

Doküman Kodu: BGYS-009

TS ISO/IEC 27001 DENETİM LİSTESİ

SÜRÜM 1.10

21.02.2008

Hazırlayan: Fikret Ottekin

ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nin misyonu, "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile, bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaşılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı araştırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sağlanmaktadır.

Bu doküman, BGYS (Bilgi Güvenliği Yönetim Sistemi) kurmak isteyen kurumlar için yardımcı kaynak olarak hazırlanmıştır. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

Bu dokümanda anlatılanlar tamamen tavsiye niteliğindedir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu değildir. Bu doküman UEKAE'nin izni olmadan değiştirilemez.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeđi geen Ađ Güvenliđi personeline ve dokümanı gözden geirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Ali Dinkan'a ve Fatih Ko'a teřekkürü bor biliriz.

İÇİNDEKİLER

1. GİRİŞ	5
1.1 Amaç ve Kapsam.....	5
1.2 Hedeflenen Kitle.....	5
1.3 Kısaltmalar.....	5
2. TS ISO/IEC 27001 DENETİM LİSTESİ	6
GÜVENLİK POLİTİKASI	6
BİLGİ GÜVENLİĞİ ORGANİZASYONU	8
VARLIK YÖNETİMİ	12
PERSONEL GÜVENLİĞİ	15
FİZİKSEL VE ÇEVRESEL GÜVENLİK	18
İLETİŞİM VE İŞLETME YÖNETİMİ	25
ERİŞİM DENETİMİ	41
BİLGİ SİSTEMİ TEDARİĞİ, GELİŞTİRİLMESİ VE BAKIMI	53
BİLGİ GÜVENLİĞİ OLAYLARI YÖNETİMİ	61
İŞ SÜREKLİLİĞİ YÖNETİMİ	65
UYUM	69

1. GİRİŞ

ISO 27001 standardı BGYS kurmak isteyen kuruluşun risk analizi çalışmasının ardından çeşitli kontrolleri devreye sokarak mevcut riskleri tedavi etmesini ve kabul edilebilir risk seviyesinin altına indirmesini şart koşturmaktadır. Bu kontroller 27001 standardı içerisinde “vazgeçilemez doküman” olarak gösterilen ISO 27002 standardında detaylı olarak açıklanmaktadır.

1.1 Amaç ve Kapsam

Bu doküman esasen ISO 27002 standardının düz yazı formatından anket formatına dönüştürülmüş bir özetidir. Dokümanın amacı bir kurumun ISO 27002 kontrolleri açısından durumunu tespit etmekle görevli uzman veya uzmanları desteklemektir.

1.2 Hedeflenen Kitle

Doküman, kurumlarının hali hazırda 27002 kontrolleri açısından ne durumda olduğunu tespit etmek isteyen BGYS uygulamacıları, BGYS çalışmalarını denetlemek isteyen kurum yönetimi, iç tetkik görevlileri veya dış tetkik elemanları tarafından kullanılabilir.

1.3 Kısaltmalar

BGYS : **Bilgi Güvenliği Yönetim Sistemi**

UEKAE : **Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü**

2. TS ISO/IEC 27001 DENETİM LİSTESİ

GÜVENLİK POLİTİKASI					
Referans		Denetim alanı, hedefi ve sorusu		Sonuçlar	
Kontrol listesi	Standart	Bölüm	Denetim sorusu	Bulgular	Uyumluluk
1.1	5.1	Bilgi Güvenliği Politikası			
1.1.1	5.1.1	Bilgi güvenliği politikası belgesi (idari) <i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi uygulamalar" arasında gösterilmiştir)</i>	Üst yönetim tarafından onaylanmış bilgi güvenliği politikası belgesi var mı? Bu belge yayınlanmış ve tüm çalışanlara ulaştırılması sağlanmış mı? Bilgi güvenliği politikası üst yönetimin bilgi güvenliği yönetimi ile ilgili taahhüdünü ve kurumsal yaklaşımı yansıtıyor mu?		
1.1.2	5.1.2	Bilgi güvenliği politikasının gözden geçirilmesi	Politikanın sahibi, tanımlanmış bir süreç eşliğinde belgeyi gözden geçiriyor mu? Gözden geçirme süreci, önemli değişikliklerin olması durumunda gözden geçirmenin olmasını sağlayacak şekilde mi? (Örnek: Önemli güvenlik olayları, yeni		

