça ödeme yapmalarına olanak sağlayan bir sözleşmeye ihtiyaç duyar.

Buradaki önemli husus, Bulut Hizmetleri RFP'lerinin, elmayla elmayı karşılaştırmak gibi basitçe birim fiyatlarını karşılaştırmak yerine, değere ve toplam sahip olma maliyetine (TCO) bakması gerektiğidir. En düşük birim

fiyatına bakma şeklindeki bu geleneksel uygulama, bulut modeli için geçerli bir yöntem değildir. Zira bu yöntemle belirlenen teklif her zaman, ekonomik açıdan en avantajlı teklife veya en düşük toplam fiyata karşılık gelmez.

*CISP fiyatlandırma değerlendirmesini kolaylaştırmak için ilk önce **asgari fiyatla ilgili gereklilikler** ile CISP ön yeterlilik tespiti yapılmalı veya kısa liste oluşturulmalıdır. Böylece, benzer özelliklere sahip CISP'ler çerçeve sözleşmesine dahil edilmeye hak kazanabilecektir. Daha sonra açık siparişlere ve küçük ihalelere ilişkin değerlendirme sürecinde, tipik kamu sektörü iş yükleriyle eşleşen bir dizi tipik örnek bulut mimarisi ve **fiyatlandırma senaryosu** incelenip CISP'lerden bunlar için fiyat teklif etmesi istenebilir. CISP'ler tarafından bulut teknolojisi hizmetlerinin performansını ve esnekliğini karşılaştırmak için Canlı Test Gösterimleri yapılması da önerilir. Bulut teknolojilerine ilişkin örnek gösterim testi metni için Ek B'ye bakın.*

2.4.1 Asgari Gereklilikler

Bir Bulut Hizmetleri RFP'sinde fiyat bölümü dört temel öge içerir:

1. **Kullanıma Dayalı Fiyatlandırma:** Bulut müşterileri, periyodik ödeme yapılmasını öngören bir kullandıkça öde modelini kullanmaktadır. Bu modele göre her ayın sonunda kullanım miktarları kadar ödeme yaparlar ve bu da hem kullanım hem de kaynak ölçümleri açısından optimum seçenektir.
2. **Şeffaf Fiyatlandırma:** CISP fiyatlandırması genel erişime açık ve şeffaf olmalıdır.
3. **Dinamik Fiyatlandırma:** Bulut fiyatlarının piyasa fiyatlandırmasına bağlı olarak dalgalanmasına izin verme esnekliğini ekleyin. Bulut fiyatlandırmasının dinamik ve rekabetçi doğasından yararlanılan bu yaklaşım, inovasyonu ve fiyat azaltımlarını destekler.
4. **Kontrollü Harcama:** CISP'ler müşterilerin (1) kullanımlarını ve harcamalarını hem özet hem de ayrıntılı olarak izlemesine, (2) kullanım ve harcama özel eşik değerlerine ulaştığında uyarılar almasına ve (3) gelecekteki bulut bütçelerini planlamak üzere kullanım ve harcamayı tahmin etmesine olanak sağlayan raporlama, izleme ve tahmin araçları sunmalıdır.

Örnek RFP Metni: Fiyatlandırma

<KURULUŞ>, başvuran CISP'lerden, son kullanıcılara sağlanan her bir hizmet için teklif ettikleri yöntemi ve fiyatlandırma modelini bir ticari bulut özelliği olarak eklemelerini ister.

CISP aşağıdakileri sağlayacaktır:

- Hizmet tanımı belgesi veya hizmet tanımlarına ilişkin bağlantılar
- Hüküm ve koşullar belgesi
- Fiyatlandırma belgesi (tam fiyat listesinin/fiyat belgesinin talep üzerine temin edilebilir olacağı varsayımıyla halka açık fiyatlandırmaya ilişkin bağlantılar kabul edilebilir)

Fiyat, hizmetin en yaygın yapılandırmasının maliyeti olacaktır. CISP'ler satın alınan hizmetlerin gerçek fiyatını ve alıcıya sağlanacak toplam değeri (örneğin optimizasyon hizmetleri ve sonuç olarak ortaya çıkacak maliyet azalması) belirlemek için hacim tabanlı indirimler ve fiyat hesaplama araçları için seçenekler sağlamalıdır.

Çerçeve Sözleşmesi'ne taraf olan alıcılar, hizmet açıklamalarını, hüküm ve koşullarını, fiyatlandırmalarını veya hizmet tanımı belgelerini/modellerini açıklamaları için tedarikçilerle konuşabilir. Tedarikçilerle yapılan tüm görüşmelerin kaydı tutulacaktır.

Ek Fiyatlandırma Gereklilikleri

- Bulut teknolojilerini, azami iş esnekliğini sunan ve hem ölçeklenebilirliğe hem de büyümeye imkan tanıyan bir dinamik fiyatlandırma modeliyle sağlayın.
- Fiyatlandırma öz nitelikleri aşağıdakileri içermelidir:
 - Fiyatlandırma istek üzerine hizmet, kullanıma dayalı hizmet veya kullandıkça öde hizmeti şeklinde mi sağlanıyor? Fiyatlandırma modelinizi açıklayın.
 - Kullanım taahhüdü verilmesi ve/veya toplu satın alım yapılması halinde ek indirimler uygulanıyor mu? Bunun nasıl yapıldığına ilişkin ayrıntıları belirtin.
 - Fiyatlandırma genel erişime açık ve şeffaf mı? Lütfen genel erişime açık fiyatlandırma bağlantılarını ekleyin.
 - Fiyatlandırma dinamik mi ve piyasa rekabetine hızlı ve verimli yanıt veriyor mu?
 - Harcama takibi için en iyi uygulamalar ve kaynaklar sağlıyor musunuz?
 - Maliyet optimizasyonu için en iyi uygulamalar ve kaynaklar sağlıyor musunuz?

Fiyatlandırma Şeffaflığı

Ticari bulut teknolojilerinde inovasyon ve rekabet nedeniyle fiyatların sürekli iniş trendi içinde olması sebebiyle, <KURULUŞ> tarafından Çerçeve Sözleşmesi kapsamında ödenen sayaçlı CISP hizmeti birim maliyeti hiçbir zaman ilgili hizmet biriminin müşteri tarafından kullanıldığı zamanda yürürlükte olan ve bulut sağlayıcısının web sitesinde yayınlanan bulut sağlayıcısı birim fiyatlandırmasını aşmayacaktır.

Bütçelendirme ve Faturalama Uyarıları/Raporları

CISP'ler, bulut teknolojilerinin sunumunu ve kullanımını göstermek için <KURULUŞ>, maliyetlerin kuruluştaki her bir hesap başına, ürün veya ürün kaynağı bazında ya da müşteri tarafından tanımlanan etiketler bazında saatlik, günlük veya aylık dökümünü veren ayrıntılı faturalama raporları oluşturma araçları sağlamalıdır. <KURULUŞ>, bulut paylaşılan sorumluluk modeli kapsamında, <KURULUŞUN> benzersiz tahmin ve raporlama gerekliliklerini karşılamak için, CISP tarafından sağlanan bütçeleme ve faturalama özellikleri ile araçlarını kullanmaktan sorumlu olacağını kabul eder.

- <KURULUŞUN>, faturalama bilgilerini hem ayrıntılı hem de özet görünümle nasıl görüntüleyebileceğine, zaman içinde CISP kaynakları için yapılan harcamalarda gözlemlenen modelleri nasıl görselleştirebileceğine ve gelecekteki harcamaları nasıl tahmin edebileceğine dair bilgi sağlayın.
- <KURULUŞUN>, kullanım/faturalama görünümünü hizmete göre, bağlı hesaba göre veya kaynaklara uygulanan özel etiketlere göre nasıl filtreleyebileceğine ve hizmetlerin kullanımı, <KURULUŞUN> tanımlandığı eşiklere/bütçelere yaklaştığında veya bunları aştığında bildirimler gönderecek şekilde tasarlanmış faturalama uyarılarını nasıl oluşturabileceğine dair bilgi sağlayın.
- <KURULUŞUN>, geçmişteki kullanımına dayalı olarak, tanımlı bir tahmin periyodu içinde ne kadar bulut hizmeti kullanacağını nasıl tahmin edebileceğine dair bilgi sağlayın. CISP, <KURULUŞUN> CISP faturasına ilişkin bir tahmin sunabilmelidir ve <KURULUŞUN> maliyet ve harcama üzerinde daha fazla yönetişime sahip olabilmesi için, kullanacağı tahmin edilen miktarlara ilişkin alarmlar ve bütçeler kullanmasına olanak sağlamalıdır.

2.4.2 Satıcıların Karşılaştırılması

Kamu sektörü kuruluşları genellikle en iyi değer, ekonomik açıdan en avantajlı teklif (EAEAT) veya en düşük fiyat gibi değerlendirme kriterlerini kullanarak istekliler arasında rekabet oluşmasını ister. Çerçeve sözleşmesi kapsamındaki açık siparişlerin veya küçük ihalelerin fiyatlandırması için planlama yapılırken, bulutun benzersiz özelliklerini dikkate alan bir yaklaşım geliştirilmesi önemlidir. Örneğin bulut sağlayıcılarının tekliflerini sadece ürün kalemleri (ör. bilgi işlem veya depolama) açısından karşılaştırmak, tekliflerin karşılaştırılması için etkin bir yöntem değildir çünkü bu yöntemde performans, bulut temelli hizmetler ve CISP izleme araçları kullanılarak elde edilen maliyet optimizasyonu veya CISP'lerin ücretsiz

olarak sunabileceği öne çıkan hizmetler gibi özellikler dikkate alınmamaktadır. Ek olarak, bir CISP'nin katalog fiyatı on binlerce ürün kaleminden oluşabilir ve fiyatlandırma modelleri bir hizmetten diğerine ve bir sağlayıcıdan diğerine farklılık gösterir.

TCO'yu Analiz Edin

Tanımlanan kullanım örnekleri için bir bulut çözümünü tüm yönleriyle (çözüm ortağı hizmetleri, standart CISP indirimleri, performansı artırabilecek ve maliyetleri azaltabilecek/optimize edebilecek teknik özellikler vb.) dikkate alan toplam sahip olma maliyetine (TCO) odaklanılması önerilir.

Senaryolar Bazında Karşılaştırın

Değerlendirme sürecinde genel sistemlere veya uygulamalara karşılık gelen tipik senaryolar da dikkate alınabilir. Bu tür senaryolar (web barındırma veya x kullanıcıları bir insan kaynakları sisteminin uygulanması vb.) kaynakların hızı ve ölçeği, uygulama veya çözümün performansı, depolama alanına erişim süreleri, yüksek hacimli basit bilgi işlem görevlerine kıyasla düşük hacimli karmaşık veriler vb. değişkenler içerebilir. Uygulamalar veya sistemler; vergi iade dönemleri, sel uyarıları gibi acil durum bildirimleri vb. sırasında yüksek hacimde verinin işlendiği tipik senaryolara da sahne olabilir. Senaryolar tüketicinin proje sırasında kullanabileceği teknoloji ve hizmetlerin kapsamını içerecek kadar geniş kapsamlı olmalıdır. Böylece, müşteri projenin toplam tahmini maliyetini karşılaştırabilir.

Senaryoları Finansal ve Teknik Olarak Karşılaştırın

CISP tekliflerinin fiyatlarını karşılaştırırken teknik avantajların dikkate alınması da önemlidir. Örneğin bir CISP, bir coğrafi bölge sınırları içindeki kümelerde veri merkezlerine sahip olma modeli sayesinde, müşterilerin bir aktif-aktif Olağanüstü Durum Kurtarma (DR) topolojisi oluşturmaya olanak sağlayabilir. Bu tür bir yedekliliğe ve veri merkezi yapılandırmasına sahip olmayan bir CISP, olağanüstü durum kurtarma ihtiyaçlarının maliyeti dikkate alındığında %x daha pahalı olabilir. Ek teknik özellikler içeren bütüncül bir fiyatlandırma yaklaşımının, CISP'leri değerlendirmede neden büyük önem taşıdığına dair bir örnek olarak, aşağıdaki "elmayı elmayla" karşılaştıran düz karşılaştırma alternatifini düşünün.

Örnek: Bir müşteri, çerçeve sözleşmesinde yeterliliğe sahip CISP'ler tarafından sağlanan nesne depolama fiyatlarını karşılaştırmak istiyor. Depolama "birimi" ögesinin fiyatı CISP 1'de 0,023 EUR/GB'dir. Aynı birimin CISP 2'deki fiyatı 0,01 EUR/GB'dir. Düz bir birim-birim karşılaştırmasında, müşteri aşağıdaki gibi kritik soruları sormayacaktır:

1. Hata durumunda nesnenin kaç yedekli kopyası bulunur? Yukarıdaki örnekte, CISP 1, iki farklı tesiste eş zamanlı veri kaybına uğrayabilecek şekilde tasarlanmıştır ve verilerin birden fazla kopyasını tutmaktadır. CISP 2'de ise yedekli kopyalar oluşturulmamaktadır.
2. Depolanan nesnelerin sürdürülebilirlik düzeyi nedir? CISP 1'de %99,999999999, CISP 2'de %99'dur.
3. Genel projenin veya iş yükünün sahip olma süreci boyunca ortaya çıkacak maliyetini ve verilerin depolanması ve kullanımı konusunda maliyet optimizasyonu özelliklerinin maliyetleri nasıl azaltabileceğini dikkate alın (örneğin Sunucusuz işlevlerinin kullanımının artırılması maliyetleri %x oranında azaltabilir).

Bunlar fiyatlandırmayı etkileyen, özellikle güvenlik ve uygunluk ile ilişkili birçok teknik husustan sadece birkaçıdır.

Fiyatlandırma senaryolarıyla ilgili hususlar aşağıdakileri içerir:

Temel oranlar: Bunlar CISP'lerin halka açık fiyatlarıdır. CISP'ler bu fiyatları genel erişime açık olarak sağlamalıdır. Ancak, yukarıda belirtildiği gibi, CISP'lerin etkin bir şekilde karşılaştırılması için müşteriler belki de 3-5 (veya müşteri için kaç adet gerekiyorsa) spesifik senaryonun tüm satıcılar tarafından fiyatlandırılmasını isteyebilir. Senaryolar, müşterinin proje süresi içinde kullanması muhtemel hizmet ve teknoloji yelpazesini içine alacak kapsamda olmalıdır. Böylece, müşteri projenin toplam tahmini maliyetini karşılaştırabilir. Ürün kalemi/SKU düzeyindeki karşılaştırmalar, müşteriler ve satıcılar açısından genellikle faydalı olmaktan ziyade daha fazla soruna yol açmaktadır. (Bu durumda, her ne kadar gerçek fiyat yalnızca hizmet tüketimine bağlı olarak belirlense de müşteriler tüm CISP'ler genelinde on binlerce ürün kalemini karşılaştırmak, satıcılar ise bu düzeyde ayrıntıları sağlamak ve yönetmek zorunda kalır.)

En iyi değeri arayan bulut müşterileri için bir CISP'nin genel özellik setinin değerlendirilmesi elzemdir. Örneğin CISP'ler ücretsiz olan veya esasen ücretsiz sayılabilecek birçok hizmet sunuyor olabilir. Fiyatlandırma değerlendirmesinde bu tür hizmetler sunulduğu ve diğer CISP'lerin benzer işlevsellikler için ücret talep edebileceği dikkate alınmalıdır.

Değerlendirme kriterleri, CISP'lerin "x varsayılan olarak dahil" özellikleri ve bu tür hizmetlerin genel olarak maliyeti nasıl etkilediğini belirtmesine olanak sağlayacak şekilde yazılmalıdır. Değerlendirme kriterlerinde ayrıca Rezerve Edilmiş Bulut Sunucuları/Spot Bulut Sunucuları gibi CISP'nin hacim temelli/katmanlı fiyatlandırmasına ve ticari indirimlerine de bakılabilir. Örneğin:

- Müşterilerin rezerve edilmiş bilgi işlem kapasitesi (1 yıl, 3 yıl vb.) satın alması halinde %x tasarruf
- Katmanlı/hacim temelli fiyatlandırmada %x indirim
- Mimari incelemelerine ve daha uygun bilgi işlem seçeneğine geçiş gibi altyapı optimizasyonuna dayalı %x tasarruf
- Yukarıda belirtildiği gibi, tüm yaşam döngüsü maliyetini ve maliyet optimizasyonu özelliklerinin maliyeti nasıl azaltabileceğini dikkate alın.

FİYATLANDIRMA SENARYOSU

İstekliler yalnızca değerlendirme amaçları doğrultusunda aşağıdaki senaryo için fiyatlandırma sağlamalıdır. Gerçek fiyat, istek üzerine kullandıkça öde modeline göre hizmet tüketimine bağlı olacaktır.

Aşağıda fiyat keşfi için temsili gereklilikler sunulmaktadır. Bu gereklilikler, sözleşme süresi boyunca bu nominal gerekliliklerin değişeceği varsayımına göre şekillendirilmiştir. Lütfen 12 ve 36 aylık istek üzerine kapasite, ayrıca 12 ve 36 aylık rezerve edilmiş kapasite için fiyatlandırma sağlayın.

Aşağıdakileri belirtin:

- Teklif edilen çözümlerin adı:
- İsteklinin en iyi fiyatlandırması:
- Hizmet Saati: 7x24x365
- Hizmet Erişilebilirliği: %99,95

Fiyatlandırma senaryoları, CISP izleme ve optimizasyon araçlarını kullanarak, optimize edilmiş bulut temelli çözümleri benimseyerek ve CISP fiyat azaltımlarından yararlanarak harcamalarını 1/2/3 yıl içinde optimize etmiş, benzer iş yüklerine sahip mevcut müşterilerden örnekler içerebilir.

2.5 Sözleşme Yürütme Planı/Hüküm ve Koşullar

CISP tarafından sağlanan bulut teknolojileri ve operasyonları, tasarımları gereği standart olduğundan sözleşme koşulları da standarttır. Ancak, yerel mevzuat ve düzenleyici gerekliliklerine uyarlamak için bu sözleşmelerde küçük değişiklikler yapılması mümkündür.

Geleneksel BT ihale yöntemlerinde genellikle başvuranların ihalenin çoğu veya tüm gerekliliklerine uymasını gerektiren katı kurallar bulunur ve bu gerekliliklere uymayan başvuranlar reddedilir. Bazı durumlarda ise katı bir zorunlu gereklilik alt kümesi içerirler. Bir özel çözüm geliştirmenize yardımcı olan ve esasen standart bir bileşen ve araç kümesinden oluşan bulut teknolojileri için bu tür bir satın alma yöntemi kullanıldığında ihaleler genellikle başarısızlıkla sonuçlanmaktadır.

2.5.1 Hüküm ve Koşullar

Bir Bulut Hizmetleri RFP'si kapsamında sözleşme yapmadan önce atılması gereken ilk adım, çoğu durumda CISP'lerin web sitelerinde genel erişime açık olarak yayınlanan mevcut CISP ticari hüküm ve koşullarını inceleyip anlamaktır. Kamu sektörü kurumları, CISP'lerin teklif ettiği ticari hüküm ve koşulları kabul etmede gün geçtikçe daha rahat bir tutum sergilemektedir. Hüküm ve koşulları anlamaya dönük bu çalışmanın bir diğer amacı da CISP'ler ve onların çözüm ortaklarıyla toplantılar düzenleyerek yaklaşımlarını ayrıntılı olarak incelemektir. Sorulması gereken kilit soru, CISP'lerin "neden" belirli hüküm ve koşullarla çalıştıklarıdır. Bu hüküm ve koşullardan bazıları geleneksel BT hüküm ve koşullarından farklı görünebilir ancak bunların bir bulut sözleşmesine dahil edilmesinin çok spesifik nedenleri bulunur. Genel erişime açık olarak yayınlanan hüküm ve koşulların kabul edilemez olduğu durumlarda, CISP'ler genellikle kurumsal müşteriler için küçük değişikliklerin yapılabileceği sözleşmeler sunabilmektedir. Bunlar da incelenebilir.

CISP hüküm ve koşullarının incelenmesinin yanı sıra mevcut politikaların, düzenlemelerin ve/veya yasaların (ör. teknoloji, veri sınıflandırması, gizlilik, personel vb. konulara ilişkin olanlar) anlaşılması da önem arz eder. Çoğu zaman geleneksel BT tekliflerinin satın alımı ve kullanımı için tasarlanmış mevcut politikalar/düzenlemeler/yasalar bulunur ve bunlar bir CISP'nin modeliyle uyumsuzluk içinde olabilir. Örneğin yalnızca Bulut Hizmetleri RFP'si yoluyla orijinal Çerçeve Sözleşmesi teklifine dahil edilmiş olan bulut teknolojilerinin kullanımına izin verilmesi bu tür uyumsuzlıklardan biridir. CISP'ler sürekli olarak yeni hizmetler ve özellikler ekler. Sırf geleneksel bir BT ürünü yenileme yaklaşımını izlediğiniz için bu tür yeni hizmetlere erişimin önünü kesmeniz son müşteri açısından anlamlı bir uygulama değildir. Bu durumda, CISP'lerle ayrıntılı görüşmeler yapılması ve görüşmeler sırasında bu tür politikalara/düzenlemelere ve/veya yasalara bakılması önemlidir.

RFP Öncesi Tartışmalardan Yararlanma

Yukarıda ifade edildiği gibi, bir RFP kaleme almadan önce zaman ayırıp CISP'ler ve ilgili satıcılar ile görüşmeler yaparak onların hüküm ve koşullarını öğrenin ve kurumunuzun yaklaşımı, politikalar, düzenlemeler ve yasalar konusunda kendilerini bilgilendirin. Bu görüşmelerin en önemli yanı, her iki tarafın da ilgili ekiplerin "neden" mevcut çalışma şekilleriyle çalıştıklarını öğrenmesidir. Örneğin bulut hüküm ve koşulları geleneksel veri merkezi, yönetilen hizmet, donanım, ambalajlı yazılım ve sistem entegrasyonu için kullanılan hüküm ve koşullardan farklıdır. Tek model olmaları ve sürekli inovasyon içermeleri nedeniyle, iş modelleri RFP sürecinin netleştirici bilgi almak üzere müzakereler veya görüşmeler düzenlenmesine izin verecek kadar esnek olmasını gerektirir.

Kamu sektörü kuruluşları, hüküm ve koşulları müzakereler veya görüşmeler sırasında netleştirme yeteneğini dahil ederek, bulut modelleri hakkında daha iyi bir anlayış edinir ve aslında ilgili kuruluşun ihtiyaçlarını

karşılayabilecek nitelikte olan sağlayıcıların reddedilmesi sorununu önleyebilir. Tipik olarak kuruluş, ihaleyi vermeden önce tartışmak ve müzakere etmek istediği belirli hüküm ve koşulları önceden tanımlayabilir. Kuruluş, kabul edilebilir nitelikteki hüküm ve koşulları isteklilerle önceden müzakere ederek ihaleyi vermek için en uygun teklifi tespit etmiş ve aksi halde etkili bir teklifin reddedilmesiyle sonuçlanabilecek farklılıkları çözüme kavuşturmuş olur. Kamu sektörü kurumları politikalarını, düzenlemeleri ve yasaları inceleyebilir ve her iki taraf da bulut kullanımının bu modellerin bağlamına nasıl uyacağını anlayabilir. Çoğu zaman mevcut maddelerle çalışılması mümkündür. Ancak, sorunlu bir alan varsa her iki ekip bir çözüm bulmak için birlikte çalışabilir (bu görüşmelerin RFP'den ve müteakip sözleşme müzakerelerinden çok önce yapılması faydalı olacaktır).

Müzakere Esnekliği

CISP'nin standart sözleşme hüküm ve koşullarını kullanarak yerel mevzuata uygun olarak sözleşme akdedilebilmesi için şunların yapılması önerilir: (1) başvuranlardan standart sözleşmelerini sunmalarını isteyin, (2) Bulut Hizmetleri RFP'si için çerçeve sözleşmesini oluştururken uygun olmayan sözleşme koşulları eklemeyin ve (3) çerçeve sözleşmesi ile sonuçlanacak istişarelerin ve tekliflerin tüm hükümlerinin (tabii ki yasalar uyarınca zorunlu olan bağlayıcı maddeler hariç) müzakere edilebilmesi seçeneğini ekleyin.

Not: Paylaşılan sorumluluğun kapsamı bulut modelinin içsel özelliklerinden biridir ve hüküm ve koşullarda yansıtılmalıdır (ör. CISP, müşteri verilerinin, bulunduğu konumda müşterilere ait olduğunu onaylar ve veri konumu seçiminin sınırlı olduğundan emin olmak için araçlar sağlar **ANCAK** bu araçları kullanmak müşterinin veya çözüm ortağının sorumluluğundadır).

*Bir Bulut Çerçeve Sözleşmesi'ndeki LOTLARDAN her biri için **farklı sözleşme hüküm ve koşul** setleri bulunmasının önemli olduğunu unutmayın. Tüm Lotlarda sözleşme yapımı için "ortak" bir yaklaşım izlenmesi teknik fizibilite ve uyumluluk açısından sorunlara yol açacaktır.*

Daha önce belirtildiği gibi, müzakere edilemez zorunlu hüküm ve koşullar içeren RFP'ler, sağlayıcılar perspektifinden bakıldığında esasen "olduğu gibi kabul et ya da bırak" anlamına gelir ve normalde kabul edilebilir bir teklifin reddedilmesiyle sonuçlanabilir. Kamu sektörü kuruluşları, **yasalar uyarınca zorunlu olmadıkları sürece**, zorunlu hüküm ve koşullar kullanmanın sonuçlarını dikkatli bir şekilde değerlendirmelidir. Bir gereksinimin veya hüküm ve koşulun zorunlu olarak sınıflandırılması halinde ileride müzakere edilmesi engellenmiş olacağından, kuruluşlar zorunlu bir gereksinime veya hüküm ve koşula gerçekten ihtiyaç duyulup duyulmadığını net olarak belirlemelidir. Kuruluşun en iyi teknolojiyi ve çözümü edinmek için ihtiyaç duyduğu esnekliğe kavuşabilmesi için zorunlu gereksinimlerin veya hüküm ve koşulların kullanımı mutlak surette en aza indirilmelidir.

