Bulut Yönetişim Çerçevesi

Yönetişim & Standartlar Bölümü

Prepared by. : **Sultanate of Oman Information Technology Authority**

Translated by: **IT Governance Turkey**

ONAYLAMA & DAĞITIM:

	İsim	Email	Yayın Tarihi
Kim yayınladı	Yönetişim & Standartlar Bölümü	standards@ita.gov.om	2017
Kim doğruladı			
Kim onayladı	Yönlendirme Komitesi		

Dağıtım Listesi	
1.	ITA (Bilgi Teknolojileri Kurumu)
2.	İlgili tüm Devlet Kurumları
3.	Çevrimiçi Yayıncılık

DÖKÜMAN REVİZYON TARİHİ:

Versiyon	Tarih	Author	Uyarılar
1.0	2017	Yönetişim & Standartlar Bölümü	Dokümanın Oluşturulması

İçindekiler

SUNULAR

1 GENEL

Bu belge, çeşitli kabul ve servis modelleri ile bulut bilişimin kullanılabilmesi için bir çerçeve sunmaktadır. Ayrıca Umman devlet kurumlarıyla ilgili bulut bilişimin kullanılmasında belli faydaları, zorlukları ve riskleri listeler. Bu çerçeve, Umman kurumları için bulutun kullanılmasına yönelik organizasyonel, teknolojik ve çevresel yönergeleri göstermektedir. Bulutun kullanılmasında Umman kuruluşlarının; yasal beklentilerin farkında olması ve bulut sağlayıcının Umman Sultanlığının görev, yasa ve politikalarına uygun olduğunu anlaması gerekir.

1.1 AMAÇ

Umman e-Devlet Çerçevesi, devlet servislerinin sunumunu e.oman'ın misyonuna uygun olarak geliştirmeyi amaçlamaktadır. Çerçeve, risklerin en aza indirilmesi ve BT girişimlerinin daha iyi sunulması için kontroller koymayı amaçlamaktadır. E.oman misyonunun bir parçası olarak bu çerçeve, bulutun kullanılmasına yönelik yol gösterici ilkeleri özetlemeyi amaçlamaktadır. Bu, riskleri belirleme ve değerlendirme sürecini, bulut altyapısına ilişkin yardımcı ve güvenli stratejileri ve stratejilerin uygulandığından emin olmak için gerekli mekanizmaları içerir.

a. Bu çerçeve, Umman kurumlarındaki çeşitli paydaşlara bulut bilişimin tanıtılması ve bulut bilişimin çeşitli Umman kuruluşlarında servis olarak kullanılması sürecini tanıtmaktadır.

b. Bu çerçeve, kurumların mevcut BT ve bulut arasında bir karşılaştırma yapmasına yardımcı olacak belirli parametrelere dayanarak hangi bulut modelinin kendileri için uygun olduğuna karar vermelerine yardımcı olur ve rehberlik sağlar

c. Bu çerçeve, bazıları herhangi bir program için geçerli olan ve bazıları buluta özgü olan, hazır olma ve kullanılma unsurlarını sağlar. Bu unsurlar TOE çerçevesinden benimsenmiştir. TOE çerçevesi; bir firmanın bağlamının üç farklı unsuru benimseme kararlarını etkileyen organizasyonel düzeyde kullanılan bir teoridir.

1.2 HEDEF KİTLE

Aşağıda, bulutun kullanılmasına yönelik çerçeve için hedef kitle listesi verilmiştir.

a. Umman Sultanlığındaki, bulut bilişimi kullanmayı düşünen ve bulutun faydalarını, zorluklarını ve ilişkili risklerini anlamak isteyen kurumlar.

b. Çerçeveden doğrudan faydalanamayacak, ancak bulut hakkında daha fazla bilgi edinmek isteyen tüm hükümet paydaşları.

2 ÇEVRESEL FAKTÖRLER

Dünyanın dört bir yanında hükümetler, özellikle vatandaşlarla doğrudan etkileşime giren devlet dairelerinde günlük faaliyetleri gerçekleştirmek için servisleri/e-servisleri mümkün olan en iyi şekilde düzenlemektedir. e-Devlet uygulamalarının geliştirilmesi ve yaygınlaştırılması, belirli iş ihtiyaçlarını karşılamak için BİT'nin (Bilgi ve İletişim Teknolojisi) uyarlanması ve uygulanmasında çevikliğin artırılması ve aynı zamanda devletin BİT verimliliğinin (yeniden kullanım ve servis ölçeklenebilirliği yoluyla) artırılması, Bulut Bilişim ile önemli ölçüde kapsanmaktadır,

Umman kurumlarının, bulut bilişim stratejisini kullanmadaki hedefleri aşağıdaki gibidir:

a. Altyapının optimum kullanımı
b. Uygulamamaların geliştirilmesi ve uygulanmasını hızlandırma
c. Benzer uygulamaların geliştirilmesinde efor ve maliyetin tekrarlanmasını önlemek için benzer kuruluşlar arasında başarılı uygulamaların kolayca çoğaltılması
d. Tek bir yerde ortak standartları sahip sertifikalı uygulamaların kullanılabilirliği.

Bulutun kullanılması hedefleri göz önüne alındığında, Umman'daki kurumlar aşağıda belirtilen iş ve teknoloji avantajlarını anlayabilmelidirler:

a. Sadece bir kuruma servis vermek yerine daha geniş kullanıcı kitlesine uygun çözüm kullanarak kurumlar içindeki birliği kolaylaştırmak
b. Standartlaştırılmış uygulamalar, yasal gereklilikler ve kısıtlamalar, bulut çözümü aracılığıyla tüm kurumlara yayılabilirken, aynı zamanda her kurumun özerkliğini de koruyabilir
c. Çapraz işbirlikleri arasında iş çözümü yoluyla daha iyi bir işbirliği yapılması
d. BT'ye büyük yatırımlar yapmaya gerek kalmadan servis sunmaya daha fazla odaklanılması
e. Yeni servisler sunmak için pazara daha çabuk girilmesi
f. Donanım, yazılım ve lisans maliyetlerinde azalma ile daha düşük operasyonel maliyetler
g. Servislerin geliştirilmesinde, servislerin barındırılmasında ve yeni özelliklerden kaynaklanan geliştirmelerde maliyetlerin azaltılması.

3 İLKELER

Bulut bilişimi kullanma çerçevesinin ilkeleri bir yönetim temelini oluşturur. Kurumlar, bulutu birinci strateji olarak göz önünde bulundurup bulutu kullanmalıdır. Birinci bulut stratejisi, paylaşılan altyapı ve servisleri kullanmanın avantajlarından yararlanarak BT maliyetlerini azaltmaya odaklanır. Kurumlar yalnızca tüketilen kaynaklar için ödeme yapacaklardır. Aşağıda Umman kurumları için bulut bilişimin kullanılmasına yönelik ilkeler belirtilmiştir.

a. Etkinleştirme: Kurumlar, bulut bilişim için; dış kaynak düzenleme veya teknik platform yerine, stratejik bir sağlayıcı olarak planlama yapmalıdır.

b. Maliyet / Fayda: Kurumlar, diğer teknoloji platformu iş çözümlerinin maliyetleriyle karşılaştırıldığında bulut maliyetlerinin tam olarak anlaşılmasına dayanarak bulutun kullanılmasının faydalarını değerlendirmelidir.

c. Kurumsal Risk: Kurumlar, bulutun kabullenilmesini ve kullanımını yönetmek için bir Kurumsal Risk Yönetimi (ERM) perspektifini dikkate almalıdır.

d. Yetenek: Bulutu kullanan kurumlar, kapsamlı bir teknik destek ve dağıtım çözümü sağlamak için bulut sağlayıcılarının dahili kaynaklarla sunduğu yeteneklerin tamamını entegre etmelidir.

e. Hesap Verebilirlik: Kurumlar, iç sorumlulukları ve sağlayıcı sorumluluklarını açıkça tanımlayarak hesap verebilirlikleri yönetmelidir.

f. Güven: Kurumlar güveni; bulut çözümlerinin önemli bir parçası haline getirmeli ve bulut bilişime bağlı tüm iş süreçlerine güven duymalıdır.

4 BULUT BİLİŞİME GİRİŞ

Bulut bilişim, üçüncü taraf bir lokasyonda (sağlayıcı) veya kurumların veri merkezinde (konsolide) barındırılan servislere (iş /uygulamalar) internet üzerinden erişme modelidir. Bu servislere (sunucular, uygulamalar, depolama, vb.) istenildiğiinde, çeşitli kanallardan (iş istasyonları, dizüstü bilgisayarlar, cep telefonları, tabletler) ve her yerden geniş bir şekilde erişilebilir. Bu servisler, birden fazla kuruluş tarafından kullanılabilen ve gereksinimlere göre küçültülebilen veya genişletilebilen bir kaynak havuzundan (sanal / fiziksel) sağlanır. Servis ölçülür, yani kuruluşlar yalnızca kaynakların kullanıldığı süre için ödeme yapar.

Bulut bilişim, kullanılabilirliği artırır ve beş temel özellik, üç ana servis modeli ve dört dağıtım modeli ile tanımlanır. Bunlar daha sonraki bölümlerde ayrıntılı olarak açıklanmaktadır.

Temel özellikler	Servis Modeli	Dağıtım Modeli
• İsteğe bağlı self servis • Geniş ağ erişimi • Hızlı esneklik • Hızlı kurulum • Ölçülen servis	• Servis olarak Yazılım (SaaS) • Servis olarak Platform (PaaS) • Servis olarak Altyapı (IaaS)	• Genel Bulut • Özel Bulut • Karma Bulut • Topluluk Bulutu

Sunu-1 - Bulut Bilişim Modeli

4.1 BULUT BİLİŞİMİN ÖZELLİKLERİ

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST- National Institute of Standards and Technology) tarafından tanımlanan bulut bilişimin beş temel özelliği, bunları geleneksel BT'den ayırır ve küresel olarak kabul edilir. Beş özellik aşağıda kısaca tanımlanmıştır:

a. İsteğe bağlı self servis: Kurum/kuruluşlar, bir servis sağlayıcı ile insan etkileşimi olmadan gerektiğinde otomatik olarak sunucu saati ve ağ depolaması gibi bilgi işlem yetenekleri sağlayabilir

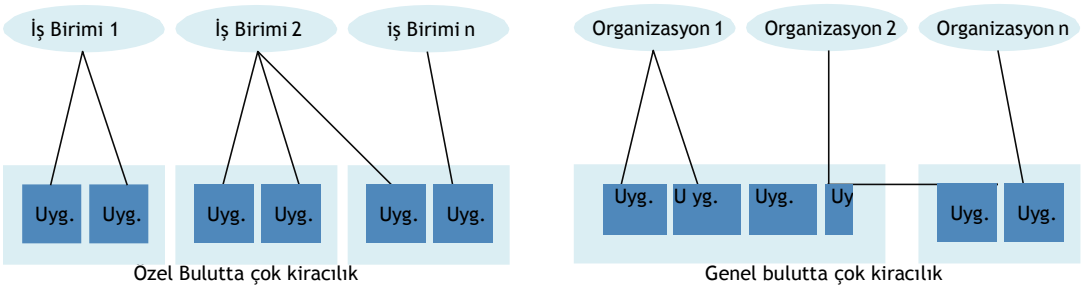
b. Geniş ağ erişimi: Herhangi bir servis (iş/destek/uygulamalar) ağ üzerinden kullanılabilir ve kuruluşlar tarafından cep telefonları, tabletler, dizüstü bilgisayarlar ve iş istasyonları aracılığıyla erişilebilir

c. Kaynak havuzu oluşturma: Sağlayıcının bilişim kaynakları, çok kiracılı bir model kullanan kuruluşlara servis vermek üzere toplanacak ve farklı fiziksel ve sanal kaynaklar isteğe göre dinamik olarak atanıp yeniden atanacak

d. Hızlı esneklik: Herhangi bir servis, bazı durumlarda otomatik olarak, talep ile orantılı olarak hızla dışa ve içe doğru ölçeklendirilebilir. kuruluşlara, kurulum için mevcut yetenekler sınırsız ve herhangi bir zamanda herhangi bir miktarda tahsis edilebilir görünecek.

e. Ölçülen servis: Bulut sistemleri, servis türüne (örn. Depolama, işleme, bant genişliği ve etkin kullanıcı hesapları) uygun bir soyutlama düzeyindeki ölçüm yeteneğinden yararlanarak kaynak kullanımını otomatik olarak kontrol eder ve optimize eder. Kaynak kullanımı izlenebilir, kontrol edilebilir ve raporlanabilir, böylece hem servis sağlayıcı hem de kullanılan servisin münferit kurumları için şeffaflık sağlanır.

Çok kiracılık, NIST tarafından yaygın olarak tanınmayan, ancak halen dünya çapında kabul gören bir diğer özelliktir. Umman kurumlarına veya farklı kuruluşlara (hem kamu hem de özel) ait olabilecek birden fazla kuruluş tarafından aynı kaynakların veya uygulamanın kullanılmasıdır ve genel bulutun çok önemli bir özelliğidir.



Sunu-2 - Bulut'ta Çoklu Kiralama

4.2 BULUT BİLİŞİMİN KULLANIM MODELLERİ

Kuruluşların bulutun kullanılmasına yönelik ilk adımı, servislerin sunulacağı dağıtım modelini seçmektir. Bulut üzerindeki servisler, aşağıdaki modellerden herhangi biri benimsenerek kullanılabilir:

a. Genel (Public) Bulut: Bir servis sağlayıcının, uygulamalar ve depolama gibi servisleri, kullanım başına ödeme modunda İnternet üzerinden kuruluşların kullanımına sunacağı genel bir bulut olarak

b. Özel (Private) Bulut: Umman kurumlarının veri merkezinde barındırılacak özel bir bulut olarak veya harici olarak sanal özel bulut olarak da bilinen bir üçüncü taraf sağlayıcı tarafından barındırılacak özel bir bulut gibi. Özel bulut, kurumlara kendi en iyi uygulamalarını standartlaştırma ve uygulama yeteneğini koruma fırsatı verecektir.

c. Karma (Hybrit) Bulut: Özel ve genel bulutun kombinasyonu, karma bir bulut olarak.

d. Topluluk (Community) Bulut: Bulut altyapısının aynı alandaki birkaç devlet kuruluşu (örneğin hükümetler, bağımlı kurumlar, vb.) tarafından paylaşılacağı bir topluluk bulutu olarak.

Aşağıdaki sunu, çeşitli bulut kullanma ve dağıtım modellerini göstermektedir.

Bulut Modeli	Altyapı Sahipliği	Altyapı Yönetimi	Lokasyon	Kullanan
Genel	Bulut Servis Sağlayıcı	Bulut Servis Sağlayıcı	Bulut Servis Sağlayıcı	Birçok organizasyon
Özel	Kuruluşlar	Kuruluşlar	Veri merkezi olan Kuruluşlar	Kuruluşlar
Sanal Özel Bulut	Bulut Servis Sağlayıcı	Bulut Servis Sağlayıcı	Bulut Servis Sağlayıcı	Kuruluşlar
Karma	İkisi de	İkisi de	İkisi de	Kuruluşlar, Özel Kuruluşlar
Topluluk	Bulut Servis Sağlayıcı veya kuruluşlar	Bulut Servis Sağlayıcı veya kuruluşlar	Bulut Servis Sağlayıcı veya kuruluşlar	Kuruluşlar, Üçüncü Parti Bağlantılı

Sunu-3 – Bulut'un Kullanma Modelleri

4.3 BULUT BİLİŞİMİN HİZMET MODELLERİ

Kuruluşların bulutu kullanmaya yönelik ikinci adımı servis türünü seçmektir.

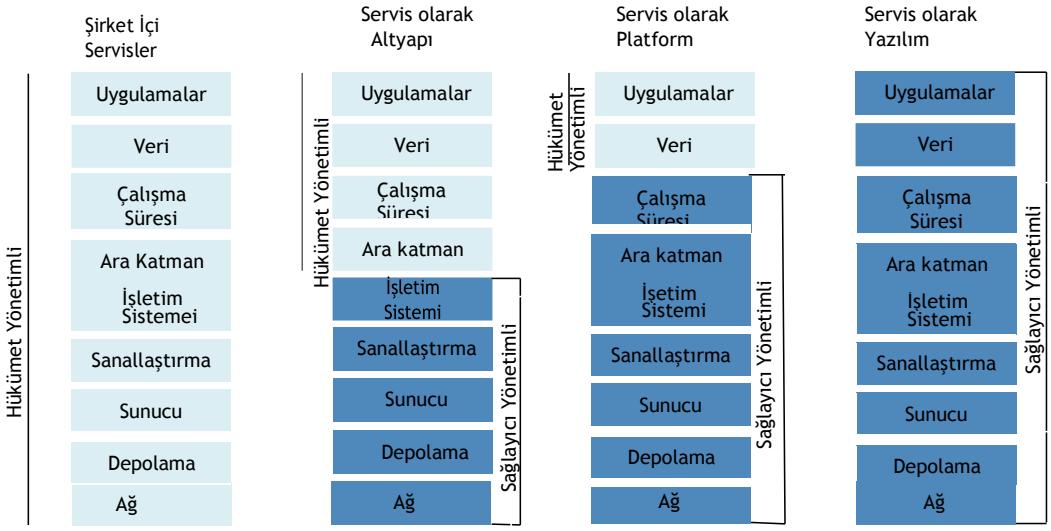
a. Servis olarak Yazılım (SaaS)

b. Servis olarak Platform (PaaS)

c. Servis olarak Altyapı (IaaS)

Her servis, temel bulut servisi modelinin üzerine inşa edilmiştir ve altındaki servislerin yapısını ve standartlarını gerektirir.

Aşağıdaki Sunu üç bulut servisi modelini ve hangi katmanların belirli bir modeli oluşturduğunu gösterir. Sunu aynı zamanda bir servis modeli içinde neyi (sağlayıcı / kuruluşlar) yöneteceklerini gösterir ve aynı zamanda modelleri şirket içi geleneksel BT modeliyle karşılaştırır.