		(idari)	<p>açıklıklar ya da kurumsal, teknik altyapıda olan değişiklikler)</p> <p>Bilgi güvenliği politikasının geliştirilmesi, değerlendirilmesi ve gözden geçirilmesinden sorumlu biri var mı? (Bilgi Güvenliği politikasının sahibi) Politika sahibinin sorumlulukları yönetim tarafından onaylanmış mı?</p> <p>Bilgi güvenliği politikasının gözden geçirilmesi ile ilgili prosedür var mı? Bu prosedür yönetimin gözden geçirme sürecine katılmasını öngörüyor mu?</p> <p>Yönetimin gözden geçirmesi sonucunda</p> <ul style="list-style-type: none">- Bilgi güvenliğine kurumsal yaklaşım,- Uygulanan kontroller ve- Bilgi güvenliği için kaynak ayrılması ve sorumluların atanması <p>konularında iyileşme sağlanıyor mu?</p> <p>Yönetimin gözden geçirmesi ile ilgili kayıtlar saklanıyor mu?</p> <p>Yeni güvenlik politikası yönetimin onayına sunuluyor mu?</p>		
--	--	---------	---	--	--

BİLGİ GÜVENLİĞİ ORGANİZASYONU					
Referans		Denetim alanı, hedefi ve sorusu		Sonuçlar	
Kontrol listesi	Standart	Bölüm	Denetim sorusu	Bulgular	Uyumluluk
2.1	6.1	Kurum İçi Organizasyon			
2.1.1	6.1.1	Yönetimin bilgi güvenliği taahhüdü (idari)	Yönetim, kurum içinde uygulanacak güvenlik tedbirlerini aktif olarak destekliyor mu? Destek, bilgi güvenliliği ile ilgili hedeflerin belirlenmesi, kurumun taahhütte bulunması ve sorumluların atanması ile verilebilir.		
2.1.2	6.1.2	Bilgi güvenliği koordinasyonu (idari)	Bilgi güvenliği çalışmalarının koordinasyonu, kuruluşun farklı bölümlerinden gelen yetkililer tarafından gerçekleştiriliyor mu?		
2.1.3	6.1.3	Bilgi güvenliği sorumluluklarının atanması (idari) <i>(ISO 27002:2005 standardının "0.6 Bilgi</i>	Kişisel varlıkların korunması ve belirli güvenlik süreçlerinin yürütülmesi için sorumluluklar açıkça tanımlanmış mı? (Bilgi güvenliği sorumlulukları tanımlanmış mı? İş tanımlarına bilgi güvenliği sorumlulukları eklenmiş mi?)		

		<i>güvenliğine giriş” başlığı altında “umumi uygulamalar” arasında gösterilmiştir)</i>			
2.1.4	6.1.4	Bilgi işleme araçları için yetkilendirme süreci (idari)	Yazılım, Donanım vb. yeni bilgi işlem araçları sisteme eklenirken kullanım amacı ve şekli göz önünde bulundurularak yönetim onayından geçiriliyor mu? Yeni araçlar tüm güvenlik politikaları ile uyumlu mu ve tüm güvenlik ihtiyaçlarına cevap veriyor mu?		
2.1.5	6.1.5	Gizlilik anlaşmaları (idari)	Kuruluşun bilgi varlıklarını korumak için yapmak zorunda olduğu gizlilik anlaşmaları ile ilgili ihtiyaçları açık olarak tanımlanmış durumda mıdır ve gözden geçirilmekte midir? Gizlilik anlaşmaları bilginin yasal yollarla korunması için gerekli şartları içeriyor mu?		
2.1.6	6.1.6	Otoritelerle iletişim (idari)	Gerektiğinde emniyet, itfaiye vb. kuruluşlarla kimin ne zaman irtibat kuracağını ve olayın nasıl rapor edileceğini tarif eden bir prosedür mevcut mu?		
2.1.7	6.1.7	Uzmanlık grupları ile iletişim	Kuruluş güvenlik konusunda uzmanlaşmış forum, topluluklar ve profesyonel derneklerle irtibat halinde mi?		