CISP bulut teknolojilerinin tamamen standart olduğunu ve tam otomatik bir şekilde sunulduğunu aklınızda bulundurun. Bu nedenle, hüküm ve koşullarda, altta yatan hizmette özelleştirme yapılmasını gerektirecek herhangi bir değişiklik yapamaz. Ayrıca, hizmetlerin fiyatları genellikle genel erişime açık şekilde yayınlanmaktadır ve tüm kullanıcılar için standarttır. Bu da bir CISP'nin belirli bir müşteri adına daha fazla risk almak için fiyatlandırmada ayarlama yapamayacağı anlamına gelir.

Dolaylı Satın Alımlar

Doğrudan bir CISP'den bulut teknolojileri satın almaya alternatif bir seçenek de bunları CISP yerine bir CISP satıcısından satın almaktır. CISP Satıcıları hakkında daha fazla bilgi için bkz. bölüm 2.1.3.

Örnek RFP Metni: Hüküm ve Koşullar

CISP'ler veya temsilci satıcılar, genel erişime açık hüküm ve koşullarını sunmalı ve <KURULUŞ> tarafından sağlanan temel hüküm ve koşullara ilişkin geri bildirim sağlamalıdır.

<KURULUŞ>, başarılı isteklinin sözleşme hüküm ve koşullarına bağlı olarak bu istekli ile yazılı bir sözleşme imzalamak istemektedir. İstekli, kendi en iyi ticari ve yasal teklifini temsil eden bir sözleşme hüküm ve koşulları setini incelemesi için <KURULUŞ> sunmalıdır. Teklif verenler ve <KURULUŞ>, <TARTIŞMA/MÜZAKERE> safhasında her iki hüküm ve koşul setini görüşebilir.

- Genel Çerçeve Ana Hüküm ve Koşulları azami olarak aşağıdaki bileşenlerden oluşur:
 - Çerçevenin süresi
 - Çerçeve yönetişi
 - Çerçevenin ifası
 - Çerçevenin feshi
 - Çerçevenin kapsamı
 - Sipariş verme süreci
 - Gizlilik hükümleri
 - Kategoriye özgü fikrî mülkiyet ve bilgi
 - CISP'ler tarafından karşılanması gereken asgari teknik gereklilikler, ör. kalite standartları, akreditasyon, güvenlik ve veri koruma
- Çerçeve Sözleşmesi lotlarının her biri için farklı hüküm ve koşullar bulunacaktır.
- CISP hizmeti ile ilgili spesifik konular açık siparişte değerlendirilip ele alınacaktır.
- Sözleşme değişikliklerine izin verin. Hüküm ve koşullar, müşterilerin ve tedarikçilerin sözleşmede değişiklikler yapmasına ve yeni hizmetler veya geliştirmeler eklemesine mani olmamalıdır. Bulut hizmetleri, sürekli değişen yapısı gereği, tamamı müşterilere verimlilik artışı sunulmasına yardımcı olabilecek sürekli hizmet geliştirmelerine konu olabilir.
- Hizmet Düzeyi Sözleşmeleri (SLA'lar) müşteri tarafından belirtilmemelidir. Müşteri hüküm ve koşulları CISP'nin standart hizmet sunumu modellerinden farklılık gösteren, komisyona özel, sipariş üzerine SLA'lar tanımlamamalıdır. CISP'lerin standart SLA'larına izin verilmesi halinde, CISP'ler maliyetleri düşük tutabilecek, bunları müşterilere aktarabilecek ve müşteriler de CISP'nin SLA'yı karşılayabileceğine güven duyacaktır.
- Yükümlülük sınırlamaları orantılı bir şekilde belirlenmelidir. Yükümlülük, satın alınan hizmetlerle orantılı olmalıdır ve yükümlülük sınırları orantısız şekilde yüksek belirlenmemelidir. Sınırların orantısız şekilde yüksek belirlenmesi, CISP'leri düşük tutarlı projeleri kabul etmekten caydıran bir unsura dönüşebilir. Bu projeler genellikle müşterilerin belirli bulut çözümlerinin kuruluşları açısından etkili çözüm sağlayıp sağlamayacağını belirlemesine olanak veren, giriş niteliğinde, "test amaçlı", faydalı projeler görevi görür.
- Müşterilerin verileri, müşterilerin mülkiyetinde olmalıdır. Müşteriler verilerini kontrol altında tutmalı, verilerinin mülkiyetini elinde bulundurmalı ve verilerinin tutulacağı coğrafi konumu belirleme yeteneğine sahip olmalıdır. Bu durum, müşterilerin satıcı bağımlılığını önlemesine ve verilerini farklı sağlayıcılara serbestçe taşımasına olanak verecektir.

2.5.2 Yazılım Hüküm ve Koşulları

Bu el kitabı CISP'ler tarafından sağlanan IaaS ve PaaS bulut teknolojilerinin satın alımına odaklı olsa da kamu sektörü kuruluşlarının satıcılardan yazılım satın alırken göz önünde bulundurabileceği yazılım hüküm ve koşullarının vurgulanması önemlidir. İyi yapılandırılmış bir Bulut Hizmetleri RFP'si kapsamında nasıl yazılım satın alınabileceğini incelemek için lütfen Şekil 1'e (sayfa 5) bakın.

Yazılım, kamu sektörü dahil olmak üzere neredeyse her işletmenin faaliyetlerinde kritik bir rol oynar. Bir Bulut Hizmetleri RFP'sine Yazılım Lisanslama Hüküm ve Koşulları gibi yükümlülüklerin eklenmesi, kamu sektörü kurumlarının yazılım satın alırken en iyi değeri bulmasına ve satıcılar arasından seçim yapabilme özgürlüğüne sahip olmasına yardımcı olur.

Daha fazla bilgi için bkz. Ten Principles of Fair Software Licensing for Cloud Customers⁹. Bu ilkeler, önde gelen Fransız şirketleri ile dijital teknoloji kullanıcılarını temsil eden kamu idarelerinden oluşan bir birlik olan Cigref¹⁰ tarafından CISPE ile iş birliği içinde ve diğer Avrupalı CIO ve Sağlayıcı ticaret birliklerinin desteğiyle hazırlanmıştır. İlkeler, her ölçekten kuruluşun buluta geçiş sürecinde kuruluşun dijital dönüşümüne zarar verdiği düşünülen uygulamaları ele almaktadır.

Örnek RFP Metni: Yazılım

<KURULUŞ>, başarılı isteklinin sözleşme hüküm ve koşullarına bağlı olarak bu istekli ile yazılı bir sözleşme imzalamak istemektedir. İstekli, kendi en iyi ticari ve yasal teklifini temsil eden bir sözleşme hüküm ve koşulları setini incelemesi için **<KURULUŞ>** sunmalıdır. Yazılım Satıcıları ve **<KURULUŞ>**, **<TARTIŞMA/MÜZAKERE>** safhasında her iki hüküm ve koşul setini görüşebilir.

Gereklilik 1.0. Yazılım satıcıları, maliyetlerin özet ve ayrıntı düzeyinde dökümünü içeren net lisanslama hüküm ve koşulları sağlamalıdır.

Gereklilik 1.1. Lisans hüküm ve koşullarına herhangi bir şekilde uyulmamasından doğacak tüm maliyetler özet ve ayrıntı düzeyinde belirtilmelidir.

Gereklilik 2.0. Yazılım lisansları **<Kuruluş>**, lisanslanan yazılımı, aynı yazılım için ayrı, yinelenen lisanslar satın almak zorunda kalmaksızın şirket içinden dilediği buluta taşıma yeteneğini sağlamalıdır.

Gereklilik 2.1. Yazılım lisansları **<Kuruluşun>**, lisanslanan yazılımı dilediği bulutta çalıştırma yeteneğini kısıtlayacak nitelikte lisanslama kısıtlamaları ve maliyet artışları içermemelidir.

Gereklilik 3.0. Yazılım lisansları **<Kuruluşun>**, lisanslanan yazılımı kendi donanımında (genellikle "şirket içi" yazılım olarak anılır) ve dilediği bulutta çalıştırmasına izin vermelidir.

Gereklilik 4.0. Yazılım lisansları, lisanslanan yazılımın sadece **<Kuruluş>** tahsis edilmiş donanım üzerinde çalıştırılmasını şart koşmamalıdır.

Gereklilik 5.0. Yazılım satıcıları, satıcının lisanslanan yazılımının başka bir satıcının bulut teklifi üzerinde kullanılması halinde, örneğin artan sıklıkta veya izinsiz ve davetsiz yazılım denetimleri gerçekleştirme ya da daha yüksek yazılım lisanslama ücretleri uygulama yönünde haklar eklenmesi suretiyle **<Kuruluş>** cezalandırmamalıdır.

Gereklilik 6.0. Dizin yazılımı; kullanıcı kimliklerinin, diğer kimlik hizmetleri için ayrımcılık yapmayan bir şekilde eşitlenmesi ve doğrulanması için açık standartları desteklemelidir.

Gereklilik 7.0. Yazılım satıcıları, sadece yazılımın yüklendiği donanımın sahibine bağlı olarak aynı yazılım için farklı fiyatlar talep etmemelidir.

Gereklilik 7.1. Yazılım fiyatları; yazılımın **<Kuruluşun>** kendi veri merkezine, bir üçüncü tarafın yönetimindeki veri merkezine, bir üçüncü taraftan kiralanmış bilgisayarlara ya da **<Kuruluşun>** seçtiği bulut sağlayıcısına yüklenmesine göre farklılık göstermemelidir.

⁹ <https://www.fairsoftware.cloud/principles/>

¹⁰ <https://www.cigref.fr/>

Gereklilik 8.0. Sözleşmenin süresi boyunca yazılım satıcıları, yasalar uyarınca ya da güvenlik endişeleri nedeniyle zorunlu olmadığı sürece, lisans hüküm ve koşullarında, <Kuruluşun>, yazılımı daha önce izin verilen kullanım amaçları doğrultusunda kullanmasına kısıtlama getirecek maddi değişiklikler yapmamalıdır.

Gereklilik 9.0. <Kuruluşun>, yazılımı <Kuruluş Gerekliliklerinde> belirtilen kullanım amacı doğrultusunda kullanabilmesi için ek lisanslar satın alması gereken durumlarda yazılım satıcıları, yazılım lisanslarının <Kuruluşun> yazılımı kullanma amacını karşılayacağını beyan ederek <Kuruluşu> yanlış yönlendirmemelidir.

Gereklilik 10.0. <Kuruluşun>, yazılım lisanslarını satma ve devretme hakkının bulunuyor olması halinde, yazılım satıcıları, yeniden satışa sunulan bir lisansı yasalara uygun olarak satın almış olan bir <Kuruluşa> adil hüküm ve koşullar altında destek ve düzeltme paketleri sunmaya devam etmemelidir.

2.5.3 Proje Bazında İstekliler Arasından Seçim Yapılması

Çerçeveye taraf olan kamu sektörü kurumları, ihtiyaç duydukları hizmetleri istedikleri zaman sipariş edebilir veya bunlar için "açık sipariş" verebilir. Bir çerçeve sözleşmesine bir açık sipariş sözleşmesinin dahil edilmesi, alıcıların bir yandan açık sipariş sözleşmesi için ek fonksiyonel şartname ile gereklilikleri düzeltmesine, diğer yandan çerçeve sözleşmesi altında sunulan avantajlarını elinde tutmasına olanak sağlar.

Gerekli görülmesi halinde, belirli bir iş yüküne veya projeye en uygun tedarikçiyi belirlemek için küçük bir ihale düzenlenebilir. Küçük ihalede, müşteri bir lot içindeki tüm tedarikçileri bir dizi gerekliliğe yanıt vermeye davet ederek çerçeve kapsamında ek rekabet sağlayabilir. Müşteri, lot içindeki yeterliliğe sahip tüm tedarikçileri teklif vermeye davet eder ve böylece her lot altında yüksek standartta seçenekler elde edilir. Bir Bulut Hizmetleri RFP'sinde isteklilere ilişkin asgari gerekliliklerin önemi de burada yatmaktadır.

Bir kez daha belirtmek gerekirse Teklif Türü lot kategorilerinden (ör. Genel IaaS/PaaS, Topluluk için IaaS/PaaS, Özel IaaS/PaaS) her biri için farklı sözleşme hüküm ve koşul setleri bulunmasının önemli olduğunu unutmayın. Zira tüm lotlarda sözleşme yapımı için "ortak" bir yaklaşım izlenmesi teknik fizibilite ve uyumluluk açısından sorunlara yol açacaktır.

İstekliler arasından seçim yapılmasına ilişkin örnek RFP metni için bkz. bölüm 2.1.4.

2.5.4 Katılım ve Çıkış

Bir Bulut Çerçeve Sözleşmesi oluşturulurken Dinamik Satın Alma Sistemi (DPS) seçeneği göz önünde bulundurulmalıdır. DPS modelinde, Çerçeve Sözleşmesi'nin asgari gerekliliklerini karşılayan tüm satıcılar Çerçeveye kabul edilir. Çerçeveye katılabilecek satıcı sayısına ilişkin bir sınır bulunmaz ve geleneksel çerçeve modelinin aksine, satıcılar "DPS Çerçevesi"nin süresi boyunca herhangi bir zaman noktasında bu çerçeveye katılmak için başvuruda bulunabilir.

Kamu sektörü kuruluşlarının yeterliliği tespit edilen satıcılardan alınacak hizmetlere ilişkin kaliteyi ve güvenceyi sağlamak üzere yüksek standartlar belirlemesi fakat CISP'lerin adil rekabeti tehlikeye atacak bir şekilde elenmesini önlemek için aşırı spesifik olmaması şiddetle önerilir. Nihai hedef bir yandan erişilebilir bulut teknolojilerinin standardını yüksek tutarken, diğer yandan son kullanıcıyı çok fazla seçenekle boğmamaktır.

3.0 En İyi Uygulamalar/Çıkarılan Dersler

Aşağıda, iyi yazılmış bir Bulut Hizmetleri RFP'siyle bir Bulut Çerçeve Sözleşmesi'nin nasıl başarıyla hayata geçirilebileceğine dair çıkarılan bazı dersler açıklanmaktadır.

3.1 Bulut Yönetişimi

Bulutta yönetim, paylaşılan bir sorumluluktur. CISP'ler bulut yönetişiminin bir bulut ortamına her yönden entegre edilmesine yönelik özellikler ve hizmetler sağlarken, müşteriler de mevcut bulut yönetişimi standartlarını beraberlerinde getirir ve bulutun, bulut yönetişimine nasıl olanak tanıdığını öğrenir.

Bulutta, müşteriler sadece sahip oldukları BT ortamını yönetmenin yanı sıra istedikleri BT ortamını oluşturma şansına sahip olur. Bulut sayesinde müşteriler: (1) tüm BT varlıklarının yer aldığı tam bir envanterle yola çıkabilir, (2) bu varlıkların tümünü merkezi olarak yönetebilir ve (3) kullanım/faturalama/güvenlik vb. hakkında uyarılar oluşturabilir. Bulutun tüm bu hayati avantajları, müşterilerin sürekli olarak yeni donanım temin edip kurmaya gerek kalmadan, optimize edilmiş ve mümkün olan en üst düzeyde otomatikleştirilmiş bir mimariye sahip olmasına yardımcı olur. Tüm bunların bulut hizmetleri sağlayıcısı (CISP) tarafından yapılması, müşterilerin tekdüze altyapı yönetimi işlerine zaman harcamak yerine, görev açısından kritik olan operasyonel seviyeye odaklanmasına olanak tanır.

Bir CISP bulutunu devasa büyüklükteki bir API gibi düşünebilirsiniz. Yeni bir sunucu başlatma veya bir güvenlik ayarını değiştirme gibi tüm işlemleri API çağrıları aracılığıyla yaparsınız. Ortamdaki her değişiklik günlüğe işlenir ve kaydedilir (her değişiklik için kim, ne, nerede ve ne zaman bilgileri kaydedilir). Sonuç olarak, yalnızca bir bulut ortamında mümkün olan yönetim, denetim ve görünürlük elde edilir. Bu, müşterilerin mevcut BT yönetim modellerini yeniden düşünmesine ve bulutun beraberinde getirdiği avantajlarla bu modellerin nasıl geliştirilebileceğini belirlemesine olanak sağlar.

Bulut yönetişimi ayrıca bulutla birlikte gelen olumlu süreç değişikliklerinin ve yeni beceri setlerinin aktarılmasını ve dahil edilmesini içerebilir. Örneğin proje yöneticileri bir BT ortamının geliştirilmesini aylarca beklemeye alışkındır ve dolayısıyla bulutta bir geliştirme veya test ortamı oluşturulması için gereken süre (bulutta bu işlem sadece dakikalar içinde tamamlanır) olduğundan çok daha uzun tahmin edebilirler. Bu yeni keşfedilen çeviklik evrimsel bir süreç şeklinde gelişir ve program bazında elde edilir. Çıkarılan bu tür dersler paylaşarak Bulut Çerçeve Sözleşmesi'nin yeni süreçler ve çeviklik için uygun gereklilikleri içerecek şekilde gelişip değişmesi sağlanmalıdır.

3.2 Bulut İçin Bütçelendirme

Kullandıkça öde bulut fiyatlandırmasını kamu sektörü satın alma ve bütçelendirme gerekliliklerine uygun şekilde yapılandırma söz konusu olduğunda, CISP hizmetlerinin tamamının **Bulut Teknolojileri** adlı bir ürün kalemi altında olacak şekilde, tek bir ürün kalemi (bilgi işlem, depolama, ağ iletişimi, veritabanı, IoT vb.) altında birlikte paketlenmesinin yararlı olabileceğini tespit ettik. Bu yaklaşım tüm mevcut ve yeni CISP teknolojilerini kullanıcılara gerçek zamanlı olarak sunma esnekliğini sağlar ve kullanıcılara ihtiyaç duydukları kaynaklara ihtiyaç duydukları anda hızla erişme imkanı verir. Ayrıca dalgalanan talebi uygun şekilde yöneterek, optimize edilmiş kullanım ve düşük maliyetler sağlar.

Kamu sektörü kuruluşları; danışmanlık hizmetlerine, profesyonel veya yönetilen hizmetlere, bir pazar yerinden yazılıma, bulut destek hizmetlerine ve CISP'nin teklifleri konusunda eğitime gerek duymaları halinde, siparişler için bir bulut çerçevesindeki diğer lotlardan ilave ürün kalemleri ekleyebilir.

Gelecekte büyümeye yer açmak için uygun kaynak kategorileri içindeki isteğe bağlı sözleşme ürün kalemleri kullanılarak ek sözleşme esnekliği sağlanabilir. Alternatif olarak, bir kuruluşun Bulut Teknolojilerini danışmanlık hizmetleri, profesyonel veya yönetilen hizmetler ile birlikte tek bir ürün kalemi içinde paketlemek istemesi halinde, bu işlem "Bulut Teknolojileri ve Yardımcı İş Gücü" gibi bir ürün kalemiyle yapılabilir.

Aşağıda bu yaklaşımın temsili bir örneği verilmiştir. Aşağıdaki örnekte, Bulut Teknolojileri adlı 1001 sayılı ürün kaleminin her bir birimi kullanılan "Bulut Teknolojilerinin" 1,00 EUR'suna eşittir. Her ay, sipariş katları mevcut ve tahmin edilen kullanım projeksiyonlarına bağlı olarak finanse edilebilir.

Tablo 3 - Örnek Tek Ürün Kalemi Fiyatlandırma Yapısı.

ÜRÜN NO.	SARF MALZEMELERİ/HİZMETLER	MİKTAR	BİRİM	BİRİM FİYATI	TUTAR
1001	Bulut Teknolojileri	1.000	Her Biri	1 EUR	1.000 EUR
1002	Danışmanlık Hizmetleri	1	Haftalık	3.000 EUR	3.000 EUR
1003	Bulut Desteği	1	Aylık	1.000 EUR	1.000 EUR
1004	Bulut Eğitimi	1	Günlük	3,00 EUR	3.000 EUR
1005	Bulut Pazar Yeri	10	Her Biri	10 EUR	100 EUR

Bu yapının nasıl işleyebileceğine dair bir örnek: Bir kamu sektörü kuruluşu, ne kadar bulut teknolojisi hizmeti kullanacağını tahmin etmesi için bir CISP ile iletişime geçer. Kuruluş, satıcıyla hüküm ve koşullar üzerinde anlaşmaya varır. Buna göre yılda 2 milyon EUR olmak üzere 5 yılda 10 milyon EUR ödeyecektir. Kuruluş, 2 milyon EUR'luk ilk yıllık ödeme tutarını fon olarak ayırıyor. Her ay fatura düzenleniyor ve para fondan çekilerek fatura ödeniyor. Bu hesabın bakiyesi izlenmektedir. CISP izleme ve tahmin araçları kullanılarak kalan bakiyedeki azalma izlenmektedir. Kalan bakiye çok azaldığında kuruluş, hizmetlerin sürdürülmesi için tahsis edilmek üzere CFO'dan ek fon talep etmektedir.

Örnek RFP Metni: Fiyatlandırma - Sözleşme Yapma

ÖDEME KOŞULLARI

Ödeme koşulları yalnızca <KURULUŞ> tarafından kullanılan kaynaklar için ödeme yapılacak şekilde aşağıda belirtildiği gibi yapılandırılmalıdır:

1. Hizmetlerin gerçekleşen kullanımına/tüketimine ve CISP'nin genel erişime açık fiyatlandırmasına dayalı olarak hesaplanan Aylık Ödeme.

ASGARİ GARANTİ VE AZAMİ HARCAMA

<KURULUŞUN> bir Bulut Hizmeti Sağlayıcısının kaynaklarının belirli bir dönemde ne kadarlık bir hacimde tüketileceğini belirlemesi imkansız olduğundan, "Bulut Teknolojileri" için siparişler tek bir sipariş ürün kaleminin sabit fiyatlı birim miktarı cinsinden belirtilecektir.

Sipariş edilen ürün kaleminin her birimi, sipariş edilen Bulut Teknolojilerinin <1,00 EUR'ya> eşit miktarına karşılık gelecektir. <KURULUŞ>, değişen süreli ihtiyaçları için tahmini kullanımına dayalı olarak CISP Bulut Teknolojilerini "EUR tutarı" cinsinden çeşitli miktarlarda önceden sipariş etme esnekliğini sağlamak amacıyla artırımlı siparişler, bu siparişte değişiklik yapılması suretiyle periyodik olarak çeşitli miktarlarda verilecektir. Miktarlar, <KURULUŞ> tarafından çeşitli gereklilikleri karşılamak için kullanılacak bulut teknolojilerinin tahmini maliyetini karşılayacak kadar yeterli tutarlarda periyodik olarak önceden sipariş edilecektir.

Ürün No.	Açıklama	Miktar	Birim	Fiyat
01	CISP Bulut Teknolojileri	1.000	EA	1.000,00 EUR

MINIMUM SİPARİŞ/ARTIMLI SİPARİŞ

Siparişler, <KURULUŞUN> tahmini bulut teknolojileri kullanımına dayalı olarak <10.000> ürün kalemlik birimlerden oluşan çeşitli miktarlarda periyodik olarak verilecektir. Bu düzenleme, <KURULUŞA>, operasyonlarını desteklemek ve bulut bilgi işlem "kullandıkça öde" ticari uygulamalarına uygunluğunu korumak için <10.000> birim "Bulut Teknolojisi"ni önceden sipariş etme esnekliğini sağlayacaktır.

Açık sipariş verildiğinde <100.000 EUR> maliyetinde <100.000> birimlik ilk artımlı sipariş verilecektir. Bir veya daha fazla ürün kalemi kullanılarak tek bir artımlı siparişe eklenebilecek toplam ürün kalemi birimlerinin minimum sayısı <x'tir>. Teslimat siparişi altında sipariş edilebilecek azami birim sayısı <x'i> aşamaz. Aynı zamanda, sipariş edilmiş tüm önceki birimlerle birleştirildiğinde hiçbir zaman açık sipariş değerini de aşamaz. <KURULUŞ>, tüm siparişlerin bu bölümde belirtilen sınırlar içinde olmasını sağlamaktan sorumludur.

AZAMİ SİPARİŞ

Azami toplam sipariş değeri, birim başına <x> fiyatlı en fazla <x> tek ürün kalemi biriminden oluşmak üzere <x'tir>. Bu değer, <KURULUŞUN> ifa dönemi boyunca tahmini gerekliliklerine dayalıdır ancak garanti edilmez.

3.3 Çözüm Ortağı İş Modelini Anlama

Kamu sektörü kurumları, CISP'lerin tekliflerini hangi modeller kapsamında sağladığını öğrenmeye çalışmalı ve danışmanlık, yönetilen hizmetler, satış vb. hizmetler sağlayan çözüm ortaklarının bu süreçte kritik bir rol oynadığını kabul etmelidir. Birçok müşteri, altyapıları için bir bulut sağlayıcısına gerek duyar ve "klavye başında" planlama, taşıma ve yönetim işlerini dış kaynak olarak bir Sistem Entegratörüne (SI) veya yönetilen hizmet sağlayıcısına devreder. Bu "hizmetler" bileşimi göz önünde bulundurulduğunda, bulut sağlayıcıları için geçerli olmayabilecek gereklilikler bulunabilir. Örnek olarak, alt yüklenicilerin, yüklenicinin bir sözleşme kapsamında iş sahibine karşı olan yükümlülükleriyle aynı yükümlülükleri yükleniciye karşı yerine getirmekle sorumlu olduğunu belirleyen sözleşme maddeleri bu tür gerekliliklerdendir.