Sunu-4 – Bulut Bilişim Modelleri

a. SaaS ile temel altyapı ve platformlar servis sağlayıcı tarafından sağlanır ve yönetilir. Sağlayıcı tüm yazılım geliştirme, bakım ve yükseltme işlemlerini üstlenecektir. Kuruluşlar böyle bir servisi seçerken yalnızca yazılım lisanslarının ücretini abonelik esasına göre ödemek zorundadırlar. SaaS örnekleri Office 365, CRM, ERP, GoToMeeting vb.

b. PaaS, kuruluşların sağlayıcı tarafından sağlanan bir dizi araçla internet üzerinden uygulama ve servis oluşturması için ideal olan IaaS'tan bir düzey daha yüksektir. Kuruluşlar, gereksinimlerine uygun uygulamalar oluşturmak için araçlar arasından seçim yapabilir. Altta yatan altyapı ve uygulamalar kuruluşlar için sağlayıcı tarafından desteklenecektir. PaaS Örnekleri sanallaştırma platformları, Java, MySQL servisleri vb.

c. IaaS'de, herhangi bir servis oluşturmak veya dağıtmak için temel altyapı sağlayıcı tarafından sağlanır. Kuruluşların bu servisleri oluşturmak için ara katman yazılımı, işletim sistemleri ve ilgili lisanslarla ilgilenmeleri gerekir. IaaS örnekleri Amazon Elastik Bilişim (AWS EC2), Rackspace ayrılmış depolama alanı (DAS, SAN, NAS çözümleri).

Üç ana servis modelinden türetilmiş, yukarıdaki üç servis modeline dayalı çözümleri olan belirli bulut servis modelleri vardır. Yukarıdaki bulut modellerinin örnekleri aşağıda belirtilmiştir.

a. Servis Olarak İş Süreci (BPaaS-Business Process as a Service) ile kuruluşlar; birleşik iletişim merkezi, zaman kartı yönetimi gibi SaaS üzerine kurulan iş servisleri için olan uygulamaları kullanabilirler.

b. Servis Olarak Felaket Kurtarma (DRaaS-Disaster Recovery as a Servise),; insan yapımı veya doğal bir felaket durumunda kuruluşların servislerinin çalışırlılığının devamını (bir değerlendirmeden sonra veya verilerin önemine ve sınıflandırmasına bağlı olarak) sağlamak için lokasyon dışında ve bulut içinde kopyalanmasını ve barındırılmasını tercih edebileceği bir çözümdür.

c. Servis olarak Güvenlik (SECaaS-Security as a Service) bulutta, geleneksel BT kurulumlarında olduğu gibi Internet üzerinden güvenli sistemler ve veriler sağlamak için bir çözümdür. Bulut servisi sağlayıcısı, virüsten korunma, Kimlik ve Erişim Yönetimi (IDAM–Identity and Access Management) gibi servisleri kuruluşlara sunacaktır.

d. Servis olarak Masaüstü (DaaS-Desktop as a Service) sanal bir masaüstünün arkaplanda sağlanmasıdır. Bulut servisi sağlayıcısı depolama, yedekleme, güvenlik ve güncellemeleri yönetir. Sağlayıcı tüm arkaplan altyapı maliyetlerini ve bakımını idare ederken, kuruluşlar kendi masaüstü görüntülerini, uygulamalarını ve güvenliğini yönetmelidir.

4.4 BİR BULUT MODELİNİN KULLANIMI İÇİN FAKTÖRLER

Kurumlar bir bulut modelini kullanmayı düşünmeden önce, belirli bir bulut modelinin kendileri için neden uygun olacağını belirlemek için gereksinimlerini değerlendirmeleri gerekecektir.

Bulut için SaaS dağıtım modelini seçmeyi tercih eden kuruluşlar aşağıdakileri dikkate almalıdırlar:

a. Kuruluşlar, bir yazılım veya teknolojiyi benimseme süreçlerinden ziyade işle ilgili süreçlere daha fazla konsantre olabilmek suretiyle, işle ilgili süreçlerinin verimliliğini artırmak ve sunulan farklı e-servislerinde işbirliğini geliştirmek istediklerinde SaaS'ı seçmelidirler.

b. Kuruluşlar SaaS yazılım servislerinden tam olarak ne istediklerini ve yazılım servislerinin sahip olması gereken özellikleri bilmelidir. Örneğin, kuruluşlar bir e - servis için harcanan zamanı azaltmak amacıyla çalışanlar arasındaki işbirliğini geliştirmek istiyorsa, çalışanların tek bir platformda olacağı bir servis olarak işbirliği yazılımını seçebilir, gerçek zamanlı iletişim kurabilir ve etkili ve verimli bir şekilde bir sorunu çözebilir.

c. Kuruluşlar, SaaS sağlayıcısının ne sunacağını ve servislerde kabul edilen standartları sağlayamazlarsa ne gibi sonuçlarla karşılaşacaklarını açıkça tanımlayan servis seviyesi sözleşmesini dikkate almalıdır.

d. SaaS ile kuruluşlar donanım ve yazılım için daha düşük maliyet ödeyecek. Örneğin, kuruluşun yalnızca 100 kullanıcısı olduğunu varsayarak, bulutta Office 365'i çözüm olarak seçiyor. Kuruluş, bulutta aktif bir Ofis 365 servisi için sadece 100 kullanıcı lisansı öder, çevresel bakım maliyeti tüm kuruluşlar arasında bölünür.

e. Servis sağlayıcı, yazılım güncellemelerini ve güvenlik yamalarını sağlamaktan sorumlu olacaktır, bu esnada kuruluşların artık güncelleme maliyetlerini karşılaması gerekmeyecek, ayrıca güncellemeleri, yamaları test etmek ve doğrulamak için teknik personele daha az bağımlı olacaktır.

Kuruluşlar bulut uygulamaları için uygulamalar ve servisler geliştirmeyi planlıyorsa kuruluşlar için PaaS modeli yararlı olacaktır. Kuruluşlar, dağıtım modeli olarak PaaS'ı seçmeden önce aşağıdakileri göz önünde bulundurmalıdır:

a. Kuruluşlar için PaaS seçim modeli, uygulamaya ve iş stratejisine bağlı olmalıdır. Örneğin, bazı PaaS sağlayıcıları araçlarla entegrasyon sunar. Yüksek düzeyde entegrasyon, uygulamaların dağıtım süresini azaltmaya yardımcı olabilir. Kuruluşlar ayrıca PaaS ortamındaki bir uygulamanın diğer uygulamalarla nasıl entegre olacağını ve verileri paylaşabileceğini de düşünmelidir.

b. Kuruluşlar için PaaS; uygulama geliştirme, veritabanı, entegrasyon, destek ve güvenlik servisleri sağlamalıdır. Kuruluşlar, söz konusu servislerin her birinde her başvuru için neye ihtiyaç duyduğuna karar vermelidir. Örneğin, herhangi bir yedek depolamaya ihtiyaç duyulursa, özel bulut servisleri daha iyi bir seçim olabilir.

c. Kuruluşlar seçim için PaaS (taşınabilir veya dikey olarak entegre) türüne karar vermek zorundadır. Kuruluşlar için en iyi seçenekler açık kaynaklı PaaS platformlarını seçmek olacaktır. Açık kaynak platformlarına örnek olarak Cloud Foundry, OpenShift, Stackato vb. verilebilir. Dikey olarak entegre edilmiş platformlar IaaS ve Paas ürünlerini sorunsuz bir şekilde birleştirir ve taşınabilir değildir. Bu teklifler genellikle Azure ve AWS platformlarında bulunabilir.

d. PaaS'ta desteklenecek geliştirme çerçeveleri ve dilleri. Kuruluşların PaaS'ta desteklenen geliştirme dillerini ve çerçevelerini kontrol etmesi ve belirlemesi önemlidir.

e. Maliyet; PaaS ile uygulamaların geliştirilmesi ve sürdürülmesi için maliyetlerin karşılanması için düşünülmesi gereken ve kuruluşların sorumluluğunda olan bir diğer faktördir.

Kuruluşlar için IaaS; ağ, depolama ve sunucuların kullanılabildiği durumlarda talep üzerine servisler sunmak için idealdir. Kuruluşlar dağıtım modeli olarak IaaS'yi seçmeden önce aşağıdakileri dikkate almalıdır.

a. IaaS, yoğun iş yükleri yürütme ihtiyacı olan ve aynı zamanda kaynakları hızlı ve düzenli bir şekilde yukarı veya aşağı ölçeklendiren kuruluşlar için ideal olacaktır

b. Sağlayıcı tarafından sunulan altyapı ve veri güvenliği, kuruluşların standartlarını karşılar

c. IaaS ile kuruluşlar, herhangi bir veri kaybı olmadan hızlı bir şekilde kurtarma ile sonuçlanan, düşük maliyetlerle birleştirilmiş bir felaket kurtarma altyapısı seçebilir

d. Kuruluşlar için cihaz bakım veya değiştirme maliyeti daha düşüktür. Kuruluşların artık çalışma süresi konusunda endişelenmesine gerek kalmayacak, çünkü güncellemeler ve bakım döngüleri için çalışma süresininden sorumlu sağlayıcı olacaktır.

Kuruluşlar, bulutun kullanılmasının etkenleri ve engelleyicilerine karşı, bir bulut servisinin uygulanabilirliğini belirlemeyi içeren bir bulut yakınlık bilgi formu değerlendirmesi yapmalıdır.

Parametreler	Bulut kullanım önleyicileri				Bulut kullanım sürücüleri		
	-3	-2	-1	0	1	2	3
Ölçeklenebilirlik							
Esneklik							
Uyumluluk							
Finansal Strateji							
Yetenekler							
Güvenlik							
Entegrasyon eforu							
Çıkış stratejisi							
Aciliyet							
Proje Süresi							

Sunu-5 - Bulut Yakınlık Değerlendirmesi

Yukarıdaki sunu, güçlü önleyicilerden güçlü sürücülere kadar -3 ila 3 arasında bir ölçek göstermektedir. Önleyici ağırlığı sürücü ağırlığından daha yüksekse, kuruluşlar belirli bulut benimseme modellerinden kaçınmayı düşünmelidir. Örneğin, hassas verileri özel bir bulutta depolamak ve kullanmak daha iyidir. Bunun tersi doğruysa ve sürücünün ağırlığı daha yüksekse, bulut karar süreci daha geniş bir potansiyel kullanma modeliyle devam edilmelidir.

Kuruluşlar, farklı servisleri ve uygulamaları değerlendirmek ve hangi bulut modelinin uygulamalar ve servisler için daha uygun olacağını seçmek için bir çözüm puanı metriği kullanmalıdır.

Skor	0=Zayıf	1=Ortalama	2=İyi	3=Mükemmel
Gereksinimlerin yerine getirilmesi	Tamamlanmadı	Kısmen tamamlandı	Tamamen tamamlandı	Fazlasıyla tamamlandı
Takas	Bu servisi / uygulamayı seçmek büyük bir uzlaşmaya yol açar	Bu servisi / uygulamayı seçerek takasa yol açar	Bu servisi / uygulamayı seçerek takas yapılmaz	Bu servisi / uygulamayı seçerek takas yapılmaz

Sunu-6 - Çözüm Puan Metriği

5 DEĞER ÖNERİSİ VE RİSKLER

Bu bölüm bulut bilişimin bir servis olarak kullanılmasına yönelik bazı faydalar, zorluklar ve riskler sunmaktadır. Bulut bilişim, ağır altyapı yatırımlarına olan ihtiyacı ortadan kaldırır ve esnek işletim modelleri sunar. Bu, Umman kuruluşlarının iş çevikliği ve piyasaya duyarlılığı geliştirmelerine yardımcı olacaktır. Bulut belirli faydalar sunmasına karşı, aşağıdaki bölümlerde vurgulanan ilgili bazı zorlukları ve riskleri de vardır.

5.1 DEĞER ÖNERİSİ

Bulut modelini Umman kuruluşları için çekici kılacak birkaç ilgi uyandıran özellik aşağıdadır:

a. Esneklik: Bulut tabanlı servisler, değişen BT gereksinimlerine sahip kuruluşlar için idealdir. Herhangi bir servisin ölçeklendirilmesi veya azaltılması gerektiğinde, gereksinimlere göre esnek bir şekilde ayarlanabilir. Bu çeviklik düzeyi, bulut bilişim kullanan kuruluşlara kısa sürede yeni servisler sunmak için gerçek bir avantaj sağlayabilir.

b. CapEx azaltma: Bulut bilişim, yüksek donanım maliyetini azaltır. Kuruluşlar, kullanılan kaynaklar ve servisler için yalnızca sunucuları ve servisleri dakikalar içinde ayarlama / ölçeklendirme kolaylığıyla ödeme yapar.

c. Varlık kullanımı: Bulut bilişim, kuruluşlar için yüksek verimli BT varlık kullanımını teşvik edecektir. kuruluşlar ve daireler arasında ekipmanın ve eforun önemli ölçüde tekrarlanmasının azaltılmasına yardımcı olacaktır. Uygulamaları, depolamayı ve bilgi işlem gücünü paylaşabildikleri için kuruluşlar en üst düzeyde kullanım için yapılanmaları gerekmeyecek.

d. Felaket Kurtarma (DR- Disaster Recovery: sınıflandırılmış ve gizli olabilecek pek çok kamusal veriyi işlemek ve ele almak zorunda olduklarından Kuruluşlar için bir DR oluşturmak çok önemlidir. Gerekli yatırım, kaynak ve uzmanlığa sahip olmayan daha küçük kuruluşlar için buluttaki bir DR çözümü gerçeklikten daha idealdir. Günün her saatinde sunulan sağlayıcı desteği ile büyük peşin yatırımlara gerek kalmadan geri dönüş senaryoları kolay olacaktır.

e. Geliştirilmiş Performans: Yüksek performanslı bir bulut platformu, kaynak yoğun uygulamaları destekleyebilir ve aynı zamanda Umman'daki kuruluşlar için Servis Seviye Anlaşmaları (SLA) elde edilmesine yardımcı olabilir.

   i. Daha hızlı işleme ile kuruluşlar, bulutta kritik uygulamaları CapEx ve OpEx'teki tasarruflarla daha uygun maliyetli ve güvenilir bir şekilde çalıştırabilir ve aynı zamanda varlıkların kopyalanmasını önleyebilir ve varlık kullanımını iyileştirebilir.

   ii. Daha hızlı disk erişimi, bellek ve işlem hacmi sayesinde büyük veri, analiz, modelleme ve simülasyon daha verimli çalışabilir.

a. Otomasyon: Otomasyon, kuruluşların bir sunucuda öz kaynak sağlamalarını (CPU, RAM, disk alanı vb.) sağlayacak ve bu sayede kuruluşların gerekli performansla ve herhangi bir müdahale olmadan servisleri verimli bir şekilde yönetmelerine yardımcı olacaktır.

b. Geliştirilmiş işbirliği: Tüm belgeler tek bir yerde merkezi olarak depolanabilir ve her kuruluş aynı anda belgeleri çalıştırabilir ve güncelleyebilir. Bulut, dağınık çalışanların bilgileri gerçek zamanlı olarak ve kolayca paylaşmalarına olanak tanıyacak ve işbirliğinin ilerlemesini sağlayacaktır.

Bu belge faydaları, zorlukları ve riskleriyle bulut bilişimin kullanılması için bir çerçeve sunmaktadır. İşbirliği servisleri hakkında her türlü bilgi için Teknik Referans Modeline başvurulmalıdır.

c. Servis ve kaynak güncellemeleri: Kuruluşların, işletmeyi sürdürmek için gereken güvenlik yamalarını veya uygulama güncellemeleri konusunda endişelenmelerine gerek yoktur. Güncellemeler ve yamalar testlerden sonra sağlayıcı tarafından test edilir ve kuruluşlara sunulur.

d. Yeşil BT: Bulut bilişim ile kuruluşlar kendi veri merkezlerinin boyutunu azaltabilir veya veri merkezini tamamen ortadan kaldırabilir. Sunucu sayısının, yazılım maliyetinin ve bakım personeli sayısının azaltılması, BT yeteneklerini etkilemeden BT maliyetlerini önemli ölçüde azaltabilir.

Bu belge faydaları, zorlukları ve riskleriyle bulut bilişimin kullanılması için bir çerçeve sunar, Yeşil BT ile ilgili standartlar ve en iyi uygulamalar için Teknik Referans Modeline bakınız.

5.2 ZORLUKLAR

İş ve BT paydaşları; kuruluşların en çok güvenlik, yatırım getirisi'ni (ROI-Return on Investment) ölçme ve çözümün doğru ekonomik değerini belirleme konusunda zorluk çektiklerini ve bunu takiben bulut tabanlı servislerin hükümet ve küresel standartlara göre yönetişimi ile ilgilenmektedir.