		(idari)			
2.1.8	6.1.8	Bilgi güvenliğinin bağımsız olarak gözden geçirilmesi (idari)	Organizasyon içerisindeki uygulama ile güvenlik politikası esaslarının aynı olduğu, güvenlik politikasının etkin ve uygulanabilir olduğu düzenli bir şekilde bağımsız bir kurum veya kuruluş tarafından veya kurum içinden bağımsız bir denetçi aracılığıyla denetleniyor mu? Gözden geçirmenin sonuçları kaydediliyor ve yönetime bildiriliyor mu?		
2.2	6.2	Üçüncü Taraf Erişiminin Güvenliği			
2.2.1	6.2.1	Üçüncü taraf erişiminde risklerin tanımlanması (idari)	Bilgi sistemlerine üçüncü tarafların erişiminden kaynaklanacak riskler belirleniyor ve erişim hakkı verilmeden önce bununla ilgili tedbirler alınıyor mu? Kurum içerisinde görevlendirilmiş üçüncü parti çalışanlar için riskler belirlenmiş ve bunun için uygun kontroller uygulamaya geçirilmiş midir?		
2.2.2	6.2.2.	Müşterilerle çalışırken güvenlik (idari)	Müşterilere kuruluşun bilgi veya varlıklarına erişme hakkı verilmeden önce güvenlik ihtiyaçları ile ilgili tedbirler alınıyor mu?		

2.2.3	6.2.3	Üçüncü taraf sözleşmelerinde güvenlik gerekleri (idari)	Üçüncü tarafın kuruma ait bilgi veya bilgi işlem araçları ile ilgili erişim, işlem veya iletişimi ile ilgili düzenlemeler yapan sözleşmelerde kurumun güvenlik ihtiyaçları karşılanıyor mu?		
-------	-------	---	---	--	--

VARLIK YÖNETİMİ					
Referans		Denetim alanı, hedefi ve sorusu		Sonuçlar	
Kontrol listesi	Standart	Bölüm	Denetim sorusu	Bulgular	Uyumluluk
3.1	7.1	Varlıklarla ilgili sorumluluklar			
3.1.1	7.1.1	Varlık envanteri (idari)	<p>Önemli tüm bilgi varlıklarını içeren bir varlık envanteri tutuluyor mu? Envanter hazırlanırken aşağıda belirtilen varlık türlerinin tamamı göz önünde bulundurulmuş mu?</p> <ul style="list-style-type: none"> - Bilgi: Veri Tabanı, sözleşme ve anlaşmalar, sistem dokümantasyonu vb. - Yazılım varlıkları: Uygulama yazılımları, sistem yazılımları ve yazılım geliştirme araçları. - Fiziksel varlıklar: Bilgisayarlar ve iletişim araçları. - Hizmete dönük varlıklar: Bilgisayar ve iletişim hizmetleri, ısıtma, aydınlatma, güç vb. - Personel: Nitelik ve tecrübeleri ile birlikte. - Soyut varlıklar: Kuruluşun itibarı ve imajı gibi. <p>Varlık envanteri herhangi bir afetten sonra normal çalışma şartlarına dönmek için gereken (varlığın türü, formatı, konumu, değeri gibi) tüm bilgileri içermelidir.</p>		-

3.1.2	7.1.2	Varlıkların sahipleri (idari)	Bütün varlıkların sahibi var mı? Varlıkların sahipleri aracılığı ile a) Her varlığın tanımlı ve onaylı bir güvenlik sınıfı ve erişim kısıtlamasına sahip olması ve b) Bunların her varlık için periyodik olarak gözden geçirilmesi güvence altına alınıyor mu?		-
3.1.3	7.1.3	Varlıkların kabul edilebilir bir biçimde kullanılması (idari)	Bilgi işlem araçları ile ilgili bilgi ve varlıkların kabul edilebilir kullanımları ile ilgili düzenlemeler yapılmış mı? Bu düzenlemeler belgelenmiş mi ve uygulanıyor mu? a) E-posta ve internet kullanımına ait düzenleme var mı? b) Mobil cihazların kullanımı konusunda bir düzenleme var mı? c) Taşınabilir depolama ortamlarının kullanımına ait bir düzenleme var mı?		
3.2	7.2	Bilgi Sınıflandırması			
3.2.1	7.2.1	Sınıflandırma rehberleri (idari)	Bilgi varlıkları değeri, yasal durumu ve hassasiyeti göz önünde bulundurularak sınıflandırılmış mı? Yönetim tarafından onaylanmış bir sınıflandırma dokümanı var mı?		
3.2.2	7.2.2	Bilginin	Kurumun benimsediği bilgi sınıflandırma planına göre		

		etiketlenmesi ve işlenmesi (idari)	bilginin etiketlenmesi ve idare edilmesi için prosedürler tanımlanmış mı? Bu prosedürler uygulanıyor mu?		
--	--	---------------------------------------	---	--	--