Bu tür sözleşme maddelerinin örnek olarak verilmesi, çözüm ortaklarının ve satıcıların CISP'ler açısından nasıl faaliyet gösterdiğinin anlaşılmasında önemlidir. Bununla birlikte, bazı satın alma türlerinde, ana yüklenicinin belirli zorunlu maddeleri tüm çözüm ortaklarına/alt yüklenicilerine yansıtmasını gerektiren maddeler bulunur. CISP'ler belirli bir nihai müşterinin benzersiz gerekliliklerine (kamu sektörü sözleşmesi kapsamındaki bir kamu sektörü müşterisinin ihtiyaçları dahil) uygun şekilde özelleştirilmeyen devasa ölçekte standart hizmetler sundukları için genellikle resmî alt yüklenici ortaklar olarak hizmet sağlamaz veya teklifte bulunmazlar. Bir dolaylı satın alma modelinde (bulut hizmetlerinin bir CISP Satıcısı aracılığıyla satın alınması) bir CISP, satıcısının yansıtmak istediği bu tür maddeleri, "2. katman" ticari hizmetler tedarikçisi için uygulanamaz olmaları nedeniyle reddedebilir. Bu durumda CISP, sözleşme kapsamındaki işi kendisi ifa etmez. Bunun yerine, bir CISP çözüm ortağı işi ifa etmek için CISP altyapısını kullanır. Dolayısıyla CISP, bir çözüm ortağının operasyonları için ticari tedarikçi görevi görür (alt yüklenici görevi görmez). Bir doğrudan satın alma modelinde (bulut hizmetlerinin doğrudan bir CISP'den satın alınması durumunda) CISP, tipik bir emtia alt yüklenicisi için uygun olan bu "zorunlu" maddeleri, sözleşmeli hizmetlerin ticari niteliği nedeniyle ve çoğu CISP'nin ticari hizmetlerini tedarik etmek için alt yüklenicilere ihtiyaç duymaması sebebiyle genellikle reddedecektir.

3.4 Bulut Aracıları

Satıcıya bağımlılık olasılığını azaltmaya yönelik olarak bir Bulut Aracısı kullanılması sorunlara neden olabilir. Bulut aracısı teoride iyi bir fikir gibi görünse de pratikte sağlayacağı değerden daha fazla karmaşıklığa ve karışıklığa yol açması muhtemeldir.

Birden fazla bulutta eş zamanlı ya da değişimli olarak çalışacak mimariler geliştirilmeye çalışıldığında kaçınılmaz olarak özelliklerden bazı ödünler verilecektir. **(Bulutta her soruna çözüm getirecek tek bir basit çözüm bulmak zordur.)** Bu yaklaşım kamu sektörü kuruluşları ve onların bulut hizmetleri arasına gereksiz bir karmaşıklık katmanı ekleyebilir. Ortaya çıkacak bu karmaşıklık ise ölçeklenebilirliği ve çevikliği azaltarak, maliyetleri artırarak ve inovasyonu yavaşlatarak, kuruluşların edinmeyi amaçladığı verimlilikleri ve güvenlik kazanımlarını tehlikeye atabilir.

3.5 RFP öncesinde dış kaynak kullanımı/pazar araştırması

Bir kamu sektörü kurumu bir Bulut Hizmetleri RFP'si planlarken üst yönetim, iş paydaşları, teknoloji, finans, satın alma, hukuk ve sözleşme departmanları gibi kuruluşun farklı paydaşlarını sürecin en başından itibaren sürece dahil etmelidir. Bu yaklaşım tüm paydaşların bulut modelini anlamasını sağlayacak ve sonuç olarak geleneksel BT satın alma yöntemlerinin yeniden değerlendirilmesine ilişkin bilgiye dayalı bir yaklaşım benimsenmesine yardımcı olacaktır.

Sektörle kurulacak diyaloglar söz konusu olduğunda, kamu sektörü kurumlarının ayrıntılı görüşmeler yaparak CISP'ler, CISP Çözüm Ortakları, PaaS/SaaS Pazar Yeri satıcıları ve sektör uzmanları gibi sektör temsilcilerinden geri bildirim alması şiddetle önerilir. Örneğin sektör günleri ya da güvenlik ve satın alma atölye çalışmaları gibi etkinlikler yoluyla bu tür diyaloglar kurulabilir. Bulut hizmeti satın alma yöntemleri hakkında kapsamlı bir anlayış edinilmesini sağlayacak bir diğer etkili yöntem de bir RFI ya da ideal olarak taslak RFP belgesinin yayınlanmasıdır. Bu belgeler genellikle potansiyel sorunlar içerir ve nihai Bulut Hizmetleri RFP'si yayınlanmadan önce bu tür sorunların tanımlanmasını, tartışılmasını ve giderilmesini sağlar.

3.6 Sürdürülebilirlik

Sürdürülebilirlik bulut bilgi işlemin içsel özelliklerinden biridir. Buluta geçiş yapma, şirket içi sunucular veya kurumsal veri merkezleri ile karşılaştırıldığında enerji verimliliği kazanımı sağlar. Sürdürülebilirliğe öncelik veren ve sürdürülebilirlik hedeflerini elde etmek için kamuya açık şekilde taahhütlerde bulunan bir CISP'nin belirlenmesi bulutun sürdürülebilir olacağına dair ek güvence sağlar. Avrupalı CISP'ler ve veri merkezi operatörleri (Avrupa Komisyonu'nun desteğiyle) İklim Nötr Veri Merkezi Paketi'nin¹¹ oluşturmuştur. Bir Öz Düzenleyici Girişim olan bu Pakt, veri merkezi sektörüne yönelik net, basit ve geniş kapsamlı sürdürülebilirlik kriterleri belirlemekte ve veri merkezi operatörleri ile bulut hizmeti sağlayıcılarının 2030'a kadar iklim nötr statüsüne ulaşmasını hedeflemektedir. Öz Düzenleyici Girişim, veri merkezlerinin enerji verimliliği, suyun korunması, sunucuların yeniden kullanımı ve onarımı, ayrıca veri merkezlerini çalıştırmak için karbonsuz enerji kullanımı ile ilgili net hedefler içermektedir. Öz Düzenleyici Girişim'e imza atan CISP'ler, iklim nötr operatör olarak sınıflandırılmak için bu hedefleri elde etmeyi ve kriterler doğrultusunda sertifikalandırılmayı kabul eder.

Bir Bulut Hizmetleri RFP'sinde CISP'lere bu tür kriterleri karşılamayı taahhüt edip etmedikleri, özellikle de bu öz düzenleme için kayıt olup olmadıkları ve bu taahhüdü ne zaman verdikleri sorulmalıdır.

¹¹ <https://www.climateutraldatacentre.net/self-regulatory-initiative/>

Örnek RFP Metni: Sürdürülebilirlik

İklim Nötr Veri Merkezi Öz Düzenleyici Girişimi'ni imzalayarak iklim nötr veri merkezleri işletme taahhüdünde bulundunuz mu? Öyleyse ne zaman imzaladınız?

Kendi kullanımınız için tarafınıza İklim Nötr Veri Merkezi Paketi mührü verildiğine dair kanıt sunabilir misiniz?

Ek A - İstekliler Arasında Karşılaştırmayla İlgili Teknik Gereklilikler

Aşağıda bir Bulut Çerçeve Sözleşmesi kapsamındaki Açık Siparişler veya Küçük İhaleler sırasında CISP'leri karşılaştırmak için kullanılabilecek bazı genel bulut teknolojisi gereklilikleri listelenmektedir.

1. Bulut sağlayıcısı profili

	Gereklilik
1.	PAZAR DENEYİMİ: Bulut sağlayıcısı, bulut pazarı segmentinde kaç yıldır faaliyet göstermektedir?
2.	AÇIKLIK VE VERİ KORUMASI: Bulut sağlayıcısı, Veri Koruma veya Tersine Çevrilebilirlik ile ilgili sektör Davranış Kurallarına uyuyor mu? Bulut sağlayıcısı açık kaynak ve açık API geliştirme ilkelerine uyuyor mu?

2. Küresel altyapı

	Gereklilik
1.	KÜRESEL KAPSAMA ALANI: Bulut sağlayıcısı, kullanıcıların düşük gecikme süresi ve yüksek aktarım hızı elde etmesine yardımcı olacak bir küresel altyapı sunuyor mu?
2.	BÖLGELER: Bulut sağlayıcısı, gerekli coğrafyalarda bölgesel varlığa sahip mi?
3.	ETKİ ALANLARI/BÖLGELER: Bulut sağlayıcısı, daha üst düzeyde yüksek erişilebilirlik ve hata toleransı sağlamak amacıyla birden fazla veri merkezinin bir düşük gecikme süreli ağ yoluyla gruplandırıldığı etki alanları veya bölgeler kavramını uyguluyor mu? Cevap Evet ise lütfen etki alanlarının veya bölgelerin sayısını ve gerekli coğrafyadaki veri merkezi sayısını belirtin.
4.	ETKİ ALANLARININ/BÖLGELERİN MESAFESİ: Bulut sağlayıcısı, yedekliliği, yüksek erişilebilirliği ve düşük gecikme süresini desteklemek için fiziksel olarak birbirinden ayrı konumlandırılmış veri merkezleriyle kendi etki alanlarını veya bölgelerini oluşturuyor mu?
5.	OLUŞTURULAN VERİ MERKEZLERİ: Bulut sağlayıcısı, diğer veri merkezlerindeki hatalardan yalıtılmış olacak şekilde tasarlanmış, yedekli güç, soğutma ve ağ iletişimi olanaklarına sahip veri merkezleri sunuyor mu?
6.	VERİ MERKEZİ ÇOĞALTMA: Bulut sağlayıcısı bir etki alanı veya bölge içindeki veri merkezleri genelinde otomatik yük devretme ile veri çoğaltma olanağı sunuyor mu?
7.	ETKİ ALANI/BÖLGE ÇOĞALTMA: Bulut sağlayıcısı bir bölgedeki etki alanları veya bölgeler genelinde veri çoğaltma olanağı sunuyor mu?

3. Altyapı

3.1 Bilgi İşlem

	Gereklilik
1.	BİLGİ İŞLEM - NORMAL BULUT SUNUCUSU - GENEL AMAÇLI: Bulut sağlayıcısı aşağıdaki türlerde bulut sunucusu sunuyor mu? - Genel amaçlı: Genel uygulamalar için optimize edilmiştir ve bilgi işlem, bellek ve ağ kaynakları arasında dengeyi sunar. - Cevap Evet ise en büyük bulut sunucusu hangisidir?
2.	BİLGİ İŞLEM - NORMAL BULUT SUNUCUSU - BELLEK İÇİN OPTİMİZE EDİLMİŞ: Bulut sağlayıcısı aşağıdaki türlerde bulut sunucusu sunuyor mu? - Bellek için optimize edilmiş: bellek kullanımı yüksek uygulamalar için optimize edilmiş - Cevap Evet ise en büyük bulut sunucusu hangisidir?
3.	BİLGİ İŞLEM - NORMAL BULUT SUNUCUSU - BİLGİ İŞLEM İÇİN OPTİMİZE EDİLMİŞ: Bulut sağlayıcısı aşağıdaki türlerde bulut sunucusu sunuyor mu? - Bilgi işlem için optimize edilmiş: bilgi işlem kullanımı yüksek uygulamalar için optimize edilmiş - Cevap Evet ise en büyük bulut sunucusu hangisidir?
4.	BİLGİ İŞLEM - NORMAL BULUT SUNUCUSU - DEPOLAMA İÇİN OPTİMİZE EDİLMİŞ: Bulut sağlayıcısı aşağıdaki türlerde bulut sunucusu sunuyor mu? - Depolama için optimize edilmiş: Büyük miktarda yerel depolama kapasitesi sunar - Cevap Evet ise tedarik edilebilecek ve bir bulut sunucusuna bağlanabilecek maksimum depolama kapasitesi (ör. 5, 10, 20, 50 TB) ve maksimum disk (HDD/SSD) sayısı nedir?
5.	BİLGİ İŞLEM - NORMAL BULUT SUNUCUSU - GRAFİK İÇİN OPTİMİZE EDİLMİŞ: Bulut sağlayıcısı aşağıdaki türlerde bulut sunucusu sunuyor mu? - Düşük maliyetli grafik: Bilgi işlem sunucularına düşük maliyetli grafik ivmesi sunar - Cevap Evet ise en büyük bulut sunucusu hangisidir?
6.	BİLGİ İŞLEM - NORMAL BULUT SUNUCUSU - GPU İÇİN OPTİMİZE EDİLMİŞ: Bulut sağlayıcısı aşağıdaki türlerde bulut sunucusu sunuyor mu? - GPU: Grafik kullanımı yüksek uygulamalar için grafik işlem birimi (GPU) donanımı sunar. - Cevap Evet ise bulut sağlayıcısı, bulut sunucusu başına kaç adet GPU ve hangi GPU modellerini sunabiliyor?
7.	BİLGİ İŞLEM - NORMAL BULUT SUNUCUSU - FPGA İÇİN OPTİMİZE EDİLMİŞ: Bulut sağlayıcısı aşağıdaki türlerde bulut sunucusu sunuyor mu? - FPGA: Uygulamalara yönelik özel donanım ivmesi geliştirmek ve dağıtmak için alanda programlanabilir kapı dizileri (FPGA'lar) sunar. - Cevap Evet ise bulut sağlayıcısı, bulut sunucusu başına kaç adet FPGA sunabiliyor?

8.	BİLGİ İŞLEM - HIZ ARTIRIMLI BULUT SUNUCUSU: Bulut sağlayıcısı, bir başlangıç seviyesi merkezi işlem birimi (CPU) performansı sağlayan ve başlangıç seviyesinin üzerine hız artırımı yapma imkanı veren hız artırımli bulut sunucuları sunuyor mu? Cevap Evet ise en büyük hız artırımli bulut sunucusu hangisidir?
9.	BİLGİ İŞLEM - G/Ç KULLANIMI YÜKSEK BULUT SUNUCUSU: Bulut sağlayıcısı, düşük gecikme süresi, çok yüksek rastgele G/Ç performansı ve yüksek ardışık okuma aktarım hızı için optimize edilmiş geçici olmayan bellek ekspres (NVMe) katı hal sürücüler (SSD'ler) kullanan bulut sunucuları sunuyor mu? Cevap Evet ise en büyük bulut sunucusunun maksimum saniyede giriş/çıkış işlemleri (IOPS) kapasitesi nedir?
10.	BİLGİ İŞLEM - GEÇİCİ YEREL DEPOLAMA: Bulut sağlayıcısı, sık değişen bilgilerin geçici olarak depolanmasında kullanılmak üzere bilgi işlem bulut sunucuları için yerel depolamayı destekliyor mu?
11.	BİLGİ İŞLEM - BİRDEN FAZLA NIC DESTEĞİ: Bulut sağlayıcısı belirli bir bulut sunucusu için birden fazla (birincil ve ek) ağ arabirimi kartı (NIC) tahsis edilmesini destekliyor mu? Cevap Evet ise bulut sunucusu başına maksimum NIC sayısı kaçtır?
12.	BİLGİ İŞLEM - BULUT SUNUCUSU BENZEŞİMİ: Bulut sağlayıcısı, kullanıcılara bulut sunucularını aynı veri merkezi içinde mantıksal olarak gruplandırma özelliğini sunuyor mu?
13.	BİLGİ İŞLEM - BULUT SUNUCUSU BENZEŞİM KARŞITI: Bulut sağlayıcısı, kullanıcılara bulut sunucularını mantıksal olarak gruplandırma ve bir bölge içindeki farklı veri merkezlerine yerleştirme özelliğini sunuyor mu?
14.	BİLGİ İŞLEM - SELF SERVİS TEDARİK: Bulut sağlayıcısı, birden fazla bulut sunucusunu bir programlanabilir arabirim, yönetim konsolu veya web portalı yoluyla eş zamanlı olarak self servis tedarik etme özelliğini sunuyor mu?
15.	BİLGİ İŞLEM - ÖZELLEŞTİRME: Bulut sağlayıcısı, özelleştirilebilir bulut sunucuları yani sanal merkezi işlem birimleri (vCPU'lar) ve rastgele erişimli bellek (RAM) gibi yapılandırma ayarlarını değiştirme yeteneği sunuyor mu?
16.	BİLGİ İŞLEM - KİRALAMA: Bulut sağlayıcısı tek bir kullanıcıya tahsis edilmiş donanım üzerinde çalışan tek kiracılı bulut sunucuları sunuyor mu? Cevap Evet ise en büyük tek kiracılı bulut sunucusu hangisidir?
17.	BİLGİ İŞLEM - ANA SUNUCU BENZEŞİMİ: Bulut sağlayıcısı bir bulut sunucusunu başlatma ve bu bulut sunucusunu her zaman aynı fiziksel ana sunucuda yeniden başlatılacak şekilde ayarlama yeteneğini sunuyor mu?
18.	BİLGİ İŞLEM - ANA SUNUCU BENZEŞİM KARŞITI: Bulut sağlayıcısı belirli bulut sunucularını bölme ve farklı fiziksel ana sunucularda barındırma özelliğini sunuyor mu?
19.	BİLGİ İŞLEM - OTOMATİK ÖLÇEKLENDİRME: Bulut sağlayıcısı, talebin yükseliş gösterdiği zamanlarda performansı korumak (ölçeklendirmek) için bulut sunucusu sayısını otomatik olarak artırma yeteneğini sunuyor mu?

20.	BİLGİ İŞLEM - GÖRÜNTÜ İÇERİ AKTARMA MEKANİZMASI: Bulut sağlayıcısı, kullanıcılara mevcut görüntülerini içeri aktarma ve daha sonra gelecekte bulut sunucuları tedarik etmede kullanılabilecek yeni, özel olarak erişilebilir görüntüler olarak kaydetme yeteneğini sunuyor mu? • Cevap Evet ise hangi formatlar destekleniyor?
21.	BİLGİ İŞLEM - GÖRÜNTÜ DIŞARI AKTARMA MEKANİZMASI: Bulut sağlayıcısı, çalışan bir mevcut bulut sunucusunu ya da bir bulut sunucusunun kopyasını alıp bulut sunucusunu bir sanal makine formatında dışarı aktarma yeteneğini sunuyor mu? • Cevap Evet ise hangi formatlar destekleniyor?
22.	BİLGİ İŞLEM - HİZMETİN AKSAMASI: Bulut sağlayıcısı, sağlayıcı ana sunucu düzeyinde herhangi bir türden donanım veya hizmet bakımı gerçekleştirirken bulut sunucusu kesintilerini ya da arıza süresini önlemeye yönelik mekanizmalar sunuyor mu?
23.	BİLGİ İŞLEM - BULUT SUNUCUSUNU YENİDEN BAŞLATMA: Bulut sağlayıcısı, orijinal fiziksel ana sunucunun hata vermesi durumunda bulut sunucularının sağlıklı bir ana sunucuda otomatik olarak yeniden başlatılmasına yönelik mekanizmalar sunuyor mu?
24.	BİLGİ İŞLEM - BİLDİRİMLER: Bir bilgi işlem esnek olay durumunda, bulut sağlayıcısı bu tür bir olayın meydana geldiğini kullanıcıya bildirme yeteneğine sahip mi ve kullanıcı self servis araçlar yoluyla bu iletişime abone olabiliyor ya da abonelikten çıkabiliyor mu?
25.	BİLGİ İŞLEM - OLAY PLANLAMA: Bulut sağlayıcısı, kullanıcıların bulut sunucuları için bulut sunucusunu ön yükleme, durdurma, başlatma veya kullanımdan kaldırma gibi olaylar planlama yeteneğini sunuyor mu?
26.	BİLGİ İŞLEM - YEDEKLEME VE GERİ YÜKLEME MEKANİZMASI: Bulut sağlayıcısı entegre bir yedekleme ve geri yükleme mekanizması sunuyor mu?
27.	BİLGİ İŞLEM - ANLIK GÖRÜNTÜ MEKANİZMASI: Bulut sağlayıcısı bir manuel, istek üzerine anlık görüntü mekanizması sunuyor mu?
28.	BİLGİ İŞLEM - META VERİ: Bulut sağlayıcısı, kullanıcıların bulut sunucusu için rastgele anahtar-değer çiftleri ayarlamasına olanak sağlayan bir bulut sunucusu meta veri hizmeti sunuyor mu?
29.	BİLGİ İŞLEM - META VERİ ÇAĞIRMA: Bulut sağlayıcısı, bulut sunucusunun kendisi hakkında bilgi edinmek için çağırabileceği bir uygulama programlama arabirimi (API) sağlayan bir bulut sunucusu meta veri hizmeti sunuyor mu?
30.	BİLGİ İŞLEM - TEKLİF VERME MEKANİZMASI: Bulut sağlayıcısı, görev açısından kritik olmayan iş yüklerini barındırmak için hemen başlatılabilecek düşük maliyetli bulut sunucularına teklif vermek üzere kullanılabilecek bir teklif verme mekanizması sunuyor mu?
31.	BİLGİ İŞLEM - PLANLAMA MEKANİZMASI: Bulut sağlayıcısı günlük, haftalık veya aylık plan gibi yinelenen bir bazda ek bilgi işlem kapasitesi planlama ve rezerve etme yöntemi sunuyor mu?
32.	BİLGİ İŞLEM - REZERVASYON MEKANİZMASI: Bulut sağlayıcısı gelecek (ör. 1 yıl, 2 yıl, 3 yıl vb.) için ek bilgi işlem kapasitesi rezerve etme yöntemi sunuyor mu?

33.	BİLGİ İŞLEM - LINUX İŞLETİM SİSTEMİ: Bulut sağlayıcısı en az bir kurumsal Linux dağıtımının (ör. Red Hat, SUSE) ve yaygın olarak kullanılan ücretsiz bir Linux dağıtımının (ör. Ubuntu, CentOS ve Debian) uzun süredir desteklenen son iki sürümünü destekliyor mu?
34.	BİLGİ İŞLEM - WINDOWS İŞLETİM SİSTEMİ: Bulut sağlayıcısı son iki ana Windows Server sürümünü (Windows Server 2017 ve Windows Server 2016) destekliyor mu?
35.	BİLGİ İŞLEM - LİSANS TAŞINABİLİRLİĞİ: Bulut sağlayıcısı lisans taşınabilirliği ve desteği sunuyor mu? Cevap Evet ise lütfen yazılım satıcısını, yazılım adlarını, edisyonlarını ve sürümlerini belirtin.
36.	BİLGİ İŞLEM - HİZMET SINIRLARI: Bulut sağlayıcısı, yukarıdaki bilgi işlem bölümüne ilişkin herhangi bir kısıtlamaya (ör. hizmet sınırları) sahip mi? Örneğin: Hesap başına maksimum bulut sunucusu sayısı Hesap başına maksimum tahsis edilmiş ana sunucu sayısı Maksimum rezerve edilmiş internet protokolü (IP) adresi sayısı

3.2 Ağ İletişimi

	Gereklilik
1.	AĞ İLETİŞİMİ - SANAL AĞLAR: Bulut sağlayıcısı, şirketin buluttaki kendi ağını temsil eden, mantıksal olarak yalıtılmış bir sanal ağ oluşturma yeteneğini destekliyor mu?
2.	AĞ İLETİŞİMİ - AYNI BÖLGEDE BAĞLANTI: Bulut sağlayıcısı, trafiği aynı bölgedeki iki sanal ağ arasında yönlendirmek için özel internet protokolü (IP) adresleri kullanarak bu ağların birbirine bağlanmasını destekliyor mu?
3.	AĞ İLETİŞİMİ - FARKLI BÖLGEDE BAĞLANTI: Bulut sağlayıcısı, trafiği farklı bölgelerdeki iki sanal ağ arasında yönlendirmek için özel internet protokolü (IP) adresleri kullanarak bu ağların birbirine bağlanmasını destekliyor mu?
4.	AĞ İLETİŞİMİ - ÖZEL ALT AĞ: Bulut sağlayıcısı, bulut sunucularının hiçbir genel internet protokolü (IP) adresi veya internet yönlendirmesi olmadan tedarik edilebileceği, tamamen yalıtılmış (özel) sanal ağlar ve alt ağlar oluşturma özelliğini sunuyor mu?
5.	AĞ İLETİŞİMİ - SANAL AĞ ADRESİ ARALIĞI: Bulut sağlayıcısı, Açıklama İsteği (RFC) 1918'in yanı sıra genel olarak yönlendirilebilir Sınıfsız Etki Alanları Arası Yönlendirme (CIDR) bloklarında belirtilen internet protokolü (IP) adresi aralıklarını destekliyor mu?
6.	AĞ İLETİŞİMİ - BİRDEN FAZLA PROTOKOL: Bulut sağlayıcısı, İletim Denetimi Protokolü (TCP), Kullanıcı Veri Birimi Protokolü (UDP) ve İnternet Denetim İletisi Protokolü (ICMP) dahil birden fazla protokolü destekliyor mu?
7.	AĞ İLETİŞİMİ - IP ADRESLERİ İÇİN OTOMATİK ATAMA: Bulut sağlayıcısı, bulut sunucularına otomatik olarak genel internet protokolü (IP) adresleri atama özelliğini destekliyor mu?

