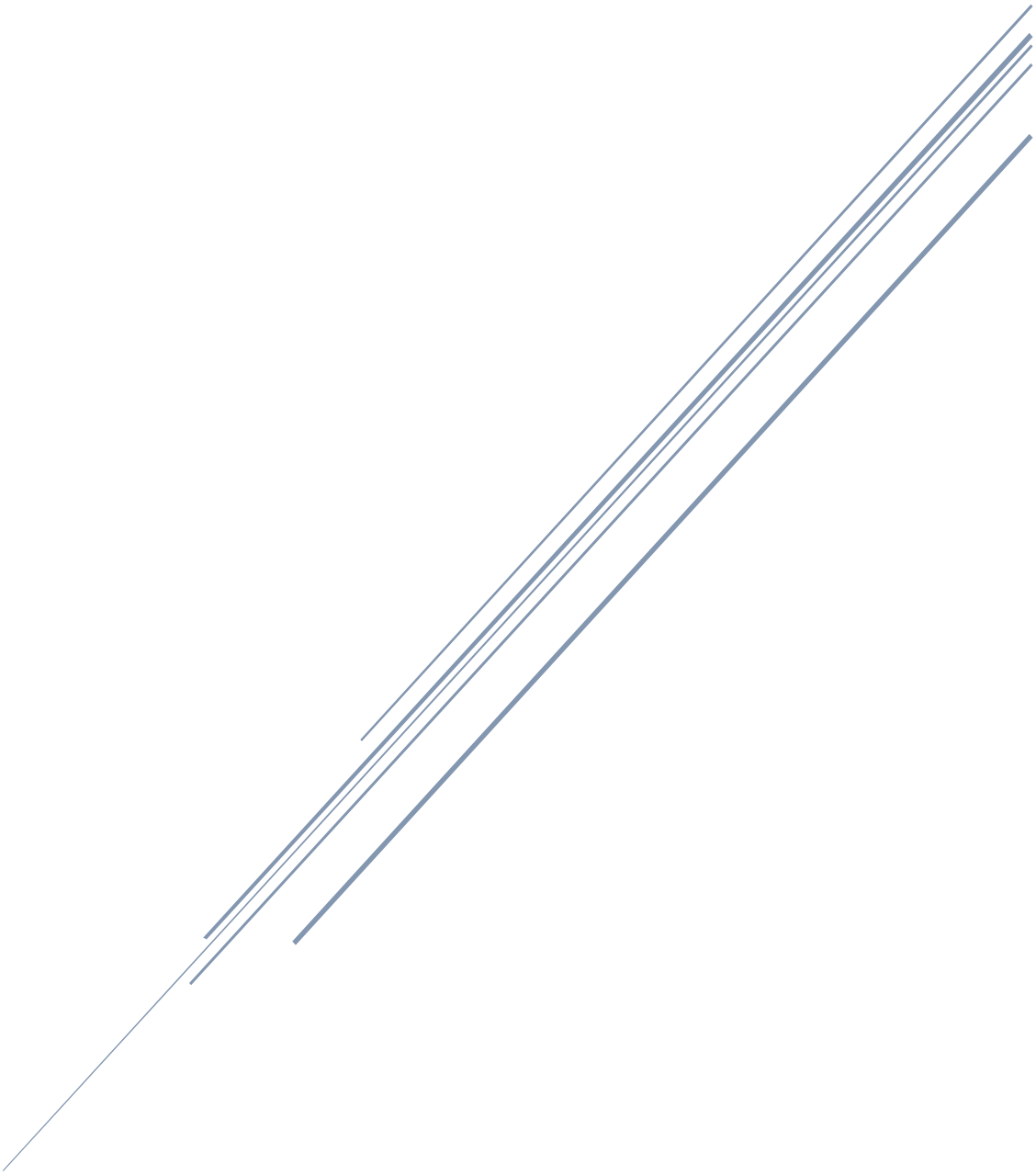
ISO 27017 BULUT HİZMETLERİNDE BİLGİ GÜVENLİĞİ KONTROLLERİ

Öner Ziya BAŞ



2022

STANDARDIN / MEVZUATIN;

Adı, Numarası ve Tarihi:	27017:2021 Bilgi Teknolojisi - Güvenlik teknikleri – Bulut hizmetlerinde ISO/IEC 27002'ye dayalı bilgi güvenliği kontrolleri için uygulama ilkesi

1. Hitap Ettiği Sektörler

Bulut hizmeti müşterileri ve bulut hizmeti sağlayıcılarına hitap etmektedir. Bazı yönergeler, kontrolleri uygulayan bulut hizmeti müşterileri içindir ve diğerleri ise bu kontrollerin uygulanmasını destekleyen bulut hizmeti sağlayıcıları içindir.