PERSONEL GÜVENLİĞİ					
Referans		Denetim alanı, hedefi ve sorusu		Sonuçlar	
Kontrol listesi	Standart	Bölüm	Denetim sorusu	Bulgular	Uyumluluk
4.1	8.1	İşe almadan önce			
4.1.1	8.1.1	Roller ve sorumluluklar (idari)	Kurumun bilgi güvenliği politikası uyarınca personele düşen güvenlik rol ve sorumlulukları belgelenmiş mi? İşe alınacak personele yüklenecek rol ve sorumluluklar açıkça tanımlanmış ve işe alınmadan önce personel tarafından iyice anlaşılması sağlanmış mı?		
4.1.2	8.1.2	Personel gözetleme (idari)	İş başvurularında, işe alınacak personel için doğrulama testleri yapılıyor mu? Doğrulama testleri iddia edilen akademik ya da profesyonel vasıfların doğruluğunu ve bağımsız kimlik doğrulama testlerini kapsıyor mu?		
4.1.3	8.1.3	İşe alınmanın şartları	Kurum çalışanlarının gizlilik ve açığa çıkarmama (non-disclosure) anlaşmalarını işe alınma şartının bir parçası		

		(idari)	olarak imzalamaları isteniyor mu? Bu anlaşma işe alınan personelin ve kuruluşun bilgi güvenliği sorumluluklarını kapsıyor mu?		
4.2	8.2	Çalışma Sırasında			
4.2.1	8.2.1	Yönetimin sorumlulukları (idari)	Yönetim, çalışanlarından ve üçüncü parti kullanıcılarından uygulamakta olduğu politika ve prosedürler uyarınca güvenlik tedbirlerini almalarını istiyor mu?		
4.2.2	8.2.2	Bilgi güvenliği bilinci ve eğitim (idari) <i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi uygulamalar" arasında gösterilmiştir)</i>	Kurumun tüm çalışanları ve üçüncü parti kullanıcıları uygun bilgi güvenliği eğitimlerini alıyorlar mı? Kurumsal politika ve prosedürlerdeki değişikliklerden haberdar ediliyorlar mı?		
4.2.3	8.2.3	Disiplin süreci (idari)	Kurum çalışanlarının, güvenlik politika ve prosedürlerine uymaması durumunda devreye girecek bir disiplin süreci var mı?		
4.3	8.3	Görev değişikliği veya işten ayrılma			
4.3.1	8.3.1	Ayrılma ile ilgili	İşten ayrılma veya görev değişikliği sırasında yapılması		

		sorumluluklar (idari)	gerekenler açık olarak belirlenmiş ve ilgili kişilere sorumlulukları bildirilmiş mi?		
4.3.2	8.3.2	Varlıkların iade edilmesi (idari)	İşten ayrılma, kontratın veya anlaşmanın sona ermesi halinde kurum çalışanlarının veya üçüncü parti kullanıcılarının üstünde bulunan kuruluşa ait tüm varlıkların iade edilmesini sağlayan bir süreç mevcut mu?		
4.3.3	8.3.3	Erişim haklarının kaldırılması (idari + teknik)	İşten ayrılma, kontratın veya anlaşmanın sona ermesi halinde veya görev değişikliği halinde kurum çalışanlarının veya üçüncü parti kullanıcılarının kuruluşun bilgi varlıklarına veya bilgi işlem araçlarına erişim hakları kaldırılıyor veya gerektiği şekilde yeniden düzenleniyor mu?		

FİZİKSEL VE ÇEVRESEL GÜVENLİK					
Referans		Denetim alanı, hedefi ve sorusu		Sonuçlar	
Kontrol listesi	Standart	Bölüm	Denetim sorusu	Bulgular	Uyumluluk
5.1	9.1	Güvenlik Alanı			
5.1.1	9.1.1	Fiziksel güvenlik sınırı (idari + teknik)	Bilgi işleme servisini korumak amacıyla herhangi bir fiziksel sınır güvenliği tesisi kurulmuş mu? (kart kontrollü giriş, duvarlar, insanlı nizamiye) Fiziksel sınır güvenliği, içindeki bilgi varlıklarının güvenlik ihtiyaçları ve risk değerlendirme sürecinin sonucuna göre oluşturulmuş mu?		
5.1.2	9.1.2	Fiziksel giriş kontrolleri (idari + teknik)	Kurum içerisinde belli yerlere sadece yetkili personelin girişine izin verecek şekilde kontrol mekanizmaları kurulmuş mu? a) Ziyaretçilerin giriş ve çıkış zamanları kaydediliyor mu? b) Hassas bilgilerin bulunduğu alanlar (kimlik doğrulama kartı ve PIN koruması gibi yöntemlerle) yetkisiz erişime kapatılmış mı? c) Tüm personel ve ziyaretçiler güvenlik elemanları		