8.	AĞ İLETİŞİMİ - REZERVE EDİLMİŞ STATİK IP ADRESLERİ: Bulut sağlayıcısı, belirli bir bulut sunucusuyla değil, bir kullanıcı hesabıyla ilişkilendirilmiş internet protokolü (IP) adreslerini destekliyor mu? IP adresi açıkça serbest bırakılana kadar hesapla ilişkilendirilmiş olarak kalmalıdır.
9.	AĞ İLETİŞİMİ - IPV6 DESTEĞİ: Bulut sağlayıcısı, ağ geçidi veya bulut sunucusu düzeyinde internet protokolü sürüm 6'yı (IPv6) destekliyor mu ve bu işlevselliği kullanıcılarına sunuyor mu?
10.	AĞ İLETİŞİMİ - NIC BAŞINA BİRDEN FAZLA IP ADRESİ: Bulut sağlayıcısı belirli bir bulut sunucusuna bağlanmış bir ağ arabirimi kartına (NIC) birincil ve ikincil internet protokolü (IP) adresi atama yeteneğini destekliyor mu?
11.	AĞ İLETİŞİMİ - BİRDEN FAZLA NIC: Bulut sağlayıcısı belirli bir bulut sunucusuna birden fazla ağ arabirimi kartı (NIC) atama yeteneğini destekliyor mu?
12.	AĞ İLETİŞİMİ - NIC VE IP MOBİLİTESİ: Bulut sağlayıcısı, ağ arabirimi kartlarını (NIC'ler) ve internet protokolü (IP) adreslerini bulut sunucuları arasında taşıma yeteneğini destekliyor mu?
13.	AĞ İLETİŞİMİ - SR-IOV DESTEĞİ: Bulut sağlayıcısı, daha yüksek performans (ör. saniye başına paket sayısı - PPS), daha düşük gecikme süresi ve daha düşük gecikme süresi değişkenliği için tek köklü giriş/çıkış sanallaştırması(SR-IOV) gibi özellikleri destekliyor mu?
14.	AĞ İLETİŞİMİ - GİRİŞ FİLTRELEME: Bulut sağlayıcısı, bulut sunucularına gelen trafik (giriş) için uygulanabilir kurallar eklenmesini veya kaldırılmasını destekliyor mu?
15.	AĞ İLETİŞİMİ - ÇIKIŞ FİLTRELEME: Bulut sağlayıcısı, bulut sunucuları kaynaklı giden trafik (çıkış) için uygulanabilir kurallar eklenmesini veya kaldırılmasını destekliyor mu?
16.	AĞ İLETİŞİMİ - ACL: Bulut sağlayıcısı, alt ağlara gelen ve giden trafiği denetlemek için erişim denetim listeleri (ACL'ler) sunuyor mu?
17.	AĞ İLETİŞİMİ - AKIŞ GÜNLÜĞÜ DESTEĞİ: Bulut sağlayıcısı, ağ trafiği akış günlüklerini yakalama özelliğini sunuyor mu?
18.	AĞ İLETİŞİMİ - NAT: Bulut sağlayıcısı bir özel ağdaki bulut sunucularının internete ya da diğer bulut hizmetlerine bağlanmasına olanak tanımak fakat internetin bu bulut sunucularına bir bağlantı başlatmasını engellemek için bir ağ adresi çevirisi (NAT) ağ geçidi yönetilen hizmeti sağlıyor mu?
19.	AĞ İLETİŞİMİ - KAYNAK/HEDEF KONTROLÜ: Bulut sağlayıcısı, ağ arabirimi kartları (NIC'ler) üzerinde kaynak/hedef denetimini devre dışı bırakma yeteneğine sahip mi?
20.	AĞ İLETİŞİMİ - VPN DESTEĞİ: Bulut sağlayıcısı, bulut sağlayıcısı ile kullanıcının veri merkezi arasında sanal özel ağ (VPN) bağlantısını destekliyor mu?
21.	AĞ İLETİŞİMİ - VPN TÜNELLERİ: Bulut sağlayıcısı, sanal ağ başına birden fazla sanal özel ağ (VPN) bağlantısını destekliyor mu?

22.	AĞ İLETİŞİMİ - IPSEC VPN DESTEĞİ: <i>Bulut sağlayıcısı, kullanıcıların genel internet üzerinden bir internet protokolü güvenliği (IPsec) sanal özel ağ (VPN) tüneli ya da güvenli yuva katmanı (SSL) sanal özel ağ (VPN) tüneli yoluyla bulut hizmetlerine erişmesine olanak sağlıyor mu?</i>
23.	AĞ İLETİŞİMİ - BGP DESTEĞİ: <i>Bulut sağlayıcısı, internet protokol güvenliği (IPsec) sanal özel ağ (VPN) tünelleri genelinde yük devretmeyi iyileştirmek için sınır ağ geçidi protokolünü (BGP) kullanıyor mu?</i>
24.	AĞ İLETİŞİMİ - ÖZEL TAHSİS EDİLMİŞ BAĞLANTI: <i>Bulut sağlayıcısı, bulut sağlayıcısının konumları ile bir kullanıcının veri merkezi, ofisi veya ortak barındırma ortamı arasında büyük ve hızlı veri aktarımlarına olanak sağlayan bir doğrudan, özel bağlantı hizmeti sunuyor mu?</i>
25.	AĞ İLETİŞİMİ - ÖN UÇ YÜK DENGELİYİCİ: <i>Bulut sağlayıcısı, internet üzerinden istemcilerden istekleri alıp bu istekleri yük dengeleyiciye kayıtlı bulut sunucuları genelinde dağıtan bir ön uç (internete dönük) yük dengeleme hizmeti sunuyor mu?</i>
26.	AĞ İLETİŞİMİ - ARKA UÇ YÜK DENGELİYİCİ: <i>Bulut sağlayıcısı, trafiği özel alt ağlarda barındırılan bulut sunucularına yönlendiren bir arka uç (özel) yük dengeleme hizmeti sunuyor mu?</i>
27.	AĞ İLETİŞİMİ - KATMAN 7 YÜK DENGELİYİCİ: <i>Bulut sağlayıcısı, birden fazla bulut sunucusu genelinde ağ trafiği yükünü dengeleyebilen bir katman 7 (köprü metni aktarım protokolü, HTTP) yük dengeleyici hizmeti sunuyor mu?</i>
28.	AĞ İLETİŞİMİ - KATMAN 4 YÜK DENGELİYİCİ: <i>Bulut sağlayıcısı, birden fazla bulut sunucusu genelinde ağ trafiği yükünü dengeleyebilen bir katman 4 (iletim denetim protokolü, TCP) yük dengeleyici hizmeti sunuyor mu?</i>
29.	AĞ İLETİŞİMİ - YÜK DENGELİYİCİLER İÇİN OTURUM BENZEŞMESİ: <i>Bulut sağlayıcısı, oturum benzeşmesini destekleyen bir yük dengeleme hizmeti sunuyor mu?</i>
30.	AĞ İLETİŞİMİ - DNS TABANLI YÜK DENGELEME: <i>Bulut sağlayıcısı, trafik yükünü aynı etki alanına ait birden fazla ana sunucuda barındırılan bulut sunucularına dengeleyebilen bir yük dengeleme hizmeti sunuyor mu?</i>
31.	AĞ İLETİŞİMİ - YÜK DENGELİYİCİ GÜNLÜKLERİ: <i>Bulut sağlayıcısı bir yük dengeleyiciye gönderilen tüm istekler hakkında ayrıntılı bilgiler yakalayan günlükler sağlıyor mu?</i>
32.	AĞ İLETİŞİMİ - DNS: <i>Bulut sağlayıcısı yüksek oranda erişilebilir ve ölçeklenebilir bir etki alanı adı sistemi (DNS) hizmeti sunuyor mu?</i>
33.	AĞ İLETİŞİMİ - GECİKME TABANLI DNS YÖNLENDİRME: <i>Bulut sağlayıcısı, gecikme tabanlı yönlendirmeyi destekleyen bir etki alanı adı sistemi (DNS) hizmeti (DNS hizmeti, DNS sorgularına en iyi gecikme süresini sağlayan kaynaklarla yanıt verir) sunuyor mu?</i>
34.	AĞ İLETİŞİMİ - COĞRAFYA TABANLI DNS YÖNLENDİRME: <i>Bulut sağlayıcısı, coğrafya tabanlı yönlendirmeyi destekleyen bir etki alanı adı sistemi (DNS) hizmeti (DNS hizmeti, DNS sorgularına kullanıcıların coğrafi konumuna dayalı olarak yanıt verir) sunuyor mu?</i>

35.	AĞ İLETİŞİMİ - YÜK DEVRETME TABANLI DNS YÖNLENDİRME: Bulut sağlayıcısı, yük devretme tabanlı yönlendirmeyi destekleyen bir etki alanı adı sistemi (DNS) hizmeti (DNS hizmeti, DNS sorgularını halihazırda etkin olan kaynağa yönlendirirken, ikinci bir kaynak bekler ve yalnızca birinci kaynakta bir hata olması durumunda etkinleşir) sunuyor mu?
36.	AĞ İLETİŞİMİ - ETKİ ALANI KAYIT HİZMETİ: Bulut sağlayıcısı, etki alanı adı kayıt hizmetleri (kullanıcılar kullanılabilir etki alanı adlarını arayabilir ve kaydedebilir) sunuyor mu?
37.	AĞ İLETİŞİMİ - DNS DURUM DENETİMLERİ: Bulut sağlayıcısı, kaynakların durumunu ve performansını izlemek için durum denetimlerini kullanan bir etki alanı adı sistemi (DNS) hizmeti sunuyor mu?
38.	AĞ İLETİŞİMİ - DNS VE YÜK DENGELİYİCİ ENTEGRASYONU: Bulut sağlayıcısı, bulut sağlayıcısının yük dengeleyicisiyle entegre bir etki alanı adı sistemi (DNS) hizmeti sunuyor mu?
39.	AĞ İLETİŞİMİ - SANAL DÜZENLEYİCİ: Bulut sağlayıcısı, kullanıcıların trafik yönetimi için politikalar oluşturmaya olanak sağlayan bir araç sunuyor mu?
40.	İÇERİK TESLİM AĞI (CDN): Bulut sağlayıcısı, içeriği düşük gecikme süresiyle ve yüksek veri aktarım hızlarıyla dağıtmak için bir içerik teslim ağı (CDN) hizmeti sunuyor mu?
41.	AĞ İLETİŞİMİ - CDN ÖN BELLEK SÜRESİNİN SONA ERMESİ: Bulut sağlayıcısı, bir nesnenin süresi sona ermeden uç ön belleklerden kaldırılmasına olanak sağlayan ve nesneleri geçersiz kılmaya ve nesne sürümünü oluşturma gibi özellikler içeren bir içerik teslim ağı (CDN) hizmeti sunuyor mu?
42.	AĞ İLETİŞİMİ - CDN HARİCİ KAYNAKLAR: Bulut sağlayıcısı, özel kaynağı [ör. köprü metni aktarım protokolü (HTTP) sunucusu] destekleyen bir içerik teslim ağı (CDN) hizmeti sunuyor mu?
43.	AĞ İLETİŞİMİ - CDN OPTİMİZASYONU: Bulut sağlayıcısı, birden fazla kaynak sunucusunun yapılandırılması ve tekdüze kaynak konum belirleyicilerinin (URL'ler) özelliklerini ön belleğe alma için ayrıntılı denetim içeren bir içerik teslim ağı (CDN) hizmeti sunuyor mu?
44.	AĞ İLETİŞİMİ - CDN COĞRAFYA TABANLI KISITLAMALI: Bulut sağlayıcısı, coğrafya tabanlı kısıtlamayı (belirli coğrafyalardaki kullanıcıların içeriğe erişimini engelleme) destekleyen bir içerik teslim ağı (CDN) hizmeti sunuyor mu?
45.	AĞ İLETİŞİMİ - CDN BELİRTEÇLERİ: Bulut sağlayıcısı, kullanıcılara içeriklerine erişim üzerinde daha fazla kontrol olanağı vermek için tipik olarak süre sona erme tarihi/saati bilgisini içeren, imzalı tekdüze kaynak konum belirleyicilerini (URL'ler) destekleyen bir içerik teslim ağı (CDN) hizmeti sunuyor mu?
46.	AĞ İLETİŞİMİ - CDN SERTİFİKALARI: Bulut sağlayıcısı, içerikleri uç konumlardan güvenli köprü metin aktarım protokolü (HTTPS) yoluyla güvenli bir şekilde teslim etmek için özel güvenli yuva katmanı (SSL) sertifikalarını destekleyen bir içerik teslim ağı (CDN) hizmeti sunuyor mu?

47.	AĞ İLETİŞİMİ - CDN ÇOK KATMANLI ÖN BELLEK: <i>Bulut sağlayıcısı, gecikme süresini azaltmak için bölgesel uç ön belleklerin kullanımıyla çok katmanlı bir ön bellek yaklaşımını izleyen bir içerik teslim ağı (CDN) hizmeti sunuyor mu?</i>
48.	AĞ İLETİŞİMİ - CDN SIKIŞTIRMA: <i>Bulut sağlayıcısı, sıkıştırmaı destekleyen bir içerik teslim ağı (CDN) hizmeti sunuyor mu?</i>
49.	AĞ İLETİŞİMİ - CDN ŞİFRELENMİŞ KARŞIYA YÜKLEMELER: <i>Bulut sağlayıcısı, kullanıcıların hassas verilerini, bu bilgiler yalnızca kullanıcının kaynak alt yapısındaki belirli bileşenler ve hizmetler tarafından görüntülenebilecek şekilde karşıya yüklemelerine olanak sağlayan bir içerik teslim ağı (CDN) sunuyor mu?</i>
50.	AĞ İLETİŞİMİ - UÇ NOKTALAR: <i>Bulut sağlayıcısının ağ iletişimi hizmeti, kullanıcılara iletişim maliyetlerini azaltmak ve trafik güvenliğini artırmak için trafiği sağlayıcının dahili ağ bağlantısı (özel bağlantı) üzerinden yönlendirme özelliğine sahip uç noktalar sunuyor mu?</i>
51.	AĞ İLETİŞİMİ - HİZMET SINIRLARI: <i>Bulut sağlayıcısı, yukarıdaki ağ iletişimi bölümüne ilişkin herhangi bir kısıtlamaya (ör. hizmet sınırları) sahip mi?</i> <i>Örneğin:</i> <i>Hesap başına maksimum sanal ağ sayısı</i> <i>Bir sanal ağın maksimum boyutu</i> <i>Hesap başına maksimum alt ağ sayısı</i> <i>Hesap başına maksimum yük dengeleyici sayısı</i> <i>Erişim denetimi listesi (ACL) girişlerinin maksimum sayısı</i> <i>Maksimum sanal özel ağ (VPN) tüneli sayısı</i> <i>Dağıtım başına maksimum kaynak sayısı</i> <i>Yük dengeleyici başına maksimum sertifika sayısı</i>

3.3 Depolama

	Gereklilik
1.	BLOK DEPOLAMA HİZMETİ: <i>Bulut sağlayıcısı, bilgi işlem bulut sunucularıyla birlikte kullanım için blok düzeyinde depolama birimleri sunuyor mu?</i>
2.	BLOK DEPOLAMA - IOPS: <i>Bulut sağlayıcısı, blok depolama birimleri üzerinde belirli sayıda saniyede giriş/çıkış işlemi (IOPS) veya aktarım hızı için saniyede megabayt (MB/s) gibi bir açık performans hedefi ya da performans katmanı satın alma seçeneği sunuyor mu?</i>
3.	BLOK DEPOLAMA - KATI HAL SÜRÜCÜLERİ: <i>Bulut sağlayıcısı, on milisaniyenin altında gecikme süreleri sunan katı hal sürücüsü (SSD) destekli depolama ortamını destekliyor mu?</i> • Cevap Evet ise bulut sunucusu başına bağlanabilecek maksimum SSD sayısı kaçtır?
4.	BLOK DEPOLAMA - ÖLÇEKLENDİRME: <i>Bulut sağlayıcısı, kullanıcılara yeni bir hacim tedarik etmek ve verileri kopyalamak/taşımak zorunda kalmadan mevcut herhangi bir blok depolama biriminin boyutunu artırma yeteneğini sunuyor mu?</i>

5.	BLOK DEPOLAMA - ANLIK GÖRÜNTÜLER: <i>Bulut sağlayıcısı blok depolama hizmeti için anlık görüntü alma özelliğini sunuyor mu?</i>
6.	BLOK DEPOLAMA - VERİLERİN SİLİNMESİ: <i>Bulut sağlayıcısı, verileri yetkisiz kullanıcılar ve/veya üçüncü taraflar tarafından artık okunamaz ya da erişilemez kılacak şekilde verilerin tamamen silinmesini destekliyor mu?</i>
7.	BLOK DEPOLAMA - BEKLEME SIRASINDA ŞİFRELEME <i>Bulut sağlayıcısı, birimlerde depolanan bekleyen veriler ve bunların anlık görüntüleri için sunucu tarafında şifreleme sunuyor mu?</i> Cevap Evet ise hangi kriptografik algoritma kullanılmaktadır?
8.	NESNE DEPOLAMA HİZMETİ: <i>Bulut sağlayıcısı, herhangi bir miktarda verinin depolanması ve web'den geri alınması için güvenli, dayanıklı, yüksek oranda ölçeklenebilir nesne depolama sunuyor mu?</i>
9.	NESNE DEPOLAMA - SEYREK ERİŞİM: <i>Bulut sağlayıcısı, daha az sıklıkla erişilen nesne ve dosyaların depolanmasını amaçlayan, düşük maliyetli bir depolama hizmeti katmanı sunuyor mu?</i>
10.	NESNE DEPOLAMA - DAHA DÜŞÜK DAYANIKLILIK: <i>Bulut sağlayıcısı, kullanıcıların kritik olmayan, kolaylıkla tekrar üretilebilir nesneleri düşük bir fiyat karşılığında depolayabileceği, daha az yedeklilik sunan bir katman sağlıyor mu?</i>
11.	NESNE DEPOLAMA - DAHA AZ SIKLIKTA ERİŞİM: <i>Bulut sağlayıcısı, daha az sıklıkla erişilen fakat yine de hızlı erişim gerektiren verilere yönelik bir katman sunuyor mu?</i>
12.	NESNE DEPOLAMA - NESNE KATMANLAMA: <i>Bulut sağlayıcısı, bir nesneyi erişim sıklığına bağlı olarak nesne depolama sınıfları veya katmanları arasında taşıma yeteneğini ifade eden nesne depolamayı katmanlama özelliğini sunuyor mu?</i>
13.	NESNE DEPOLAMA - YAŞAM DÖNGÜSÜ YÖNETİMİ: <i>Bulut sağlayıcısı, nesnelerin oluşturulmadan silinmeye kadar tüm yaşam döngüleri boyunca nasıl yönetileceğini tanımlayan bir yaşam döngüsü yapılandırması kullanılarak nesnelerin yaşam döngüsünü yönetmeyi destekliyor mu?</i>
14.	NESNE DEPOLAMA - POLİTİKA ODAKLI YÖNETİM: <i>Bulut sağlayıcısı, depolanan verileri, verilerin yaşam döngüsünü ve katmanlama ayarlarını yönetmek için politikalar oluşturma ve kullanma yeteneğini sunuyor mu?</i>
15.	NESNE DEPOLAMA - KONUM VE ZAMAN TABANLI İLKELER: <i>Bulut sağlayıcısı, kullanıcılara, kullanıcı konumuna ve istek zamanına bağlı olarak verilere erişimi kısıtlayabilen politikalar oluşturma özelliğini sunuyor mu?</i>
16.	NESNE DEPOLAMA - WEB SİTESİ BARINDIRMA: <i>Bulut sağlayıcısı, statik web sitelerinin kendi nesne depolama hizmeti dışında barındırılmasını destekliyor mu?</i>
17.	NESNE DEPOLAMA - BEKLEME SIRASINDA ŞİFRELEME: <i>Bulut sağlayıcısı, bekleyen veriler için şifreleme anahtarlarının bulut sağlayıcı tarafından yönetildiği sunucu tarafı şifrelemeyi (SSE) destekliyor mu?</i> Cevap Evet ise hangi kriptografik algoritma kullanılmaktadır?
18.	NESNE DEPOLAMA - KULLANICI ANAHTARLARIYLA ŞİFRELEME: <i>Bulut sağlayıcısı, müşteri tarafından sağlanan şifreleme anahtarlarının kullanıldığı sunucu tarafı şifreleme (SSE) özellikleri sunuyor mu?</i>

19.	NESNE DEPOLAMA - ANAHTAR YÖNETİMLİ HİZMET: Bulut sağlayıcısı, şifreleme anahtarları oluşturan, anahtarların nasıl kullanılabileceğini kontrol eden politikalar tanımlayan ve anahtarların doğru kullanıldığını kanıtlamak için anahtar kullanımını denetleyen bir anahtar yönetim hizmeti kullanarak sunucu tarafı şifrelemeyi (SSE) destekliyor mu?
20.	NESNE DEPOLAMA - İSTEMCİ TARAFI ANA ANAHTARI: Bulut sağlayıcısı, kullanıcılara şifreleme anahtarlarının kontrolünü elinde bulundurma ve nesneler için şifreleme/şifre çözme işlemlerini istemci tarafında gerçekleştirme seçeneğini sunuyor mu?
21.	NESNE DEPOLAMA - GÜÇLÜ TUTARLILIK: Bulut sağlayıcısı, yeni nesnelere yönelik PUT işlemleri için yazma sonrası okuma tutarlılığını destekliyor mu?
22.	NESNE DEPOLAMA - VERİ YERELLİĞİ: Bulut sağlayıcısı, bir bölgede depolanan nesnelerin, kullanıcı tarafından başka bir bölgeye açıkça aktarılmadıkları sürece, bölgeden asla ayrılmaması için güçlü bölgesel izolasyon sunuyor mu?
23.	NESNE DEPOLAMA - ÇOĞALTMA: Bulut sağlayıcısı, nesneleri kullanıcı tarafından seçilen bölgeler genelinde otomatik olarak çoğaltacak bir bölgeler arası çoğaltma özelliği sunuyor mu?
24.	NESNE DEPOLAMA - SÜRÜM OLUŞTURMA: Bulut sağlayıcısı, sürüm oluşturmaya yani bir nesnenin birden çok sürümünü depolama ve tutma yeteneğini destekliyor mu?
25.	NESNE DEPOLAMA - SİLİNEMEZ İŞARETİ: Bulut sağlayıcısı bir kullanıcının bir öğeyi silinemez olarak işaretlemesine olanak sağlıyor mu?
26.	NESNE DEPOLAMA - MFA SİLME: Bulut sağlayıcısı, silme işlemleri için ek güvenlik seçeneği olarak çok faktörlü kimlik doğrulamayı (MFA) destekliyor mu?
27.	NESNE DEPOLAMA - BİRDEN FAZLA PARÇA HALİNDE KARŞIYA YÜKLEME: Bulut sağlayıcısı, her parça nesne verilerinin bitişik bir kısmını oluşturacak ve bu nesne parçaları bağımsız olarak ya da herhangi bir sırayla karşıya yüklenebilecek şekilde bir nesnenin bir dizi parça halinde karşıya yüklenmesine olanak sağlıyor mu?
28.	NESNE DEPOLAMA - ETİKETLER: Bulut sağlayıcısı, nesne düzeyinde değiştirilebilir, dinamik etiketler oluşturma ve ilişkilendirme yeteneğini sunuyor mu?
29.	NESNE DEPOLAMA - BİLDİRİMLER: Bulut sağlayıcısı, nesne düzeyinde belirli olaylar (ör. ekleme/silme işlemleri) gerçekleştiğinde bildirimler gönderme yeteneğini sunuyor mu?
30.	NESNE DEPOLAMA - GÜNLÜKLER: Bulut sağlayıcısı tek bir erişim isteği hakkında istekte bulunan, istek zamanı, istek eylemi, istek durumu ve hata kodu gibi ayrıntılar içeren denetim günlükleri oluşturma özelliğini sunuyor mu?
31.	NESNE DEPOLAMA - NESNE ENVANTERİ: Bulut sağlayıcısı, kullanıcılara nesneleri ve durumlarını hızla görselleştirme yeteneğini vermek ve böylece kullanıcıların genel erişime açık nesneleri hızlıca belirlemesine olanak tanımak için nesne envanteri özelliği sunuyor mu?

32.	NESNE DEPOLAMA - META VERİ ENVANTERİ: Bulut sağlayıcısı, kullanıcılara nesnelerin meta verilerini hızlıca görselleştirme yeteneğini vermek için nesne envanteri özelliği sunuyor mu?
33.	NESNE DEPOLAMA - KARŞIYA YÜKLEME OPTİMİZASYONU: Bulut sağlayıcısı, optimize edilmiş bir ağ yolunu kullanarak verileri uç konumlarından depolama hizmetine yönlendirme yeteneğine sahip mi?
34.	NESNE DEPOLAMA - SORGU ÖZELLİĞİ: Bulut sağlayıcısı, kullanıcılara yapılandırılmış sorgu dili (SQL) ifadeleri kullanarak nesne depolama hizmetini sorgulama yeteneğini sunuyor mu?
35.	NESNE DEPOLAMA - ALT KÜME ALMA: Bulut sağlayıcısı, kullanıcılara basit yapılandırılmış sorgu dili (SQL) ifadelerini kullanarak bir nesneden verilerin yalnızca bir alt kümesini alma yeteneğini sunuyor mu?
36.	DOSYA DEPOLAMA HİZMETİ: Bulut sağlayıcısı, bulutta bilgi işlem bulut sunucularıyla birlikte kullanım için basit ve ölçeklenebilir bir dosya depolama hizmeti sunuyor mu?
37.	DOSYA DEPOLAMA - YEDEKLİLİK: Bulut sağlayıcısı, daha yüksek düzeylerde erişilebilirlik ve dayanıklılık elde etmek için dosya sistemi nesnelerini (ör. dizin, dosya ve bağlantı) birden fazla veri merkezi veya tesis genelinde yedekli olarak depoluyor mu?
38.	DOSYA DEPOLAMA - VERİLERİN SİLİNMESİ: Bulut sağlayıcısı, dosya depolama verilerini yetkisiz kullanıcılar veya üçüncü taraflar tarafından artık okunamaz ya da erişilemez kılacak şekilde bu verilerin tamamen silinmesini destekliyor mu?
39.	DOSYA DEPOLAMA - YÜKSEK ERİŞİLEBİLİRLİK: Bulut sağlayıcısının yönetilen dosya sistemi yüksek düzeyde erişilebilirlik sağlıyor mu?
40.	DOSYA DEPOLAMA - NFS: Bulut sağlayıcısı, ağ dosya sistemi (NFS) protokolünü destekliyor mu?
41.	DOSYA DEPOLAMA - SMB: Bulut sağlayıcısı, sunucu ileti bloku (SMB) protokolünü destekliyor mu?
42.	DOSYA DEPOLAMA - BEKLEME SIRASINDA ŞİFRELEME Bulut sağlayıcısının dosya depolama hizmeti, bekleme sırasında şifrelemeyi destekliyor mu?
43.	DOSYA DEPOLAMA - TAŞIMA SIRASINDA ŞİFRELEME Bulut sağlayıcısının dosya depolama hizmeti, verilerin taşıma sırasında şifrlenmesini destekliyor mu?
44.	DOSYA DEPOLAMA - VERİ TAŞIMA ARACI: Bulut sağlayıcısı, kullanıcıların verileri şirket içi sistemlerden bulut tabanlı dosya sistemine taşınmasına olanak sağlayan bir veri taşıma aracı sunuyor mu?
45.	ARŞİV DEPOLAMA HİZMETİ: Bulut sağlayıcısı, daha az sıklıkla erişilen ve neredeyse değiştirilemez olan nesnelerin ve dosyaların arşivlenmesini amaçlayan, çok düşük maliyetli bir depolama hizmeti sunuyor mu?