2. Terminoloji

- **Kabiliyet** Belirli bir eylemi gerçekleştirebilme niteliği.
- **Veri İhlali** İletilen, saklanan veya başka bir şekilde işlenen korumalı verilerin kazara ya da yasa dışı bir şekilde tahrip/imha edilmesine, kaybına, değişmesine, izinsiz ifşa edilmesine veya bunlara yetkisiz erişilmesine yol açan güvenlik ihlali.
- **Güvenli Çoklu Kullanım (multi-tenancy)** Veri ihlallerine karşı açıkça koruma sağlayan güvenlik kontrollerini uygulayan ve bu kontrollerin doğrulanmasını da sağlayan bir yönetişim modeli ile işletilen çoklu kullanım (multi-tenancy) tipi.
- **Sanal Makine (VM- Virtual Machine)** Misafir yazılımın yürütülmesini destekleyen ortamın bütünü. Bir sanal makine, sanal donanım, sanal diskler ve bununla ilişkili meta verilerin bütünüyle bir araya toplanmasıdır. Sanal makineler, temel fiziksel makinenin, hipervizör olarak adlandırılan bir yazılım aracılığıyla çoklanmasına olanak verir.
- **IaaS** Hizmet olarak altyapı (Infrastructure as a Service). Hizmet olarak altyapı isteğe bağlı olarak kullandıkça öde modeliyle temel bilgi işlem, depolama ve ağ kaynakları sunan bir bulut bilişim hizmeti türüdür.
- **PaaS** Hizmet olarak platform (Platform as a Service). Hizmet olarak platform, bulut basit tabanlı uygulamalardan bulut özellikli gelişmiş kurumsal uygulamalara kadar her şeyi dağıtmanıza olanak tanıyan kaynakların yer aldığı, geliştirme ve dağıtıma yönelik eksiksiz bir bulut ortamıdır.
- **SaaS** Hizmet olarak yazılım (Software as a Service). Hizmet olarak yazılım, kullanıcıların bulut tabanlı uygulamalara İnternet üzerinden bağlanmasını ve bunları İnternet üzerinden kullanmasını sağlar.
- **PII** Kişisel veri (Personally Identifiable Information). Kişisel Tanımlanabilir Bilgiler, bir bireyin benzersiz kimliğini tanımlayan bir veri türüdür.
- **SLA** Hizmet seviyesi anlaşması (Service Level Agreement).

3. Ana Konu Başlıkları

5 Bilgi güvenliği politikaları
5.1 Bilgi güvenliği için yönetimin yönlendirmesi
5.1.1 Bilgi güvenliği politikaları
5.1.2 Bilgi güvenliği politikalarının gözden geçirilmesi
6 Bilgi güvenliği organizasyonu
6.1 İç organizasyon
6.1.1 Bilgi güvenliği rolleri ve sorumlulukları
6.1.2 Görevlerin ayrılığı
6.1.3 Yetkililerle iletişim
6.1.4 Özel ilgi grupları ile iletişim
6.1.5 Proje yönetiminde bilgi güvenliği
6.2 Mobil cihazlar ve uzaktan çalışma

6.2.1 Mobil cihaz politikası
6.2.2 Uzaktan çalışma
CLD.6.3 Bulut hizmeti müşterisi ile bulut hizmeti sağlayıcısı arasındaki ilişki
CLD.6.3.1 Bir bulut bilişim ortamı içinde paylaşılan roller ve sorumluluklar
7 İnsan kaynakları güvenliği
7.1 İstihdam öncesi
7.1.1 Tarama
7.1.2 İstihdam hüküm ve koşulları
7.2 İstihdam sırasında
7.2.1 Yönetimin sorumlulukları
7.2.2 Bilgi güvenliği farkındalık, eğitimi ve öğretimi
7.2.3 Disiplin süreci
7.3 İstihdamın sonlandırılması ve değiştirilmesi
7.3.1 İstihdam sorumluluklarının sonlandırılması veya değiştirilmesi
8 Varlık yönetimi
8.1 Varlıkların sorumluluğu
8.1.1 Varlık envanteri
8.1.2 Varlık sahipliği
8.1.3 Varlıkların kabul edilebilir kullanımı
8.1.4 Varlıkların iadesi
CLD.8.1.5 Bulut hizmeti müşterisinin varlıklarının kaldırılması
8.2 Bilgi sınıflandırma
8.2.1 Bilgilerin sınıflandırması
8.2.2 Bilgi etiketleme
8.2.3 Varlıkların idaresi
8.3 Ortam idaresi
8.3.1 Taşınabilir ortam yönetimi
8.3.2 Ortamın imhası
8.3.3 Fiziksel ortam aktarımı
9 Erişim kontrolü
9.1 İş gereksinimleri erişim kontrol
9.1.1 Erişim kontrol politikası
9.1.2 Ağlara ve ağ hizmetlerine erişim
9.2 Kullanıcı erişim yönetimi
9.2.1 Kullanıcı kaydetme ve kayıt silme
9.2.2 Kullanıcı erişimine izin verme
9.2.3 Ayrıcalıklı erişim haklarının yönetimi
9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi
9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi
9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi
9.3 Kullanıcı sorumlulukları
9.3.1 Gizli kimlik doğrulama bilgisinin kullanımı
9.4 Sistem ve uygulama erişim kontrolü
9.4.1 Bilgiye erişimin kısıtlanması
9.4.2 Güvenli oturum açma prosedürleri
9.4.3 Parola yönetim sistemi
9.4.4 Ayrıcalıklı destek programlarının kullanımı
9.4.5 Program kaynak koduna erişim kontrolü
CLD.9.5 Paylaşılan sanal ortamdaki bulut hizmeti müşteri verilerine erişim kontrolü
CLD.9.5.1 Sanal bilişim ortamında ayrım
CLD.9.5.2 Sanal makine sıkılaştırılması
10 Kriptografi