Aşağıda güvenlik, entegrasyon zorlukları ve bilgi yönetişimi ile ilgili endişeleri içeren bir hükümet kuruluşu perspektifinden tipik zorluklar listelenmiştir.

a. Servis kalitesi: Sağlayıcıların Servis Seviye Anlaşmaları (SLA'lar), servislerin istenen kullanılabilirlik, performans ve güvenilirlik düzeyinde çalışmasını sağlamak için sıkı ve yeterli değildir. Kuruluşların akılda tutması gereken belirli yönler vardır ve bulut sağlayıcısı, servis kalitesi ile ilgili olarak:
   i. Bir kuruluş tarafından istenen minimum servis seviyeleri
   ii. Bir arıza oluştuğunda mevcut olan çözümler
   iii. Felaket kurtarma ve iş sürekliliği prosedürleri
   iv. Kuruluş verilerinin taşınabilirliği
   v. Sağlayıcının izlediği değişiklik yönetimi süreci
   vi. Sağlayıcının altyapı ve güvenlik standartları
   vii. Sağlayıcı tarafından sorunları tanımlamak ve izole etmek için geçen süre
   viii. Bulut sağlayıcı ile yükseltme işlemi
   ix. Rol ve sorumluluklar dahil olmak üzere sağlayıcıyla çıkış stratejisi
   x. Sağlayıcı ile sözleşme feshi süreci.

b. Satıcı Kilitleme: Bulut servis sağlayıcıları, bulutlarının kullanımı konusunda esnek olmaları ve diğer sağlayıcılarla veya şirket içi servislerle kolayca entegre edilebilmeleri için kuruluşların güvence altına alınmasını sağlar, ancak başka bir sağlayıcıya geçiş (anahtarlama sağlayıcı) tamamen gelişmemiştir. Bu nedenle kuruluşlar, sağlayıcılar arasındaki birlikte çalışabilirlik ve destek sorunları nedeniyle servisleri bir satıcıdan diğerine taşımayı zor bulabilir.

c. Kesinti ve Erişilebilirlik: Kuruluşlar, yerel bir bağlantı yerine bir internet bağlantısı üzerinden servislere ve verilerine erişmelidir. Bu, ağ veya internet bağlantısı kesildiğinde, bulut servislerinin kesileceği anlamına da gelecektir. Bulut altyapısının performansı yük, ortam ve kullanıcı sayısından etkilenebilir. Bulut altyapısının kesintilere dayanıklı olmasını sağlamak kuruluşlar için hayati önem taşır. Tüm kesintileri azaltmak neredeyse imkânsız olsa da, hükümet verilerini korumak için güçlü ve esnek önlemlere sahip bir sağlayıcı seçilmelidir.

d. Ağ bağımlılıkları: Kuruluşlar karma bulut entegrasyon modelini seçmeye karar verirse ağ bağımlılıkları aşağıdaki parametreleri içeren özenli bir tasarım gerektirir:

   i. Özel bulut ve genel bulut altyapısı arasındaki gecikmenin (zaman gecikmesi olarak da bilinir) etkisi

   ii. Geniş alan ağları üzerinde çalışmak için mücadele edecek bant genişliği kullanan uygulamalarının belirlenmesi

   iii. Büyük veri gruplarını aktarmak için bant genişliği

   iv. Hibrit bir topolojide mevcut IP bloklarının kullanımı ve gerektiğinde IPv6 kullanımı

   v. Geleneksel BT/özel bulutta kullanılan güvenlik cihazlarını ve çözümlerini genel bulutta kullanma.

Bu belge faydaları, zorlukları ve riskleriyle bulut bilişimin benimsenmesi için bir çerçeve sunmaktadır. Ağ bağımlılıklarına ilişkin herhangi bir referans için, politikalar Teknik Referans Modelinde belirtilecektir.

e. Buluta geçiş: Buluta geçiş karmaşık ve kapsamlı bir süreçtir, kuruluşlar önerilen çözümün iş modellerini tamamladığından emin olmalıdır. Kuruluşların bir bulut sağlayıcısının bilmek isteyeceği belirli yönler vardır:

   i. Kuruluşlar için servis talep modelleri

   ii. Kruluş için en büyük veri akışı

   iii. Kuruluşlar için yıllık veri büyümesi

   iv. Verilerin lokasyonu olan kuruluşlar için kısıtlamalar

   v. Kuruluş tarafından talep edilen veriler üzerindeki kontrol

   vi. Kuruluşların SLA beklentileri.

f. Sistem Yönetimi: Hibrit bulut sistemlerinin yaşam döngüsü yönetimi, yanlış yapılırsa zor olabilir ve kuruluşların aşağıdakileri anlamak ve başarmak için kapsamlı bir şekilde hazırlanması gerekir:

   i. Altyapı kaynakları, ortamlar arasında self servis olarak sağlandığında etkili yapılandırma yönetimi

   ii. Birden fazla ortamın güvenliğini sağlama ve yamalama

   iii. Esnek kaynak havuzlarıyla uğraşırken kapasite planlamasının doğası değişir

   iv. Hibrit bulutta entegre ve etkili izleme

Bu belge faydaları, zorlukları ve riskleriyle bulut bilişimin benimsenmesi için bir çerçeve sunmaktadır. Ağ bağımlılıklarına ilişkin herhangi bir referans için, politikalar Teknik Referans Modelinde belirtilecektir.

5.3 RİSKLER

Teknolojinin her kullanılması, bilinen ve bilinmeyen faktörlerden kaynaklanabilecek bazı engeller getirir. Aşağıda, bulutun kullanılması ile ilişkili riskler verilmiştir.

a. Güvenlik ve Gizlilik: Buluttaki veri ve bilgi güvenliği genellikle en uygun düzeydedir olup genellikle güvenilir ve yeterlidir. Hem kamu hem de özel bulut sağlayıcıları çeşitli standartlarla uyumludur, ancak kuruluşlar kısıtlı ve gizli verilerle uğraşırken önemli verileri üçüncü taraf bir sağlayıcıya teslim etmekte daha isteksiz olabilir ve buluttaki veriler herhangi dünyada bir yerde saklanabilir ve yedeklenebilir Kuruluşlar tarafından dikkate alınması gereken birkaç güvenlik durumu:

   v. Buluttaki veri konumu

   vi. Verilerin güvenliği ve şifrelenmesi

   vii. Bulut sağlayıcısının güvenlik ve yönetişim politikaları

   viii. Kuruluşların verileri ve ortam üzerindeki kontrolü

   ix. Kuruluşun verilerini bulutta yedeklemek için geçen süre

   x. Sağlayıcının veri denetim prosedürleri

   xi. Veri bozulması durumunda veri kurtarma

   xii. Servisin kurum içinde veya başka bir bulut sağlayıcıya taşınması gerekiyorsa kurumlar için veri çıkarma prosedürleri..

Bu belge, ilişkili faydalar, zorluklar ve risklerle birlikte bulutun benimsenmesine yönelik yönergeler sağlarken, bilgi ve güvenliği ile ilgili tüm politikalar bilgi güvenliği yönetimine bakılmalıdır.

b. Sınırlı Kontrol: Bulut altyapısı tamamen servis sağlayıcıya ait olduğu, yönetildiği ve izlendiği için genel bulutlarda kuruluşlara minimum kontrol verilebilir. Kuruluşlar, arkaplan altyapısını değil, yalnızca bunun üzerinde çalışan uygulamaları, verileri ve servisleri kontrol edebilir ve yönetebilir. Kuruluşlar, sağlayıcının yönetişim, uyum ve yönetim politikalarını kabul etmek zorundadır.

Bu belge, ilişkili faydalar, zorluklar ve risklerle birlikte bulutun benimsenmesine yönelik yönergeler sağlarken, bilgi ve güvenliği ile ilgili tüm politikalar bilgi güvenliği yönetimine bakılmalıdır.

c. Verilerin lokasyonu: Bulut bilişim, sınırsız bir kavramdır ve çoğu sağlayıcı verisi veya verinin bir kopyası, bir terslik veya felaketten kurtulmak için temel konumdan farklı bir coğrafi yerde saklanır. Umman'da kuruluşların aşağıdakileri dikkate alması gerekir:
   i. Veri sahipliği, erişilebilirlik, gizlilik ve güvenlik ile ilgili koşullar
   ii. Verilerin depolanması ve farklı bulut modellerine iletilmesine ilişkin karar..
   iii. Uygulama hassasiyeti, veri sınıflandırması ve diğer ilgili gizlilik ve güvenlik
   iv. Barındırma yetkisinin düzenleyici ve yasal çerçevesi.

Bu belge, ilişkili faydalar, zorluklar ve risklerle birlikte bulutun benimsenmesine yönelik yönergeler sağlarken, bilgi ve güvenliği ile ilgili tüm politikalar bilgi güvenliği yönetimine bakılmalıdır..

d. Birlikte Çalışabilirlik ve Uyumluluk: Herhangi bir kuruluş farklı bir bulut sağlayıcısına veya belki de içerde farklı altyapıya geçmeye karar verirse, farklı çözümlerin farklı altyapı ve yazılım yığınları çalıştırma olasılıkları olabilir. Bu, aynı değişiklik yönetimi süreçlerinin karma bulutta kullanılıp kullanılmadığını veya sağlayıcıya bağlı olarak her birinin benzersiz olup olmadığını dikkate alma riski taşır.

e. Yasal düzenlemeler: Kuruluşlar için yasal ve yasal standartlara uyum çok önemlidir. Bulut sağlayıcısı ve kuruluşlar yasal düzenlemelere uymakla yükümlüdür. Herhangi bir kuruluş bir bulut modeli kullandığında ve uyguladığında, kuruluşun sözleşme sürecinin tüm aşamalarında aşağıdaki gibi düşünmesi gereken bazı sorunlar vardır:
   i. İlk durum tespiti
   ii. Sözleşme görüşmesi
   iii. Uygulama
   iv. Fesih (bitiş veya anorma durumda)
   v. Tedarikçi devri.

Bu belge, ilişkili faydalar, zorluklar ve risklerle birlikte bulutun benimsenmesine yönelik yönergeler sağlarken, bilgi ve güvenliği ile ilgili tüm politikalar bilgi güvenliği yönetimine bakılmalıdır..

5.4 GELENEKSEL BT'NİN BULUT İLE KARŞILAŞTIRILMASI

Bulutu benimsemenin geleneksel veri merkezi yaklaşımıyla karşılaştırıldığında kendi yararları vardır. Kuruluşlar, fizibilite değerlendirmeleri, maliyet fayda analizi, vb. uygulayarak bulutu kullanmanın faydalarını geleneksel bir yaklaşımla değerlendirebilir. kuruluşların aşağıdakileri dikkate alması gerekir:

a. Bir veri merkezine sahip olmak büyük bir ön yatırıma gerektirecek ve barındırılan servisleri yönetmek ve sürdürmek için nitelikli insan gücü gerektirecektir.

b. Veri merkezi cabinet ve rafı dışında, alternatif bir kaynak aracılığıyla servisleri bir yedekleme sistemi ile yerinde tutmak ve çalıştırmak için enerji gereksinimi vardır.

c. Sorun olmadan altyapıyı çalışır durumda tutmak için verimli soğutma ve kablo dolapları gereksinimleri vardır

d. Sürekli artan servis ihtiyacı ve talebi nedeniyle her zaman daha fazla alan talebi

e. Ayrıca, kuruluşlar ağ, sunucu ve depolama altyapısını temin etmek ve en son yükseltmeler ve yamalar, istihdam / dış kaynak yönetimi ve bakım personeli ile güncel tutmak zorunda kalacaklar. Ayrıca, servislerin satın alınması ve oluşturulması, kullanıcı sayısına bağlı olarak lisans maliyetlerini gerektirecektir ve bu maliyet, kullanıcı sayısında ve servis yeteneklerinde bir artışla artmaya devam edecektir. RTO ve RPO ihtiyaçlarına göre servislerin kullanılabilirliğini izlemek ve yönetmek için kalifiye personel gereksinimi ile izleme ve yönetim araçlarıyla ilişkili maliyetler olacaktır.

f. BT yenilemesi; çözümlerin, servislerin ve ürünlerin kullanım ömrünün sonunda olacağı ve OEM'lerin güncelleme ve güvenlik yamaları yayınlamayacağı için kuruluşların bu süre boyunca takip etmesi gereken başka bir büyük çalışma olacak.

Aşağıdaki sunu, geleneksel BT'nin bulut ile servis modeli olarak karşılaştırılmasını sağlar.

Parametre	Açıklama	Geleneksel	Bulut
BT İzleme / Yönetim Eforları	Ekipmanların izlenmesi için otomasyon seviyesini ifade eder	Araçlara rağmen yüksek manuel çaba	Bulut yönetim / izleme araçları nedeniyle önemli ölçüde azaltılmıştır. Daha hızlı yatırım getirisi sağlar; Azaltılmış Operasyonel harcama (OpEx)
CapEx	Veri merkezi ve BT altyapısını kurmak için tek seferlik maliyet gerekir	Adanmış altyapı Yüksek Maliyet	Kurumsal bulut oluşturmak için Capex gerekiyordu. İzleneen hesaplama/depolama/ ağ uygulamalarının kullanımına dayalı ters ibraz, yatırım getirisini daha hızlı gösterir; Ters ibraz yoluyla bulut yatırımı kurtarma
OpEx	Belirli bir süre, belki de 3-5 yıllık bir süre için gereken operasyonel harcamaları ifade eder	FTE sayısı, güç, soğutma vb. Nedeniyle daha yüksek.	Sanallaştırma ve otomasyon nedeniyle geleneksel BT ile karşılaştırıldığında azalır; VM'ler özeldir ve servis yenilenmesi O/S'nin yeniden konuşlandırılması, varlıkların daha kolay yönetimi; İndirgenmiş OpEx;

Parameter	Explanation	Traditional	Cloud
Kullanım (Utilization)	Kullanım, herhangi bir zamanda tüketilen BT kaynaklarının miktarını ifade eder	Genellikle % 5-20	Optimize edilmiş (% 60-70 genelde). Genel altyapı gereksinimini azaltarak diğer havuz türlerinden kaynakları yeniden dağıtabilir. Daha düşük OpEx, daha hızlı TTM, daha fazla çeviklik
Kullanılabilirlik (Availability)	Kullanılabilirlik, anlaşmalara göre istenen ekipman ve servis çalışma süresidir.	Cluster yapı % 99,9 ancak 2xmaliyet sağlayabilir	Uygun uygulamalar, 0 kesinti süresi anlamına gelen yeniden başlatılabilir işlemlerle yatay olarak ölçeklenir Daha hızlı geri dönüş; Düşük OpEx
Esneklik (Elasticity)	Sistem kapasitesinin gerektiği gibi artırılma veya azaltılabilme derecesi	Yukarı / aşağı ölçeklendirme tedarik temelli planlı bir çalışmadır	Ölçekleme yukarı / aşağı otomatik talep üzerine yapılır ve teorik olarak ihtiyaç duyulan sonsuz dalgalanmalar bulut tarafından talep üzerine servis edilir (bulut patlamaları)
Ölçeklenebilirlik (Scalability)	Bir sistemin mevcut donanım kaynakları üzerindeki iş yükünü arttırma yeteneği	Başlangıçta maksimum yük boyutu. Yeniden boyutlandırma hantal	Talep üzerine tahsis edilmiş bulut havuzunda donanım olarak isteğe bağlı otomatik ölçeklendirme Azaltılmış OpEx; Ortalama yükler için kapasite planlaması CapEx'i azaltır

Sunu-7 - Geleneksel BT'nin Bulut ile Karşılaştırılması

5.5 PAYDAŞLAR, ROLLER VE SORUMLULUKLAR

Bulut bilişim kullanım çerçevesini benimsemek ve kuruluşlar arasında gelecekte rehberliği sağlamak için paydaşlar, kurumları bu çerçeveyi benimsemeye yönlendirmede iş, teknoloji veya süreç açısından rol alacaktır.

Kuruluşların BT Başkanı aşağıdakilerden sorumludur, ancak bunlarla sınırlı değildir:

a. Kuruluş içindeki çeşitli paydaşların ihtiyaçları doğrultusunda çerçevenin stratejik olarak gözden geçirilmesi ve kuruluşların kilit misyonları ile uyumlu tutulması

b. Bütçeyi ve ilişkili fonları yönetmek için sponsorlarla birlikte çalışılması, uygun aralıklarla gözden geçirilmesi

c. İlgili zorluklar, riskler ve paydaşların girdileri ile çerçevenin kullanımını denetlemek

Kuruluşların BT mimarları aşağıdakilerden sorumlu olacak:

a. Veri merkezi, uygulamalar ve teknoloji dahil olmak üzere mevcut BT'nin olgunluğunun değerlendirilmesi

b. Bulutun benimsenmesi ve standartlara ve düzenlemelere uygunluğun sağlanması için yönetişim modelinin tanımlanması

c. Bulut bilişimin benimsenmesi için bir plan hazırlanması.

5.6 BULUT'UN KULLANIMI İÇİN YASAL ÇIKARIMLAR

Umman kuruluşları ve bulut sağlayıcıları, verileri ve bilgi güvenliğini korumak için yasalara, düzenlemelere ve yükümlülüklere uymak zorundadır. Kuruluşlar, bulut sağlayıcılarının, kuruluş verilerini kayıp, yanlış kullanım veya değişiklikten korumak için makul teknik, fiziksel ve idari önlemleri aldıklarından emin olmalıdır.

Bulut bilişim ortamında gizlilik ve veri koruma ile ilgili temel hususlardan bazıları:

a. Umman kuruluşlarının kendi veri güvenliği ve erişim yönetimi politikaları olacaktır. Bulut sağlayıcısının politikaları, kuruluşların politikalarıyla uyumlu olmalıdır

b. Umman kuruluşları için verinin lokasyonu birincil derecede önemlidir. Her durumda veri veya herhangi bir kopya / yedekleme Umman'ın yasal sınırları içinde kalmalıdır

c. Kuruluş verilerinin kaybolduğu bir saldırı durumunda, sağlayıcının kayıp verileri nasıl kurtaracağına dair prosedürler olmalıdır

d. Umman yetkisi altındaki bulut sağlayıcısı; hem çevrimiçi hem de çevrimdışı veriler olmak üzere, farklı veri saklama ve sızıntı ve veri yok etme yükümlülüklerine uymak zorundadır.

e. Bulut sağlayıcı farklı olmamalı ve gelecekte bulutta bulunan verilerin güvenliğini güçlendirmek için veri şifreleme standartları ile ilgili yasal ve düzenleyici gereklilikleri değiştirmemelidir

f. Umman'daki yasalar herhangi bir zamanda değiştirilirse, sağlayıcı artan kontrol yükümlülüklerine uymalıdır.

g. Gerektiğinde, sağlayıcı güvenlik politikalarını paylaşmaya açık olmalı ve aynı zamanda dış denetimlere açık olmalı ve iç denetim raporlarını paylaşmalıdır.

h. Kuruluşlar, sağlayıcının ayrıntıları önemli ölçüde değişmeyen ulusal standartları uygulamasını isteyebilir.

i. Sağlayıcı, kuruluşların bulut ortamı üzerindeki kontrolünü kaybedip kaybetmeyeceğini ve ne ölçüde kontrol edeceğini belirtmelidir.

j. Sağlayıcı, kuruluşların değişiklik yönetimi sürecinden haberdar olmalı ve gerekirse değişiklik yönetimi sürecini güncellemeli ve paylaşmalıdır.

k. Bir ihlal durumunda, sağlayıcıya karşı sorumluluk, kuruluşlara proaktif yanıt ve sağlayıcı tarafından uygunsuzluk nedeniyle tazminat sağlanmalıdır.

l. Umman kuruluşları tedarikçiden sözleşme kağıt üzerinde imzalanana kadar emanet koşulların yerine getirmesini isteyebilir.

m. Kuruluşlar, kesintiler ve ihlaller hakkında uyarılar (e-posta / SMS / aramalar), aylık olarak servis kullanılabilirliği raporları talep edecektir. Mücbir sebep durumunda bulut sağlayıcısı servisleri mümkün olan en kısa sürede sunmak için elinden geleni yapacaktır.

n. Kuruluşların, servis bakımı ve desteği için herhangi bir üçüncü tarafla sözleşme yapılıp yapılmadığını bilmeleri gerekir.

o. Herhangi bir zamanda veya bir anlaşma imzalandığı sırada bir kuruluş, bulut sağlayıcı personelinin yetkinliklerini bilmek isteyebilir ve kuruluşları destekleyen sağlayıcılarda çalışanların geçmiş kontrollerini yapmak isteyebilir.

p. Kuruluşlar, bulut sağlayıcısının önceden haber vermeksizin sözleşme şartlarını, ücretleri ve ücret yapısını değiştirme yetkisine sahip olup olmadığının farkında olmalıdır

q. Kuruluşlar, sunulan servis türünü, işlevsellikleri ve servislerin sözleşme sırasında gelişip gelişmeyeceğini içermesi gereken bulut servisinin açık tanımını bilmelidir. Bu, kurumların SLA'leri tanımlamasına yardımcı olacaktır.

r. Kuruluşlar, uygun bir onay süreci yapılmadıkça ve gerçekleşene kadar, verilerine bulut sağlayıcısı ve ilişkili üçüncü taraf tarafından erişim ve kullanımlarını sınırlamak isteyeceklerdir.

s. Kuruluşlar, bir sözleşmenin sona ermesi ve sözleşmenin feshedilebileceği veya uzatılabileceği koşullar hakkında önceden bilgilendirilmelidir.

t. Bir sözleşmenin feshi halinde, kuruluş verilere ne olacağını öğrenme hakkını sahiptir. Kuruluş verileri nasıl ve hangi biçimde ve formatta alabilecek? Geçiş dönemi boyunca, sağlayıcı verileri gerekli bir süre boyunca tutabilmek için destekleyici olmalıdır.