46.	ARŞİV DEPOLAMA - HATA TOLERANSI: Bulut sağlayıcısının mimarisi arşiv depolama hizmeti için hata toleransı sağlıyor mu?
47.	ARŞİV DEPOLAMA - DEĞİŞTİRİLEMEZLİK: Bulut sağlayıcısı, arşivlenen nesnelerin ve dosyaların değiştirilemezliğini destekliyor mu?
48.	ARŞİV DEPOLAMA - WORM: Bulut sağlayıcısı bir kez yazma birçok kez okuma (WORM) özelliğini sunuyor mu?
49.	ARŞİV DEPOLAMA - ALT KÜME ALMA: Bulut sağlayıcısı, kullanıcılara basit yapılandırılmış sorgu dili (SQL) ifadelerini kullanarak bir arşivlenmiş nesneden verilerin yalnızca bir alt kümesini alma yeteneğini sunuyor mu?
50.	ARŞİV DEPOLAMA - HIZLI ALMA: Bulut sağlayıcısı, kullanıcılara farklı maliyetlerde ve alım sürelerinde birden fazla veri alma seçeneği sunuyor mu?
51.	ARŞİV DEPOLAMA - BEKLEME SIRASINDA ŞİFRELEME Bulut sağlayıcısının arşiv depolama hizmeti, bekleme sırasında şifrelemeyi destekliyor mu?
52.	DEPOLAMA - HİZMET SINIRLARI: Bulut sağlayıcısı, yukarıdaki depolama bölümüne ilişkin herhangi bir kısıtlamaya (ör. hizmet sınırları) sahip mi? Örneğin: Maksimum birim boyutu Bir bulut sunucusuna bağlanan maksimum sürücü sayısı Saniyede giriş/çıkış işlemlerinin (IOPS) maksimum sayısı Maksimum nesne boyutu Depolama hesabı başına maksimum nesne sayısı Maksimum anlık görüntü sayısı

4. İdare

	Gereklilik
1.	İDARE - KULLANICILAR VE GRUPLAR: Bulut sağlayıcısı, altyapısının ve kaynaklarının kullanıcılarını ve kullanıcı gruplarını oluşturmak ve yönetmek için bir hizmet sunuyor mu?
2.	İDARE - PAROLA SIFIRLAMA: Bulut sağlayıcısı, kullanıcıların kendi parolalarını self servis şekilde sıfırlamasına olanak sağlıyor mu?
3.	İDARE - İZİNLER: Bulut sağlayıcısı, kullanıcılara ve gruplara kaynak düzeyinde izin ekleme yeteneğini sunuyor mu?
4.	İDARE - GEÇİCİ İZİNLER: Bulut sağlayıcısı belirli bir zaman aralığı boyunca geçerli izinler oluşturma yeteneğini sunuyor mu?

5.	İDARE - GEÇİCİ KİMLİK BİLGİLERİ: Bulut sağlayıcısı, kullanıcılara, güvenilen kullanıcılar için birkaç dakika ila birkaç saat boyunca geçerli olacak şekilde yapılandırılmış geçici güvenlik kimlik bilgileri oluşturma ve sağlama yeteneğini sunuyor mu?
6.	İDARE - ERİŞİM DENETİMİ: Bulut sağlayıcısı, altyapı kaynaklarına erişim için ayrıntılı erişim denetimleri sunuyor mu? • Cevap Evet ise bu denetimler hangi koşulları (ör. günün saati, kaynak IP adresi vb.) kullanabilir?
7.	İDARE - YERLEŞİK POLİTİKALAR: Bulut sağlayıcısı altyapısı, kullanıcılara ve gruplara bağlanabilecek yerleşik erişim denetimi politikaları içeriyor mu?
8.	İDARE - ÖZEL POLİTİKALAR: Bulut sağlayıcısı altyapısı, kullanıcılara ve gruplara bağlanabilecek yerleşik erişim denetimi politikalarının oluşturulmasına ve özelleştirilmesine olanak sağlıyor mu?
9.	İDARE - POLİTİKA SİMÜLATÖRÜ: Bulut sağlayıcısı, erişim denetimi politikaları üretime geçirilmeden önce bu politikaların etkilerini test etmeye yönelik bir mekanizma sunuyor mu?
10.	İDARE - BULUTTA MFA: Bulut sağlayıcısı, alt yapısı için bir ek erişim denetimi ve kimlik doğrulaması katmanı olarak çok faktörlü kimlik doğrulama (MFA) kullanımını destekliyor mu?
11.	İDARE - HİZMET SINIRLARI: Bulut sağlayıcısı, yukarıdaki idare bölümüne ilişkin herhangi bir kısıtlamaya (ör. hizmet sınırları) sahip mi? Örneğin: Maksimum kullanıcı sayısı Maksimum grup sayısı Maksimum yönetilen politika sayısı

5. Güvenlik

	Gereklilik
1.	GÜVENLİK - GEÇMİŞ ARAŞTIRMASI: Hizmet altyapısına (fiziksel ya da sanal) erişimi olan bulut sağlayıcısının tüm personeli için geçmiş araştırması yapıyor mu?
2.	GÜVENLİK - FİZİKSEL ERİŞİM: Bulut sağlayıcısı, belirli bir sorun bileti, değişiklik isteği veya benzer bir resmî izin olmadığı sürece personelin hizmet altyapısına erişimini kısıtlıyor mu?
3.	GÜVENLİK - ERİŞİM GÜNLÜKLERİ: Bulut sağlayıcısı, altyapısındaki personel erişimini günlüğe kaydediyor mu, bu tür erişimler her zaman günlüğe kaydediliyor mu ve günlükler en az 90 gün süreyle saklanıyor mu?
4.	GÜVENLİK - ANA SUNUCUDA OTURUM AÇMA İŞLEMLERİ: Bulut sağlayıcısı, sağlayıcı personelinin bilgi işlem ana sunucularında oturum açmasını kısıtlayıp bunun yerine işlem ana sunucularında gerçekleştirilen tüm görevleri otomatik hale getiriyor mu ve bu otomatik görevlerin içeriği en az 90 gün süreyle saklanan günlüklere kaydediliyor mu?
5.	GÜVENLİK - ŞİFRELEME ANAHTARLARI:

	<i>Bulut sağlayıcısı, kullanıcı verilerini şifrelemede kullanılan şifreleme anahtarlarının oluşturulması ve kontrol edilmesi için bir hizmet sunuyor mu?</i>
6.	GÜVENLİK - ERİŞİM ANAHTARI YÖNETİMİ: <i>Bulut sağlayıcısı bir erişim anahtarının en son ne zaman kullanıldığını tespit etme, eski anahtarları değiştirme ve etkin olmayan kullanıcıları kaldırma yeteneğini sunuyor mu?</i>
7.	GÜVENLİK - MÜŞTERİ TARAFINDAN SAĞLANAN ANAHTARLAR: <i>Bulut sağlayıcısı, kullanıcıların, anahtarları kendi anahtar yönetimi altyapılarından, bulut hizmeti sağlayıcısının anahtar yönetim hizmetine aktarmasına olanak sağlıyor mu?</i>
8.	GÜVENLİK - ŞİFRELEME ANAHTARLARI HİZMETİ ENTEGRASYONU: <i>Bulut sağlayıcısının anahtar yönetimi hizmeti, bekleme halindeki verilerin şifrelenmesi özelliğini sağlamak için diğer bulut hizmetleriyle entegre mi?</i>
9.	GÜVENLİK - HSM: <i>Bulut sağlayıcısı, tahsis edilmiş donanım güvenlik modülleri (HSM), yani kurcalamaya dayanıklı donanım modülü içinde güvenli anahtar depolama ve şifreleme işlemleri sağlayan donanım cihazları sunuyor mu?</i>
10.	GÜVENLİK - ŞİFRELEME ANAHTARLARININ DAYANIKLILIĞI: <i>Bulut sağlayıcısı, anahtarların ihtiyaç duyulduğunda kullanılabilir olmasını sağlamak için birden fazla kopyasının saklanması dahil olmak üzere anahtar dayanıklılığını destekliyor mu?</i>
11.	GÜVENLİK - SSO: <i>Bulut sağlayıcısı, kullanıcıların birden fazla hesaba ve iş uygulamasına erişimi merkezi olarak yönetmesine olanak sağlayan bir yönetilen tek oturum açma (SSO) hizmeti sunuyor mu?</i>
12.	GÜVENLİK - SERTİFİKALAR: <i>Bulut sağlayıcısı, güvenli yuva katmanı (SSL)/aktarım katmanı güvenliği (TLS) sertifikalarının tedariki, yönetimi ve dağıtımı için bir yönetilen hizmet sunuyor mu?</i>
13.	GÜVENLİK - SERTİFİKA YENİLEME: <i>Bulut sağlayıcısının sertifika yönetim hizmeti, sertifikaların yenilenmesini kolaylaştırıyor mu?</i>
14.	GÜVENLİK - JOKER SERTİFİKALAR: <i>Bulut sağlayıcısının sertifika yönetim hizmeti, joker sertifikaların kullanımını destekliyor mu?</i>
15.	GÜVENLİK - SERTİFİKA YETKİLİSİ: <i>Bulut sağlayıcısının sertifika yönetim hizmeti aynı zamanda bir sertifika yetkilisi (CA) görevi görüyor mu?</i>
16.	GÜVENLİK - ACTIVE DIRECTORY <i>Bulut sağlayıcısı, bulutta bir yönetilen Microsoft Active Directory (AD) hizmeti sunuyor mu?</i>
17.	GÜVENLİK - ŞİRKET İÇİ ACTIVE DIRECTORY: <i>Bulut sağlayıcısının yönetilen Microsoft Active Directory (AD) hizmeti, şirket içi Microsoft Active Directory (AD) ile entegrasyonu destekliyor mu?</i>
18.	GÜVENLİK - LDAP: <i>Bulut sağlayıcısının yönetilen Microsoft Active Directory (AD) hizmeti, basit izin erişim protokolünü (LDAP) destekliyor mu?</i>
19.	GÜVENLİK - ACTIVE DIRECTORY <i>Bulut sağlayıcısının yönetilen Microsoft Active Directory (AD) hizmeti, güvenlik onayı biçimlendirme dilini (SAML) destekliyor mu?</i>
20.	GÜVENLİK - KİMLİK BİLGİSİ YÖNETİMİ:

	<i>Bulut sağlayıcısı, kullanıcıların uygulama programlama arabirimi (API) anahtarları, veritabanı kimlik bilgileri ve diğer gizli bilgiler gibi kimlik bilgilerini kolayca değiştirmesine, yönetmesine ve almasına yardımcı olan bir yönetilen hizmet sunuyor mu?</i>
21.	GÜVENLİK - WAF: <i>Bulut sağlayıcısı, web uygulamalarının uygulama erişilebilirliğini etkileyebilecek, güvenliği tehlikeye atabilecek veya aşırı kaynak kullanabilecek yaygın web açıklarından korumaya yardımcı olan bir web uygulaması güvenlik duvarı (WAF) sunuyor mu?</i>
22.	GÜVENLİK - DDOS: <i>Bulut sağlayıcısı yaygın, sık karşılaşılan ağ ve aktarım katmanını dağıtılmış hizmet reddi (DDoS) saldırılarına karşı koruma ve gelişmiş uygulama katmanını saldırılarını hafifletmek için özelleştirilmiş kurallar yazma yeteneğini sağlayan bir hizmet sunuyor mu?</i>
23.	GÜVENLİK - GÜVENLİK ÖNERİLERİ: <i>Bulut sağlayıcısı, uygulamalar ve kaynaklardaki potansiyel güvenlik açıklarının otomatik olarak değerlendirilmesini sağlayan bir hizmet sunuyor mu?</i>
24.	GÜVENLİK - TEHDİT ALGILAMA: <i>Bulut sağlayıcısı bir yönetilen tehdit algılama hizmeti sunuyor mu?</i>
25.	GÜVENLİK - HİZMET SINIRLARI: <i>Bulut sağlayıcısı, yukarıdaki güvenlik bölümüne ilişkin herhangi bir kısıtlamaya (ör. hizmet sınırları) sahip mi?</i> <i>Örneğin:</i> <i>Maksimum müşteri ana anahtar sayısı</i> <i>Maksimum donanım güvenlik modülü (HSM) sayısı</i>

6. Uygunluk

Aşağıdaki liste yalnızca örnek olarak verilmiştir. Bulut hizmetleri için geçerli olabilecek sertifika ve standartların tam kapsamlı listesi olarak kabul edilmemelidir.

Lütfen bulut sağlayıcısının karşıladığı uluslararası ve sektöre özel uygunluk standartlarını belirtin:

Sertifikalar/Tasdikler	Yasalar, Düzenlemeler ve Gizlilik	Uyumlaştırmalar/Çerçeveler
☐ C5 [Almanya]	☐ AB Veri Koruma Direktifi	☐ CDSA
☐ CISPE Veri Koruma Davranış Kuralları	☐ AB Model Maddeleri	
☐ CNDP (İklim Nötr Veri Merkezi Paketi)		
☐ DIACAP	☐ FERPA	☐ CIS
☐ DoD SRG Düzey 2 ve 4	☐ GDPR	☐ Criminal Justice Info. Service (CJIS)
☐ FedRAMP	☐ GLBA	☐ CSA
☐ FIPS 140-2	☐ HIPAA	☐ AB-ABD Gizlilik Kalkanı

☐ HDS (Fransa, Sağlık)	☐ HITECH	☐ AB Güvenli Liman
☐ ISO 9001	☐ IRS 1075	☐ FISC
☐ ISO 27001	☐ ITAR	☐ FISMA
☐ ISO 27017	☐ PDPA - 2010 [Malezya]	☐ G-Cloud [Birleşik Krallık]
☐ ISO 27018	☐ PDPA - 2012 [Singapur]	☐ GxP (FDA CFR 21 Bölüm 11)
☐ IRAP [Avustralya]	☐ PIPEDA [Kanada]	☐ ICREA
☐ MTCS Katman 3 [Singapur]	☐ Gizlilik Kanunu [Avustralya]	☐ IT Grundschutz [Almanya]
☐ PCI DSS Düzey 1	☐ Gizlilik Kanunu [Yeni Zelanda]	☐ MARS - E
☐ SEC Kural 17-a-4(f)	☐ İspanya DPA Yetkisi	☐ MITA 3.0
☐ SOC1 / ISAE 3402	☐ Birleşik Krallık DPA - 1988	☐ MPAA
☐ SOC2/SOC3	☐ VPAT/Bölüm 508	☐ NIST
☐ SWIPO IaaS Davranış Kuralları		☐ Uptime Institute Katmanları
		☐ Birleşik Krallık Bulut Güvenliği İlkeleri

Yukarıdaki uygunluk raporlarının kullanılması kamu sektörü kuruluşlarının benzersiz teklifleri, kabul gören güvenlik, uygunluk ve operasyon standartları temelinde değerlendirmesine olanak sağlar. Bu tür raporlar CISP'nin, ilgili standartlara uygunluğu yoluyla, genel bulut hizmeti sağlayıcıları için zorunlu olan aşağıdaki veri merkezi operasyon kontrollerini karşıladığını gösterebilir. Bu tür raporlara uygunluk talep edilmesi, kamu sektörü kurumlarının aşağıdaki denetimlerin uygulandığına dair güvence edinmesine yardımcı olur.

- **Yakından takip edilen erişim:** CISP, fiziksel erişimi yalnızca haklı bir iş gerekçesiyle konumda bulunması gereken kişilere izin verilecek şekilde kısıtlamalıdır. Erişim izni verilirse gerekli iş tamamlanır tamamlanmaz izin iptal edilmelidir.
- **Kontrollü ve izlemeye tabi giriş:** Çevre Veri Merkezi Katmanına girişte kontrollü bir süreç uygulanmalıdır. CISP, her kapiya güvenlik görevlisi koymalı ve güvenlik kameraları yoluyla görevlileri ve ziyaretçileri izleyen süpervizörler atamalıdır. Onaylanan kişiler sahaya geldiğinde bu kişilere, çok faktörlü kimlik doğrulaması gerektiren ve erişimi önceden onaylanmış alanlarla sınırlandıran bir kimlik kartı verilmelidir.
- **CISP veri merkezi çalışanları:** Bir veri merkezine rutin olarak erişmesi gereken CISP çalışanlarına, iş fonksiyonlarına bağlı olarak tesisin ilgili alanlarına erişim izni verilmelidir ve erişim düzenli olarak irdelenmelidir. Personel listeleri bir alan erişim yöneticisi tarafından rutin olarak gözden geçirilerek her çalışanın yetkisinin hâlâ gerekli olduğundan emin olunmalıdır. Bir çalışanın veri merkezinde bulunmasını gerektiren bir iş ihtiyacı yoksa bu çalışanın ziyaretçi sürecinden geçmesi zorunlu kılınmalıdır.
- **Yetkisiz giriş izlemesi:** CISP'ler güvenlik kameralarını, yetkisiz erişim algılama ve erişim günlüğü izleme sistemlerini kullanarak veri merkezi tesisine yetkisiz girişi sürekli olarak izlemelidir. Girişler bir kapının zorlanması veya açık tutulması durumunda sesli alarm veren cihazlarla güvenlik altına alınmalıdır.
- **CISP Güvenlik Operasyonları Merkezi küresel güvenliği izler:** CISP'nin dünya genelinde Güvenlik Operasyonları Merkezi bulunmalıdır. Bu merkezler, CISP veri merkezleriyle ilgili güvenlik programlarını izlemek, önceliklendirmek ve yürütmekten

sorumludur. Fiziksel erişim yönetimini ve yetkisiz erişim algılama müdahalelerini denetlemeleri gerekir. Ayrıca, sahadaki veri merkezi güvenlik ekiplerine küresel, 7/24 destek sağlamaktan, erişim etkinliklerinin sürekli olarak izlenmesinden, erişim izinlerinin iptal edilmesinden ve tüm potansiyel güvenlik olaylarına yanıt vermek ve analiz etmekten sorumludurlar.

- **Katman katman erişim incelemesi:** Altyapı Katmanına erişim iş ihtiyacına dayalı olarak kısıtlanmalıdır. Katman katman erişim inceleme süreci uygulandığında her katmana giriş hakkı varsayılan olarak verilmez. Belirli bir katmana erişim izni yalnızca söz konusu katmana erişim için özel bir neden varsa verilmelidir.
- **Ekipman bakımlarının yapılması düzenli operasyonların bir parçasıdır:** CISP ekipleri makineler, ağlar ve yedek ekipmanlar üzerinde tanılama işlemleri gerçekleştirerek iyi çalışır durumda olduklarından ve bir acil durumda da kullanıma hazır olacaklarından emin olmalıdır. Veri merkezi ekipmanları ve altyapı hizmetleri üzerindeki rutin bakım kontrolleri düzenli CISP veri merkezi operasyonlarının bir parçası olmalıdır.
- **Acil duruma hazır yedek ekipmanlar:** CISP'nin bir acil durumda faaliyetlerini sürdürebilmesi için su, güç, telekomünikasyon ve dahili bağlantılar yedekli olarak tasarlanmalıdır. Bir elektrik kesintisi sırasında, belirli işlevler için kesintisiz güç kaynaklarının devreye alınabilmesi ve jeneratörlerin tüm tesise güç sağlayabilmesi için elektrik gücü sistemleri tamamen yedekli olarak tasarlanmalıdır. Çalışanlar ve sistemler sıcaklığı ve nemi izleyip kontrol ederek aşırı ısınmayı önlemeli, olası hizmet kesintilerini daha da azaltmalıdır.
- **Teknoloji ve insanlar daha fazla güvenlik için birlikte çalışır:** Veri Katmanına girme yetkisini elde etmek için zorunlu prosedürler olmalıdır. Bunlara kişinin erişim başvurusunun yetkili bireyler tarafından incelenmesi ve onaylanması dahildir. Bu arada, tehdit ve elektronik yetkisiz erişim algılama sistemleri tehditleri veya şüpheli etkinlikleri izlemeli ve tespit edilenler için otomatik olarak uyarılar tetiklemelidir. Örneğin bir kapı tutuluyorsa veya zorla açılırsa alarm tetiklenir. CISP, güvenlik kameraları yerleştirmeli ve görüntü kayıtlarını yasal ve uygunluk gerekliliklerine göre saklamalıdır.
- **Fiziksel ve teknolojik yetkisiz erişimi engelleme:** Sunucu odalarına erişim noktalarının güvenliği, çok faktörlü yetkilendirme gerektiren elektronik denetim cihazlarıyla donatılmalıdır. CISP ayrıca teknolojik yetkisiz erişimleri engellemeye hazırlıklı olmalıdır. CISP sunucuları, çalışanları, verileri kaldırmaya yönelik her türlü girişime karşı uyarmalıdır. Her ne kadar düşük olasılıklı olsa da bir güvenlik ihlali oluşması durumunda sunucu otomatik olarak devre dışı bırakılmalıdır.
- **Sunucuların ve ortam depolama cihazlarının titizlikle korunması:** Müşteri verilerini depolamak için kullanılan ortam depolama cihazları, CISP tarafından Kritik olarak sınıflandırılmalı ve tüm yaşam döngüleri boyunca kritik öneme sahip varlıklar olarak ele alınmalıdır. CISP, cihazların nasıl kurulacağı, bakımlarının nasıl yapılacağı ve kullanım ömürlerinin sonunda nasıl bertaraf edileceği konusunda titizlikle hazırlanmış standartlara sahip olmalıdır. Bir depolama cihazı yararlı ömrünü doldurduğunda CISP, NIST 800-88'de ayrıntılı şekilde açıklanan teknikleri kullanarak ortamı kullanımdan kaldıracaktır. Müşteri verilerinin depolandığı ortamlar, güvenli bir şekilde kullanımdan kaldırılana kadar CISP kontrol biriminden kaldırılmaz.
- **CISP prosedür ve sistemlerinin üçüncü taraf denetçiler tarafından denetlenmesi:** CISP, dış denetçiler tarafından denetlenmelidir. Bu kapsamda, veri merkezleri denetlenmeli ve CISP'nin güvenlik sertifikalarıyla ilişkili kabul gören kurallara uyduğunu onaylamak için ayrıntılı bir inceleme gerçekleştirilmelidir. Uygunluk programına ve bunun gerekliliklerine bağlı olarak, dış denetçiler ortamları nasıl kullandıklarını ve bertaraf ettiklerini öğrenmek için CISP çalışanlarıyla görüşebilir. Denetçiler ayrıca güvenlik kamerası akışlarını izleyerek veri merkezi genelindeki girişleri ve koridorları gözlemleyebilir. CISP'nin elektronik erişim denetimi cihazları ve güvenlik kameraları gibi ekipmanları inceleyebilirler.
- **Beklenmedik durumlara hazırlıklı olma:** CISP, doğal afet ve yangın gibi potansiyel çevre tehditlerine karşı proaktif olarak hazırlanmalıdır. CISP, veri merkezlerini koruma altına almak için otomatik sensörler ve müdahale ekipmanları kurabilir. Su basması sorunlarına karşı çalışanları uyarmak için su sensörü cihazları kurulmalı ve otomatik pompalar devreye girerek suyu atıp hasarı önlemelidir. Benzer şekilde, otomatik yangın algılama ve söndürme ekipmanları riski azaltır ve yangın durumunda CISP çalışanlarını ve itfaiyeyi uyarır.
- **Birden Çok Erişilebilirlik Bölgesi ile Yüksek Erişilebilirlik:** CISP, daha yüksek hata toleransı için birden çok Erişilebilirlik Bölgesi sağlamalıdır. Her Erişilebilirlik Bölgesi bir veya daha fazla veri merkezinden oluşmalı, fiziksel açıdan birbirinden ayrı olmalı, yedekli güç ve ağ iletişimi olanaklarına sahip olmalıdır. Kesintiye uğramadan Erişilebilirlik Bölgeleri arasında otomatik olarak yük devretme yapabilecek uygulamalar geliştirilebilmesi için Erişilebilirlik Bölgeleri hızlı, özel fiber optik ağ iletişimi yoluyla birbirine bağlanmalıdır.
- **Kesintileri simüle etme ve yanıtı ölçme:** CISP, doğal afetler nedeniyle oluşabilecek kesintilerin nasıl önlenebileceğini ve azaltılabileceğini açıklayan, olay öncesinde, esnasında ve sonrasında atılması gereken adımları ayrıntılı olarak belirten bir

İş Sürekliliği Planına sahip olmalıdır. CISP, beklenmedik olaylara hazırlıklı olmak ve bu tür olayların etkilerini azaltmak için İş Sürekliliği Planını, farklı senaryoları simüle eden tatbikatlarla düzenli olarak test etmelidir. CISP, çalışanlarının ve süreçlerinin nasıl performans gösterdiğini belgelemeli, ardından çıkarılan dersler konusunda bilgilendirme yapmalı ve yanıt oranını iyileştirmek için gerekli olabilecek düzeltici eylemleri belirlemelidir. CISP personeli bir kesinti meydana geldikten sonra faaliyetleri hızla normale döndürme konusunda eğitilmiş ve hazırlıklı olmalıdır ve hatalar nedeniyle arıza süresinin daha da uzamaması için metodolojik bir kurtarma süreci izlemelidir.