10.1 Kriptografik kontroller
10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika
10.1.2 Anahtar yönetimi
11 Fiziksel ve çevresel güvenlik
11.1 Güvenli alanlar
11.1.1 Fiziksel güvenlik sınırı
11.1.2 Fiziksel giriş kontrolleri
11.1.3 Ofislerin, odaların ve tesislerin güvenliğinin sağlanması
11.1.4 Dış ve çevresel tehditlere karşı koruma
11.1.5 Güvenli alanlarda çalışma
11.1.6 Teslimat ve yükleme alanları
11.2 Teçhizat
11.2.1 Teçhizat yerleştirme ve koruma
11.2.2 Destekleyici altyapı hizmetleri
11.2.3 Kablolama güvenliği
11.2.4 Teçhizat bakımı
11.2.5 Varlıkların kaldırılması
11.2.6 Teçhizat ve kuruluş dışındaki varlıkların güvenliği
11.2.7 Teçhizatın güvenli olarak imhası veya tekrar kullanımı
11.2.8 Gözetimsiz kullanıcı teçhizatı
11.2.9 Temiz masa ve temiz ekran politikası
12 İşletim güvenliği
12.1 İşletim prosedürleri ve sorumlulukları
12.1.1 Yazılı işletim prosedürleri
12.1.2 Değişiklik yönetimi
12.1.3 Kapasite yönetimi
12.1.4 Geliştirme, test ve işletim ortamlarının birbirinden ayrılması
CLD.12.1.5 Yöneticinin operasyonel güvenliği
12.2 Zararlı yazılımlardan koruma
12.2.1 Zararlı yazılımlara karşı kontroller
12.3 Yedekleme
12.3.1 Bilgi yedekleme
12.4 Kaydetme ve izleme
12.4.1 Olay kaydetme
12.4.2 Kayıt(log) bilgisinin korunması
12.4.3 Yönetici ve operatör kayıtları
12.4.4 Saat senkronizasyonu
CLD.12.4.5 Bulut Hizmetlerinin izlenmesi
12.5 İşletimsel yazılımın kontrolü
12.5.1 İşletimsel sistemler üzerine yazılım kurulumu
12.6 Teknik zafiyet yönetimi
12.6.1 Teknik zafiyetlerin yönetilmesi
12.6.2 Yazılım kurulumu kısıtlamaları
12.7 Bilgi sistemleri denetim hususları
12.7.1 Bilgi sistemleri denetim kontrolleri
13 Haberleşme güvenliği
13.1 Ağ güvenliği yönetimi
13.1.1 Ağ kontrolleri
13.1.2 Ağ hizmetlerinin güvenliği
13.1.3 Ağlarda ayrım
CLD.13.1.4 Sanal ve fiziksel ağlar için güvenlik yönetiminin uyumlulaştırılması
13.2 Bilgi transferi

13.2.1 Bilgi transfer politikaları ve prosedürleri
13.2.2 Bilgi transferine ilişkin anlaşmalar
13.2.3 Elektronik mesajlaşma
13.2.4 Gizlilik ya da ifşa etmeme anlaşmaları
14 Sistem edinimi, geliştirme ve bakımı
14.1 Bilgi sistemlerinin güvenlik gereklilikleri
14.1.1 Bilgi güvenliği gereksinimlerinin analizi ve tanımlanması
14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması
14.1.3 Uygulama hizmet işlemlerinin korunması
14.2 Geliştirme ve destek süreçlerinde güvenlik
14.2.1 Güvenli geliştirme politikası
14.2.2 Sistem değişiklik kontrolü prosedürleri
14.2.3 İşletim platformu değişikliklerinden sonra uygulamaların teknik gözden geçirilmesi
14.2.4 Yazılım paketlerindeki değişikliklere ilişkin kısıtlamalar
14.2.5 Güvenli sistem mühendisliği esasları
14.2.6 Güvenli geliştirme ortamı
14.2.7 Dışardan sağlanan geliştirme
14.2.8 Sistem güvenlik testi
14.2.9 Sistem kabul testi
14.3 Test verileri
14.3.1 Test verilerinin korunması
15 Tedarikçi ilişkileri
15.1 Tedarikçi ilişkilerinde bilgi güvenliği
15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası
15.1.2 Tedarikçi anlaşmalarında güvenliği ele almak
15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri
15.2 Tedarikçi hizmet sağlama yönetimi
15.2.1 Tedarikçi hizmetlerinin izlenmesi ve gözden geçirilmesi
15.2.2 Tedarikçi hizmetlerindeki değişikliklerin yönetimi
16 Bilgi güvenliği ihlal olayı yönetimi
16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirmelerinin yönetimi
16.1.1 Sorumluluklar ve prosedürler
16.1.2 Bilgi güvenliği olaylarının raporlanması
16.1.3 Bilgi güvenliği zafiyetlerinin raporlanması
16.1.4 Bilgi güvenliği olaylarında değerlendirme ve karar verme
16.1.5 Bilgi güvenliği ihlal olaylarına müdahale
16.1.6 Bilgi güvenliği ihlal olaylarından ders çıkarma
16.1.7 Kanıt toplama
17 İş sürekliliği yönetiminin bilgi güvenliği hususları
17.1 Bilgi güvenliği sürekliliği
17.1.1 Bilgi güvenliği sürekliliğinin planlanması
17.1.2 Bilgi güvenliği sürekliliğinin uygulanması
17.1.3 Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi
17.2 Yedeklilik
17.2.1 Bilgi işleme tesislerinin erişilebilirliği
18 Uyumluluk
18.1 Yasal ve sözleşmeye tabi gereksinimlere uyum
18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama
18.1.2 Fikri mülkiyet hakları
18.1.3 Kayıtların korunması
18.1.4 Kişisel verilerin gizliliği ve korunması
18.1.5 Kriptografik kontrollerin düzenlenmesi