6 BULUT HAZIRLIK VE KULLANIM KILAVUZLARI

Barındırılan servislerin internet üzerinden iş yenilikleri ve maliyet avantajlarıyla sunulması ile bulut bilişim paradigması servis sunumunu değiştirmektedir. Bulut bilişim, arka plan çalışmalara rağmen kuruluşların iş esnekliğini artırmasına yardımcı olmaktadır. Kuruluşlar, sıkı uyum ve güvenlik önlemleri ile sosyal, mobil ve analitik teknolojilerinin veri güvenliğinden ödün vermemesini sağlayan çevik ve yenilikçi bulut sunumları ile kritik görev operasyonlarını destekleyebilecekler.

Kuruluşların bulutun kullanılması ile odaklanabilecekleri bazı temel alanlar:

a. BT Konsolidasyonu

b. Paylaşılan Servisler

c. Vatandaş Servisleri

BT'nin konsolidasyonu, çeşitli kurumların çok sayıda dağınık veri merkezinin merkezileştirilmesini içerecektir. Her bir veri merkezi, servislerin maliyeti, uygulamaları ve sunucu konsolidasyonu ve sanallaştırılması ile değerlendirilmesi gerekir.

Kuruluşlar, daireler arasında ortak olabilecek servislere, uygulamalara, veritabanlarına, ağ geçitlerine vb. sahip olacaktır. Paylaşılan servisler, kuruluşlar için, finansal belirsizlikleri azaltan ve para tasarrufu sağlayan ölçekli ekonomileri destekleyen servis sunma fırsatı ve ayrıca çalışanların, vatandaşlar ve işletmeler için yeni servisleri daha hızlı sunma fırsatları sunacaktır.

Sayısallaştırılmış belgeler için depolama alanı, çevrimiçi tasdik servisleri, doğum kayıtları vb. vatandaş servisleri bulut üzerinde sunulabilir. Bu servisleri sunan yeni bir sunucu, herhangi bir manuel müdahale olmadan bulutta dakikalar içinde kurulabilir.

Kuruluşlar, bulutun kullanılmasında uygun aday olabilmek için başvuruları aşağıdaki gibi tanımlamalı ve sınıflandırmalıdır:

a. Genel: Portallar, insan kaynakları yönetimi, depolar vb. tüm kurumlarda kullanılan genel uygulamalardır.

b. Grup: Eğitim, sağlık yönetimi, BT gereksinim yönetimi gibi grup uygulamaları olarak adlandırılan ve bulutta kullanılan uygulamalar adaylar için uygun olabilir.

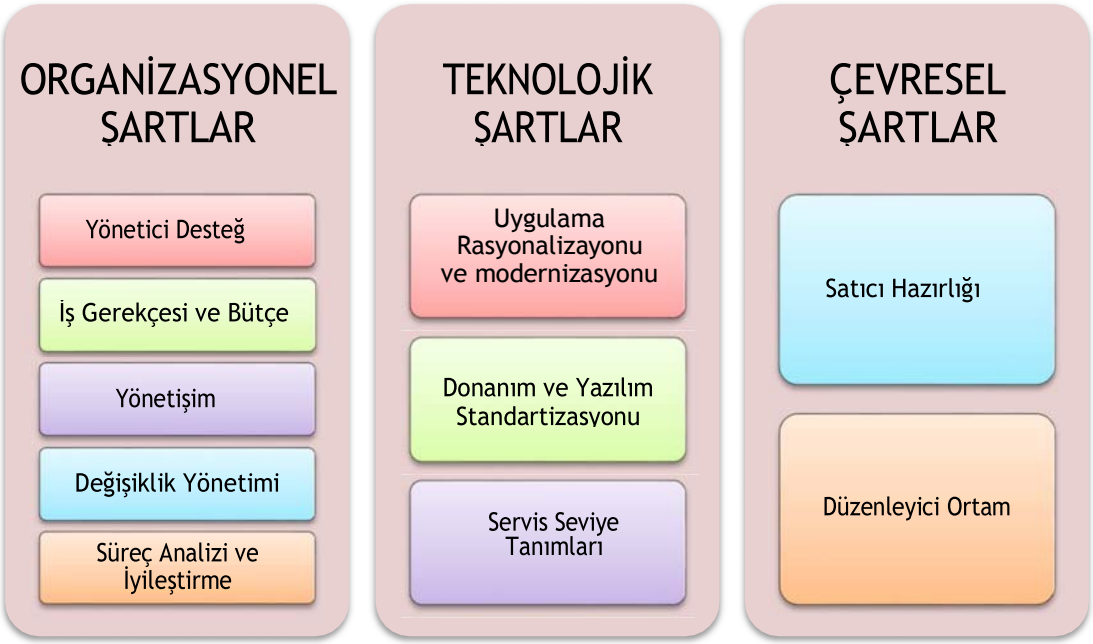
c. Daire: birkaç dairede yaygın olarak kullanılan uygulamalar genelleştirilebilir ve polis, kovuşturma, belediyelerin vb. bulutlu kullanmaları için uygun olabilir.

Bulutun kullanılmasına ilişkin kılavuzlar, teknolojinin kullanılması ve olasılığını etkileyen faktörleri açıklayan Teknolojik, Organizasyonel ve Çevresel (TOE) şartlara dayanmaktadır.

6.1 HAZIRLIK KILAVUZU

Bulutun kullanılması, teknolojinin kullanım biçiminde köklü bir değişimdir ve en üst düzeyde paydaşların bilgilendirilmesi, iş gerekçesi oluşturulması ve bir sponsor bulma konusunda destek ve hazır olma gerektirecektir.

Farklı benimseme aşamalarınki hazır olma unsurları aşağıda belirtilmiştir.



Sunu-8 – Bulut'a Hazırlık Esasları

6.1.1 ORGANİZASYONEL ŞARTLAR

Organizasyon perspektifinden bakıldığında; kuruluşlar, bulutun kullanılmasında temel faktörler olarak değişimi barındıran yeniliğe ve süreçlere odaklanırlar.

a. Yönetici desteği: Bulutun başarılı bir şekilde kullanılması için, Umman kuruluşlarının iş işlevlerine kesin dahil olması ve mevcut teknolojik ortamlarını elden geçirmeye ihtiyacları olacaktır. Bu, programın hedeflerini oluşturmak, benimseme planına ayak uydurmak ve sürdürülebilir bir seviyede gözetim sağlamak için kuruluşlar içinde ve arasında çeşitli düzeylerde yönetici desteğini gerektirecektir.

b. İş gerekçesi ve bütçe: Bulutun kullanılması, bir iş gerekçesi oluşturmayı gerektirecek diğer birçok program ve adımla ilişkilendirilecektir. Tüm kuruluşlar için iş hedefleri, istenen gelecek ve gerekli yatırımlarla açıkça ifade edilmelidir.

c. Yönetişim: Zaman ve maliyet aşımlarından kaçınmak için tüm bulut kullanılmasının, ilgili programların ve adımlarının yönetişimi kuruluşlar açısından önemlidir. Bulut programı, kullanımının başarılı olması için, iş ve BT yönetişiminin bir kombinasyonuna ihtiyacı olacaktır. Kuruluşların bulutun kullanılması veya bağımsız bir yönetişim ekibi oluşturmaları için yönetişim organizasyonlarını yeniden düzenlemeleri gerekebilir

d. Değişim yönetimi: Bulutun kullanılması ile kuruluşarın BT organizasyonlarında bir değişiklik yapması gerekecektir. Bulut kullanma çalışmalarının doğasına bağlı olarak, bu değişiklikler sık sık, çok yönlü ve sürekli değişiklik müdahalesi gerektiren şekilde kapsamlı olabilir. Kuruluşların bu kültürel değişime hazır olmaları gerekecek.

e. Süreç analizi ve iyileştirme: Kuruluşların BT organizasyonu buluta geçişten faydalanacak. Süreç analizi ve iyileştirmeler; iş sürecini yazılım uygulaması ve servislerindeki değişikliklerle uyumlu hale getireceğinden SaaS'ı seçmenin en büyük yararı olacaktır ve bu da iş süreçlerinin, uygulamalar tarafından sunulan yetenekleri en iyi şekilde kullanılmasını sağlayacaktır.

6.1.2 TEKNOLOJİK ŞARTLAR

Kuruluşların iç teknolojilere ve piyasadaki mevcut bulut teknolojilerine ve çözümlerine odaklanması gerekecektir. Dahili olarak, bulutun kullanılması, uygun bir teknik altyapıyı yönetebilen ve e-iş bilgisine sahip yetkili çalışanlara dayanacaktır. Harici olarak, e-iş teknolojisinin kullanılabilirliği gereklidir.

a. Uygulamanın rasyonelleştirilmesi ve modernizasyonu: Kuruluşlar için buluta geçiş, uygulama ortamlarını değerlendirmelerine, uygulamaların kullanışlılığını anlamalarına ve bir temizleme gerçekleştirmelerine olanak sağlayacaktır. Uygulama modernizasyonu, portföyü rasyonelleştirmeye ve iki ortama (bulut ve eski ortam) sahip olmaktan kaçınmaya yardımcı olacağı için buluta geçmenin önemli bir yönüdür. Bu iki ortamın bakım maliyeti olacaktır. Herhangi bir kuruluş için modernizasyon ve buluta geçiş, beklenen kuruluş standartlarına göre olmalıdır.

b. Donanım ve yazılım standardizasyonu: Herhangi bir kuruluşun bulut bilişimi kullanabilmesi için ilk adım altyapılarını, platformlarını ve yazılımlarını birleştirmek olacaktır. Her kuruluşun kendi standartlarını geliştirmesi gerekir. Bulutun kullanılması için, her kuruluşun bulut kullanma yolculuğu boyunca dönüşüm geçirecek olan mimari grup girişimleri ile yönlendirilecek standartlara ihtiyacı olacaktır. Zaman standardizasyon aşılmadığı sürece her kuruluş esneklik ve çeviklik sağlayabilecektir. Donanım ve yazılım standardizasyonu bulut yararlarının çoğu için kritik bir itici güç olacaktır ve her kuruluş için bugünün öncelikleri ve gelecekteki beklentileri arasında bir denge kurmasını gerektirecektir.

Bu belge faydaları, zorlukları ve riskleriyle bulut bilişimin benimsenmesi için bir çerçeve sunmaktadır. Donanım ve yazılım standartlarına ilişkin herhangi bir referans için Teknik Referans Modeline bakınız.

c. Servis seviyesi tanımı: Kuruluşlar için teknoloji gereksinimleri bulutta servisler olarak sunulacaktır. Servis seviyeleri, kuruluşun servisten ne istediğini tanımlar. Kuruluşlardaki BT organizasyonu için Kilit Performans Göstergelerine (KPI) karşı bir ölçü olarak servis edecektir.

6.1.3 ÇEVRESEL ŞARTLAR

Çevresel şartlar, tedarikçinin bulut servisleri sunmaya hazır olmasını, piyasadaki bulut rakiplerini, makroekonomik şartları ve yasal ortamı içerir.

a. Satıcı Hazırlığı: Bir bulut modelini kullanmak isteyen herhangi bir kuruluş, geçmiş değerlendirmelerinin bir parçası olan veya olmayan satıcıların hazır olup olmadığını dikkate almak zorundadır. Kuruluşun ayrıca açık kaynak standartları olan çözümleri de dikkate alması gerekecektir. Satıcı hazırlığı, bulut sağlayıcılarını değiştirirken bulutun benimsenmesini büyük ölçüde etkiler.

b. Düzenleyici ortam: Düzenleyici ortam, bulutun kullanılmasını ve dönüştürülmesini hem teşvik edebilir hem de yavaşlatabilir. Hükümet ve küresel yönetmelikler kaynakları uyum için zorlayabilir.

6.2 KULLANIM KILAVUZU

Bulut kullanmak isteyen veya bulut kullanma sürecinde olan Umman kuruluşları için, bulut yolculuğunun belirli kilometre taşları olacaktır. Bulutu kullanacak herhangi bir kuruluş, kilometre taşlarının aşamalarından birini geçmek zorunda kalacak. Bu kilometre taşları normalde ilericidir, biri diğerine yol açar ve nihai durum barındırılan bir bulut çözümüdür. Bu kilometre taşları kuruluşların bulut programlarını nasıl tanımlayacağına kesinlikle bağlı olacaktır.

6.2.1 ORGANİZASYONEL ŞARTLAR

a. RFP ve ihale süreci: Kuruluşun büyüklüğüne bağlı olarak, büyük bir kuruluş genellikle, hedeflerini ve gereksinimlerini ifade etmek ve uygulama ve bulut konusunda danışmanlık sağlayacak kuruluşları belirlemek için bir RFP sürecinden geçecektir. RFP süreci hem dış ortaklar hem de kuruluş için bir öğrenme fırsatı olacak ve bulut kullanma programından servis seviyesi tanımları ve genel beklentileri tanımlamaya yardımcı olacaktır.

6.2.2 TEKNOLOJİK ŞARTLAR

a. Kavramın ispatı (POC): kavramın ispatı, benimsenecek ve dağıtılacak bulut servislerinin, çeşitli bulut katmanları arasında entegrasyonun gerçekleştirilmesine yardımcı olacak ve teknolojilerin seçimi için girdi sağlayacaktır. Bulutta kullanılan araçların çoğu açık kaynak olduğu ve BT organizasyonu aracı ilk kez kullanıyor olabileceğinden, kavramın ispatı herhangi bir kuruluş için dikkate alınması gereken önemli bir husustur.

b. Tedarikçi seçimi: Herhangi bir kuruluş için RFP ve PoC aşamasından gelen girdiler bulut uygulaması için ortakların belirlenmesine yardımcı olacaktır. Bu iş ortakları bulut danışmanlığı, uygulama rasyonelleştirme servisleri, altyapı bakımı, bulut araçları ve teknolojileri ve değişiklik yönetimi sağlayabilir. Bu aşamada kuruluşlar, bulut teknolojileri seçeneklerini ve hangi iş ortağının stratejisini uygulayacağını belirlemelidir.

c. Bulut servis modeli: Sürecin bu aşamasında kuruluşlara çeşitli bulut servis modelleri sunulacaktır. Olgunluğa bağlı olarak, yönetişim ve kontrol ihtiyacı olan bir kuruluş, doğrudan IaaS, PaaS & SaaS ve yerleşik bulut modellerinden herhangi bir bulut servisi modelini seçebilir..

   i. Daha büyük veya daha olgun bir kurum, IaaS'yi, kendi yazılım standartlarını ve

her talepteki ölçekli servislerini, gelecekteki gereksinimlere göre kontrol etmek, ayarlamak ve dağıtmak için bir servis olarak seçebilir

ii. Başka bir kuruluş için DaaS, politikaların merkezi uygulamasını sunan ve aynı zamanda bireysel değişimi odaklayan uygun bir model olabilir. Kendi Cihazınızı Getirin (BYOD) eğilimi ile bir çalışan veya kullanıcı kendi cihazını getirebilir ve veri gizliliği ve güvenliğine tam uyumla çalışabilir. Uzaktan çalışan veya seyahat eden çalışanlar için DaaS, paralel bir masaüstü ortamı olarak iyi bir çözüm olabilir

iii. Benzer şekilde, kendi servis / uygulama setini oluşturmak isteyen herhangi bir kuruluş, geliştirme platformlarının kullanılabilirliğine sahip geliştirme ve test ortamları için PaaS'ı seçebilir.

d. Entegre bulut platformu: Kuruluşların kendilerini, tüm altyapı, platform ve yazılım servislerinin kullandığın kadar öde temelinde ölçüleceği, faturalandırılacağı ve ücretlendirileceği bir duruma başarıyla dönüştürüleceği aşamadır.

6.2.3 ÇEVRESEL ŞARTLAR

a. Rekabetçi teklifler: Güvenlik ve yasal konular, her kuruluşun veri yetki alanını, veri gizliliğini ve güvenlik riskini sıralamak için bulut sağlayıcısı ile çalışması gereken başlıca çevresel faktörlerdir. Bu sayede kuruluşlar çalışanlarına, vatandaşlarına ve iş evlerine daha iyi servis sunabilecekler. Kuruluşlar, düzenleme ile veya düzenleme olmadan SaaS tekliflerini kullanabilir ve daha fazla çalışanının işe odaklanmasını sağlar.