- **Verimlilik hedeflerinin karşılanması:** CISP, veri merkezi tasarımıyla çevresel riskleri ele almanın yanı sıra sürdürülebilirlik hususlarını da dikkate almalıdır. CISP, veri merkezlerinde yenilenebilir enerji kullanma taahhüdünün ayrıntılarını sağlamalı ve müşterilerinin kendi veri merkezlerini kullanmak yerine CISP veri merkezlerini kullanarak karbon emisyonlarını nasıl azaltabileceğine dair bilgi vermelidir.
- **Saha Seçimi:** CISP bir konum seçmeden önce ön çevresel ve coğrafi değerlendirmelerde bulunmalıdır. Veri merkezi konumları; sel, olumsuz hava olayları ve sismik aktivite gibi çevresel riskleri azaltacak şekilde dikkatli olarak seçilmelidir. CISP Erişilebilirlik Bölgeleri birbirinden bağımsız ve fiziksel olarak ayrılmış şekilde inşa edilmelidir.
- **Yedeklilik:** Veri merkezleri, hizmet düzeylerini sürdürürken hataları öngörebilecek ve tolere edebilecek şekilde tasarlanmalıdır. Hata durumunda, otomatik süreçler trafiği etkilenen alandan uzaklaştırmalıdır. Temel uygulamalar N+1 standardına göre dağıtılmalıdır. Böylece, bir veri merkezi hatası durumunda, trafiğin yük dengeleme yoluyla geri kalan sahalarla yönlendirilebilmesi için yeterli kapasite bulunacaktır.
- **Erişilebilirlik:** CISP, sistemini erişilebilir tutmak ve bir kesinti durumunda hizmeti normale döndürmek için gerekli kritik sistem bileşenlerini tanımlamalıdır. Kritik sistem bileşenleri birden fazla, yalıtılmış konumda yedeklenmelidir. Her konum veya Erişilebilirlik Bölgesi, birbirinden bağımsız olarak, yüksek güvenilirlikte çalışacak şekilde tasarlanmalıdır. Uygulamaların kesinti olmaksızın Erişilebilirlik Alanları arasında otomatik olarak yük devredebilmesi için Erişilebilirlik Alanları birbirine bağlanmalıdır. Yüksek derecede dayanıklı sistemler ve dolayısıyla yüksek hizmet erişilebilirliği, sistem tasarımının bir fonksiyonu olmalıdır. Erişilebilirlik Alanları ve veri çoğaltma özelliklerine sahip veri merkezi tasarımı, CISP müşterilerinin son derece kısa kurtarma süreleri ve kurtarma noktası hedeflerinin yanı sıra en üst düzeyde hizmet erişilebilirliği elde etmesine olanak sağlamalıdır.
- **Kapasite Planlaması:** CISP, erişilebilirlik taahhütlerini ve gerekliliklerini desteklemek için hizmet kullanımını sürekli olarak izlemeli ve gerektiğinde altyapı dağıtımını gerçekleştirmelidir. CISP, CISP altyapısı kullanımını ve talebini en azından aylık bazda değerlendiren bir kapasite planlama modeli uygulamalıdır. Bu model, gelecekteki talebin planlanmasına destek olmalı ve bilgi işleme, telekomünikasyon ve denetim günlükünün depolanması gibi hususları dikkate almalıdır.

İŞ SÜREKLİLİĞİ VE OLAĞANÜSTÜ DURUM KURTARMA

- **İş Sürekliliği Planı:** CISP'nin İş Sürekliliği Planında, çevre kaynaklı kesintileri önlemeye ve azaltmaya yönelik önlemler açıklanmalıdır. Bir olay öncesinde, esnasında ve sonrasında atılması gereken adımlarla ilgili operasyonel ayrıntıları içermelidir. İş Sürekliliği Planı, farklı senaryolara ilişkin simülasyonları içeren testlerle desteklenmelidir. CISP, sürekli gelişim amaçları doğrultusunda, test sırasında ve sonrasında, çalışanların ve süreçlerin performansını, düzeltici eylemleri ve çıkarılan dersleri belgelemelidir.
- **Pandemi Yanıtı:** CISP, bulaşıcı hastalık salgını tehditlerine hızla yanıt verme konusunda hazırlıklı olmak için olağanüstü durum kurtarma planına pandemi müdahalesi politika ve prosedürlerini dahil etmelidir. Risk azaltma stratejileri, kritik süreçleri bölge dışındaki kaynaklara aktarmak için alternatif personel kullanımı modellerini ve kritik iş operasyonlarının desteklenmesi için bir kriz yönetim planının devreye sokulmasını içerir. Pandemi planlarında uluslararası sağlık kuruluşları ve sağlık düzenlemeleri dikkate alınmalı ve uluslararası kuruluşlardaki irtibat kişilerinin bilgileri eklenmelidir.

İZLEME VE GÜNLÜĞE KAYDETME

- **Veri Merkezine Erişimin İncelenmesi:** Veri merkezlerine erişim düzenli olarak incelenmelidir. CISP'nin İK sisteminde bir çalışanın kaydı sonlandırıldığında ilgili çalışanın erişim izni otomatik olarak iptal edilmelidir. Ek olarak, bir çalışan veya yüklenicinin erişim izninin süresi, onaylanan isteğin süresi dolduktan sonra sona erer. Bu durumda, ilgili kişi CISP çalışanı olarak kalsa bile, bu kişinin erişim izni iptal edilmelidir.
- **Veri Merkezi Erişim Günlükleri:** CISP veri merkezlerine fiziksel erişim günlüğe kaydedilmeli, izlenmeli ve ilgili veriler saklanmalıdır. CISP, gerekli durumlarda güvenliği artırmak için mantıksal ve fiziksel izleme sistemlerinden elde edilen bilgilerin korelasyonunu sağlamalıdır.

- **Veri Merkezine Erişimin İzlenmesi:** CISP, güvenlik programlarını izlemek, önceliklendirmek ve yürütmekten sorumlu küresel Güvenlik Operasyonları Merkezini kullanarak veri merkezlerini izlemelidir. Veri merkezi erişim etkinliklerini yönetip izleyerek 7/24 küresel destek sağlamalı ve önceliklendirme yaparak, ilgili yerlere danışarak, olayları analiz ederek ve yanıt ekipleri göndererek güvenlik olaylarına yerel ekipler ve diğer destek ekipleri tarafından müdahale edilmesini sağlamalıdır.

GÖZETİM VE ALGILAMA

- **CCTV:** Sunuculara fiziksel erişim noktaları, Kapalı Devre Kamera Sistemi (CCTV) ile kayıt altına alınmalıdır. Görüntüler, yasal ve uygunluk gerekliliklerine göre saklanmalıdır.
- **Veri Merkezi Giriş Noktaları:** Fiziksel erişim, bina giriş noktalarında profesyonel güvenlik personeli tarafından gözetim, algılama sistemleri ve diğer elektronik araçlar kullanılarak denetlenmelidir. Yetkili personel, veri merkezlerine erişmek için çok faktörlü kimlik doğrulama mekanizmaları kullanılmalıdır. Sunucu odalarına girişler, kapıların zorla açılması veya açık tutulması halinde olay müdahalesinin başlatılması için sesli alarm veren cihazlarla donatılmalıdır.
- **Yetkisiz Erişim Algılama:** Güvenlik olaylarını izlemek, algılamak ve bir olay algılandığında ilgili personeli otomatik olarak uyarmak üzere veri katmanına elektronik yetkisiz erişim algılama sistemleri kurulmalıdır. Sunucu odalarının giriş ve çıkış noktaları, giriş veya çıkış izni verilmeden önce her bireyin çok faktörlü kimlik doğrulamasından geçmesini gerektiren cihazlarla güvenlik altına alınmalıdır. Kapıların kimlik doğrulamasından geçilmeden zorla açılması ya da kapıların açık tutulması halinde bu cihazlar sesli alarm verecektir. Kapı alarm cihazları ayrıca bireylerin çok faktörlü kimlik doğrulamasından geçmeden bir veri katmanına giriş veya çıkış yaptığı durumları algılayacak şekilde yapılandırılmalıdır. Alarmlar hemen 7/24 CISP Güvenlik Operasyonları Merkezine iletilerek derhal günlüğe kaydedilmeli, analiz edilmeli ve müdahale edilmelidir.

CİHAZ YÖNETİMİ

- **Varlık Yönetimi:** CISP varlıkları, varlıklarla ilgili sahip, konum, durum ve bakım bilgilerinin yanı sıra diğer açıklayıcı bilgileri saklayan ve takip eden bir envanter yönetim sistemi yoluyla merkezi olarak yönetilmelidir. Varlıklar, satın alma sonrasında taranıp takip edilmeli ve bakıma giren varlıklar sahip, durum ve çözüm bilgileri açısından kontrol edilip izlenmelidir.
- **Ortamların İmhası:** Müşteri verilerini depolamak için kullanılan ortam depolama cihazları, CISP tarafından Kritik olarak sınıflandırılmalı ve tüm yaşam döngüleri boyunca kritik öneme sahip varlıklar olarak ele alınmalıdır. CISP, cihazların nasıl kurulacağı, bakımlarının nasıl yapılacağı ve kullanım ömürlerinin sonunda nasıl bertaraf edileceği konusunda titizlikle hazırlanmış standartlara sahip olmalıdır. Bir depolama cihazı yararlı ömrünü doldurduğunda CISP, NIST 800-88'de ayrıntılı olarak açıklanan teknikleri kullanarak ortamı kullanımdan kaldırmalıdır. Müşteri verilerinin depolandığı ortamlar, güvenli bir şekilde kullanımdan kaldırılana kadar CISP kontrol biriminden kaldırılmamalıdır.

OPERASYONEL DESTEK SİSTEMLERİ

- **Güç:** CISP veri merkezinin elektrikli sistemleri tamamen yedekli olarak ve günün 24 saati operasyonlar üzerinde hiçbir olumsuz etkiye neden olmadan bakımları yapılabilecek şekilde tasarlanmalıdır. CISP, elektrik kesintisi durumunda tesisteki kritik ve temel yüklerle ilgili operasyonların sürdürülebilmesi için veri merkezlerinin yedek güç kaynağı ile donatıldığından emin olmalıdır.
- **İklim ve Sıcaklık:** CISP veri merkezleri, aşırı ısınmayı önlemek ve hizmet kesintisi olasılığını azaltmak amacıyla uygun iklimlendirme mekanizmalarını kullanarak sunucular ve diğer donanımlar için uygun çalışma sıcaklığını sağlayıp korumalıdır. Personel ve sistemler, sıcaklığı ve nemi izleyip kontrol ederek uygun düzeylerde tutmalıdır.
- **Yangın Algılama ve Söndürme:** CISP veri merkezleri otomatik yangın algılama ve söndürme ekipmanlarıyla donatılmalıdır. Yangın algılama sistemleri; ağ iletişimi ve altyapı alanlarının yanı sıra mekanik alanlara kurulmuş duman algılama sensörleri içermelidir. Bu alanlar da yangın söndürme sistemleriyle korunmalıdır.
- **Sızıntı Algılama:** CISP veri merkezlerinde olası su sızıntılarını tespit etmek için uygun algılama cihazları bulunmalıdır. Su sızıntısı tespit edilmesi halinde su hasarını önlemek için suyun giderilmesini sağlayacak mekanizmalar bulunmalıdır.

ALTYAPI BAKIMI

- **Ekipman Bakımı:** CISP, veri merkezlerindeki sistemleri iyi çalışır durumda tutmak için elektrikli ve mekanik ekipmanların önleyici bakımlarını izlemeli ve bakımların yapıldığından emin olmalıdır. Ekipman bakım prosedürleri yetkili personel tarafından gerçekleştirilmeli ve belgelenen bir bakım programına uygun olarak tamamlanmalıdır.
- **Ortam Yönetimi:** CISP, sorunların anında tespit edilmesi için hem elektrikli hem de mekanik sistem ve ekipmanları izlemelidir. Bu işlem, sürekli denetim araçları ve CISP Bina Yönetim ve Elektronik İzleme Sistemleri yoluyla sağlanan bilgiler kullanılarak gerçekleştirilmelidir. Ekipmanları sürekli çalışır halde tutmak için önleyici bakım yapılmalıdır.

YÖNETİŞİM VE RİSK

- **Veri Merkezi Sürekli Risk Yönetimi:** CISP Güvenlik Operasyonları Merkezi, veri merkezleri için düzenli olarak tehdit ve güvenlik açığı incelemeleri yapmalıdır. Veri merkezi risk değerlendirme etkinlikleri yoluyla sürekli değerlendirme yapılmalı ve tespit edilen potansiyel güvenlik açıkları giderilmelidir. Bu değerlendirme, bir bütün olarak işletmenin maruz kaldığı riskleri tanımlamak ve yönetmek için kullanılan kurumsal düzeydeki risk değerlendirme sürecine ek olarak gerçekleştirilmelidir. Bu süreçte bölgesel mevzuat riskleri ve çevre riskleri de dikkate alınmalıdır.
- **Üçüncü Taraf Güvenlik Onayı:** CISP veri merkezlerinin üçüncü taraf testlerinde, üçüncü taraf raporlarında belgelendiği üzere, CISP'nin, güvenlik sertifikalarıyla ilişkili kabul gören kurallara uyduğundan ve bu doğrultuda gerekli güvenlik önlemlerini aldığından emin olunmalıdır. Uygunluk programına ve onun gerekliliklerine bağlı olarak, dış denetçiler ortam bertaraf işlemlerini test edebilir, güvenlik kamerası görüntülerini inceleyebilir, veri merkezi girişlerini ve koridorlarını gözlemleyebilir, elektronik erişim denetim cihazlarını test edebilir ve veri merkezi ekipmanlarını inceleyebilir.

7. Taşıma

	Gereklilik
1.	TAŞIMA HİZMETİ: Bulut sağlayıcısı kaç adet farklı veri taşıma hizmeti sunuyor?
2.	TAŞIMA - MERKEZİ İZLEME: Bulut sağlayıcısı, kuruluşlara sunucu ve uygulama taşıma işlemlerinin durumunu takip edip izleyebilecekleri merkezi (birleşik) bir hizmet sunuyor mu?
3.	TAŞIMA - PANO: Bulut sağlayıcısının taşıma aracı, taşıma durumunun, ilgili ölçümlerin ve taşıma geçmişinin hızlıca görselleştirilmesini sağlayan bir pano sunuyor mu?
4.	TAŞIMA - BULUT SAĞLAYICISI ARAÇLARI: Bulut sağlayıcısının taşıma aracı, sunucu ve uygulama taşıma işlemlerini gerçekleştirebilen bulut sağlayıcısının diğer taşıma araçlarıyla entegrasyon sunuyor mu?
5.	TAŞIMA - ÜÇÜNCÜ TARAF ARAÇLARI: Bulut sağlayıcısının taşıma aracı, üçüncü taraf taşıma araçlarının dahil edilmesine imkan tanıyor mu? • Cevap Evet ise desteklenen üçüncü taraf taşıma araçları nelerdir?
6.	TAŞIMA - ÇOK BÖLGELİ TAŞIMA: Bulut sağlayıcısının taşıma aracı, farklı bölgelerde meydana gelen sunucu ve uygulama taşıma işlemleri için takip ve izleme yeteneği sunuyor mu?
7.	TAŞIMA - SUNUCU TAŞIMA: Bulut sağlayıcısının taşıma aracı, şirket içi sanallaştırılmış sunucuları taşımak için yöntem sunuyor mu? • Cevap Evet ise halihazırda hangi sanallaştırılmış ortamlar destekleniyor?
8.	TAŞIMA - SUNUCU KEŞFİ: Bulut sağlayıcısının taşıma aracı, buluta taşınacak şirket içi sanal sunucuların otomatik olarak bulunmasını sağlayan keşif özelliğine sahip mi?

9.	TAŞIMA - SUNUCU PERFORMANSI VERİLERİ: Bulut sağlayıcısının taşıma aracı, merkezi işlem birimi (CPU) ve rastgele erişimli bellek (RAM) kullanımı gibi sunucu ve/veya sanal makine performansı ile ilgili bilgileri toplama ve görüntüleme özelliğine sahip mi?
10.	TAŞIMA - KEŞİF VERİTABANI: Bulut sağlayıcısının taşıma aracı, toplanan tüm verileri merkezi bir veritabanında depolama yeteneğine sahip mi? Cevap Evet ise kuruluşların bu verileri dışarı aktarma yeteneği var mı? Hangi formatlarda dışarı aktarım yapılabilir?
11.	TAŞIMA - BEKLEME SIRASINDA ŞİFRELEME: Bulut sağlayıcısı, toplanan ve keşif veritabanında depolanan tüm bilgileri bekleme sırasında şifreliyor mu?
12.	TAŞIMA - ARTIMLI SUNUCU ÇOĞALTMA: Bulut sağlayıcısının taşıma aracı, sunucu veya sanal makinede yapılan tüm değişikliklerin taşınan nihai görüntüye dahil edilmesini desteklemek amacıyla sunucu veya sanal makine taşıma işlemi sırasında otomatik, eş zamanlı, artımlı sunucu çoğaltma olanağına sunuyor mu? Cevap Evet ise bu hizmet ne kadar süreyle çalıştırılabilir?
13.	TAŞIMA - VMWARE: Bulut sağlayıcısının taşıma aracı, VMWare sanal makinesinin şirket içinden buluta taşınmasını destekliyor mu?
14.	TAŞIMA - HYPER-V: Bulut sağlayıcısının taşıma aracı, Hyper-V sanal makinesinin şirket içinden buluta taşınmasını destekliyor mu?
15.	TAŞIMA - UYGULAMA KEŞFİ: Bulut sağlayıcısının taşıma aracı, taşınmadan önce uygulamaları keşfetme ve gruplandırma yeteneğine sahip mi?
16.	TAŞIMA - BAĞIMLILIK EŞLEME: Bulut sağlayıcısının taşıma aracı, taşınmadan önce sunucular ile uygulamalar arasındaki bağımlılıkları keşfetme yeteneğine sahip mi?
17.	TAŞIMA - VERİTABANI TAŞIMA: Bulut sağlayıcısının taşıma aracı, şirket içi veritabanlarını buluta taşıma özelliğine sahip mi?
18.	TAŞIMA - VERİTABANI TAŞIMA KESİNTİ SÜRESİ: Bulut sağlayıcısının taşıma aracı, buluta veritabanı taşıma işlemini minimum kesinti süresiyle gerçekleştirme özelliğine sahip mi (kaynak veritabanı, taşıma işlemi sırasında tamamen operasyonel kalmalıdır)?
19.	TAŞIMA - KAYNAK VERİTABANI: Bulut sağlayıcısının taşıma aracı; Oracle, SQL Server vb. farklı veritabanı kaynaklarının taşınmasını destekliyor mu? Cevap Evet ise lütfen buluta taşınabilecek tüm desteklenen kaynak veritabanlarını listeleyn.
20.	TAŞIMA - HETEROJEN TAŞIMA: Bulut sağlayıcısının taşıma aracı, heterojen veritabanı taşıma işlemleri (bir kaynak veritabanından farklı bir hedef veritabanına taşıma, örneğin Oracle'dan SQL Server'a) gerçekleştirme yeteneğine sahip mi? Cevap Evet ise lütfen mümkün olan tüm heterojen veritabanı taşıma kombinasyonlarını listeleyin.
21.	TAŞIMA - PETABAYT ÖLÇEĞİNDE VERİ TAŞIMA: Bulut sağlayıcısı, büyük miktarda veriyi bulut içine ve dışına aktarmak için güvenli aygıtların kullanıldığı, petabayt ölçeğinde bir veri taşıma çözümü sunuyor mu?

22.	TAŞIMA - EKŞABAYT ÖLÇEĞİNDE VERİ TAŞIMA: Bulut sağlayıcısı, son derece büyük miktarda veriyi buluta taşımak için eksabayt ölçeğinde bir veri taşıma çözümü sunuyor mu?
23.	TAŞIMA - KURUMSAL YEDEKLEMELER: Bulut sağlayıcısı, bir müşterinin veri merkezinin bulut depolama hizmetleriyle sorunsuz bir şekilde entegre edilmesine, verilerin taşınarak bulut sağlayıcısının depolama hizmetinde depolanmasına olanak sağlayan bir hizmet sunuyor mu?
24.	TAŞIMA - KURUMSAL YEDEKLEME - NESNE DEPOLAMA: Bulut sağlayıcısının kurumsal yedekleme hizmeti, sağlayıcının bulut nesne depolama hizmetiyle entegrasyon sunuyor mu?
25.	TAŞIMA - KURUMSAL YEDEKLEME - DOSYA ERİŞİMİ: Bulut sağlayıcısının kurumsal yedekleme hizmeti, kullanıcıların ağ dosya sistemi (NFS) protokolü gibi dosya protokolleri kullanarak nesneleri depolamasına ve almasına olanak sağlıyor mu?
26.	TAŞIMA - KURUMSAL YEDEKLEME - BLOK ERİŞİMİ: Bulut sağlayıcısının kurumsal yedekleme hizmeti, kullanıcıların internet küçük bilgisayar sistemi arabirimi (iSCSI) protokolü gibi blok protokolleri kullanarak nesneleri depolamasına ve almasına olanak sağlıyor mu?
27.	TAŞIMA - KURUMSAL YEDEKLEME - BANT ERİŞİMİ: Bulut sağlayıcısının kurumsal yedekleme hizmeti, kullanıcıların verilerini bir sanal bant kitaplığı yoluyla yedeklemesine ve bu bant yedekleri sağlayıcının bulutunda depolamasına olanak sağlıyor mu?
28.	TAŞIMA - KURUMSAL YEDEKLEME - ŞİFRELEME: Bulut sağlayıcısının kurumsal yedekleme hizmeti, bekleyen ve taşınan verilerin şifrlenmesini destekliyor mu?
29.	TAŞIMA - KURUMSAL YEDEKLEME - ÜÇÜNCÜ TARAF YAZILIM ENTEGRASYONU: Bulut sağlayıcısının kurumsal yedekleme hizmeti yaygın olarak kullanılan üçüncü taraf yedekleme yazılımlarıyla entegre mi?
30.	TAŞIMA - HİZMET SINIRLARI: Bulut sağlayıcısı, yukarıdaki taşıma bölümüne ilişkin herhangi bir kısıtlamaya (ör. hizmet sınırları) sahip mi? Örneğin: Maksimum eş zamanlı sanal makine taşıma işlemi sayısı Maksimum sipariş edilebilir veri taşıma çözümü sayısı

8. Faturalama

	Gereklilik
1.	FATURALAMA - TAKİP VE RAPORLAMA: Bulut sağlayıcısı, kullanıcıların bulut teklifleri kullanımını yönetmesine ve izlemesine yardımcı olmak için bir faturalama takip ve raporlama hizmeti sunuyor mu?
2.	FATURALAMA - ALARMLAR VE BİLDİRİMLER: Bulut sağlayıcısı, kullanıcıların, harcamaları belirli bir eşiği geçtiğinde uyarı almak için bildirimli alarmlar oluşturmasını sağlayan bir mekanizma sunuyor mu?
3.	FATURALAMA - MALİYET YÖNETİMİ: Bulut sağlayıcısı, maliyetleri ve harcamayı özetleyen grafiklerin oluşturulması ve görüntülenmesi için bir mekanizma sunuyor mu?