			<p>tarafından rahatça teşhis edilmelerini sağlayacak kimlik kartlarını devamlı takıyorlar mı?</p> <p>d) Güvenli alanlara erişim hakları düzenli olarak gözden geçiriliyor mu?</p>		
5.1.3	9.1.3	<p>Ofislerin ve odaların güvenliğinin sağlanması (idari + teknik)</p>	<p>Ofisler ve odalarla ilgili fiziksel güvenlik önlemleri alınmış mı?</p> <p>a) Personel güvenliği ve sağlığı ile ilgili yönetmelikler uygulanmış mı?</p> <p>b) Kritik tesisler kolayca ulaşılamayacak yerlere kurulmuş mu?</p> <p>c) Binada bilgi işlem faaliyetlerinin yürütüldüğüne dair işaret, tabela vb. bulunmamasına dikkat edilmiş mi?</p> <p>d) Bilgi işlem merkezlerinin konumunu içeren dâhili/harici telefon rehberleri halka kapalı mı?</p>		
5.1.4	9.1.4	<p>Harici ve çevresel tehditlerden korunma (idari + teknik)</p>	<p>Yangın, sel, deprem, patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınmış ve uygulanmakta mıdır?</p> <p>a) Komşu tesislerden kaynaklanan potansiyel tehdit var mı?</p> <p>b) Yedeklenmiş materyal ve yedek sistemler ana tesisten yeterince uzak bir yerde konuşlandırılmış mı?</p>		

5.1.5	9.1.5	Güvenli alanlarda çalışma (idari + teknik)	Güvenli bir alanın mevcut olduğu ile ilgili olarak veya burada yürütülmekte olan çeşitli faaliyetlerle ilgili olarak personel ve üçüncü parti çalışanları için “İhtiyacı kadar bilme” prensibi uygulanıyor mu? Kayıt cihazlarının güvenli alanlara sokulmasına engel olunuyor mu? Kullanılmayan güvenli alanlar kilitleniyor ve düzenli olarak kontrol ediliyor mu? Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara nezaret ediliyor mu?		
5.1.6	9.1.6	Halka açık alanlardan, yükleme ve dağıtım alanlarından erişim (idari + teknik)	Bilgi işlem servisleri ile a) Dağıtım ve yükleme alanları ve b) Yetkisiz kişilerin tesislere girebileceği noktalar birbirinden izole edilmiş mi?		
5.2	9.2	Ekipman Güvenliği			
5.2.1	9.2.1	Ekipman	Ekipman yerleşimi yapılırken çevresel tehditler ve yetkisiz		

		yerleşimi ve koruması (idari + teknik)	erişimden kaynaklanabilecek zararların asgari düzeye indirilmesine çalışılmış mı? a) Ekipman, gereksiz erişim asgari düzeye indirilecek şekilde yerleştirilmiş mi? b) Kritik veri içeren araçlar yetkisiz kişiler tarafından gözlenemeyecek şekilde yerleştirilmiş mi? c) Özel koruma gerektiren ekipman izole edilmiş mi? d) Nem ve sıcaklık gibi parametreler izleniyor mu? e) Hırsızlık, yangın, duman, patlayıcılar, su, toz, sarsıntı, kimyasallar, elektromanyetik radyasyon, sel gibi potansiyel tehditlerden kaynaklanan riskleri düşürücü kontroller uygulanmış mı? Paratoner var mı? f) Bilgi işlem araçlarının yakınında yeme, içme ve sigara içme konularını düzenleyen kurallar var mı?		
5.2.2	9.2.2	Destek hizmetleri (idari + teknik)	Elektrik, su, kanalizasyon ve iklimlendirme sistemleri destekledikleri bilgi işlem dairesi için yeterli düzeyde mi? a) Elektrik şebekesine yedekli bağlantı, kesintisiz güç kaynağı gibi önlemler ile ekipmanları elektrik arızalarından koruyacak tedbirler alınmış mı? Yedek jeneratör ve jeneratör için yeterli düzeyde yakıt var mı? b) Su bağlantısı iklimlendirme ve yangın söndürme sistemlerini destekleyecek düzeyde mi? c) Acil durumlarda iletişimin kesilmemesi için servis sağlayıcıdan iki bağımsız hat alınmış mı? Kurum bu konuda yasal yükümlülüklerini yerine getirmiş mi?		