18.2 Bilgi güvenliğinin gözden geçirilmesi
18.2.1 Bilgi güvenliğinin bağımsız gözden geçirilmesi
18.2.2 Güvenlik politikaları ve standartları ile uyum
18.2.3 Teknik uyum gözden geçirilmesi

4. Standardın Getirdiği Kurallar/Kontroller

BULUT HİZMETLERİNDE ISO/IEC 27002'YE DAYALI BİLGİ GÜVENLİĞİ KONTROLLERİ
BHM: Bulut Hizmetleri Müşterisi
BHS: Bulut Hizmetleri Sağlayıcısı

- **Varlık envanteri**

BHM: Varlık envanterine, bulut bilişim ortamında depolanan bilgiler ve ilişkili varlıklar dahil edilmelidir.
BHM: Sağlayıcı ile anlaşmanın sonlanması ile müşteri varlıklarının iadesi veya kaldırılması sonucu tüm müşteri verilerinin sağlayıcı sistemlerinden silindiğine dair belgelenmiş bir kanıt istenmelidir.
BHS: Varlık envanterinde bulut hizmeti müşteri verileri ve bulut hizmetinden türeyen veriler tanımlanmalıdır**.**
BHS: Müşteri ile anlaşmanın sonlanmasını takiben müşteri varlıkları zamanında kaldırılmalı ve eğer gerekliyse iade edilmelidir.

- **Ağlara ve ağ hizmetlerine erişim**

BHM: Kullanılan her bir ayrı bulut hizmetine kullanıcı erişimi için gereksinimler belirtilmelidir.

- **Kullanıcı erişim yönetimi**

BHS: Kullanıcı kaydetme ve kayıt silme fonksiyonları müşteriye sağlanmalıdır.
BHS: Kullanıcılarının erişim haklarını yönetmek için müşteriye teknik özellikleri sağlamalıdır.
BHS: Müşterinin bulut hizmetlerini yönetmesi için yeterli kimlik doğrulama teknikleri sağlamalıdır.
BHS: Müşterinin gizli kimlik doğrulama bilgilerinin yönetimine dair prosedürler oluşturmalıdır.
BHM: Bulut hizmetinin yönetimi için yeterli kimlik doğrulama teknikleri kullanılmalıdır.
BHM: Tedarikçinin sağladığı gizli kimlik doğrulama bilgileri ile ilgili prosedür kendi prosedürlerini doğrulamalıdır.

- **Sistem ve uygulama erişim kontrolü**

BHM: Bulut hizmetindeki bilgilere erişimin, erişim kontrol politikasına uygun olarak kısıtlanabileceğinden emin olmalıdır.
BHM: Ayrıcalıklı destek programlarının kullanımı bulut hizmetinin kontrolleri ile çatışmamalıdır.
BHS: Müşterinin bulut hizmetindeki verilere erişimi kısıtlamasına olanak tanıyan erişim kontrollerini sağlamalıdır.
BHS: Bulut hizmeti içinde kullanılan her tür destek programı için gereklilikleri tanımlamalıdır.

- **Kriptografik kontroller**

BHM: Kriptografik kontrollerin kullanımına ilişkin politika bulut hizmetlerini kapsamalıdır.
BHM: Her bir bulut hizmeti için kriptografik anahtarları tanımlamalı ve anahtar yönetimi için prosedürler uygulamalıdır.
BHS: Kriptografi kullandığı durumlarla ilgili bulut hizmeti müşterisine bilgi vermelidir.

- **Teçhizat**

BHM: Teçhizatın güvenli olarak imhası veya tekrar kullanımına yönelik bulut hizmeti sağlayıcısının politikalara ve prosedürlere sahip olduğunu doğrulamalıdır.
BHS: Teçhizatın güvenli olarak imhası veya tekrar kullanımıyla ilgili gerekli düzenlemeler zamanında yapılmalıdır.

- **İşletim prosedürleri ve sorumlulukları**

BHM: Değişiklik yönetimi süreci, bulut hizmeti sağlayıcısı tarafından yapılan herhangi bir değişikliğin etkilerini hesaba katmalıdır.
BHM: Kapasitenin sağlayıcı tarafından karşılandığından emin olmalıdır.
BHM: Bulut hizmeti sağlayıcısından yedekleme hizmeti alınıyorsa işlevin teknik özellikleri talep edilmelidir.

BHS: Bulut servisini olumsuz olarak etkileyebilecek değişikliklerle ilgili bilgileri müşteriye sağlamalıdır.
BHS: Kaynak yetersizliğinden kaynaklanan bilgi güvenliği ihlali olaylarını önlemek üzere toplam kaynak kapasitesini izlemelidir.
BHS: Sunduğu yedekleme işlevlerinin teknik özelliklerini bulut hizmeti müşterisine sağlamalıdır.