4.	FATURALAMA - BÜTÇELER: <i>Bulut sağlayıcısı, bütçelerin görüntülenip yönetilmesi ve tahmini maliyetlerin hesaplanması için bir mekanizma sunuyor mu?</i>
5.	FATURALAMA - BİRLEŞİK GÖRÜNÜM: <i>Bulut sağlayıcısı, birden fazla hesaba ait faturaların tek bir birincil ödeyen hesabı altında birleştirilmesi için bir mekanizma sunuyor mu?</i>
6.	FATURALAMA - HİZMET SINIRLARI: <i>Bulut sağlayıcısı, yukarıdaki faturalama bölümüne ilişkin herhangi bir kısıtlamaya (ör. hizmet sınırları) sahip mi?</i> <i>Örneğin:</i> <i>Birlikte gruplandırılacak maksimum hesap sayısı</i> <i>Oluşturulabilecek maksimum alarm sayısı</i> <i>Yönetilebilecek maksimum bütçe sayısı</i>

9. Yönetim

	Gereklilik
1.	YÖNETİM - İZLEME HİZMETİ: <i>Bulut sağlayıcısı, bulut kaynaklarının ve uygulamalarının yönetilmesi için önceden tanımlanmış ölçümleri kullanarak verileri toplayan, izleyen ve raporlayan bir izleme hizmeti sunuyor mu?</i>
2.	YÖNETİM - ALARMLAR: <i>Bulut sağlayıcısının izleme hizmeti, alarmlar oluşturulmasına olanak sağlıyor mu?</i>
3.	YÖNETİM - ÖZEL ÖLÇÜMLER: <i>Bulut sağlayıcısının izleme hizmeti, kullanıcıların özel ölçümler oluşturmaya olanak sağlıyor mu?</i>
4.	YÖNETİM - İZLEME AYRINTI DÜZEYİ: <i>Bulut sağlayıcısının izleme hizmeti, 1 dakikalık ayrıntı düzeyine kadar çeşitli izleme ayrıntı düzeyleri sağlıyor mu?</i>
5.	YÖNETİM - API TAKİP HİZMETİ: <i>Bulut sağlayıcısı, daha fazla görünürlük için hem konsol hem de uygulama programlama arabirimi (API) düzeyinde bulut kaynaklarıyla ilişkili etkinlikleri günlüğe kaydeden, izleyen ve depolayan bir hizmet sunuyor mu?</i> • Cevap Evet ise bulut sağlayıcısının, bu takip hizmetiyle entegre hizmetleri hangileridir?
6.	YÖNETİM - BİLDİRİM: <i>Bulut sağlayıcısı, uygulama programlama arabirimi (API) etkinlik düzeylerine bağlı olarak bildirimler gönderme özelliğine imkan sağlıyor mu?</i>
7.	YÖNETİM - SIKIŞTIRMA: <i>Bulut sağlayıcısı, kullanıcıların bu hizmetle ilişkili depolama maliyetlerini azaltmasına yardımcı olmak için uygulama programlama arabirimi (API) takip sistemi tarafından oluşturulan günlüklerin sıkıştırılmasına yönelik bir mekanizma sunuyor mu?</i>
8.	YÖNETİM - BÖLGE BİRLEŞTİRME: <i>Bulut sağlayıcısı, hesapta gerçekleşen uygulama programlama arabirimi (API) etkinliklerini tüm bölgeler genelinde kaydetme ve bu bilgileri, kullanım kolaylığı için birleştirilmiş bir şekilde iletme özelliğini sunuyor mu?</i>

9.	YÖNETİM - KAYNAK ENVANTERİ: <i>Bulut sağlayıcısı bir kullanıcı tarafından dağıtılan kaynakların yapılandırılmalarının değerlendirilmesi ve denetlenmesine yönelik bir hizmet sunuyor mu?</i>
10.	YÖNETİM - YAPILANDIRMA DEĞİŞİKLİKLERİ: <i>Bulut sağlayıcısı bir kaynak yapılandırma değişikliğini, meydana geldiği anda otomatik olarak kaydediyor mu?</i>
11.	YÖNETİM - YAPILANDIRMA GEÇMİŞİ: <i>Bulut sağlayıcısı geçmişteki herhangi tek bir zaman noktasındaki kaynak yapılandırmasını inceleme yeteneğini sunuyor mu?</i>
12.	YÖNETİM - YAPILANDIRMA KURALLARI: <i>Bulut sağlayıcısı, uygunluk tedarik edilmesi, yapılandırılması ve sürekli olarak izlenmesine ilişkin kılavuzlar ve öneriler sunuyor mu?</i>
13.	YÖNETİM - KAYNAK ŞABLONLARI: <i>Bulut sağlayıcısı, kullanıcılara bir dizi kaynağı, şablon benzeri bir şekilde oluşturma, tedarik etme ve yönetme özelliğini sunuyor mu?</i>
14.	YÖNETİM - KAYNAK ŞABLONLARINI ÇOĞALTMA: <i>Bulut sağlayıcısı, bu kaynak şablonlarını, potansiyel olarak olağanüstü durum kurtarma (DR) durumlarında kullanılmak üzere farklı bölgeler genelinde hızlıca çoğaltma yeteneğini sunuyor mu?</i>
15.	YÖNETİM - ŞABLON TASARIMCISI: <i>Bulut sağlayıcısı bu tür kaynak şablonlarını oluşturma işlemini hızlandıran, sürükle-bırak işlevselliğine sahip, kullanımı kolay bir grafiksel araç sunuyor mu?</i>
16.	YÖNETİM - HİZMET KATALOĞU: <i>Bulut sağlayıcısı; sunucular, sanal makineler, yazılım veritabanları vb. hizmetlerin bir kataloğunun oluşturulmasına ve yönetilmesine yönelik bir hizmet sunuyor mu?</i>
17.	YÖNETİM - KONSOL ERİŞİMİ <i>Bulut sağlayıcısı, bulut hizmetlerinin yönetimini ve izlenmesini kolaylaştırmak için web tabanlı bir kullanıcı arabirimi sunuyor mu?</i>
18.	YÖNETİM - CLI ERİŞİMİ: <i>Bulut sağlayıcısı birden fazla bulut hizmetinin, komut satırı arabiriminden (CLI) yönetilip yapılandırılmasına ve yönetim görevlerinin, betikler yoluyla otomatik hale getirilmesine imkan tanıyan bir birleştirilmiş araç sunuyor mu?</i>
19.	YÖNETİM - MOBİL ERİŞİM: <i>Bulut sağlayıcısı, kullanıcıların bulut hizmetine bağlanmasına ve kaynaklarını yönetmesine olanak sağlayan bir akıllı telefon uygulaması sunuyor mu?</i> • Cevap Evet ise bu uygulama hem iOS hem de Android için kullanılabilir mi?
20.	YÖNETİM - EN İYİ UYGULAMALAR <i>Bulut sağlayıcısı, kullanıcıların bulut kullanımlarını en iyi uygulamalarla karşılaştırmasına yardımcı olan bir hizmet sunuyor mu?</i>
21.	YÖNETİM - HİZMET SINIRLARI: <i>Bulut sağlayıcısı, yukarıdaki yönetim bölümüne ilişkin herhangi bir kısıtlamaya (ör. hizmet sınırları) sahip mi?</i> <i>Örneğin:</i> <i>Hesap başına maksimum yapılandırma kuralı sayısı</i> <i>Oluşturulabilecek maksimum alarm sayısı</i>

	Depolanabilecek maksimum günlük sayısı
--	--

10. Destek

	Gereklilik
1.	DESTEK - HİZMET: Bulut sağlayıcısı günün 24 saati, haftanın 7 günü, yılın 365 günü telefon, sohbet ve e-posta yoluyla sürekli destek sunuyor mu?
2.	DESTEK - DESTEK KATMANLARI: Bulut sağlayıcısı farklı destek katmanı düzeyleri sunuyor mu?
3.	DESTEK - KATMAN TAHSİSİ: Bulut sağlayıcısı, kullanıcıların kullanılan kaynakları/hizmetleri, ayrıntı düzeyi sınıflandırmasına dayalı olarak farklı hizmet düzeylerine self servis olarak atamasına olanak sağlıyor mu ve bunu, kullanıcıları farklı düzeylerde hizmet elde etmek ve almak için ayrı bulut hesapları tutmaya zorlamadan yapıyor mu?
4.	DESTEK - FORUMLAR: Bulut sağlayıcısı, müşterilerin kendi sorunlarını tartışabilmeleri için genel erişime açık destek forumları sunuyor mu?
5.	DESTEK - HİZMET DURUMU PANOSU: Bulut sağlayıcısı, birden fazla bölge genelindeki hizmet erişilebilirliği ile ilgili bilgileri dakika düzeyinde ayrıntılarla görüntüleyen bir hizmet durumu panosu sunuyor mu?
6.	DESTEK - KİŞİSELLEŞTİRİLMİŞ PANO: Bulut sağlayıcısı, kullanıcının belirli kaynaklarının altında yatan hizmetlerin performansına ve erişilebilirliğine ilişkin kişiselleştirilmiş bir görünüm görüntüleyen bir pano sunuyor mu?
7.	DESTEK - PANO GEÇMİŞİ: Bulut sağlayıcısı, son 365 günü kapsayan bir hizmet durumu panosu geçmişini sunuyor mu?
8.	DESTEK - BULUT DANIŞMANI: Bulut sağlayıcısı, özelleştirilmiş bulut uzmanı görevi gören ve kaynak kullanımının en iyi uygulamalarla karşılaştırılmasına yardımcı olan bir hizmet sunuyor mu?
9.	DESTEK - TAM: Bulut sağlayıcısı, tüm bulut hizmetleri için teknik uzmanlık sağlayan bir teknik hesap yöneticisi (TAM) sunuyor mu?
10.	DESTEK - ÜÇÜNCÜ TARAF UYGULAMA DESTEĞİ: Bulut sağlayıcısı, yaygın işletim sistemleri ve yaygın uygulama yığını bileşenleri için destek sunuyor mu?
11.	DESTEK - GENEL API: Bulut sağlayıcısı, destek vakalarının oluşturulması, düzenlenmesi ve kapatılması için bu vakalarla programlı olarak etkileşim kuran bir genel uygulama programlama arabirimi (API) sunuyor mu?
12.	DESTEK - HİZMET BELGELERİ: Bulut sağlayıcısı, tüm hizmetleri için kullanım kılavuzları, öğreticiler, sık sorulan sorular (SSS) ve sürüm notları dahil ancak bunlarla sınırlı kalmamak üzere iyi kalitede, genel erişime açık teknik belgeler sunuyor mu?
13.	DESTEK - CLI BELGELERİ: Bulut sağlayıcısı, komut satırı arabirimi (CLI) için iyi kalitede, genel erişime açık teknik belgeler sunuyor mu?

14.	DESTEK - REFERANS MİMARİLER: <i>Bulut sağlayıcısı, müşterilerin bulut sağlayıcısına ait birçok bulut hizmetini bir araya getirerek özel çözümler geliştirmesine yardımcı olmak için çeşitli referans mimari belgelerini ücretsiz ve çevrimiçi olarak sunuyor mu?</i>
15.	DESTEK - REFERANS DAĞITIMLAR: <i>Bulut sağlayıcısı, yaygın çözümlerin (ör. DevOps, Büyük Veri, Veri Ambarı, Microsoft iş yükleri, SAP iş yükleri) kendi bulut tekliflerinde uygulanması için ayrıntılı, test edilmiş ve doğrulanmış adım adım prosedürlerin yanı sıra en iyi uygulamaları içeren bir dizi belgeyi ücretsiz ve çevrimiçi olarak sunuyor mu?</i>

Ek B - Canlı Teknik Değerlendirme

Bir CISP seçilirken, CISP'nin genel erişime açık hizmetleri ve altyapısı kullanılarak bulut platformu özelliklerinin "canlı" olarak değerlendirilmesi önemlidir. Teknik değerlendirme için kısa listeye alınan CISP başına en az 1 tam gün ayrılması önerilir. Değerlendirme sırasında: 1) Gösterilen özelliklerin RFP gereklilikleriniz ve CISP'nin yazılı cevapları ile örtüşüp örtüşmediğini belirlemek için ayrıntılı bir değerlendirme yapabilirsiniz, 2) CISP'nin spesifik teknik ve organizasyonel ihtiyaçlarınıza uygunluğundan emin olmak için uzmanlarınızın CISP'yi derinlemesine sorgulayabileceği bir platform sağlayabilirsiniz ve 3) CISP'nin Hizmetlerine ve CISP'nin ölçeklendirme, güvenli işletim, dayanıklı işletim ve gelecekteki ihtiyaçları karşılamak üzere sürekli inovasyon yapma kabiliyetine dair güven temin edebilirsiniz.

CISP'ler bir Bulut Hizmetleri RFP'sine yanıt verirken gerekliliklere ilişkin genel yorumlamalarına dayalı olarak uygunluklarını ifade edebilirler ve bu genel yorumlamada, kuruluşun işletim ortamı/uygulama ihtiyaçları tam olarak göz önünde bulundurulmamış olabilir. Önde gelen teknik, operasyon, güvenlik ve uygulama uzmanlarını içeren bir teknik değerlendirme paneli oluşturularak canlı değerlendirme yapılması önerilir. Değerlendirmeciler, değerlendirme boyunca CISP'yi sorgulamalı ve en iyi uygulama olarak, senaryoları örneğin 0-4 arası belirlenmiş bir ölçeğe (0=Kabul Edilemez, 1=Sınırdı, 2=Kabul Edilebilir, 3=İyi, 4=Olağanüstü) göre derecelendirerek CISP'leri bağımsız olarak puanlandırmalıdır. Daha sonra gösterim puanları birleştirilebilir, her değerlendirme senaryosunun ortalama puanı dikkate alınarak genel CISP değerlendirme puanı elde edilir. Yüksek bir standart sapma içeren senaryolar sonuçlandırılmadan önce bir değerlendirme ekibi dahilinde tartışılabilir. Puanlar birleştirildikten sonra senaryoların önem düzeyine göre bir ağırlıklandırma uygulanabilir.

Gösterim kapsamı açısından, CISP'nin platformunun bir bütüncül bakış açısından değerlendirilmesi ve ardından platform üzerinde çalışan spesifik iş yüklerinin ayrıntılı olarak incelenmesi önerilir. Aşağıda bir platform ve iş yükü değerlendirmesinin örnek genel hatları sunulmaktadır. Kuruluşlar bu referansı temel olarak kullanabilir veya seçilen CISP'nin kendi spesifik fonksiyonel ve fonksiyonel olmayan gerekliliklerini karşıladığından emin olmak için özelleştirebilir. En iyi uygulama olarak, senaryo ve gerekliliklerin listesi sunulan tedarikçilerin, canlı değerlendirme için azami değerlendirme kapsamını sağlayan ve %20 oranında bir soru-cevap süresi içeren bir gündem teklif etmesine izin verilebilir.

Platform Değerlendirmesi: Birçok CISP, optimum değeri sunan ve riskleri en aza indiren bir bulut yaklaşımını ifade etmek için "İyi Mimarilendirilmiş" terimini kullanmaktadır. Bir canlı teknik gösterimde yer alacak İyi Mimarilendirilmiş senaryolar aşağıdakileri içerebilir:

1. **Güvenlik:** Kimlik, Merkezi Yönetişim, Otomatik Tehdit Algılama, Veri Koruma, Olay Hazırlık Durumu
2. **Performans Verimliliği:** Doğru Boyutlandırma, Ölçeklenebilirlik/Esneklik, Sunucusuz
3. **Güvenilirlik:** Yüksek Erişilebilirlik (Hatalara Dayanıklılık), Azaltılmış Değişiklik Riski, Olağanüstü Durum Kurtarma, Yedekleme
4. **Maliyet Yönetimi:** Finansal Operasyonlar, Ticari Optimizasyon, Bütçeler ve Maliyet Tahsisi
5. **Operasyonel Mükemmellik:** Otomasyon, İzleme, Destek, Yönetim, Ayrıca Buluta Taşıma ve Bulutta Çalışma İçin Gerekli Özellikler

İş Yükü Değerlendirmesi: Gösterilebilecek yaygın uygulama türleri aşağıdakileri içerir:

- **Web Uygulaması:** Arka uç veritabanı ve statik nesne depolama alanı dahil olmak üzere dinamik bir web sitesinin genel erişime açık olarak barındırılması.
- **Veri Analizi:** Ayrı veri sağlayıcılarından gelen verilerin birleştirilmesine imkan tanıyan ve verileri yüksek Hacim (TB/PB düzeyinde veri), Çeşitlilik (Yapılandırılmış, yapılandırılmamış, farklı formatlar vb.) ve Hız (Veri oluşturma, değiştirme ve sorgu düzenlerinin hızı) ile işleme yeteneğini sağlayan bir Veri Gölü veya Göl Evi mimarisi.

- **Veri Bilimi Platformu:** Yapay zeka/makine öğrenimi tabanlı özelliklerin kuruluşunuz genelinde geliştirilmesini, dağıtılmasını ve kullanımını mümkün kılan bir platform.
- **IoT Uygulaması:** Bulutu, ağ özelliklerini ve cihazları kapsayan bir IoT platformu/özellği.

Kuruluşunuz açısından önem taşıyan her bir temsili iş yükü için CISP tarafından gösterilecek senaryoları tanımlayabilirsiniz. Senaryolar iş yükünün iyi Mimarilendirilmiş bir şekilde dağıtımına olanak sağlayan genel özellikleri göstermelidir. Aşağıdaki sayfalarda 1) CISP'nin Platformu ve 2) örnek bir Web Uygulaması iş yükü için örnek Canlı Teknik Değerlendirme kriterleri yer almaktadır.

Platform - Örnek Canlı Teknik Değerlendirme

Senaryo Kimliği	Senaryo Adı	Önem Düzeyi (1=Düşük, 4=Kritik)	Gösterim Gereklilikleri	Puanlandırmada Dikkate Alınacak Hususlar
Plat.Sec.1	Kimlik Federasyonu	4	Mevcut bir kimlik deposundan bulut hizmetine birleştirme yeteneğini gösterin.	- SAML gibi standart protokoller desteği. - SCIM tabanlı kimlik çoğaltma desteği. - Kurumsal kimlik deposunda farklı erişim düzeyleri tanımlama ve bunların bulut sağlayıcısında uygulanmasını sağlama yeteneği. - Spesifik ekipleri/bireyleri yalnızca belirli hesaplar/projeler/iş yükleri ile sınırlandırma yeteneği. - Bulut kaynaklarına erişimi denetlemek için Öznitelik Tabanlı Erişim Denetimi'ni (ABAC) destekleme ve bu öznitelikleri bulut sağlayıcısının Kimlik ve Erişim Yönetimi (IAM) sisteminde kullanma yeteneği.
Plat.Sec.2	Merkezi Yönetişim	4	Politika ve gereklilikleri merkezi olarak, bir kuruluş düzeyinde (küresel politikalar) ve ayrıca bir iş birimi ve proje düzeyinde tanımlama yeteneğini gösterin.	- Politika şunları içermelidir: Hizmetleri etkinleştirme/devre dışı bırakma, Coğrafi kısıtlamaları uygulama (bölgeleri sınırlandırma). - Politikalar yöneticiler de dahil olmak üzere kullanıcıların herhangi bir denetim/yönetişim denetimini devre dışı bırakmasını kısıtlamalıdır.
Plat.Sec.3	Kullanıcı İzni Sınırlaması	3	Kullanıcı izinlerinin sıkılaştırılmasına yönelik otomatik önerileri gösterin.	- Mevcut izinleri gerekli izinlerle karşılaştırma yeteneği. - En az ayrıcalığı desteklemek için politikaların otomatik olarak oluşturulması.
Plat.Sec.4	Denetim Günlüğü	4	Hem izin verilen hem de izin verilmeyen eylemler dahil olmak üzere, bulut etkinliğiyle ilgili eylemlerin denetim günlüğüne kaydedilmesini gösterin.	- Tüm kuruluş için merkezi günlükler. - Düşük düzeyli takip ve hesap verebilirliği desteklemek için hesaba/projeye özel günlükler. - Günlüklerin sorgulanmasını sağlayan araçlar. - Belirli olaylara/günlük girişlerine dayalı olarak eylemlerin tetiklenmesini sağlayan araçlar. - Tedarikçi destek etkinliğini görüntüleme yeteneği. - Günlüklerin yöneticiler tarafından dahi silinmesini önleme yeteneği.
Plat.Sec.5	Ağ Yalıtımı	4	Buluttaki farklı kiracıların yalıtımını gösterin ve mümkün olan durumlarda buna ilişkin	VPN ve bağlantılar arası hizmetler üzerinde dahil olmak üzere kiracıların ayrılması.

Senaryo Kimliği	Senaryo Adı	Önem Düzeyi (1=Düşük, 4=Kritik)	Gösterim Gereklilikleri	Puanlandırmada Dikkate Alınacak Hususlar
			kanıtları sunun. Yalıtılmış (bağılantısız), özel (internet erişimsiz) ve genel (internet erişimli) alt ağların yapılandırmasını gösterin.	- Bulut altyapısının dışından (şirket içi), bulut altyapısının içindeki ve internete trafik akışını denetleme yeteneği. - Container barındırma veya hizmet olarak işlev gibi paylaşılan hizmetler kullanırken ayırmanın nasıl uygulanacağı.
Plat.Sec.6	Bekleme sırasında şifreleme	4	Kendi anahtarını getir (KAG) ve istemci tarafı şifreleme seçenekleri dahil olmak üzere bekleyen verileri şifreleme yeteneğini gösterin.	- Hassas veriler için şifrelemeyi zorunlu kılma yeteneği. - Sağlayıcı tarafından yönetilen ve müşteri tarafından yönetilen anahtarlar kullanma yeteneği. - FIPS 140-2'ye uyum. - Şifreleme gerekliliklerine uygunsuzluk için uyarı oluşturma ve günlüğe kaydetme yeteneği. - Ek maliyet etkisi. - Performans etkisi. - Kuantum kanıtı algoritmaları ve anahtar boyutları desteği.
Plat.Sec.7	Taşıma sırasında şifreleme	4	Taşınan verileri şifreleme yeteneğini gösterin.	- Hizmet API'leri için varsayılan olarak şifreleme. - Yük dengeleyicilerde ve yönetilen API'lerde, taşıma sırasında şifreleme sağlama yeteneği. - Karşılıklı (istemci ve sunucu) kimlik doğrulama desteği.
Plat.Sec.8	Anahtar Yönetimi	4	Anahtar yönetimi özelliğinizi gösterin. Anahtarın tüm yaşam döngüsünü dahil edin. Bulut hizmetleriyle entegrasyonu dahil edin.	Anahtar oluşturmaya, kullanımını, değişimini ve imhasını günlüğe kaydetme.
Plat.Sec.9	Yapılandırma Yönetimi	3	Bulut platformu yapılandırma yönetim özelliklerinizi gösterin.	- Doğru CMDB (yapılandırma yönetimi veritabanı) tutma. - Uygunluğu denetleyin. - Uygunsuzluklara dayalı olarak eylemleri otomatik olarak tetikleyin. - Yapılandırma değişikliklerini en iyi uygulamalara veya özel kurallara göre değerlendirme yeteneği.
Plat.Sec.10	Ağ Güvenliği	3	3. taraf kural kümeleri/güvenlik duvarları ve volümetrik saldırı koruması ile entegrasyon dahil olmak üzere Web	- WAF (Web Uygulaması Güvenlik Duvarı) özellikleri: ölçeklenebilirlik. - Özel ve genel ağ desteği. - Kural kümeleri için sektör/satıcı akışlarına abone olma yeteneği.

Senaryo Kimliği	Senaryo Adı	Önem Düzeyi (1=Düşük, 4=Kritik)	Gösterim Gereklilikleri	Puanlandırmada Dikkate Alınacak Hususlar
			Uygulaması Güvenlik Duvarı ve Güvenlik Duvarı özelliğini gösterin.	• WAF'den gelen olaylara bağlı olarak altyapı içinde eylemleri otomatik olarak tetikleme. • Güvenlik duvarı özellikleri: ölçeklenebilirlik. • Ana sunucu tabanlı ve ağ tabanlı güvenlik duvarları. • CIDR IP Bloklarını belirtme yeteneğine ek olarak mantıksal grupları veya nesneleri referans alma yeteneği. • Her düzeyde/bileşende desteklenen kural sayısı. • Politika ve ağ yapılandırması yoluyla dağıtılmış bir işletim modelini (Ağ ekibi + Geliştirme ekibi) destekleme yeteneği.
Plat.Sec.11	Ağ Bağlantısı	3	Şirket içi ağlara bağlanmanın yanı sıra uç noktaları/istemcileri buluttaki özel ağlara bağlama yeteneğini gösterin.	• Özel bağlantı (yüksek bant genişliği >10 GBps). • Kuruluş genelinde yönlendirme ve güvenlik duvarı politikalarını denetleme yeteneği. • VPN Bağlantısı (siteden siteye ve istemci tabanlı). • IPv6 Desteği.
Plat.Sec.12	Bulut Sunucusu Yönetimi	3	Bulut sunucusu yönetim özelliklerini gösterin.	• Çok sayıda bulut sunucusunun düzeltme eki durumunu izleme ve yönetme yeteneği. • Linux ve Windows işletim sistemi düzeltme eki yönetimi için destek. • SSH'ye gerek olmadan bir sunucu filosu genelinde komut yürütme yeteneği. • Sanal makinelere uzaktan erişimi merkezi olarak kontrol etme ve denetleme yeteneği. • Konsol, CLI ve API yoluyla bir bulut sunucusu boyutunu değiştirme, ek birimler bağlama, ağ yapılandırmasını değiştirme vb. yeteneği.
Plat.Sec.13	Politika uygulama	3	Hizmetleri genel İnternette erişimi önleyecek şekilde yapılandırma yeteneğini gösterin.	• Trafiği, kritik/gizli veri içerme olasılığı yüksek hizmetlere yönelik özel ağ iletişimi ile yalıtma yeteneği. • Kaynak ağı dayalı olarak verilere erişimi denetleyen politikalar tanımlama yeteneği. • Bu erişim kısıtlamalarının, yüksek düzey kimlik bilgilerine sahip kullanıcılar dahil olmak üzere tüm kullanıcılara uygulanması.