5.2.3	9.2.3	Kablolama güvenliği (idari + teknik)	Güç ve iletişim kablolarının fiziksel etkilere ve dinleme faaliyetlerine karşı korunması için önlemler alınmış mı? a) Kablolar yeraltında mı? b) Karışmanın (“interference”) olmaması için güç kabloları ile iletişim kabloları ayrılmış mı? c) Hatalı bağlantıların olmaması için ekipman ve kablolar açıkça etiketlenmiş ve işaretlenmiş mi? Hassas ve kritik bilgiler için ekstra güvenlik önlemleri alınmış mı? d) Alternatif yol ve iletişim kanalları mevcut mu? e) Fiber optik altyapı mevcut mu? f) Bağlantı panelleri ve odalara kontrollü erişim altyapısı kurulmuş mu?		
5.2.4	9.2.4	Ekipman bakımı (idari + teknik)	Ekipmanın bakımı doğru şekilde yapılıyor mu? a) Ekipmanın bakımı, üreticinin tavsiye ettiği zaman aralıklarında ve üreticinin tavsiye ettiği şekilde yapılıyor mu? b) Bakım sadece yetkili personel tarafından yapılıyor mu? c) Tüm şüpheli ve mevcut arızalar ve bakım çalışmaları için kayıt tutuluyor mu? d) Ekipman bakım için kurum dışına çıkarılırken kontrolden geçiyor mu? İçindeki hassas bilgiler siliniyor mu? e) Ekipman sigortalıysa, gerekli sigorta şartları		

			sağlanıyor mu?		
5.2.5	9.2.5	Kurum dışı ekipmanın güvenliği (idari + teknik)	<p>Kurum alanı dışında bilgi işleme için kullanılacak ekipman için yönetim tarafından yetkilendirme yapılıyor mu?</p> <p>a) Tesis dışına çıkarılan ekipmanın başıboş bırakılmamasına, seyahat halinde dizüstü bilgisayarların el bagajı olarak taşınmasına dikkat ediliyor mu?</p> <p>b) Cihazın muhafaza edilmesi ile ilgili olarak üretici firmanın talimatlarına uyuluyor mu?</p> <p>c) Evden çalışma ile ilgili tedbirler alınmış mı?</p> <p>d) Sigorta cihazların tesis dışında korunmasını kapsıyor mu?</p> <p>Kurum alanı dışında kullanılacak ekipmanlar için uygulanacak güvenlik önlemleri, tesis dışında çalışmaktan kaynaklanacak farklı riskler değerlendirilerek belirlenmiş mi?</p>		
5.2.6	9.2.6	Ekipmanın güvenli imhası ya da tekrar kullanımı (idari + teknik)	<p>a) Ekipman imha edilmeden önce gizli bilginin bulunduğu depolama cihazı fiziksel olarak imha ediliyor mu?</p> <p>b) Depolama cihazının içerdiği bilginin bir daha okunamaması için klasik silme veya format işlemlerinin ötesinde yeterli düzeyde işlem yapılıyor mu?</p>		
5.2.7	9.2.7	Varlıkların	Ekipman, bilgi veya yazılımın yetkilendirme olmadan tesis		

		kurumdan çıkarılması (idari + teknik)	dışına çıkarılmamasını sağlayan kontrol mekanizması oluşturulmuş mu? Kurum varlıklarının yetkisiz olarak kurum dışına çıkarıldığını saptamak için denetleme yapılıyor mu? Kurum çalışanları bu tip denetlemelerden haberdar mı?		
--	--	---	---	--	--

İLETİŞİM VE İŞLETME YÖNETİMİ					
Referans		Denetim alanı, hedefi ve sorusu		Sonuçlar	
Kontrol listesi	Standart	Bölüm	Denetim sorusu	Bulgular	Uyumluluk
6.1	10.1	İşletme Prosedürleri ve Sorumluluklar			
6.1.1	10.1.1	Belgelenmiş işletme prosedürleri (idari)	<p>İşletme prosedürleri yazılmış mı ve güncelleniyor mu?</p> <p>Bilgi işlem ve iletişim ile ilgili</p> <p>a) Sistem açma/kapama, b) Yedekleme, c) Cihazların bakımı, d) Bilgisayar odasının kullanılması,</p> <p>gibi sistem faaliyetleri prosedürlere bağlanmış mı?</p> <p>İşletme prosedürlerine, ihtiyacı olan tüm kullanıcılar erişebiliyor mu?</p> <p>Bu prosedürlere resmi belge muamelesi yapılıyor mu? (Yapılan tüm değişiklikler için yönetim yetkilendirmesi gerekiyor mu?)</p>		
6.1.2	10.1.2	Değişim kontrolü	Bilgi işlem sistemlerinde yapılan değişiklikler denetleniyor		