- **Kaydetme ve izleme**

BHM: Bulut hizmetinin olay kaydetme gereksinimlerini karşıladığı doğrulanmalıdır.
Bulut hizmeti müşterisi ile bulut hizmeti sağlayıcısı arasındaki sorumlulukların tahsisi bulut hizmetine ilişkin ayrıcalıklı işlemleri kapsamalıdır.
BHM: Bulut hizmeti sağlayıcısının sistemleri için kullanılan saat senkronizasyonu hakkında bilgi talep etmelidir.
BHM: Bulut hizmeti sağlayıcısından teknik zafiyetlerin yönetilmesi hakkında bilgi talep edilmelidir.
BHS: Müşteriye sistemler tarafından kullanılan saat ve senkronizasyon hakkında bilgi verilmelidir.
BHS: Müşteriye teknik zafiyetlerin yönetilmesi hakkında bilgi sağlanmalıdır.

- **Haberleşme Güvenliği**

BHM: Ağların ayrılması ile ilgili gerekliliklerin sağlayıcı tarafından karşılandığı doğrulanmalıdır.
BHS: Ağlarda ayrımla ilgili olarak; çok kullanıcılı bir ortamda kullanıcılar arasında ayrım ve sağlayıcı ve müşteri ağı arasındaki ayrım sağlanmalıdır.

- **Bilgi sistemlerinin güvenlik gereklilikleri**

BHM: Sunulan hizmetlerin bulut hizmeti için bilgi güvenliği gereksinimlerini karşılayıp karşılamadığı değerlendirmelidir.
BHM: Sağlayıcıdan güvenli geliştirme prosedürlerinin ve uygulamalarını kullanımı hakkında bilgi talep edilmelidir.
BHS: Müşterilere, kullandıkları bilgi güvenliği yetileri hakkında bilgi sağlamalıdır.
BHS: Müşteriye güvenli geliştirme prosedürleri ve uygulamaların kullanımı hakkındaki bilgi sağlanmalıdır.

- **Tedarikçi ilişkilerinde bilgi güvenliği**

BHM: Tedarikçi ilişkileri için bilgi güvenliği politikasına bulut hizmeti sağlayıcısı dahil edilmelidir.
BHM: Tedarikçi anlaşmalarında bulut hizmetleri ile ilgili güvenliği ele almalıdır.
BHS: Müşteri ile yapılacak anlaşmalarda bilgi güvenliği önlemleri sözleşmeye dahil edilmelidir.
BHS: Eş bulut hizmeti sağlayıcıları kullanılıyorsa veya bulut hizmetlerini tedarik zincirine dayalı olarak tedarik ediyorsa bilgi güvenliği seviyelerine dikkat edilmelidir.

- **Bilgi güvenliği ihlal olaylarının ve iyileştirmelerinin yönetimi**

BHM: Bilgi güvenliği ihlali olayının yönetimi için sorumluluklar belirlenmelidir.
BHM: Sağlayıcıdan bilgi güvenliği olaylarının raporlanması ile ilgili bilgi talep edilmelidir.
BHS: Müşteri ile arasındaki bilgi güvenliği ihlali olayının yönetim sorumluluklarının tahsisine ve ilgili prosedürlere ilişkin hususları tanımlamalıdır.
BHS: Müşteriye bilgi güvenliği olaylarının raporlanması ile ilgili bilgi sağlanmalıdır.
Bulut hizmeti müşterisi ve bulut hizmeti sağlayıcısı, kanıt toplamaya yönelik prosedürler üzerinde anlaşmaya varmalıdır.

- **Yasal ve sözleşmeye tabi gereksinimlere uyum**

BHM: İş için gerekli olan düzenleme ve standartlarla ilgili sağlayıcıdan uyumluluk kanıtı istenmelidir.
BHM: Buluta özgü lisans hakkı gerekliliklerini tanımlamaya yönelik bir prosedür olmalıdır.
BHM: Sağlayıcı tarafından toplanan ve depolanan kayıtların korunması hakkında bilgi talep edilmelidir.
BHM: Kriptografik kontroller dizisi, ilgili anlaşmalar, yasalar ve düzenlemelere uygun olmalıdır.
BHM: Bilgi güvenliği kontrollerinin uygulandığına dair sağlayıcıdan kanıt talep edilmelidir.
BHS: Geçerli yasalar ve sözleşme gerekliliklerine mevcut uyumluluğunun kanıtını müşteriye sağlanmalıdır.
BHS: Fikri mülkiyet hakları şikayetlerine yanıt vermeye yönelik bir süreç kurulmalıdır.

BHS: Toplanan ve depolanan kayıtların korunması hakkında müşteri bilgilendirilmelidir.
BHS: Uygulanan kriptografik kontroller müşteriye açıklamalıdır.
BHS: Bilgi güvenliği kontrollerinin uygulandığına dair kanıtlar müşteriye sunulmalıdır.

- **Bulut hizmeti müşterisi ile bulut hizmeti sağlayıcısı arasındaki ilişki**

Bulut hizmetinin kullanımında paylaşılan bilgi güvenliği rollerine yönelik sorumluluklar, tanımlanmış taraflara tahsis edilmeli, belgelenmeli, tebliğ edilmeli ve uygulanmalıdır.

- **Paylaşılan sanal ortamdaki bulut hizmeti müşteri verilerine erişim kontrolü**

BHS: Müşterinin bulut hizmeti üzerinde çalışan sanal ortamı, diğer bulut hizmeti müşterilerinden ve yetkisiz kişilerden korunmalıdır.
BHS: Bulut ortamındaki sanal makineler iş ihtiyaçlarını karşılamak üzere sıkılaştırılmalıdır.

- **Operasyonel prosedürler ve sorumluluklar**

Bir bulut bilişim ortamındaki yönetimsel işlemlere yönelik prosedürler tanımlanmalı, belgelenmeli ve izlenmelidir.