Senaryo Kimliği	Senaryo Adı	Önem Düzeyi (1=Düşük, 4=Kritik)	Gösterim Gereklilikleri	Puanlandırmada Dikkate Alınacak Hususlar
Plat.Sec.14	Güvenlik açığı taraması	2	Görüntülerde (container ve VM) güvenlik açıklarını tarama yeteneğini gösterin.	- Bir kayıt defterindeki container'ları otomatik olarak tarama yeteneği. - Sanal makineleri, bilinen güvenlik açıklarına karşı tarama yeteneği. - Ağ taraması gerçekleştirme yeteneği.
Plat.Sec.15	Ağ Denetimi	2	Bir müşteri ortamının içinden gelen ağ trafiğini (NetFlow ve tam paket) yakalama/yansıtma yeteneğini gösterin.	- Tam paket yakalama dahil olmak üzere bulut sağlayıcısının altyapısı içindeki trafiğin bir kısmını/tümünü yansıtma yeteneği (müşteri kiracı perspektifinden). - Yakalamak istenilen trafiği kolayca seçme yeteneği. - Çok fazla trafik hacimlerine (>50 GBps) ölçeklendirme yeteneği.
Plat.Sec.16	Tehdit Algılama	3	Bir ağdan, kimlik bilgisi kullanımından ve kullanım modeli analizinden kaynaklanan tehditler dahil olmak üzere, platformunuzun yetkisiz erişim algılama özelliğini gösterin.	"Madencilik" gibi şüpheli etkinlikleri algılama yeteneği. - SSH oturum açma girişimleri gibi kimlik doğrulaması saldırıları için deneme yanılma saldırılarını algılama yeteneği. - Kimlik bilgisi sızıntılarını veya suistimallerini algılama yeteneği. - Makine öğrenimini uygulama, çok sayıda olayı analiz etme ve öncelikli olayları açığa çıkarma. - Etkinleştirme/yapılandırma girişi (en iyisi basit olanıdır). - Harici hizmetlerle entegrasyon ve bildirim tetikleme yeteneği. - IDS'yi tüm projeler/hesaplar için genel düzeyde yapılandırma yeteneği.
Plat.Perf.1	Bilgi İşlem Optimizasyonu	2	Sanal Makine ve Hizmet Olarak İşlev maliyetlerinin optimizasyonu için otomatik önerileri gösterin.	- Gerçek kullanım ve iş yükü modellerine dayalı öneriler. - Önerilere tahmini tasarruflar, beklenen yük düzeyi/teknik anlamları ile ilgili öngörüler dahildir. - Optimizasyonlar hem tasarrufu hem de sanal makinelerin olması gerekenden düşük boyutlu olduğu durumlar için "performans riskini" içermelidir.
Plat.Perf.2	Ortam Optimizasyonu	2	Yük dengeleyiciler, ağ iletişimi, veritabanları, depolama vb. gibi diğer bulut	Öneriler, temel bilgi işlemin ötesinde diğer bileşenler için tasarrufları ve potansiyel verimlilik fırsatlarını tanımlar.

Senaryo Kimliği	Senaryo Adı	Önem Düzeyi (1=Düşük, 4=Kritik)	Gösterim Gereklilikleri	Puanlandırmada Dikkate Alınacak Hususlar
			bileşenlerine yönelik otomatik önerileri gösterin.	
Plat.Perf.3	Bilgi İşlem Otomatik Ölçeklendirme	4	Sanal bilgi işlem ortamında bir yük dengeleyicinin arkasında dağıtılmış bir uygulamanın otomatik ölçeklendirme özelliklerini gösterin. Kullanılabilir farklı seçenekleri/yaklaşımları ve ölçeklendirme olaylarından önce/sonra bildirim gibi diğer (isteğe bağlı) eylemleri tetikleme yeteneğini gösterin.	- Tetikleyici tabanlı, zaman tabanlı ve manuel yaklaşımlar veya gerekli kapasiteyi tahmin etmek için makine öğrenimini uygulayan daha akıllı yaklaşımlar gibi farklı ölçeklendirme seçenekleri. - Bir yük dengeleyiciyle kayıt ve durum denetimleri dahil olmak üzere tam otomatik ölçeklendirme. - Ölçeklendirme yaşam döngüsünün belirli noktalarında rastgele bir kod parçasını yürütme yeteneği.
Plat.Perf.4	Depolama İçin Çevrimiçi Ölçeklendirme	3	Blok depolamanın hem kapasitesini hem de aktarım hızını, iş yükünde aksaklığa yol açmadan ölçeklendirme yeteneğini gösterin.	- Hizmetleri tamamen yeniden oluşturmaya gerek duymadan blok depolama için farklı depolama türleri arasında geçiş yapma yeteneği. - VM'lere sunulan birimlerin boyutunu artırma yeteneği.
Plat.Perf.5	Yönetilen Hizmetler İçin Otomatik Ölçeklendirme	3	Nesne Deposu, API Ağ Geçidi, FaaS platformu ve NoSQL veritabanını birkaç (10'larca) eş zamanlı kullanıcıdan çok daha fazla (1000'lerce) eş zamanlı kullanıcıya ölçeklendirme yeteneğini gösterin.	- İdeal olarak yönetici müdahalesi gerektirmeyen sorunsuz otomatik ölçeklendirme. - Üretim ölçeklendirme gerekliliklerine uygun bir ölçek artırma döneminde istikrarlı performans. - FaaS gibi bazı bileşenler için gerekliyse ön ısıtma ve eş zamanlı yürütme sınırlarını yönetme gibi seçenekleri inceleyin.
Plat.Perf.6	Container tabanlı iş yükleri	3	Container tabanlı iş yüklerini barındırma yeteneğini gösterin.	- Container barındırma platformlarına ilişkin seçenekler. - Yük dengeleyiciler gibi diğer IaaS bileşenleriyle entegrasyon. - Bir hizmet ağı çözümünün kullanılabilirliği. - Container barındırma için, Kubernetes gibi müseccel olmayan seçenekler. - Container denetim düzleminde yüksek erişilebilirlik için yerel destek. - Şirket içi container ana sunucularını yönetme yeteneği.

Senaryo Kimliği	Senaryo Adı	Önem Düzeyi (1=Düşük, 4=Kritik)	Gösterim Gereklilikleri	Puanlandırmada Dikkate Alınacak Hususlar
Plat.Rel.1	Bölgesel Dayanıklılık	4	Bir ilişkisel veritabanı bulut sunucusunun, coğrafi olarak sınırlandırılmış bir hata (güç kesintisi gibi) simüle edildiğinde bölge içindeki otomatik yük devretmesini gösterin.	- Otomatik yük devretme. - Bir bulut bölgesi içindeki yalıtılmış hata bölgeleri. - Sınırları net olarak çizilmiş ve Yüksek Erişilebilirlik için kolaylıkla mimarilendirilebilir.
Plat.Rel.2	Bulut Sunucusu Otomatik Kurtarma	2	Bir bulut sunucusu/bulut sunucusu kümesi için başarısız durum denetiminin ardından uygulanan otomatik kurtarmayı gösterin.	- Yapılandırılabilir durum denetimleri. - Tam otomatik bulut sunucusu kurtarma/yeniden tedarik etme.
Plat.Rel.3	Yük Dengeleyici Durum Farkındalığı	3	Bir yük dengeleyicinin hatalı bulut sunucusunu otomatik olarak nasıl algıladığını ve trafiği diğer sağlıklı ana sunuculara nasıl yeniden yönlendirdiğini gösterin.	- Yapılandırılabilir durum denetimleri. - Trafiği otomatik olarak sağlıklı ana sunuculara yönlendirme.
Plat.Rel.4	Bölgesel yük devretme	3	Trafiğin ikincil bir bölgeye otomatik olarak yönlendirilmesini de kapsayacak şekilde çok bölge bir mimariyi gösterin.	- Küresel farkındalığı olan durum denetimleri. - Otomatik yönlendirme seçenekleri: gecikme süresi, ağırlıklandırılmış ve yük devretme. - Sanal makine iş yüklerinin yanı sıra Nesne Deposu/NoSQL veritabanı hizmeti gibi yönetilen hizmetler için destek.
Plat.Rel.5	Yedekleme ve Kurtarma	4	Sanal makineler, veritabanları ve yönetilen hizmetler için Yedekleme ve Kurtarma seçeneklerini gösterin.	- Otomasyon düzeyi. - Aynı/başka bir bulut bölgesine geri yükleme yeteneği. - Yedekleri başka bir bulut bölgesine kopyalama yeteneği.
Plat.Cost.1	Bütçeler	3	Bütçe yönetim özelliğinin alt hesaplar ve projeler için nasıl yapılandırılacağı de dahil olmak üzere bir bütçe yönetim özelliğini gösterin.	- Kuruluşunuzun farklı düzeylerinde bütçe denetimleri ve izleme etkinlikleri uygulama yeteneğini göz önünde bulundurun. - Esnekliği kontrol edin. Örneğin, bileşenleri gruplandırma (etiketleme yoluyla), belirli bulut hizmetleri için bütçeler belirleme ve uyarı/izleme eşik değerlerini yapılandırma yeteneği açısından esnekliği kontrol edin.
Plat.Cost.2	Bütçe Tahsisi	1	Proje için bütçe tahsis işlemi de dahil olmak üzere, yeni bir proje ortamının	Uygun onaylarla birlikte kendi kendine tedarik etme yeteneği.

Senaryo Kimliği	Senaryo Adı	Önem Düzeyi (1=Düşük, 4=Kritik)	Gösterim Gereklilikleri	Puanlandırmada Dikkate Alınacak Hususlar
			(hesap) nasıl tedarik edildiğini gösterin. Tedarik süreci; 1) Teknik inceleme/BT, 2) Ticari inceleme/Finans için manuel onay adımlarını da kapsamalıdır.	Uygun bütçe ayarını, bildirimleri veya bütçe politikalarını kuruluşunuza uygun şekilde yapılandırma otomasyonu.
Plat.Cost.3	Bütçe Raporlama	2	Kuruluş genelinde bütçe raporlama özelliğini gösterin. Belirli bir departmana özel veya kuruluşun tamamı için raporlama (bilmesi gereken kişiler esasına göre). Raporlama, "gerçekleşen" harcama değerlerinin yanı sıra öngörülen/tahmin edilen harcama değerlerini içermelidir.	- Kuruluşun farklı düzeylerinde bilmesi gereken kişiler esasına göre görünürlük sağlama, farkındalık ve şeffaflık oluşturma yeteneği. - Tahminler güncel ve geçmiş kullanım trendlerini esas almalı ve potansiyel bütçe aşımaları için erken uyarı sağlamalıdır.
Plat.Cost.4	Bütçe Denetimleri	1	Bir bütçe eşliğine ulaşıldığında eyleme geçme yeteneğini gösterin. Eylemler arasında bildirimler gönderilmesi, kısıtlamalar uygulanması veya bütçe aşımını önlemek için etkin müdahalede bulunulması yer alabilir.	- Farklı projeler için eylemleri kolayca tanımlama yeteneği. - Eylemleri bir projeden diğerine farklılaştırma yeteneği. Örneğin Geliştirme veya Üretim hesabı açısından sonuçlar değerlendirilerek farklı eylemler alınması. - Aynı bütçe/proje için birden fazla eylem ve eşik tanımlama yeteneği. - Standart özelliklere ek olarak özel eylemler tanımlama yeteneği.
Plat.Cost.5	Bütçe Periyotları	1	Farklı zaman dönemleri için (örneğin, günlük/aylık/yıllık) bütçeler uygulama yeteneğini gösterin. Yıllık bütçeler için beklenen harcamanın yıl geneline değişken bir dağılımını uygulama yeteneğini gösterin.	- Farklı zaman dönemleri için bütçeler tanımlama yeteneği. - Yıllık bütçeler için harcamanın yıl geneline dağılımını yapılandırma yeteneği. Bu, örneğin yıllık vergi iadesi gibi, özellikle mevsimsel/yüksek düzeyde esneklik içeren iş yükleri için önemlidir.
Plat.Cost.6	3. Taraf Pazar Yeri	3	3. taraf ürünleri satın alma ve dağıtma yeteneğini gösterin. Bir pazar yeri yoluyla erişilebilen bir dizi 3. taraf ürünü için nasıl bir bütçe belirleneceğini ve ayrıca erişilebilir ürünleri kısıtlama yeteneğini gösterin.	- Belirli bir ürün için bütçe belirleme yeteneği; genel bir bütçe, bir dizi projeye/hesaba özel bir bütçe vb. - Bulut kullanıcılarına kapsamlı pazar yerinin yalnızca bir alt kümesini sunma yeteneği.

Senaryo Kimliği	Senaryo Adı	Önem Düzeyi (1=Düşük, 4=Kritik)	Gösterim Gereklilikleri	Puanlandırmada Dikkate Alınacak Hususlar
Plat.Cost.7	Bilgi işlem fiyatlandırma modelleri	3	Sanal makinelere uygulanabilecek farklı fiyatlandırma modellerini/ticari modelleri gösterin.	- Özellikler istek üzerine, uzun süreli taahhüt gerektirmeyen ve ayrıntılı (dakika/saat başına) fiyatlandırmayı içermelidir. - İndirim karşılığında isteğe bağlı uzun süreli taahhütler. - İndirim karşılığında aksama yaşanması olasılığını kabul ederek bulut sunucuları satın alma yeteneği. - Bu modellerin aynı proje/hesaplar içinde karışık olarak kullanılması ve avantajların farklı hesaplar genelinde paylaşılması önemlidir.
Plat.Cost.8	Ticari Optimizasyon Önerileri	3	Harcamayı (teknik değişiklikler yapmak zorunda kalmadan) optimize etmek için ticari optimizasyon önerileri alma yeteneğini gösterin.	- Birden çok hizmet (ör. Sanal Makineler ve Yönetilen Veritabanları) için bütüncül öneriler. - Önerileri kolayca eyleme geçirme ve beklenen tasarrufları/avantajları anlama yeteneği.
Plat.Cost.9	Tahsis Edilmiş Ana Sunucular	4	Belirli bir ana sunucuya bağlı şirket içi lisanslamanın kullanılabilmesi için bir tahsis edilmiş ana sunucu tedarik etme yeteneğini gösterin.	- Tedarik kolaylığı. - Ana sunucu kullanımını yönetme yeteneği. - Ana sunucuyu farklı projeler/kiralamalar genelinde paylaşma yeteneği.
Plat.Ops.1	Sanal Makine Taşıma	3	Bir sanal makinenin şirket içinden bir bulut temelli VM hizmetine aktarımını gösterin.	- Hem Windows hem de Linux tabanlı işletim sistemlerini içeri aktarma yeteneği. - Tek seferde birden fazla makineyi içeri aktarma yeteneği. - Buluta hızlı "yük devretmeyi" etkinleştirmek için bir çoğaltma oturumunu sürdürme yeteneği.
Plat.Ops.2	DevOps ve Otomasyon Özellikleri	4	Ortamların nasıl kod olarak tanımlandığı, tam otomatik dağıtımlardan gelen destek, otomatik test ve geri alma dahil olmak üzere DevOps/otomasyon özelliklerinizi gösterin.	- Ağ, sanal makineler, depolama ve veritabanları dahil olmak üzere tüm sistem bileşenlerini kod olarak tanımlama yeteneği. - İşlem hattı oluşturma yeteneği. - Kod deposu oluşturma yeteneği. - Derlemeleri otomatik hale getirme yeteneği. - Mavi/yeşil dağıtımlar gerçekleştirme yeteneği. - Birden fazla ortam oluşturma ve dağıtımlar için birden fazla aşama uygulama yeteneği. - Başarısız dağıtımlar için otomatik geri alma.

Senaryo Kimliği	Senaryo Adı	Önem Düzeyi (1=Düşük, 4=Kritik)	Gösterim Gereklilikleri	Puanlandırmada Dikkate Alınacak Hususlar
Plat.Ops.3	Uygulama Barındırma	2	Basit bir 2 katmanlı uygulamanın bir düşük kod/platform hizmetinde barındırılmasını gösterin. Uygulama/web katmanı için bir ilişkisel veritabanı ve otomatik ölçeklendirmenin dahil edilmesi.	- Kullanıcı arabirimi yoluyla basit yapılandırma. - Durum denetimleri, ölçeklendirme ve yüksek erişilebilirliğin dahil edilmesi. Platform desteği, Windows ve Linux.
Plat.Ops.4	Güvenlik Entegrasyonu	2	Güvenlik Olayı ve Olay Yönetimi perspektifinden platformunuzun entegrasyon özelliklerini gösterin.	Entegrasyon için bulut sağlayıcısından + API'lerden alınan güvenlikle ilgili günlükleri kolayca entegre etme ve kullanma yeteneği.
Plat.Ops.5	ITSM Entegrasyonu	3	Bir ITSM (BT Hizmet Yönetimi) perspektifinden platformunuzun entegrasyon özelliklerini gösterin.	- API yoluyla bir destek vakası oluşturma, izleme ve güncelleme yeteneği. - API yoluyla hizmetleri veya hizmet kümelerini "ürünler" olarak tedarik etme yeteneği.
Plat.Ops.6	Destek	4	Destek teklifinizi gösterin.	- Farklı iş yükü türleri için farklı destek düzeyleri. - Belirli bir hizmet için uygun şekilde İşletim Sistemini/Veritabanı Motorunu vb. destekleme yeteneği. - Kritik iş yükleri için destek liderlerinin tanımlandığı titizlikle hazırlanmış bir teklif sunma yeteneği. - Bir yapılandırılmış olay hazırlık durumu ve mimari inceleme süreci sunma yeteneği. - Sağlayıcı yol haritasına ilişkin öngörü.
Plat.Ops.7	Denetlenebilirlik	4	Uygunluk denetimlerini desteklemek için sahip olduğunuz araçları gösterin.	- Konsol yoluyla uygunluk denetimlerini edinme yeteneği. - Ortam denetimlerini yönetme ve otomatik hale getirme yeteneği.
Plat.Ops.8	VM'den Container'a	1	Sanal makinedeki bir uygulamanın bir container'a dönüşümünü ve bulut sağlayıcısının container platformunu kullanarak bunun sunulmasını gösterin.	- Dönüşüm özelliğinin kullanım kolaylığı. - Dönüştürme süresi. - Platform desteği, .Net ve Java.

İş Yüğü: Web Uygulaması - Örnek Canlı Teknik Değerlendirme

Aşağıdaki bölümde belirli bir "Web Uygulaması" iş yükü için örnek iş yükü değerlendirmesi sunulmaktadır. Belirli bir uygulama için bir değerlendirme hazırlanırken gereklilikler, mevcut zorluklar ve kısıtlamalar konusunda en iyi bilgiye sahip taraf olacakları için uygulama kullanıcılarının, geliştiricilerin ve yöneticilerin sürece dahil edilmesi şiddetle önerilir.

Senaryo Kimliği	Senaryo Adı	Önem Düzeyi (1=Düşük, 4=Kritik)	Gösterim Gereklilikleri	Puanlandırmada Dikkate Alınacak Hususlar
Web.Sec.1	Güvenlik - Uygulama Koruması	3	SQL Eklemesi, XSS Betik saldırısı ve diğer saldırılar yoluyla uygulamayı istismar etmeye yönelik kötü amaçlı girişimleri engelleme yeteneğinizi gösterin.	- Standart kurallar/özellikler ile yaygın saldırılara karşı "kullanıma hazır" koruma yeteneği. - Özel kontroller/kurallar/işlevler oluşturma yeteneği.
Web.Sec.2	Güvenlik - Oran Tabanlı Koruma	3	Bir uygulamaya yönelik yüksek istek oranları veya veri hacimleri içeren saldırıları önleme/bunlara karşı koruma yeteneğinizi gösterin.	Sınırlar yapılandırma ve belirli bir IP adresinden veya adres listesinden gelen istek oranlarını kısıtlama yeteneği.
Web.Sec.3	Güvenlik - Kaynak Tabanlı Koruma	3	Ağa/coğrafi kaynağa dayalı olarak erişimi kısıtlama yeteneğinizi gösterin.	- Ağ bloğuna veya bir ağ bloğu listesine göre kısıtlama yeteneği. - Kaynak ülkeye göre (IP listelerini yönetmek zorunda kalmadan) kısıtlama yeteneği.
Web.Sec.4	Güvenlik - Ağ Segmentasyonu	4	Altyapı üzerinden hem Kuzey-Güney hem de Doğu-Batı hattında yayılmaya karşı koruma için bileşenleri (Web Sunucusu, Uygulama Sunucusu/Veritabanı Sunucusu) yalıtma/koruma yeteneğinizi gösterin.	- Bileşenleri farklı alt ağlara yerleştirme ve farklı alt ağlar arasındaki trafik akışını denetleme yeteneği. - Bir ağ arabirimi düzeyinde trafik akışını denetleme yeteneği. - Mantıksal grupları ve CIDR bloklarını referans alma yeteneği.
Web.Sec.5	Güvenlik - TLS Desteği ve Sertifika Yönetimi	4	TLS ile güvenliği sağlanmış uç nokta sunma ve bunu sunmak üzere destekleyici bileşenleri (ör. sertifikaların otomatik olarak değişimi) otomatik olarak yönetme yeteneğinizi gösterin.	- En son TLS protokolleri desteği ve gerekirse eski sürümleri devre dışı bırakma yeteneği. - Basit sertifika oluşturma, yönetimi ve değişimi (ideal olarak tam otomatik).
Web.Perf.1	Performans - Ölçeklenebilirlik	4	Dinamik otomatik ölçeklendirme yoluyla web uygulamasının eş zamanlı kullanıcı	Zaman temelli ve tetikleyici temelli ölçeklendirme kuralları tanımlama yeteneği.

Senaryo Kimliği	Senaryo Adı	Önem Düzeyi (1=Düşük, 4=Kritik)	Gösterim Gereklilikleri	Puanlandırmada Dikkate Alınacak Hususlar
			sayısını 10'dan 100.000'e çıkarma yeteneğinizi gösterin.	- Son kullanıcı ve yönetici için sorunsuz ölçeklendirme. Yük arttığında otomatik ölçek artırma, yük azaldığında otomatik ölçek azaltma. - Web uygulamasının her katmanının (Yük Dengeleyici, Web Katmanı, Veri Katmanı vb.) ölçeklenebilir olduğundan emin olun. - Uygulamanın farklı katmanlarında gerekli şekilde ön belleğe alma hizmetlerinin erişilebilirliği.
Web.Perf.2	Performans - Küresel Teslim	3	Avustralya, Asya, Afrika, Orta Doğu, Kuzey Amerika, Güney Amerika ve Avrupa dahil olmak üzere dünyanın farklı noktalarından gecikme süresinin gösterilmesi dahil olmak üzere CDN özelliğinizi gösterin.	- CISP konsolu/API'ler aracılığıyla bir CDN oluşturma ve yapılandırma yeteneği. - Farklı coğrafyalar için yapılandırılabilir dağıtım kuralları. - Farklı kullanım örnekleri/uygulamalar için yapılandırılabilir ön bellek.
Web.Rel.1	Güvenilirlik - Tek Bölge Dayanıklılık	4	CISP veri merkeziyle ağ bağlantısının kopması gibi, sınırlandırılmış bir olayı tolere etme yeteneğini gösterin.	Bir bulut bölgesinde (Şehir) otomatik yük devretme ve yüksek erişilebilirlik.
Web.Rel.2	Güvenilirlik - Çok Bölge Dağıtım	3	Küresel olarak çoğaltılan bir veritabanı dahil olmak üzere bir web uygulamasının çok bölgesel dağıtımını gösterin.	- Çok bölgesel bir uygulamayı programlı olarak dağıtma yeteneği. - Veri deposu için bölgeler arasında çoğaltma. - Kullanıcıları ideal bölgeye otomatik olarak yönlendirme.
Web.Rel.3	Güvenilirlik - Çok Bölge Yük Devretme	3	Bölge genelini etkileyen bir hizmet sorunu olması durumunda web uygulaması yükünün nasıl otomatik olarak devredildiğini gösterin.	Birden fazla bulut bölgesi genelinde otomatik yük devretme ve yüksek erişilebilirlik.
Web.Cost.1	Maliyet - Görünürlük	2	Uygulamaya göre maliyeti takip etme yeteneğini gösterin	Belirli bir uygulamanın, ölçek artırma/azaltma dönemleri dahil olmak üzere geçmişteki maliyetlerini görüntüleme yeteneği.
Web.Cost.2	Maliyet - Bütçeler	2	Uygulamaya göre bütçeler belirleme ve ilgili uyarıları ayarlama yeteneğini gösterin.	Uygulamaya göre yapılandırılan bütçeler ve yapılandırılan eşiklere dayalı olarak eylemleri/uyarıları tetikleme yeteneği.

Senaryo Kimliği	Senaryo Adı	Önem Düzeyi (1=Düşük, 4=Kritik)	Gösterim Gereklilikleri	Puanlandırmada Dikkate Alınacak Hususlar
Web.Ops.1	Operasyonlar - Bakım Aralıkları	3	Özellikle de bakımın uygulama erişilebilirliğini olumsuz etkileyebileceği durumlarda, bakım aralıklarını iş gerekliliğine uygun olarak yapılandırma yeteneğini gösterin.	Bir ilişkisel veritabanı hizmeti gibi bileşenlerin yapılandırılabilir bakım aralıkları.
Web.Ops.2	Operasyonlar - Günlüğe Kaydetme	3	Günlüklerin sanal makineler sonlandırıldıktan/hata verdikten sonra korunması dahil olmak üzere, birden çok bileşen içeren bir uygulama için günlüğe kaydetme hizmetini merkezileştirme yeteneğini gösterin.	- Uygulama gereklilikleri doğrultusunda ölçeklendirilebilen merkezi günlüğe kaydetme hizmetini yapılandırma yeteneği. - Belirli günlük olaylarına dayalı olarak uyarıları veya eylemleri tetiklemek için kurallar/filtreler tanımlama yeteneği.
Web.Ops.3	Operasyonlar - İzleme	3	Performans, erişilebilirlik, yanıt süreleri, hata sayıları ve benzerinin yanı sıra farklı ölçüm eşiklerine dayalı olarak eyleme geçme/bildirimleri tetikleme işlevselliği dahil olmak üzere uygulamanın nasıl izlendiğini gösterin.	- Disk G/Ç'si, CPU, veritabanı ölçümleri, ağ ve yük dengeleyici gibi mevcut olan standart ölçümler seti. - Özel ölçümler ve eşikler tanımlama yeteneği. - En önemli ölçümleri gösteren özel bir pano oluşturma ve bu panoyu ilgili kullanıcılarla paylaşma yeteneği.