6.3 DOĞRU BULUT MODELİNİ TANIMLAMA

Her kuruluş farklı bir altyapı ve değişken iş yükleri ile farklı olacaktır. Talepler de değişecek, bu nedenle kuruluşların yapacağı altyapı seçimleri yeni yetenekler sunulmasını etkileyecektir.

a. Kuruluşlar iş yüklerini bilmeli

b. Kuruluşlar iş birliği yapmalı

c. Yukarıdan aşağıya altyapıyı analiz edin

d. Süreç gereksinimlerini göz önünde bulundurun

e. Doğru bulut çözümünü bulun ve kullanın.

Aşağıda, genel buluta geçmeye uygun olabilecek uygulama kategorileri belirtilmiştir:

a. Geliştirme/test uygulamaları: Büyük bulut sağlayıcılarındaki (Amazon Web Services gibi) bilgi işlem çalışmalarının en büyük yüzdesi, geliştirme/test iş yükleridir. yapım ve test süreci, bilgi işlem açısından yoğundur ve bu nedenle genel bulut bilişim için uygundur.

Kuruluşlar için, uygulamaları test etme ve geliştirme eğer varsa kukla veriler kullanılarak yapılırsa riski daha az olacaktır.

b. Kişisel üretkenlik uygulamaları: Kelime işlem, elektronik tablo ve sunum tasarımı, e-posta yazılımı uygulamaları iyi bir uyum sağlama eğilimindedir. Bu uygulamalar yapılandırılmamış verilere dayanır ve genellikle düşük gecikme süresi gerektirmez.

Kuruluşlar için, veriler ve kopyaları, yüksek düzeyde veri güvenliği olan Umman'ın yargı bölgelerinde saklanıyorsa, kuruluşlar bu tür uygulamalar için genel bulut tercih edebilirler.

c. Ortak uygulamalar: Sosyal ağ, web konferansı ve diğer ortak uygulamalar, özellikle bu çözümlerin birçoğu bulut için başta yazıldığından bulut için iyidir. Kuruluşlar için bu tür platformlar Umman'daki vatandaşlara ve işletmelere ulaşmanın ve iletişim kurmanın bir yolu olarak servis edecektir. SharePoint gibi eski uygulamalar genel bulutta da çalıştırılabilir.

d. Yüksek performanslı bilgi işlem (HPC- High-performance computing) uygulamaları: Kuruluşlar çok yüksek miktarda kaynak tüketen uygulamalara sahipse (CPU, RAM, Disk Alanı, vb.), bu tür uygulamalar genellikle veri ihtiyaçları yönetilebildiği sürece genel bulut bilişim için uygundur.

Özel buluta geçiş için uygun uygulamalar:

a. Görev açısından kritik uygulamalar: ERP gibi görev açısından kritik uygulamalar, işlem yoğunluğu yüksek, yüksek iş hacmi (throughput) ve düşük gecikme süresi gereksinimlerine sahiptir. ERP çalıştıran kuruluşlar için hassas veriler ve genellikle büyük veri kümeleri içerecek ve yüksek kullanılabilirlik gereksinimlerine sahip olacaklardır. Bu tür bazı uygulamaların genel bulutta yerine getirilmesi zor olabilecek yasal uyumluluk gereksinimleri de olabilir.

b. Ağ yoğun uygulamalar: Bu tür uygulamalar, sürekli olarak büyük miktarlarda veri ileten ve alan; hızlı, yüksek kaliteli ağ kaynakları gerektirir. Bu uygulamalar genellikle veri paylaşmak için diğer uygulamalara erişim veya bu uygulamalarla entegrasyon gerektirebilir.

Hangi uygulamaların buluta mimari ve stratejik olarak daha uygun olduğunu anlamak için teknik bir değerlendirme gerekecektir. Kuruluşlar önce hangi uygulamaların buluta taşınacağını, hangi uygulamaların daha sonra taşınacağını ve herhangi bir uygulamanın şirket içinde kalması gerekip gerekmediğini belirlemelidir.

Teknik değerlendirme aşamasında kuruluşlar aşağıdakilere bir çözüm bulmalıdır:

a. Hangi iş uygulamaları önce buluta geçecek?

b. Bulut, gerekli tüm altyapı yapı taşlarını sağlamalıdır

c. Kuruluşlar, varsa mevcut kaynak yönetimi ve yapılandırma araçlarını yeniden kullanabilir mi?

d. Kuruluşlar donanım, yazılım ve ağ destek sözleşmelerinden kurtulabilir mi?

Aşağıdaki sunu, kuruluşların bulut için en uygun adayları seçmek ve tanımlamak için kullanabileceği genel bulut seçim parametrelerini göstermektedir.

Parametreler	Genel Bulut	Özel Bulut	Karma Bulut
Ayırma (Soyutlama) Düzeyi	Yüksek	Düşük	Orta
Kiracılık	Tek kiracılı (özel) veya çok kiracılı (paylaşılan) işletim ortamı	Tek kiracılı (özel) çalışma ortamı	Geçişli bilgi alışverişine izin veren genel ve özel bulut tekliflerinin bir kombinasyonu
Güvenlik Seviyesi	Düşük. Sağlayıcı tesisindeki verilere erişim yok	Yüksek. Verilere tam erişim mevcuttur	Yüksek. Verilere tam erişim mevcuttur
Satıcı Kilitleme	Kullanılan teknolojiye bağlıdır	Yüksek. Kullanılan teknolojiye bağlıdır	Kullanılan teknolojiye bağlıdır
CapEx	Düşük. Altyapının çoğu sağlayıcı tarafından sağlandığından	Yüksek. Kurum içi altyapı devreye alınmaya hazır olmalıdır	Yüksek. Genel ve özel bulutun birleşimidir
OpEx	Yüksek. Kullanım başına sürekli ödeme	Orta. Sadece bir kerelik kurulum ücreti yüksektir	Orta
Tarafından yönetilen	Üçüncü parti	Kuruluşlar veya üçüncü taraf	Hem kuruluşlar veya hem de üçüncü taraf
Sanallaştırma Düzeyi	Kullanılan teknolojiye bağlıdır	Sanallaştırma üzerinde zeka sağlar	Sanallaştırma düzeyi özel buluttaki düzeyden düşük
SLA Garantisi	Elde etmesi zor	Elde edilmesi ve izlenmesi daha kolay	Elde edilmesi ve izlenmesi daha kolay
Kim için uygun	SMB (Small&Medium Business)	Kurumsal	Her ikiside
Veri Gizliliği	Düşük	Yüksek	Orta
Yasal ve uyum sorunlar	Verilerin yabancı lokasyonlarda depolanması gerekebileceğinden yüksek	Veriler kendi veri merkezimizde bulunduğundan düşük	Veriler kendi veri merkezimizde bulunduğundan düşük
Uygun uygulama türleri	Daha az entegrasyon seviyesine sahip daha az görev kritik uygulaması	Çok gizli verilerle ilgili uygulama	Çok gizli verilerle ilgili uygulama
Altyapı Sahipliği	Üçüncü parti	Kuruluşlar veya üçüncü taraf	Hem kuruluşlar veya hem de üçüncü taraf

Sunu-9 - Bulut Geliştirme Modeli Seçim Parametreleri

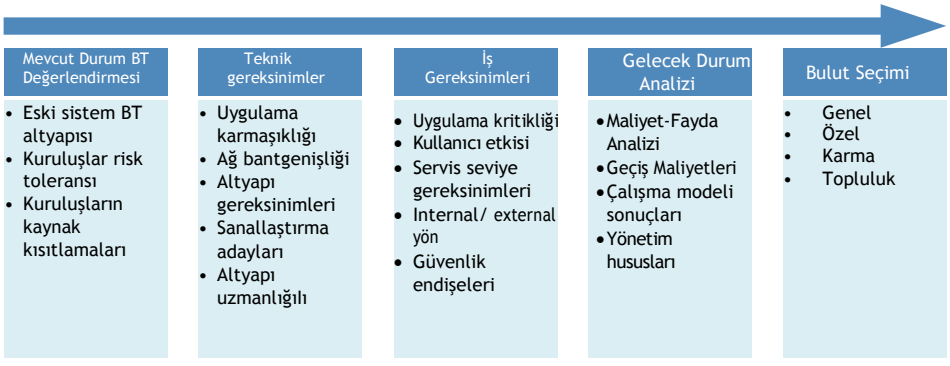
6.4 BULUT'A HAZIRLIK DEĞERLENDİRMESİ

Değerlendirme aşaması, mevcut durumun, gereksinimlerin tanımının yapılmasını ve bulutun benimsenmesi için bir vizyonun geliştirilmesini içerecektir. Mevcut durum değerlendirmesi, git/gitme raporu sunacaktır ve olup aşağıdakilere dayanmalıdır

Mevcut durum değerlendirmesi	Gereksinim tanımı	Vizyon tanımı
a. Eski sistemleri - teknik ve operasyonel ortamı anlama b. Ürün teklifinin uygunluğunu değerlendirin c. Kuruluşların veri uyumluluğu ve güvenlik ihtiyaçlarını değerlendirin d. Kuruluşların BT altyapısını süreklilik ve uygulama bağımlılıkları açısından değerlendirin e. Kuruluşların risk toleransı ve kaynak kısıtlamalarını değerlendirin	a. Kilit paydaşlarla görüşme b. Gereksinim tanımlamaları çalıştayı yürütmek c. Gereksinimler belgesini doğrulama d. Yeni bulut çözümü için uyumluluk ve güvenlik ihtiyaçlarını tanımlayın	a. Kuruluşların hedeflerini tanımlayın b. Kısa vadeli ve uzun vadeli vizyonu tanımlar c. Yeni bulut çözümüne geçiş düzeyini tanımlayın

Sunu-10 – Bulut'a Hazırlık Değerlendirmesi

Kuruluşlar için mevcut durum değerlendirmesinin çıktısı, mevcut durum belgeleri, gereksinimler belgesi ve bir kapsam ve vizyon beyanı olacaktır.



Sunu-11 – Değerlendirme Yaklaşımı

a. Kuruluşlar, bir sonraki aşamaya geçmeden önce her adımda değerlendirme kriterlerini karşılamalıdır. Her kriter için bir puan verilmelidir (kırmızı / sarı / yeşil).

b. Herbir alanda bile, temel değerlendirme kriterlerini karşılamada yetersizlik; uygunluğun artık geçerli olmadığı ve uygulamanın şu anda bulut için uygun olmadığı anlamına gelecektir.

c. Kuruluş başvuruları aşağıdaki nitelikleri sergilemeli ve buna göre değerlendirilmelidir.

   i. Düşük veya orta düzeyde uygulama kritikliği

   ii. Diğer uygulamalardaki / verilerdeki bazı bağımlılıklar minimumlaştırma

   iii. Sıradan-grup donanım kullanımı

   iv. Bant genişliği gereksinimleri

   v. Bağımsız ortamlar veya yazılım yığını

   vi. Özelleştirilmiş cihazlara bağlı değildir

   vii. Düşük / orta SLA gereksinimleri

   viii. Hiçbir gizli veri veya veri kolayca maskelenemez.

Faz	Kriter	Açıklama
Mevcut Durum Değerlendirmesi	Eski sistem kritikliği	Üretim kuruluşları için çevre tarafından tanımlanır
	Eski sistem karmaşıklığı	Mimari karmaşıklığı, diğer uygulamalara bağımlılıklar, veritabanları, ara katman yazılımı
	Sanallaştırma adayı	İş yükü sanallaştırılabilir mi? Bu platform işletim sistemine ve sanallaştırma platformuna bağlıdır
	Sıradan-grup altyapı	İş yükü altyapısı sıradan-grup altyapısında çalışır
Bulut için Uygunluğu Belirleme	Teknik Fizibilite	
	Ağ bantgenişliği	İş yükünün bulutta çalışacağı LAN veya WAN ağ bant genişliği gereksinimleri
	Altyapı gereksinimleri	İş yükünü desteklemek için bilgi işlem, depolama ve ağ gereksinimlerinin ölçeği
	Paylaşılan ortamlar	Paylaşılan bir ortam tarafından desteklenecek türler
	Paylaşılan yazılım	Yazılım (ör. Veritabanları, ara katman yazılımı) diğer yazılımlarla paylaşma

Faz	Kriter	Açıklama
Bulut için Uygunluğu Belirleme	Özel altyapı	Özel amaçlı tescilli cihazlara, cihazlara, lisansa, donanıma vb. bağımlılık
	Ticari Fizibilite	
	Internal / External yön	Sistem müşteriye yönelik bir servis veya arka ofis işlevi (ör. HR-İnsan kaynakları) sağlıyor mu?
	Kullanıcı etkisi	İş yükünün buluta taşınması nedeniyle kullanıcı topluluğu üzerindeki etki (ör. Bir kullanıcı alt kümesine erişim eksikliği)
	Servis seviye gereksinimleri	Kullanılabilirlik, yanıt süresi, Kurtarılabilirlik, Felaket Durum vb.
	Müşteri / Gizli Veriler	Sağlayıcının konumu veya bulut servisinin diğer özellikleri, verilerin nasıl ve nerede depolanması gerektiğinin güvenlik gereksinimlerini karşılıyor mu?
İş Gerekçesi ve Operasyonel Analiz	İş Gerekçesi Analizi	Başlangıç ve taşıma maliyetleri, devam eden maliyetler ve ROI zaman dilimi dahil maliyet / fayda analizi
	Detaylı teknik analiz	Uygulama için ne gibi değişiklikler gerekli olacak? Gelecekteki uygulama mimarisi nasıl görünecek?
	Operasyonel Analiz	Buluta taşınan iş yükü nedeniyle operasyonel etki nedir? İş yükü buluta taşındıktan sonra destek modeli nedir? Servis sağlayıcıya karşı müşteri sorumluluğu ve elden çıkarma nedir?
	Yönetim hususları	İş yükü bulutta nasıl yönetilir? Ör. Şirket içi ve satıcı tarafından sağlanan araçlar, süreçler ve personel kullanılarak; Değerlendirme Puan Kartına Dayalı Git/Gitme.

Sunu-12 – Değerlendirme Kriterleri

Değerlendirme ve yukarıdaki hususları göz önünde bulundurarak, kurumlar bulutun kullanılıp kullanılmayacağına karar verebilirler.

	Kırmızı	Sarı	Yeşil	Git / Gitme Kararı
Mevcut Durum Değerlendirmesi				
Teknik Fizibilite				
Ticari Fizibilite				
Git / Gitme Kararı				

Sunu-13 – Karar Matrisi

a. "Kırmızı" derecelendirmelerin sayısı en fazla 1 ise, kuruluş bulut çözümüne "Git" e karar verebilir, aksi takdirde bu bir "Gitme" olabilir.

b. "Sarı" derecelendirmelerin sayısı en fazla 2 ise, kuruluş bulut çözümüne "Git" e karar verebilir, aksi takdirde bu bir "Gitme" olabilir.

c. Kuruluşun bulut çözümüne "Git" karar vermesi için "Yeşil" derecelendirme sayısı en fazla 2 olmalıdır, aksi takdirde bu bir "Gitme" olabilir.

Ek bölümünde, kurumların bilmesi gereken çeşitli risk alanları ve bulut için bir risk değerlendirme anketi hakkında bilgi verilmektedir.

Aşağıdaki bölüm, kuruluşların bulutu kullanması için dikkate almaları gereken ayrıntılı bir yol haritası sunmaktadır.

6.5 BULUT'UN KULLANIMI İÇİN YOL HARİTASI

Kuruluşların bulutu kullanmaları için aşağıdaki sayfadaki sunuda belirtilen beş aşama ve yirmi bir aşamadan geçmeleri gerekecek.

a. İlk aşama, kuruluşların bulut servislerini iş perspektifinden anlaması ve bulutu kullanmanın mevcut BT üzerindeki etkisini içerir

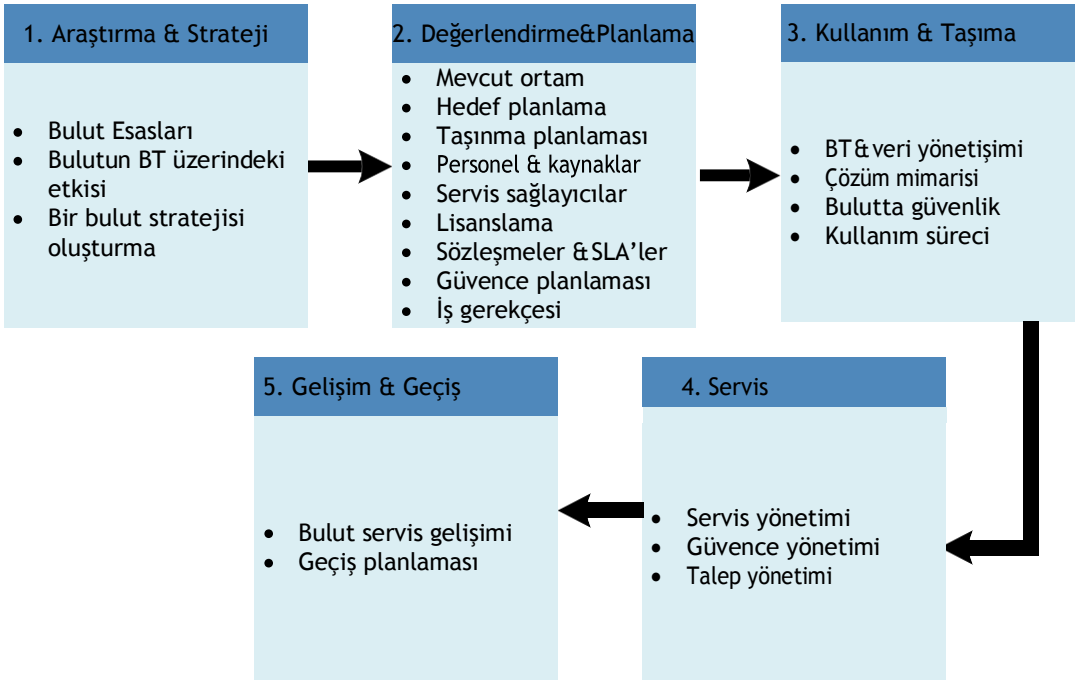
b. Kuruluşlar için ikinci aşama, mevcut BT ortamının iş süreçlerini anlanması, mevcut uygulama ortamı ve taşıma senaryolarının değerlendirmesi, gerekli personel ve kaynaklar, servis sağlayıcıların desteği ve benzeri bir iş vakası oluşturmak için hedefe yönelik planlamaların değerlendirmesi olacak,

c. Kabullenme ve taşıma aşaması, BT ve veri yönetişim mimarilerini, çözüm mimarileriyle politikaları tanımlamayı ve buluttaki güvenliği tanımlamayı ve anlamayı içerecektir

d. Bir sonraki aşama, kuruluşların garanti edilen SLA'larını yönetmek için sağlayıcı ile birlikte çalışılması gereken servis yönetimidir. Herhangi bir zamanda kuruluşların ek kaynaklar için bir gereksinimi olabilir ve bulut isteğe bağlı kaynakların kullanılabilirliğine odaklanır. Servis sunumundaki herhangi bir uzlaşma veya

başarısızlık için sağlayıcı, kuruluşu hatanın niteliği ve etkisi hakkında bilgilendirmesi ve güncellemesi için mekanizmalar belirlemelidir.

e. Bir servis olarak bulut yıllar içinde gelişti. Kuruluşlar, sağlayıcı bulutunun kuruluş için uygunluk gereksinimlerine göre süreçler ve teknolojilerin nasıl geliştiğini ve gelişeceğini anlamak için sağlayıcıyla birlikte çalışmalıdır. Bu açıkça belgelendikten sonra kuruluşlar ve sağlayıcılar servislerin taşınması için çalışmalıdır.