- **Kayıt tutma ve izleme**

BHM: Kullanılan bulut hizmetlerinin belirtilen hususları izlenebilmelidir ve izleme işlevleri hakkında sağlayıcıdan bilgi almalıdır.
BHS: Hizmet izleme işlevlerinin izlenmesine olanak sağlayan işlevler ve dokümantasyonu müşteriye sağlamalıdır.

- **Ağ güvenliği yönetimi**

BHS: Sanal ve fiziksel ağlar için güvenlik yönetimi uyumlulaştırılarak belgelenmelidir.

5. Mini Denetim Kontrol Listesi

Üst Yönetim Sorumlulukları da dahil olmak üzere standardın uygulanıp uygulanmadığını tespit etmeye yönelik değerlendirme soruları

	Denetim Bulgusu			
Bulut Hizmet Müşterisi Kontrol Maddesi	Yok	Var ama yetersiz	Yeterli	Not
Bulut bilişime özel bir bilgi güvenliği politikası var mıdır?				
Kurum, bulut hizmeti sağlayıcısı ile bilgi güvenliği rollerinin ve sorumluluklarının uygun bir şekilde tahsis edilmesi konusunda anlaşmış mıdır?				
Kurum ve bulut hizmeti sağlayıcısının birlikte çalışmasını gerektiren operasyonlara ilişkin yetkililer tanımlanmış mıdır?				
Bulut hizmeti kullanıcıları için farkındalık, eğitim ve öğretim programları sağlanmakta mıdır?				
Varlık envanterine, bulut bilişim ortamında depolanan bilgileri ve ilişkili varlıklar dahil edilmiş midir?				
Bulut bilişim ortamında tutulan bilgiler ve ilişkili varlıklar, etiketleme için benimsenen prosedürlere uygun olarak etiketlenmiş midir?				
Ağ hizmetlerinin kullanımına yönelik erişim kontrol politikasında, kullanılan her bir ayrı bulut hizmetine kullanıcı erişimi için gereksinimler belirlenmiş midir?				
Bulut hizmetini yöneten yöneticilere, tanımlanmış riskler için yeterli kimlik doğrulama teknikleri kullanılmakta mıdır?				
Bulut hizmeti sağlayıcısının gizli kimlik doğrulama bilgilerinin tahsis edilmesine yönelik yönetim prosedürü, gereksinimleri karşılamak için yeterli midir?				
Kurum, bulut hizmetindeki bilgilere erişimin, erişim kontrol politikasına uygun olarak kısıtlanabileceğinden ve bu kısıtlamaların uygulandığından emin midir?				
Destek programlarının kullanımına izin verildiği yerlerde, kurum kendi bulut bilişim ortamında kullanılacak olan destek programlarını tanımlamış ve bunların bulut hizmetinin kontrolleri ile çatışmadığını temin etmiş midir?				
Bulut hizmetlerinin kullanımına yönelik kriptografik kontroller uygulanmakta mıdır?				
Kurum, bulut hizmeti için kriptografik anahtarları tanımlamakta ve anahtar yönetimi için prosedürler uygulamakta mıdır?				