		(idari)	<p>mu?</p> <p>a) Asıl sistemler ve uygulama programları sıkı bir değişim kontrolüne tabi tutuluyor mu?</p> <p>b) Değişikliklerle ilgili planlama ve test yapılıyor mu?</p> <p>c) Programlarda yapılan değişiklikler için kayıtlar tutuluyor mu?</p> <p>d) Değişikliklerin, güvenlik dahil olmak üzere potansiyel etkileri değerlendiriliyor mu?</p> <p>e) Değişiklikler için resmi onay prosedürleri var mı?</p> <p>f) İlgili personele değişiklik detayları bildiriliyor mu?</p> <p>g) Başarısız değişikliklerin onarılması ve geri alınması ile ilgili sorumlulukları belirleyen prosedürler var mı?</p> <p>Bilgi işlem sistemlerinde yapılan değişikliklerin yönetilmemesi sonucunda sık sık sistem hatalarının ve güvenlik açıklarının ortaya çıktığı unutulmamalıdır.</p>		
6.1.3	10.1.3	Görevler ayrılığı (idari)	<p>Bilginin veya bilgi servislerinin kazara ya da kasten yanlış kullanımını veya yetkisiz değiştirilme riskini azaltmak için görevler ve sorumluluklar ayrılmış mı?</p> <p>Bir işin yetkilendirilmesi ile o işin gerçekleştirilmesi farklı kişiler tarafından yapılıyor mu?</p>		
6.1.4	10.1.4	Geliştirme sistemi, test	<p>Geliştirme ve test ortamları esas çalışma ortamından ayrılmış mı? Örneğin, geliştirilmekte olan yazılım ile</p>		

		sistemi ve aktif sistemlerin ayrılması (idari + teknik)	kullanılmakta olan yazılım farklı bilgisayarlarda çalıştırılmalıdır. Gerekli görüldüğü yerde geliştirme ve test ortamları da birbirinden ayrılmalıdır.		
6.2	10.2	Üçüncü taraflardan alınan hizmetin yönetilmesi			
6.2.1	10.2.1	Hizmet alma (idari)	Üçüncü taraftan hizmet alma anlaşmasında belirtilen hizmetlerin tanımının, güvenlik seviyesinin ve denetiminin gerçekleştirilmesini ve sürdürülmesini güvence altına almak için üçüncü taraf gerekli tedbirleri almış mı?		
6.2.2	10.2.2	Üçüncü taraf hizmetlerinin gözden geçirilmesi (idari + teknik)	Üçüncü taraflardan alınan hizmetler, raporlar ve kayıtlar düzenli olarak izleniyor ve gözden geçiriliyor mu? Üçüncü taraflardan alınan yukarıdaki hizmetler, raporlar ve kayıtlar düzenli aralıklarla denetime tabii tutuluyor mu?		
6.2.3	10.2.3	Üçüncü taraf hizmetlerindeki değişikliklerin yönetilmesi	Bilgi güvenliği politikaları, prosedürleri ve denetimlerinde yapılan bakım ve iyileştirmeleri de içeren hizmet alımı değişiklikleri yönetiliyor mu? Değişiklik yönetimi çerçevesinde işin içindeki süreçlerin		

		(idari)	kritikliği hesaba katılıyor ve riskler gözden geçiriliyor mu?		
6.3	10.3	Sistem Planlama ve Kabul Etme			
6.3.1	10.3.1	Kapasite yönetimi (idari + teknik)	Gereken sistem performansını sağlamak için sistem kaynaklarının ne oranda kullanıldığı izleniyor ve ileriye dönük kapasite ihtiyacının projeksiyonu yapılıyor mu? (Önemli sunumcuların üstündeki sabit disk alanının, RAM ve CPU kullanımlarının izlenmesi gerekir) Mevcut aktiviteler ve yeni başlayacak aktiviteler için kapasite ihtiyaçları belirleniyor mu? Tedarik süresi uzun veya fiyatı yüksek ekipmanın alınması ile ilgili planlamalar dikkatle gerçekleştiriliyor mu?		
6.3.2	10.3.2	Sistem kabulü (idari + teknik)	Yeni bilgi sistemleri, yükseltmeler ve yeni versiyonlar için sistem kabul etme kriterleri tespit edilmiş ve belgelenmiş mi? Resmi kabulden önce gerekli testler yapılıyor mu? Resmi kabul gerçekleşmeden yeni sistemin kullanılmamasına dikkat ediliyor mu?		