Sunu-14 - Bulut Kullanımı için Yol Haritası

6.6 BULUT İÇİN SLA'LER

Bulut Servis Seviyesi Anlaşmaları (SLA'lar), bulutu kullanmak için farklı sağlayıcılar üzerinde düşünürken, BT ve işletme paydaşlarının bulut servis sözleşmelerini analiz etmelerine yardımcı olacaktır. Servis Seviyesi Sözleşmeleri, kuruluşların bulut sağlayıcısından, kuruluşlarla sağlayıcı arasında net servis beklentilerini belirlemelerine yardımcı olacaktır. Bulutta SLA'er için on önemli adım aşağıda belirtilmiştir.

a. Kuruluşların (tüketiciler), sağlayıcıların ve taşıyıcılar vb. gibi ilgili diğer tarafların rolleri ve sorumlulukları SLA'larda açık bir şekilde belirlenmeli ve açıklanmalıdır.

b. SLA servisleri oluşturulurken kuruluşların strateji ve politikaları göz önünde bulundurulmalıdır, çünkü bulut servisleri ile işletmenin durumu arasında bağımlılıklar vardır.

c. Bulut kaynaklarının ve servislerinin seviyeleri, bulut servis modeline (IaaS, PaaS ve SaaS) göre anlaşılmalıdır. Her servis modelinin, kuruluşlar tarafından açıkça anlaşılması gereken kendi SLA hususları olacaktır.

d. Bulut bilişimin performans hedefi genellikle kullanılabilirlik, işlem oranı, yanıt süresi ve işlem hızını içerir. Bulut servisleriyle ilgili konfor düzeylerini sağlamak için hedefler denetlenebilir ve ölçülebilir olmalıdır

e. Geleneksel BT ile karşılaştırıldığında veri güvenliği ve gizlilik açısından riskler daha yüksek olarak kabul edilir ve bu nedenle sağlayıcı ve kuruluşlar tarafından dikkatli bir şekilde yönetilmelidir. Servis Seviyesi Sözleşmeleri, tanımlanmış güvenlik seviyeleri, koruma kontrolleri, veri saklama ve imha politikaları ile verilerin ayrıntılarına ve veri sahipliğine ilişkin önemine ve hassasiyetine dayalı bir güvenlik sınıflandırma şeması tanımlamalıdır.

f. Bulut servislerini izlemek için şeffaf ve genişletilebilir sistemler, beklenen performansları karşılamak için kritik öneme sahiptir. Kuruluşlar, raporlama, ölçme, hızlı tedarik, yükseltme ve denetim prosedürlerini ve politikalarını sağlayıcı ile doğrulamak zorundadır.

g. Kuruluşlar, bir servis arızasının giderilmesi / önlenmesi için servis yeteneklerinin ve performans beklentilerinin net bir şekilde belgelenmesini talep etmelidir. Hem servis sağlayıcı hem de kuruluşlar, beklenen servis teslimatlarının gerçekleşmeyeceği ihtimaline karşı önleyici ve düzeltici faaliyetler hazırlamalıdır

h. Sağlayıcı, kuruluşlara BT bileşenleri için teknoloji süreçlerine odaklanan bir BCP sunmalıdır. DR planının ayrıntı düzeyi, iş hedefleri ve kuruluşlar için bulut servislerinin önemine göre düzenlenmelidir.

i. Kuruluşlar ve sağlayıcılar, tanımlanan sorunların doğru bir şekilde ele alınmasını sağlamak için rutin toplantılar, koordinasyon ve üste devir mekanizmaları yoluyla yapılacak etkili bir yönetim planı üzerinde karar vermelidir

j. Kuruluşların beklentisi sağlanamazsa veya herhangi bir faktör nedeniyle servise devam edilemezse, hem kuruluşlar hem de sağlayıcı ayrılış prosedürlerinin tanımlaması gereken ayrılış SLA'lerıne başvurmalıdır.

6.7 BULUT İÇİN MALİYET FAKTÖRLERİ

Bulut, bilgi işlem servisini yararımıza sunar. Bulut, kuruluşların pahalı BT altyapılarının bazılarından kurtulmasına ve bilgi işlem maliyetlerini daha yönetilebilir işletim giderlerine kaydırmasına izin verecektir. Kuruluşlar ayrıca BT sistemleri desteği ve bakımıyla ilgili teknolojik sorumluluktan kurtulacaktır. Ancak Cloud, kuruluşların akılda tutması gereken bazı ön yatırım ve tekrarlayan maliyetlere sahiptir ve aşağıda belirtilmiştir.

a. Bulutu kurmak için gereken ilk yatırımdan oluşacak ön maliyetler.

   i. Ağ kurulumunu gerçekleştirmek veya buluta bağlantı için gerekli belirli bileşenleri yükseltmek için teknik hazırlık maliyetleri.

   ii. Uygulama ve entegrasyon: buluta geçişi yönetmek ve şirket içi veya diğer bulut servisleriyle (hibrit bulut) entegre etmek için gereken profesyonel servisler.

iii. Yapılandırma / özelleştirme: herhangi bir kuruluş tabanlı SaaS uygulamasını yapılandırma maliyetleri

iv. Eğitim: bulut sağlayıcılarını ve servislerini yönetmek için gerekli kaynaklar

v. Organizasyonel değişiklik: iç denetim, değişiklik yönetimi, izleme vb. gibi buluta özgü ihtiyaçları karşılamak için gerekli süreçler.

b. Rutin ücretler ve bulut servislerinin kullanımını sürdürme ile ilgili yinelenen maliyetler.

i. Abonelik ücretleri: bulut servislerinin aboneliği için periyodik ücret konusunda anlaşma (kullandıkça öde)

ii. Değişiklik yönetimi: sistem değişikliği istenirken oluşan maliyetler

iii. Tedarikçi yönetimi: bulut servisi sağlayıcısı etkinlikleri, SLA ve diğer değerlendirmelerde rutin izleme ile ilgili maliyetler

iv. Bulut koordinasyonu: Bulutlar arasındaki koordinasyonu yönetme maliyetleri (birden fazla bulut sağlayıcısı olması durumunda)

v. Son kullanıcı desteği ve yönetimi: kuruluşlarda tutulan maliyetler

vi. Risk azaltma: riskleri kabul edilebilir seviyelere indirmek için gerekli efor

vii. Küçültme / büyütme: bilgi işlem kaynaklarının yükseltilmesi veya küçültülmesi ile ilgili maliyetler (esneklik).

7 BAĞLANTILAR VE BAĞLILIKLAR

Bulutun kullanılmasına ilişkin çerçeve, aşağıdaki politikalara ve çerçevelere bağımlı olacaktır.

a. Umman devlet kurumları için Web Sitesi ve Hosting Politikası.

b. Umman kurumları için en değerli varlıklardan biri olan veri ve bilgilerin korunması için bilgi güvenliği politikaları. Bilgi güvenliği yönetim kılavuzları, verilerin yetkisiz erişim ve değişikliklerden korunmasına yardımcı olacak ve bilgilerin doğru zamanda doğru kişilere ulaşmasını sağlayacaktır.

c. OeGAF - BT'nin Umman'ın tüm kurumları arasında entegrasyonunu ve birlikte çalışabilirliğini yönetmek için teknik standartların ve en iyi uygulamaların benimsenmesine yönelik rehberlik sağlayan Teknik Referans Modeli (TRM).

8 EK - A - BULUT HOSTİNG / BİLİŞİM GEREKSİNİMLERİ

(Sözleşme yükümlülükleri)

Devlet kurumları, üçüncü taraf Bulut Servis Sağlayıcısı (CSP) ile yapılan sözleşmelerde aşağıdaki gereksinimleri sağlamalıdır.

1. Güvenlik Gereksinimleri - Devlet kurumlarına bulut servisleri sunan CSP, aşağıdakiler dahil ancak bunlarla sınırlı olmamak üzere güvenlik standartlarına uyumu sağlamak için uygun kontrol setini uygulayacaktır:
   - ISO/IEC 27001,
   - ISO/IEC 27017,
   - ISO/IEC 27018,
   - Bulut Güvenliği Birliği (CSA-Cloud Security Alliance) – Kontrol Matrisi.
   - PCI-DSS Uyumu - Online Ödeme Çözümlerini barındırmak için.
2. Gizlilik Gereksinimleri - CSP, aşağıdaki gizlilik ve güvenlik önlemlerinden sorumlu olacaktır:
   a. CSP tarafından toplanan ve depolanan kamuya açık olmayan Hükümet verilerinin güvenliği, bütünlüğü ve gizliliğine yönelik tehdit ve tehlikelere karşı korunmak için, CSP; hükümetin tesislerine, kurulumlarına, teknik yeteneklerine, operasyonlarına, belgelerine, kayıtlarına ve veritabanlarına gerekli olduğu ölçüde erişimini sağlar.
   b. Hükümet ya da CSP tarafından yeni ya da beklenmeyen tehditler ya da tehlikeler tespit edilirse ya da mevcut önlemler işlevlerini yerine getirmezse, keşfeden taraf durumu derhal diğer tarafın dikkatine sunacaktır.
   c. CSP, hükümetin gerektirdiği ek gizlilik şartlarına da uymalıdır.
3. Hükümet, Devlete servis sağlamak veya kolaylaştırmak için kullanılan CSP'lerin BT ortamının manuel veya otomatik denetimlerini, taramalarını, incelemelerini veya diğer denetimlerini yapma hakkına sahiptir:
   a. CSP, Sözleşme Makamının yazılı izni olmadan, bu sözleşme kapsamında CSP tarafından tasarlanan veya geliştirilen veya Hükümet tarafından başka şekilde sağlanan herhangi bir önlemin ayrıntılarını hiçbir şekilde yayınlamayacak veya ifşa etmeyecektir. İstisna?
   b. Devlet verilerinin güvenliği, bütünlüğü ve gizliliğine yönelik tehdit ve tehlikelere karşı koruma sağlamak için bir denetim programı yürütülmesi gerektiğinde, CSP hükümetin CSP'nin tesislerine, kurulumlarına, teknik yeteneklerine, operasyonlarına, belgelerine, kayıtlarına ve veritabanlarına 72 saat içinde erişmesini sağlayacaktır. Denetim programı aşağıdakileri içermekle birlikte bunlarla sınırlı değildir:
      i. Kimliği doğrulanmış ve kimliği doğrulanmamış işletim sistemi / ağ güvenlik açığı taramaları
      ii. Kimliği doğrulanmış ve kimliği doğrulanmamış web uygulaması güvenlik açığı

taramaları

iii. Kimliği doğrulanmış ve kimliği doğrulanmamış veritabanı uygulaması güvenlik açığı taramaları

iv. Otomatik taramalar, Devlet personeli veya Devlet adına hareket eden aracılar, Devlet tarafından işletilen ekipmanları hükümet tarafından belirtilen araçlar kullanarak gerçekleştirilebilir.

CSP kendi otomatik taramalarını veya denetimlerini çalıştırmayı seçerse, bu taramalardan elde edilen sonuçlar, hükümetin takdirine bağlı olarak, hükümetin gerçekleştirdiği güvenlik açığı taramaları yerine kabul edilebilir. Bu durumlarda tarama araçları ve bunların yapılandırılması hükümet tarafından onaylanacaktır.

4. Hassas Bilgilerin Saklanması ve İşlenmesi

a. Devlet verileri ve / veya bilgileri yalnızca Umman Sultanlığı'nın coğrafi sınırları içinde barındırılmalı / işlem görmeli / işlenmelidir. Bu, birincil depolama alanının yanı sıra yedekleme veya felaket kurtarma düzenlemelerini içerir.

b. Hassas bilgi, veri ve / veya ekipman sadece Need to Know esasına göre yetkili personele açıklanacaktır. CSP, bu bilgilerin, verilerin ve / veya ekipmanın güvenliğinin ve gizliliğinin düzgün bir şekilde korunmasını sağlamak için uygun idari, teknik ve fiziksel korumaların oluşturulmasını sağlayacaktır. Artık gerekli olmadığında, bu bilgi, veri ve / veya ekipman devlet kontrolüne geri döndürülecek, imha edilecek veya aksi belirtilmedikçe tutulacaktır. Bu kalemlerin imhası, üzerinde mutabık kalınan Medya Temizlik yöntemleri izlenerek gerçekleştirilecektir.

c. CSP, kuruluşun yeni bir CSP'ye geçiş yapması veya alternatif olarak servisleri şirkete geri getirmesi durumunda servislerin serbest bırakılması ve geçişine ilişkin plan geliştirecek ve sürdürecektir.

d. Devreden çıkarılma durumunda, kuruluş tarafından onaylanan formatlarda tüm verilerin (birincil depolama ile yedekleme veya olağanüstü durum kurtarma düzenlemeleri dahil) alınması / iadesi için anlaşma.

5. Bilgilerin Korunması

a. CSP, bu sözleşme kapsamında yapılan çalışmalar sonucunda kullanılan, toplanan veya geliştirilen tüm bilgilerin uygun şekilde korunmasından sorumludur. CSP ayrıca, tüm hassas bilgileri, bilgileri vb. Ele alarak tüm Hükümet verilerini, ekipmanlarını vb. koruyacaktır. Bu bilgilerin birincil iş lokasyonunda toplanması, oluşturulması ve saklanması beklenmektedir. CSP personelinin herhangi bir bilgiyi birincil çalışma alanından kaldırması gerekiyorsa, bu bilgileri kendi mülkiyet verilerini ve / veya şirket ticari sırlarını koruyacak şekilde korumalıdır.

b. Hükümet, hükümet verilerinin sınırsız haklarını elinde tutacaktır. Sipariş etkinliği, kullanıcı tarafından oluşturulan/yüklenen verilerin ve satıcının altyapısında barındırılan uygulamaların sahipliğini korur ve bunların her zaman tam kopyalarını isteme hakkını korur.

c. Ağ altyapısındaki çeşitli uygulamalar tarafından işlenen ve depolanan veriler, finansal verileri ve kişisel olarak tanımlanabilir bilgileri (PII-Personally Identifiable Information) içerir. Bu veriler ve PII, yetkisiz erişim, açıklama veya değiştirme, hırsızlık veya imhaya karşı korunmalıdır. CSP, ağ altyapısını barındıran tesislerin fiziksel olarak güvenli olmasını sağlayacaktır.

d. Veriler, talep edilmesi halinde bir iş günü içinde veya başka bir şekilde belirtilen süre içinde Hükümete açık olmalıdır ve burada belirtilenler dışında başka bir amaçla kullanılmamalıdır. CSP, talep edilen verileri hükümete hiçbir ek ücret ödemeden sunacaktır.

e. Hükümetin yazılı izni olmadan CSP tarafından hiçbir veri açıklanamaz. Tüm sürüm talepleri kuruluş temsilcisine yazılı olarak bildirilmelidir.

6. Gizlilik ve Açıklamama

a. CSP tarafından bu sözleşmenin yerine getirilmesinde oluşturulan kuruluş tarafından ilgili görülen başlangıç ve nihai çıktılar ile ilgili tüm çalışma kağıtları ve diğer materyaller, Umman Hükümeti'nin malıdır ve sözleşmenin imzalanmasının ardından sözleşme veren kuruluşa sunulmalıdır.

b. Umman Hükümeti, tüm çıktılar ve ilgili çalışma kağıtları ve materyalleri için sınırsız veri haklarına sahiptir.

c. Bu proje için üretilen tüm belgeler Umman Hükümeti'ne aittir ve CSP tarafından çoğaltılamaz veya saklanamaz. Bu sözleşme sırasında ve sonunda tüm uygun proje belgeleri kuruluşa verilecektir.

d. CSP, Sözleşme Makamının yazılı onayı olmadan hiçbir bilgi vermeyecektir.

e. Açıklanan görevlerden herhangi biri üzerinde çalışan herbir personelin, Hükümet talebi üzerine, Hükümet bilgi ve belgelerinin korunmasını ve bütünlüğünü garanti altına almak için resmi gizlilik ve / veya çıkar çatışması anlaşmaları imzalaması gerekebilir.

f. Ayrıca, Hükümet tarafından CSP'ye sunulan tüm bilgiler yalnızca bu sözleşmenin hükümlerini yerine getirmek amacıyla kullanılacaktır ve ve sözleşmenin yerine getirilmesi için gerekli olabilecek durumlar dışında hiçbir kimseye açıklanamaz veya tanıtılamaz. Bu sözleşmenin yerine getirilmesinde, CSP, Devlet kayıtlarının gizliliğinin korunması sorumluluğunu üstlenir ve alt yüklenicisi tarafından gerçekleştirilen tüm çalışmaların CSP veya CSP'nin sorumlu çalışanlarının gözetiminde olmasını sağlayacaktır. Herhangi bir Devlet kaydının sunulacağı veya açıklanacağı durumda CSP yetkilisi veya herhangi bir alt yüklenicisi CSP tarafından sözkonusu memura veya çalışanlara ifşa edilen bilgilerin sadece bu amaç için ve burada izin verilen ölçüde kullanılabileceği yazılı olarak bildirilecektir. Bu tür bilgilerin herhangi bir yolla, bir amaç için veya bir ölçüde yetkisiz olarak açıklanması, suçluyu [burada geçerli / ilgili yasa maddelerinden bahsedin] tarafından uygulanan cezai yaptırımlara tabi tutabilir.