Kaynakların güvenli olarak imhası veya yeniden kullanılmasına yönelik bulut hizmeti sağlayıcısının politikalara ve prosedürlere sahip olduğunu doğrulamış mıdır?				
Kurumun değişiklik yönetimi süreci, bulut hizmeti sağlayıcısı tarafından yapılan herhangi bir değişikliğin etkilerini hesaba katmakta mıdır?				
Kurum, bulut hizmetince sağlanan mutabık kalınan kapasitenin, kurumun gerekliliklerini karşıladığından emin midir?				
Yedekleme işlevi bulut hizmetinin bir parçası olarak alınıyorsa, sağlayıcıdan yedekleme işlevinin teknik özellikleri talep edilmiş midir?				
Olay kaydetme için gereksinimler tanımlamış ve bulut hizmetinin bu gereksinimleri karşıladığı doğrulanmış mıdır?				
Eğer kuruma ayrıcalıklı bir işlem yetkisi devredilmişse, bu işlemlerin işlem ve performansı kayıt altına alınmakta mıdır? Sağlayıcı tarafından sağlanan kayıt tutma işlevlerinin uygun olup olmadığı veya kurumun ek kayıt tutma işlevleri uygulaması gerekip gerekmediği belirlenmiş midir?				
Kurum bulut hizmeti sağlayıcısının sistemleri için kullandığı saat senkronizasyonu hakkında bilgi talep etmiş midir?				
Bulut hizmetlerini etkileyebilecek teknik zafiyetlerin yönetilmesi hakkında sağlayıcıdan bilgi talep edilmiş midir? Kurum, yönetmekten sorumlu olacağı teknik zafiyetleri belirlemiş ve bunları yönetmeye yönelik süreçleri tanımlamış mıdır?				
Paylaşılan bir bulut ortamında ağların ayrılmasına yönelik gereklilikler tanımlamış ve sağlayıcının bu gereklilikleri karşıladığı doğrulanmış mıdır?				
Bulut hizmeti için bilgi güvenliği gereksinimleri belirlenmiş midir? Alınan hizmetlerin bu gereksinimleri karşılayıp karşılamadığı değerlendirilmiş midir?				
Güvenli geliştirme prosedürleri ve uygulamaların kullanımı hakkında, sağlayıcıdan bilgi talep edilmiş midir?				
Bulut hizmeti sağlayıcısı, tedarikçi ilişkilerine yönelik bilgi güvenliği politikası içerisine bir tedarikçi türü olarak dâhil edilmiş midir?				
Hizmet anlaşmasında tarif edildiği şekilde, bulut hizmetiyle ilgili bilgi güvenliği rolleri ve sorumlulukları teyit edilmiş midir?				
Bilgi güvenliği ihlali olayının yönetimi için sorumlulukların belirlenmiş olduğunu doğrulanmış ve bunun kurumun gereksinimlerini karşıladığı doğrulanmış mıdır?				
Kurum, bulut hizmeti sağlayıcısından aşağıdaki mekanizmalar hakkında bilgi talep etmiş midir? - kurumun, tespit ettiği bir bilgi güvenliği olayını bulut hizmeti sağlayıcısına bildirmesi; - bulut hizmeti sağlayıcısının, kurum tarafından tespit edilen bir bilgi güvenliği olayı ile ilgili raporları alması; - kurumun, raporlanan bir bilgi güvenliği olayının durumunu izlemesi.				
Sağlayıcı ile bulut bilişim ortamından gelen olası dijital kanıt veya başka bilgi taleplerine yanıt vermeye yönelik prosedürler üzerinde anlaşmaya varılmış mıdır?				
Bulut hizmeti sağlayıcısı için geçerli hukuk sisteminin yasaları ve düzenlemeleri olabileceği hususu dikkate alınmakta mıdır? İş için gerekli olan düzenlemelere ve standartlara, bulut hizmeti sağlayıcısı uyumlu mudur?				
Buluta özgü lisans hakkı gerekliliklerini tanımlamaya yönelik bir prosedür hazırlanmış mıdır?				
Bulut hizmeti sağlayıcısı tarafından toplanan ve depolanan kayıtların korunması hakkında sağlayıcıdan bilgi talep edilmiş midir?				
Bulut hizmetinin kullanımında geçerli olan kriptografik kontroller dizisinin, ilgili anlaşmalar, yasalar ve düzenlemelere uygun olduğunu doğrulanmış mıdır?				
Bulut hizmeti sağlayıcısından bilgi güvenliği kontrolleri ve yönergeleri uygulaması ile ilgili kanıt talep edilmiş midir?				
Kurum, bulut hizmeti kullanımındaki rollerini ve sorumluluklarını belgelemiş midir?				
Sözleşme sona erdiğinde varlıkların sağlayıcı sistemlerinden silinmesi ile ilgili bilgi alınmış mıdır?				

Sanal makine sıkılaştırılması ile ilgili teknik bilgi alınmış mıdır?				
Bulut bilişim ortamındaki yönetimsel işlemlere yönelik prosedürler belgelenmiş midir?				
Bulut hizmetlerinin izlenebilmesi için sağlayıcıdan bilgi alınmış mıdır?				
	Denetim Bulgusu			
Bulut Hizmeti Sağlayıcısı Kontrol Maddesi	Yok	Var ama yetersiz	Yeterli	Not
Kurumun bulut bilişime özel bir bilgi güvenliği politikası var mıdır?				
Kurum, bulut hizmeti müşterileriyle, bulut hizmeti sağlayıcılarıyla ve tedarikçileriyle, bilgi güvenliği rol ve sorumluluklarının uygun şekilde tahsisi üzerinde anlaşmış mıdır?				
Kullanılan coğrafi konumlar ve müşteri verilerinin saklayabileceği ülkeler hakkında müşteriler bilgilendirilmekte midir?				
Müşteri verilerinin ve bulut hizmetinden türeyen verilerin uygun şekilde ele alınması ile ilgili, çalışanlara farkındalık, eğitim ve öğretimi sağlamakta mıdır?				
Varlık envanterinde, bulut hizmeti müşteri verileri ve bulut hizmetinden türeyen veriler tanımlanmış mıdır?				
Kurum, müşterilerinin bilgilerini ve ilişkili varlıklarını sınıflandırmasına ve etiketlemesine olanak sağlayan, sağladığı her tür hizmet fonksiyonunu belgelemiş ve bildirmiş midir?				
Kullanıcı kaydetme ve kayıt silme fonksiyonlarını ve bu fonksiyonların kullanımına ilişkin teknik özellikleri müşteriye sağlamakta mıdır?				
Müşterinin kullanıcılarının erişim haklarını yönetmesi için fonksiyonlar ve bu fonksiyonların kullanımına ilişkin teknik özellikler sağlanmış mıdır?				
Müşterinin bulut hizmeti yöneticilerine, tanımlanmış risklere göre yeterli kimlik doğrulama teknikleri sağlanmakta mıdır?				
Gizli kimlik doğrulama bilgilerinin yönetimine dair prosedürler hakkında müşteriye bilgi sağlanmakta mıdır?				
Müşterinin kendi bulut hizmetlerine, fonksiyonlarına ve verilerine erişimi kısıtlamasına olanak tanıyan erişim kontrolleri sağlanmakta mıdır?				
Bulut hizmeti içinde kullanılan her tür destek programı için gereklilikler tanımlanmış mıdır?				
Kriptografi kullanılan durumlarla ilgili bulut hizmeti müşterisine bilgi verilmekte midir?				
Kaynakların güvenli olarak imhası veya yeniden kullanılması için gerekli düzenlemelerin zamanında yapılmakta mıdır?				
Bulut servisini olumsuz olarak etkileyebilecek değişikliklerle ilgili bilgiler müşteriye sağlanmakta mıdır?				
Toplam kaynak kapasitesi izlenmekte midir?				
Sunulan yedekleme işlevlerinin teknik özellikleri müşteriye sağlanmakta mıdır?				
Kurum bulut hizmeti müşterisine kayıt tutma işlevlerini sağlayabilecek midir?				
Müşterinin yerel saati ile bulut hizmeti saatinin nasıl senkronize edebileceğine ilişkin bilgi verilmekte midir?				
Bulut hizmetlerini etkileyebilecek teknik zafiyetlerin yönetilmesi hakkında müşteriye bilgi sağlanmakta mıdır?				
Kurum, ağlarda ayrım için; çok kullanıcılı (multi-tenant) bir ortamda kullanıcılar arasında ayrım ve kurumun iç yönetim ortamı ve bulut hizmeti müşterisinin bulut bilişim ortamı arasında ayrımı sağlamakta mıdır?				
Müşteriye, kullanılan bilgi güvenliği yetileri hakkında bilgi sağlanmakta mıdır?				
Güvenli geliştirme prosedürleri ve uygulamaların kullanımı hakkında müşteriye bilgi sağlamakta mıdır?				
Bilgi güvenliği önlemleri müşteri ile yapılan sözleşmenin bir parçası olarak belirtilmekte midir?				
Eş (peer) bulut hizmeti sağlayıcı hizmeti kullanıldığında, müşterilerin bilgi güvenliği seviyelerinin eş düzeyde ya da fazlasının sağlandığı temin edilmekte midir? Bulut hizmetleri bir tedarik zincirine dayalı olarak tedarik ediliyorsa, tedarikçilere bilgi güvenliği hedefleri sunulmakta ve hedeflere erişilmesi için risk yönetimi gerçekleştirmesi talep edilmekte midir?				

Bilgi güvenliği ihlali olayının yönetim sorumluluklarının tahsisine ve ilgili prosedürlere ilişkin hususlar tanımlanmakta mıdır?				
Bulut hizmeti müşterisi aşağıdakiler için gerekli mekanizmaları sağlamakta mıdır? - bulut hizmeti müşterisinin, bir bilgi güvenliği olayını bulut hizmeti sağlayıcısına raporlaması; - bulut hizmeti sağlayıcısının bir bilgi güvenliği olayını bir bulut hizmeti müşterisine raporlaması; - bulut hizmeti müşterisinin, raporlanan bir bilgi güvenliği olayının durumunu izlemesi.				
Bulut bilişim ortamından gelen olası dijital kanıt veya başka bilgi taleplerine yanıt vermeye yönelik müşteriyle prosedürler üzerinde anlaşmaya varılmış mıdır?				
Müşteri, bulut hizmetini yöneten yasal hukuk sistemler konusunda bilgilendirilmekte midir? Kurum kendi ilgili yasal gerekliliklerini (ör. kişisel verileri (PII) korumak için şifrelemeyle ilgili olanlar) belirlemiş midir?				
Fikri mülkiyet hakları şikayetlerine yanıt vermeye yönelik bir süreç kurulmuş mudur?				
Müşterinin kullanımına ilişkin toplanan ve depolanan kayıtların korunması hakkında müşteriye bilgi sağlanmakta mıdır?				
Kurum tarafından uygulanan kriptografik kontroller müşteriye açıklanmakta mıdır?				
Bilgi güvenliği kontrollerinin uygulanmasına dair müşteriye belgelenmiş kanıt sağlanmakta mıdır?				
Müşterinin bulut hizmeti kullanımına yönelik bilgi güvenliği yetileri, rolleri ve sorumlulukları belgelenmiş midir?				
Bulut hizmetleri için uygulama yönergesi sağlanmakta mıdır?				
Paylaşılan sanal bulut bilişim ortamı kullanılırken bilgi güvenliği risklerinin azaltılmakta mıdır?				
Bulut hizmeti üzerinde çalışan sanal ortam, diğer bulut hizmeti müşterilerinden ve yetkisiz kişilerden korunmakta mıdır?				
Bulut ortamındaki sanal makineler için sıkılaştırma yapılmakta mıdır?				
Kritik işlemler ve prosedürler hakkında belgelendirme var mıdır?				
Bulut Hizmetlerinin izlenmesi ilgili işlevler sağlanmakta mıdır?				
Sanal ve fiziksel ağlar için güvenlik yönetiminin uyumlulaştırılması belgelendirilmiş midir?				

6. Uygulandığı Takdirde Standardın İlgili Organizasyona Sağlayabileceği Kazanımlar

- Bulut hizmeti kullanıcıları için rolleri ve sorumlulukları özetler.
- Çevrimiçi operasyonlar ve mimari hakkında daha kapsamlı bir anlayış sağlar.
- Bulutta işlenen bilgilerin güvenli olduğuna dair güvence sağlar.
- Güvenlik ihlali riskinin ve diğer risklerin azaltılmasına yardımcı olur.
- Müşteriler için kapsamlı bir bilgi güvenliği yönetimi çerçevesi sağlar, sağlayıcıları da sorumlu tutar.
- ISO 27001 sertifikasını genişletir ve geliştirir.
- Sağlayıcılar için kapsamlı bir bilgi güvenliği yönetimi çerçevesi sağlar.
- Bulut müşterilerine bulut hizmeti sağlayıcılarından ne beklenmesi gerektiği konusunda pratik bilgiler sağlar.