9 EK – B - RİSK DEĞERLENDİRMESİ

Yeni bir iş çözümü geliştirmek ve yayımlamak için bir program göz önüne alındığında, bununla ilişkili riskler vardır, bu da çözümün hedeflerine ulaşma yeteneğini etkileyecektir.

Bulut bilişim kabullenme risklerini değerlendirmek, birbiriyle ilişkili bir dizi karmaşık faktörün dikkate alınmasını içerir. Bulut kullanma risklerinin değerlendirilmesi, sağlayıcılarla görüşmeler, anket toplama belgeleri ve incelemeleri, sağlayıcılarla grup tartışmaları içerecektir.

Bulutun kullanılmasına ilişkin zorluklar, verilerin konumu, bulut servislerinden, sağlayıcıdan çıkılması, bulut servislerine katılan tarafların sayısı ve kuruluşların gözetimi gibi şeylere dayanmaktadır.

Risk seviyesi, dikkate alınan bulut mimarisinin türüne göre önemli ölçüde değişecektir. Tanımlanan riskler aşağıdaki gibi sınıflandırılabilir.:

a. Uyum riskleri
b. Stratejik riskler
c. Operayonel riskler
d. Piyasa ve finans riskleri

Aşağıdaki sunular model şablonlardır ve ilgili kurum tarafından uygun şekilde özelleştirilebilir. İlk sunu, ilişkili riskin olasılığı ve etkisi ile çeşitli risk alanlarını kapsamaktadır. İkinci sunu, gizlilik, güvenlik, uyumluluk, yönetişim vb. İle ilgili risklerin değerlendirilmesi kontrol listesidir.

RİSK ÇERÇEVE ŞABLONU				
Risk Alanı	Risk Kontrol Alanı	Açıklama	Risk Olasılığı	Risk Etkisi
Uyum Riskleri	Yönetişim & Kurumsal Risk yönetimi	Etkin dahili bilgi güvenliği yönetişiminin olmaması, risk yönetimi ve uygunluk, ve sağlayıcının kendi güvenlik yönetişimine uyum sağlama	Muhtemel	Hafif
	Yasal Konular Sözleşmeler Elektronik Keşif	Depolama, işleme, üçüncü taraflara açıklama, kişisel verilerin diğer yasal yetki alanlarına aktarılması ve mahkeme celbi durumunda sağlayıcının iş verisi üretememe riski.	Beklenen	Şiddetli

RİSK ÇERÇEVE ŞABLONU				
Risk Alanı	Risk Kontrol Alanı	Açıklama	Risk Olasılığı	Risk Etkisi
	Olay Müdahalesi	Sağlayıcının, adli soruşturmalarda yasal gereklilikleri karşılamak için kolayca analiz edilebilen verilerle olayları tespit edememesi, ele almaması ve kuruluşlara raporlamaması	Muhtemel	Ciddi
	Verilerin birden fazla yetki alanındadepolanması ve şeffaflık eksikliği	Verilerin nerede depolandığı ile ilgili bilgiler olmadan, dağıtım ve yedekli depolama için verileri kopyalama. Kuruluşlar, özellikle de depolamanın yargı yetkisine ilişkin net bilgi verilmezse, bilinçsizce ihlal edebilir.	Beklenen	Ciddi
	Uyum ve Denetim Yönetimi	Devlet tarafından zorunlu kılınan ve sektöre özgü düzenlemelere ve standartlara uyulmaması riski ve sağlayıcıdan denetim bilgisi alamama riski.	Muhtemel	Ciddi
	Veri Koruma Riskleri	Artık uyumlu bir seviyede tutulmayan verilerin korunması riski	Muhtemel	Ciddi
	Hassas Medya Temizliği	Medya fiziksel olarak yok edilememesi, uygun şekilde tanımlanmaması veya uygun bir prosedür olmaması	Oldukça Muhtemel	Ciddi
	Denetim veya Sertifika Olmaması	Sistem gerektiği gibi denetlenmemesi ve / veya sertifikalandırılmaması	Muhtemel	Ciddi
	Uyum Bozulması	Uyumluluğun sağlanamaması veya sürdürülememesi (düzenleme, yönetişim, standartlara)	Muhtemel	Ciddi
	Yönetişim Bozulması	Kuruluşlar, genel yönetişimi etkileyebilecek bir dizi konuda sağlayıcıyı kontrol altına alabilir	Oldukça Muhtemel	Ciddi

RİSK ÇERÇEVE ŞABLONU				
Risk Alanı	Risk Kontrol Alanı	Açıklama	Risk Olasılığı	Risk Etkisi
Stratejik Riskler	Bilgi Yönetimi ve Veri Güvenliği	Hassas verilerin zayıf tanımlanması, aktarılan veya bulutta depolanan verilerin korunmasında eksiklik ve veri sızıntısının önlenmesinde eksiklik	Muhtemel	Ciddi
	Birlikte Çalışabilirlik ve Taşınabilirlik	Sağlayıcılar arasında İş uygulamaları birlikte çalışamaması ve satıcının kilitlenme riskini en aza indirmek için standartların eksikliği.	Muhtemel	Ciddi
	Kötü Sağlayıcı Seçimi	Teknoloji veya servis seçiminde uygun olmayan seçim sistemde bozulma ile sonuçlanır	Muhtemel değil	Ciddi
	Organizasyonel Hazırlık	Stratejik uyum, kültürel ve işgücü hazırlığı, şampiyonluk ve paydaş katılımı sağlanamaması	Muhtemel değil	Ciddi
	Tedarikçi Yedekliliği Eksikliği	Alternatif bir tedarikçi kaynağı tanımlanamaması / sözleşme imzalanamaması	Oldukça Muhtemel	Ciddi
	Kilitleme	Şirket içi BT ortamından harici bir sağlayıcıya ve bir sağlayıcıdan diğerine taşınmayla ilişkili risk	Muhtemel	Ciddi
	Kuruluşlar tarafında veri sınıflandırması	Uygunsuz veri sınıflandırması ve sağlayıcıya yönelik gereksinimleri tanımlayamamaya neden olan hafif kontrollerin tanımı	Oldukça Muhtemel	Ciddi
	Şirket içinde buluta veri taşıma (genel, özel veya karma)	Eski verileri bulut tabanlı bir ortama taşıma zorluğu	Muhtemel	Ciddi

RİSK ÇERÇEVE ŞABLONU				
Risk Alanı	Risk Kontrol Alanı	Açıklama	Risk Olasılığı	Risk Etkisi
Operasyonel Riskler	Veri Merkezi Operasyonları	Servis sağlayıcının; iş servislerinin hassasiyetine göre yönetim standartlarına ve en iyi uygulamalara uymaması ve güvenlik denetimlerini uygulamaması	Muhtemel	Ciddi
	Kayıt ve İzleme (Log and Trace) Hatası	Operasyonel kayıtların (güvenlik kayıtları dahil) kaybı veya uyumsuzluğu	Muhtemel değil	Ciddi
	Yedekleme (Backup) Hatası	Yedek bilgilerin yanlış yere alınması veya çalınması	Muhtemel	Ciddi
	Bilgi Yönetimi ve Veri Güvenliği	Hassas verilerin tanımlanması, aktarılan veya bulutta depolanan verilerin korunması, veri sızıntısının önlenmesinde gevşeklik	Muhtemel	Ciddi
	Mevcut dahili operasyonel prosedürler üzerindeki etki	Değişim yönetimi, olay/problem yönetimi, iş sürekliliği yönetimi ile ilgili operasyonel prosedürlerin gözden geçirilmesi	Muhtemel	Ciddi
	Kaynak Kullanımı / Kaynak Yorgunluğunun Yanlış Modellenmesi	Ek kapasite sağlama ve/veya Servis Seviye Anlaşmasını karşılamada geçici başarısızlık.	Muhtemel değil	Ciddi
	Mevcut iş çözümlerine entegrasyon	Eski / mevcut ortama (arayüzler) entegrasyon zorluğu	Muhtemel	Ciddi
	Malicious Activities from an Insider	Privileged users (e.g. Administrator) performing unauthorized activities on the system (data theft, tampering…)	Muhtemel	Ciddi
	Hassas Bilgi Kaçağı	Hassas bilgilerin yanlışlıkla veya kötü amaçlı etkinliklerle yetkisiz bir gruba maruz kalmasına	Muhtemel	Ciddi

RİSK ÇERÇEVE ŞABLONU				
Risk Alanı	Risk Kontrol Alanı	Açıklama	Risk Olasılığı	Risk Etkisi
	Operasyon Yönetimi	Sağlayıcı;operasyonlarını uyumluluk gereksinimlerini karşılamayacak şekilde gerçekleştirir (Değişiklik yönetimi, yama yönetimi vb.)	Muhtemel	Ciddi
	Mahkeme celbi ve e- keşfi	Mahkeme celbi sonucu, mahkeme makamlarının kritik sisteme el koyması	Muhtemel	Ciddi
	Tesislere yetkisiz erişim	Makinelere ve diğer tesislere fiziksel erişim dahil	Muhtemel	Ciddi
	Bilgisayar Ekipmanlarının Çalınması	Sistemler veya verilerin çalınması	Muhtemel	Ciddi
	Bulut servisinin kullanıldığı uç noktanın güvenliği (laptop,pc, smartphone vb.)	Son noktayı güvence altına almak için yeterli politika / kontrol sağlanamaması	Muhtemel değil	Ciddi
	İnsan Kaynakları Kısıtlamaları	Servis ve desteği sağlamak için doğru kaynakları bulamama ve elinde tutamama	Hafif	Ciddi
	Doğal Afetler	Doğal Afet Durumlarının Ele Alınması (İş Sürekliliği Yönetimi)	Muhtemel	Ciddi
	Lisanslama Riskleri	Lisanslamaların düzgün sağlanmaması	Muhtemel değil	Ciddi
	Geleneksel Güvenlik, İş Sürekliliği ve Felaket Kurtarma	Sağlayıcının veri merkezleri güvenliği, iş sürekliliği ve felaket kurtarma planlarını uygulamaması	Muhtemel	Ciddi

RİSK ÇERÇEVE ŞABLONU				
Risk Alanı	Risk Kontrol Alanı	Açıklama	Risk Olasılığı	Risk Etkisi
Piyasa ve Finans Riskleri	İtibar kaybı	Kurum içi sistem: bazı önemli ve kamu olayları riski Bulutta: Bulut Sağlayıcısı veya ortak faaliyetlerle risk	Oldukça Muhtemel	Ciddi
	Servis Sonlandırma veya Arıza	Servis artık varsayılan şekilde sağlanamaz	Muhtemel	Ciddi
	İzolasyon Hatası	Servise erişim geçici olarak reddedilir ve muhtemelen itibar, kritik veya finansal sorunlara yol açar	Muhtemel	Ciddi
	Kapasite yönetimi	Yetersiz Kaynak Sağlama ve Altyapı Yatırımı	Muhtemel	Ciddi
	Çevre Çevikliği / Market zamanı	Değişen çevreyebelirlemek için sistem özelliklerini (performans, mimari, ayrışma) ayarlayabilme gecikmesi veya genel zorluk	Hafif	Ciddi
	Olay Müdahalesi	Sağlayıcının, adli soruşturmalarda yasal gereklilikleri karşılamak için kolayca analiz edilebilen verilerle olayları tespit edememesi, işleyememesi ve bunları kuruluşlara raporlayamaması.	Muhtemel	Ciddi

Sunu-15 - Risk Alanları

RİSK DEĞERLENDİRME KONTROL LİSTESİ	
S No	Soru
	Bilginin Değeri, Kritikliği ve Hassasiyeti
1	Bilginin sahibi kimdir?
2	Bilgi ile desteklenen kuruluşların iş süreçleri nelerdir?
3	Resmi bilgilerin korunması için kuruluşların kurallarına göre, bilgilerin güvenlik sınıflandırması nedir, nasıldır?
4	Bulut servisi tarafından saklanacak veya işlenecek bilgilerin gizliliği ile ilgili herhangi bir endişe var mı?
5	Veriler kişisel bilgiler içeriyor mu?
6	Bilgilerin kullanıcıları kimlerdir?
7	Kullanıcılar bilgiye erişim için ne gibi izinler talep eder? (yani okuma, yazma, değiştirme ve / veya silme)
8	Bilgiler için hangi mevzuat geçerlidir?
9	Bilgiler için uygulanan sözleşme yükümlülükleri nelerdir? (Örn. Bir dizi standartla uyumlu, vb.)
10	Bilginin yetkisiz bir şekilde açıklanmasının kuruluş üzerindeki etkisi ne olur?
11	Bilginin bütünlüğü riske atılırsa, kuruluş üzerindeki etkisi ne olur?
12	Kuruluşun, yetkisiz bir açıklamanın etkisini en aza indirmek için herhangi bir olay müdahale ve yönetim planı var mı?
13	Eğer bilgiler mevcut değilse kuruluş üzerindeki etkisi ne olur?
13.a	Bir kesinti meydana geldikten sonra tolere edilebilecek maksimum veri kaybı miktarı nedir?
13.b	Bir kesinti meydana geldikten sonra, asgari servis seviyelerinin geri yüklenmesi için gereken maksimum süre nedir?
13.c	İş hedeflerinden kalıcı olarak taviz vermemek için tüm servisin geri yüklenmesi için gereken maksimum süre nedir?
	Veri Egemenliği
14	Bulut sağlayıcısının kayıtlı merkez ofisi nerede??
15	Bulut servisleri hangi ülkelerden sunuluyor?
16	Kuruluşun verileri hangi yasal yetki alanlarında saklanacak ve işlenecek?
17	Bulut sağlayıcı, kurumlara verilerinin depolanıp işlenemeyeceği yerleri belirlemesine izin verecek mi?

RİSK DEĞERLENDİRME KONTROL LİSTESİ	
S No	Soru
18	Servisin ek yargı riski taşıyan herhangi bir üçüncü tarafa (örneğin taşeronlar, alt yükleniciler veya başka bir bulut sağlayıcısı) bağımlılığı var mı? Evetse, bulut sağlayıcısı servisin sunumunda yer alan her üçüncü taraf için aşağıdaki ayrıntıları sağlayabilir mi?
18.a	Üçüncü tarafın kayıtlı merkezi.
18.b	Servislerinin sunulduğu ülke veya ülkeler.
18.c	Bulut servisi tarafından depolanan, işlenen ve iletilen kuruluş verilerine erişim
19	Verilerin saklanacağı ve işleneceği ülke veya ülkelerin yasaları, bilgilerin güvenliğini ve / veya gizliliğini nasıl etkileyebileceklerini değerlendirmek için incelendi mi?
20	Yasalar bulut sağlayıcısı ve / veya müşterinin bilgileri için gerçekten geçerli mi? (Örneğin, bazı gizlilik yasaları belirli iş türlerinden muaftır veya yabancıların kişisel bilgileri için geçerli değildir.)
21	Geçerli gizlilik yasaları, eşdeğer veya daha güçlü bir koruma sağlıyor mu?
21.a	Hayır ise, kuruluşlar sözleşmede eşdeğer gizlilik korumalarının belirtildiğinden emin olmak için bulut sağlayıcısı ile görüşebilecekler mi?
22	Bulut sağlayıcısı, düzenleyici kurumların kuruluş bilgilerine erişim taleplerini nasıl ele alıyor?
22.a	Sağlayıcı sadece geçerli bir mahkeme kararına cevap olarak bilgileri açıklayacak mı?
22.b	Sağlayıcı, böyle bir talebe cevap olarak bilgileri açıklaması durumunda kuruluşu bilgilendirecek mi?
22.c	Sağlayıcının, kuruluşlar da dahil olmak üzere müşterilere, bilgilerine erişim isteyen bir mahkeme emri aldığını bildirmesi engelleniyor mu?
	Gizlilik
23	Kuruluşlar; sağlayıcıyla, bulut servisinin kullanımıyla ilgili gizlilik risklerini ve bunları etkin bir şekilde yönetmek için gereken kontrolleri tanımlamak üzere bir Gizlilik Etki Değerlendirmesi (PIA- Privacy Impact Assessment) yapabilir mi? Yoksa sağlayıcı kurumların gizlilik şartlarına uyacak mı?
24	Bulut sağlayıcısının kişisel bilgileri kullanımı gizlilik politikasında açıkça belirtilmiş mi?
24.a	Bulut sağlayıcısının gizlilik politikası kuruluşun iş gerekliliklerıyle tutarlı mı?
25	Bulut sağlayıcısı, verilerine yetkisiz bir kişi tarafından erişilirse veya bu kişilere açıklanırsa kuruluşları bilgilendirir mi?
26	Bir gizlilik ihlali varsa, kuruluş, çalışanları ve/veya müşterileri kime şikayet edebilir?

RİSK DEĞERLENDİRME KONTROL LİSTESİ	
S No	Soru
	Yönetişim
	Kullanım Şartları
27	Bulut sağlayıcı kurumlarla sözleşmeler yapacak mı yoksa standart Servis Şartları'nı kabul etmeleri mi gerekecek?
28	Bulut sağlayıcısının Servis Şartları ve SLA; kendisine verilen tüm kuruluş bilgilerini özellikle resmi bilgiler; ve kişisel olarak tanımlanabilir tüm bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini nasıl koruduğunu açıkça tanımlıyor mu?
29	Bulut sağlayıcısının Servis Şartları kuruluş verilerinin sahipliğini koruyacağını belirtecek mi?
30	Bulut sağlayıcı, verileri servisin sunulması dışında herhangi bir amaçla kullanacak mı?
31	Bulut sağlayıcısının servisi herhangi bir üçüncü taraf servisine bağlı mı?
	U
32	Bulut sağlayıcısının Servis Şartları bir kuruluşun; servisi ve içinde tutulan verileri korumak için mevcut güvenlik önlemlerinin uygulanmasını ve yönetimini doğrudan denetlemesine izin veriyor mu?
32.a	Evetse, bu, güvenlik açığı taramaları ve servis ile destekleyici altyapının sızma testlerini gerçekleştirmeyi içeriyor mu?
32.b	Hayır ise, bulut sağlayıcısı bağımsız bir üçüncü tarafça uluslararası kabul görmüş bir bilgi güvenliği standardı veya çerçevesine göre resmi düzenli değerlendirmeden geçiyor mu? (Örn. ISO / IEC 27001 ile uyumlu oldukları onaylı mı? ISAE 3402 SOC 2 Tip II değerlendirmesi yapıldı mı?)
33	Bulut sağlayıcısı, bir kuruluşun servise kayıt olmadan önce son denetim raporlarını ayrıntılı bir şekilde gözden geçirmesine izin veriyor mu? (Ör. Bulut sağlayıcısı, dış denetçilerinin tam denetim raporlarının bir kopyası ve son zamanlarda yapılan iç denetimlerin sonuçları ile birlikte Uygulanabilirlik Bildirimi sunabiliyor mu?)
34	Bulut sağlayıcısı, mevcut müşterilerinin iki veya daha fazlasının iletişim bilgilerini vererek potansiyel müşterilerin referans kontrolleri yapmasını sağlayacak mı?
35	Bulut sağlayıcı tamamlanmış bir Bulut Bilişim Uygulama Kodu yayınladı mı?

RİSK DEĞERLENDİRME KONTROL LİSTESİ	
S No	Soru
	Gizlilik
	Kimlik Doğrulama ve Erişim Kontrolü
36	Bulut servisi kuruluşun kimlik yönetimi stratejisini destekleyecek mi?
37	Bulut sağlayıcı, kimliklerin yaşam döngüleri boyunca yönetilmesini ve korunmasını sağlayan etkili bir dahili sürece sahip mi?
38	Sağlayıcının, kullanıcı hesaplarının uygun şekilde yönetilmesini ve korunmasını sağlamak için düzenli aralıklarla gerçekleştirilen etkin bir denetim süreci var mı?
39	Bulut tarafından sağlanan her yerde, erişim ile ilişkili riskleri yönetmek için gerekli kontroller tanımlandı mı?
39.a	Bulut servisi bu kontrol gereksinimlerini karşılıyor mu?
40	Tüm şifreler, özellikle sistem / servis yöneticileri karmaşıklık gereksinimlerine uygun olarak şifreleniyor mu?
	Çoklu Kiracılık
41	Bulut sağlayıcı; kuruluşun, müşteri verilerinin sanallaştırılması ve ayrılmasıyla ilgili güvenlik kontrolleri ve uygulamalarının değerlendirmesini içeren yakın zamanda yapılan üçüncü taraf denetim raporunu (ör. ISO 27001 veya ISAE 3402 SOC 2 Tip II) incelemesine izin veriyor mu?
42	Bulut sağlayıcı; kuruluşların, müşteri verilerinin ayrılmasını sağlamak için kullanılan erişim kontrollerinin etkinliğini değerlendirmek için güvenlik testi (sızma testleri dahil) gerçekleştirmesine izin veriyor mu?
	Starndart Çalışma Ortamları
43	Bir kuruluşun yönetmekten sorumlu olduğu servis bileşenleri için tanımlanmış ve belgelenmiş uygun yapı ve katılaşma standartları var mı?
44	Bir kuruluş işletim sistemlerini ve uygulamalarını dahili yapı veya katılaşma standartlarına göre yayınlayabilir mi?
44.a	Hayırsa, bulut sağlayıcısı herhangi bir kuruluşun güvenlik gereksinimlerini karşılayan uygun yapı ve katılaşma standartlarına sahip mi?
44.b	Sanal görüntü, yalnızca servisi desteklemek için gerekli gelen ve giden trafiğe izin verecek şekilde yapılandırılmış ana bilgisayar tabanlı bir güvenlik duvarı içeriyor mu?
44.c	Bulut sağlayıcısı, sanal makinelere ana bilgisayar tabanlı saldırı tespit ve önleme servisi (IDS / IDP) uygulamalarının yüklenmesine izin veriyor mu?

RİSK DEĞERLENDİRME KONTROL LİSTESİ	
S No	Soru
45	Bulut sağlayıcısı, güvenlik süreçleri ve kontrolleri için düzenli testler yapıyor mu?
45.a	Kuruluşlara ilişkili raporların bir kopyasını verecekler mi?
46	Servisin güvenli bir şekilde dağıtıldığından emin olmak için bir sızma testi yapılabilir mi?
	Yama ve Güvenlik Açığı Yönetimi
47	Bulut sağlayıcısı, bulut servisini oluşturan tüm bileşenlerin yamasından sorumlu mu?
47.a	Bulut sağlayıcısı, bulut servisini oluşturan tüm bileşenlerin yamasından sorumlu DEĞİLSE, yama için sorumlulukların ayrıntılarını paylaşır mı?
48	Bulut sağlayıcısının Servis Şartları veya SLA'sı, belirli bir maksimum maruz kalma durumunda, yama ve güvenlik açığı yönetimi için servis düzeyleri içeriyor mu?
49	Bulut sağlayıcı bir kuruluşun düzenli güvenlik açığı değerlendirmeleri yapmasına izin veriyor mu?
50	Servis Şartları veya SLA, servisteki güvenlik açıklarından kaynaklanan ihlaller için bir tazminat maddesi içerecek mi?
50.a	Servis Şartları veya SLA, servisteki güvenlik açıklarından kaynaklanan ihlaller için tazminat maddesi içeriyorsa, ihlal olması durumunda yeterli bir tazminat düzeyi sağlıyor mu?
	Şifreleme
51	Bulut servisi yalnızca onaylanmış şifreleme protokolleri ve algoritmalarını mı kullanıyor?
52	Kriptografik anahtarların yönetiminden kim sorumlu olacak?
53	Sağlayıcının, kuruluşların gereksinimlerini karşılayan bir anahtar yönetim planı var mı?
	İç Tehtid'de Bulur Sağlayıcı
54	Bulut sağlayıcısı, kuruluş verilerine erişimi olan tüm personeli için istihdam öncesi uygun inceleme yapacak mı?
54.a	Bulut sağlayıcısı, istihdam süresince sürekli kontroller yapıyor mu?
55	Bulut sağlayıcı, servislerinin herhangi bir bölümünü sunmak için bir üçüncü tarafa bağımlıysa, üçüncü taraf, müşteri verilerine erişimi olan tüm personel için istihdam öncesi uygun araştırma yapmayı taahhüt ediyor mu?

RİSK DEĞERLENDİRME KONTROL LİSTESİ	
S No	Soru
56	Bulut sağlayıcısının, müşteri verilerine tüm mantıksal erişimi, günlüğe kaydeden ve izleyen bir SIEM servisi olacak mı?
57	Bulut sağlayıcısı, denetim günlüklerinin yetkisiz değişiklik ve silinmeye karşı korunmasını sağlamak için görevlerin ayrılmasını zorunlu kılıyor mu?
58	Servis Şartları veya SLA, bulut sağlayıcının çalışanları tarafından müşteri verilerine yetkisiz erişimi bildirmesini gerektiriyor mu?
58.a	Evetse, bulut sağlayıcısının, ilgili etkiyi değerlendirmelerini ve yönetmelerini sağlamak için etkilenen kuruluşlara olayla ilgili ayrıntılar sağlaması gerekiyor mu?
	Veri Kalıcılığı
59	Bulut sağlayıcısı, başka bir müşteriye sunulmadan önce depolama ortamının güvenli bir şekilde temizlenmesi için denetlenebilir bir işleme sahip mi?
60	Bulut sağlayıcı, müşteri verilerini içeren ICT ekipmanının ve depolama ortamının (örn. Sabit disk sürücüleri, yedekleme bantları vb.) güvenli bir şekilde imhası veya imha için denetlenebilir bir işleme sahip mi?
	Fiziksel Güvenlik
61	Bunu yapmak pratikte mümkünse, bulut sağlayıcısının fiziksel güvenlik kontrolleri doğrudan kuruluş tarafından incelenebilir veya değerlendirilebilir mi?
61.1	Hayır ise, bulut sağlayıcı, fiziksel güvenlik kontrollerinin bir değerlendirmesini içeren güncel bir üçüncü taraf denetim raporunu (ör. ISO 27001 veya ISAE 3402 SOC 2 Tip II) kurumun incelemesine izin veriyor mu?
62	Bulut sağlayıcısının fiziksel güvenlik denetimleri, bulut servisinde depolanan bilgileri korumak için kuruluşların güvenlik yönergelerinde tanımlanan minimum gereksinimleri karşılıyor mu?
	Veri Bütünüğü
63	Bulut sağlayıcı, veri kaybına veya bozulmasına karşı koruma sağlamak için standart servis tekliflerinin bir parçası olarak veri yedekleme veya arşivleme servisleri sunuyor mu? Hayır ise, veri kaybı veya bozulmasına karşı koruma sağlamak için ek bir servis olarak veri yedekleme veya arşivleme servisleri sunuyorlar mı?
64	Veri yedekleme ve arşivleme servisleri nasıl sağlanır?
65	SLA veri yedekleme zamanlamasını belirtiyor mu?
66	Veri yedekleme veya arşivleme servisi, veri kaybına karşı koruma ile ilgili iş gereksinimlerinin karşılanmasını sağlıyor mu? (Yani servis, iş Kurtarma Noktası Hedefi'ni (Recovery Point Objective) destekliyor mu?)

RİSK DEĞERLENDİRME KONTROL LİSTESİ	
S No	Soru
67	Bulut sağlayıcısı veri geri yüklemesi için ne düzeyde ayrıntı sunuyor?
68	Bulut sağlayıcısının geri yükleme başlatma süreci nasıldır?
69	Bulut sağlayıcı, verilerin yedekleme ortamından kurtarılabilmesini sağlamak için düzenli olarak geri yükleme testleri yapıyor mu?
70	Kuruluşun, veri kaybına veya bozulmasına yol açan bir olaydan kurtulabilmesini sağlamak için bir veri yedekleme stratejisi uygulaması gerekiyor mu?
71	Önerilen veri yedekleme ve arşivleme stratejisi kuruluşun yükümlülüklerini yerine getirmesinde destekliyor mu?
	Kullanılabilirlik
	Servis Seviye Anlaşması
72	SLA, açıkça belirlenmiş bir dönem için, beklenen ve minimum kullanılabilirlik performans yüzdesini içeriyor mu?
72.a	Servis Seviyesi Sözlemesi, açıkça belirlenmiş dönemde beklenen ve asgari kullanılabilirlik performans yüzdesini içeriyorsa, kuruluşun uygunluk için ticari gereksinimleri karşılanıyor mu? Yani, servisin Kurtarma Süresi Hedefi (Recovery Time Objective) ve Kabul Edilebilir Kesinti Penceresini (Acceptable Interruption Window) destekliyor mu?
73	SLA, tanımlanmış, planlanmış kesinti pencereleri içeriyor mu?
73.a	Servis Seviyesi Sözleşmesi tanımlı, planlanmış kesinti pencereleri içeriyorsa, belirtilen kesinti pencereleri ticari işlemleri etkiliyor mu?
73.b	SLA tanımlı, planlanmış kesinti pencerelerini İÇERMEZSE, bulut sağlayıcısı bir kesinti gerekmeksizin bakım faaliyetlerini gerçekleştirmelerini sağlayan teknolojiler uyguluyor mu?
74	SLA, garantili kullanılabilirlik yüzdelerinin ihlalinde bir tazminat maddesi içeriyor mu?
74.a	SLA, garantili kullanılabilirlik yüzdelerinin ihlali için bir tazminat maddesi içeriyorsa, bulut sağlayıcı SLA'yı ihlal etmesi durumunda bu yeterli bir tazminat düzeyi sağlıyor mu?
	Servisi Engelleme Saldırıları (Denial of Service Attacks)
75	Bulut sağlayıcısı DDoS saldırılarına karşı koruma sağlayabilecek protokoller ve teknolojiler kullanıyor mu?
75.a	Evetse, bulut sağlayıcısının DDoS koruma servislerini etkinleştirmek 15, 16 ve 17. soruların cevabını etkiler mi?
76	Kuruluş, EDoS / fatura şokuna karşı koruma sağlamak için kaynak kullanım sınırları belirleyebiliyor veya yapılandırabiliyor mu?

RİSK DEĞERLENDİRME KONTROL LİSTESİ	
S No	Soru
	Ağ Kullanılabilirliği ve Performans
77	Kurum tarafından doğrudan yönetilen veya abone olunan ağ servisleri yeterli düzeyde kullanılabilirlik sağlıyor mu?
78	Doğrudan yönetilen veya kuruluş tarafından abone olunan ağ servisleri yeterli düzeyde yedeklilik / hata toleransı sağlıyor mu?
79	Doğrudan yönetilen veya kuruluş tarafından abone olunan ağ servisleri yeterli düzeyde bant genişliği sağlıyor mu?
80	Kuruluş ağları ile bulut sağlayıcısının servisi arasındaki gecikme, istenen kullanıcı deneyimini elde etmek için kabul edilebilir seviyede mi?
80.a	Hayır ise, ağ servislerinde oluşan gecikme doğrudan kuruluş tarafından yönetiliyor mu veya abonelik mi gerekiyor?
80.b	Sorun ağ bulut sağlayıcısı veya kuruluş tarafından çözülebilir mi?
81	Kuruluş ağları ile bulut sağlayıcısının servisi arasındaki paket kaybı, istenen kullanıcı deneyimini elde etmek için kabul edilebilir seviyede mi?
81.a	Hayır ise, bir ağ servislerinde oluşan paket kaybı doğrudan kuruluş tarafından yönetiliyor mu veya abonelik mi gerekiyor?
81.b	Sorun ağ bulut sağlayıcısı veya kuruluş tarafından çözülebilir mi?
	İş Sürekliliği ve Felaket kurtarma
82	Bulut sağlayıcısının iş sürekliliği ve felaket kurtarma planları var mı?
83	Bulut sağlayıcı kuruluşun iş sürekliliği ve felaket kurtarma planlarını gözden geçirmesine izin veriyor mu?
84	Bulut sağlayıcısının planları, kuruluş verilerinin kurtarılmasını mı yoksa yalnızca servisin geri yüklenmesini mi kapsıyor?
85	Bulut sağlayıcısının planları kuruluş verilerinin geri yüklenmesini kapsıyorsa, müşteri verilerinin kurtarılmasına öncelik veriliyor mu?
85.a	Öyleyse nasıl? Kuruluşlar, büyüklük ve sözleşme değerine göre önceliklendirilecek mi?
86	Bulut sağlayıcı, iş sürekliliği ve felaket kurtarma planlarını düzenli bir şekilde resmi olarak test ediyor mu?
86.a	If yes, how regularly are such tests performed?
86.b	Will the provider provide agencies with a copy of the associated reports?

RİSK DEĞERLENDİRME KONTROL LİSTESİ	
Q No	Question
	Olay Müdahalesi ve Yönetimi
87	Bulut sağlayıcısının resmi bir olay yanıtı ve yönetim süreci var mı ve bilgi güvenliği olaylarını nasıl tespit ettiklerini ve bunlara nasıl yanıt verdiklerini açıkça tanımlayan planlar var mı?
87.a	Evetse, kuruluşa süreçlerinin bir kopyasını veriyor ve yeterli olup olmadığını belirlemeyi planlıyorlar mı?
88	Bulut sağlayıcı olay yanıtını ve yönetim sürecini ve planlarını düzenli olarak test ediyor ve geliştiriyor mu?
89	Bulut sağlayıcı olay yanıtını ve yönetim süreçlerini ve planlarını test ederken kuruluşlarla etkileşime girecek mi?
90	Bulut sağlayıcı, personeline olay yanıtı ve yönetim süreçleri hakkında eğitim sağlıyor ve olaylara etkili ve verimli bir şekilde yanıt vermelerini planlıyor mu?
91	Bir bilgi güvenliği olayı meydana geldiğinde bulut sağlayıcısının Servis Şartları veya SLA'sı kuruluşa sağlayacağı desteği açıkça tanımlıyor mu?
91.a	Bulut sağlayıcısı, bilgilerinin veya birbirine bağlı sistemlerin güvenliğini etkileyebilecek bir olay tespit edildiğinde veya raporlandığında kuruluşlara bildirimde bulunacak mı?
91.b	Kuruluşların şüpheli bilgi güvenliği olaylarını rapor etmeleri için bir iletişim noktası ve kanal belirli mi?
91.c	Bir bilgi güvenliği olayı sırasında tarafların rol ve sorumlulukları tanımlı mı?
91.d	Kuruluşlara, olayla ilgili araştırma yapmalarını sağlamak için kanıtlara erişim sağlanıyor mu? (örn., zaman belirli denetim günlükleri ve/veya sanal makinelerin adli görüntüleri vb.)?
91.e	Kuruluşun düzenleyici bir organ tarafından yürütülen bir soruşturma ile etkili bir şekilde işbirliği yapmasını sağlayacak yeterli bilgi sağlanıyor mu?
91.f	Bir bilgi güvenliği olayı gerçekleştikten sonra veri ve servislerin kurtarılmasından hangi tarafın sorumlu olduğunu tanımlı mı?
91.g	Olay sonrası raporları, olayın nedenini anlamalarını ve bulut servisini kullanmaya devam edip etmeme konusunda bilinçli bir karar vermelerini sağlamak için etkilenen kurumlarla paylaşılıyor mu?
91.h	Bilgi güvenliği olayları için; sözleşme sınırlarında ve sigorta yükümlülüklerinde sorumluluk ve tazminat belirli mi?
92	Bulut sağlayıcıları olay yanıtı ve yönetim prosedürleri, kuruluşun olayları zamanında ve etkili bir şekilde yönetme yeteneğini engellemeyen veya geciktirmeyen kurumun dâhili politikası ve prosedürleriyle eşleşiyor mu (veya bunlara uyuyor mu?)

Sunu-16 – Risk Değerlendirme Kontrol Listesi

Teşekkürler

Kaynak. : https://www.moheri.gov.om/userupload/Policy/Cloud%20Governance%20Framework.pdf

Çeviri : Gülsün Yıldız