			Resmi kabulden önce aşağıdaki hususlara dikkat ediliyor mu? a) Mevcut sistemlerle birlikte çalışabilirlik b) Toplam sistem güvenliği üstündeki etkileri c) Eğitim ihtiyacı d) Kullanım kolaylığı (kullanıcı hatalarına meydan vermeme açısından)		
6.4	10.4	Kötü Niyetli Yazılımlara Karşı Korunma			
6.4.1	10.4.1	Kötü niyetli yazılımlara karşı kontroller (idari + teknik)	Kötü niyetli yazılımlara karşı bulma, önleme ve düzeltme tedbirleri alınmış mı? Kullanıcı bilinci oluşturulmuş mu? a) Güvenlik politikası yetkisiz yazılım kullanmayı yasaklıyor mu? b) Yabancı ağlardan ve diğer medyadan dosya veya yazılım alınmasına ilişkin risklerden nasıl korunulacağına ilişkin politika var mı? c) Kritik iş süreçlerini çalıştıran sistemler düzenli olarak taranarak yetkilendirilmemiş yazılım ilaveleri veya dosyaların mevcut olup olmadığı araştırılıyor mu? d) Kötü niyetli yazılımlara karşı bulma ve önleme fonksiyonlarını yerine getiren programlar kurulmuş ve düzenli olarak güncellemeleri yapılıyor mu? Tarama motorları ve imza dosyaları güncelleniyor mu? e) Ağ üstünden veya diğer ara yüzlerden masaüstü bilgisayarlara veya sunuculara giren dosyalar, e-posta ekleri ve bağlanılan internet sayfalarının		

			<p>çerikleri kontrol ediliyor mu?</p> <p>f) Kötü niyetli yazılımlardan korunma sistemleri, bunlarla ilgili eğitimler, saldırıların rapor edilmesi ve saldırı sonrası tedavi ile ilgili yönetim prosedürleri ve sorumluluklar belirlenmiş mi?</p> <p>g) Saldırı sonrası iş sürekliliği için plan yapılmış mı?</p> <p>h) Kötü niyetli yazılımlarla ilgili güncel bilgiler izleniyor mu?</p>		
6.4.2	10.4.2	<p>Mobil yazılımlarla ilgili denetimler</p> <p>(idari + teknik)</p>	<p>Sadece yetkilendirilmiş mobil yazılımlar kullanılıyor mu?</p> <p>Yetkilendirilmemiş mobil yazılımın çalışmasına engel olunuyor mu?</p> <p>Yetkilendirilmiş mobil yazılımın güvenlik politikası uyarınca çalışması konfigürasyon aracılığı ile güvence altına alınıyor mu?</p> <p>(Mobil yazılım, bir bilgisayardan diğerine taşınan ve otomatik olarak çalışan yazılımlara denir. Kullanıcının herhangi bir müdahalesi olmadan belli bir görevi yerine getirirler).</p>		
6.5	10.5	Yedekleme			
6.5.1	10.5.1	Bilgi yedekleme	Yedekleme politikası uyarınca bilgi ve yazılımların		

		(idari + teknik)	<p>yedeklenmesi ve yedeklerin test edilmesi düzenli olarak yapılıyor mu? Bir felaket veya sistem hatasından sonra gerekli tüm bilgilerin ve yazılımların kurtarılmasını sağlayacak yedekleme kabiliyeti mevcut mu?</p> <p>a) Yedeklemenin hangi düzeyde yapılacağı tanımlanmış mı? Yedeklemenin hangi sıklıkla yapılacağı kurumun ihtiyaçları uyarınca ayarlanmış mı?</p> <p>b) Onarım (geri dönüş) prosedürleri belgelenmiş mi? Yedek kopyalar kayıt altına alınmış mı?</p> <p>c) Alınan yedeklerin bir kopyası ana sitede meydana gelebilecek bir felaketten etkilenmeyecek mesafede fiziksel ve çevresel etkenlerden korunarak saklanıyor mu?</p> <p>d) Yedekleme ortamı düzenli olarak test ediliyor mu?</p> <p>e) Onarım prosedürleri düzenli olarak kontrol ve test ediliyor mu? İşletim prosedürlerinde belirtilen zaman dilimlerinde geri dönüş yapıldığı kontrol ediliyor mu?</p> <p>f) Ömrünü tamamlayan yedekleme ünitelerinin takibi yapılıyor mu?</p> <p>g) Gizliliğin önem arz ettiği durumlarda yedekler kriptolanıyor mu?</p> <p>h) Yedekleme ortamının güvenli biçimde imhası için izlenen bir yöntem var mı?</p>		
6.6	10.6	Ağ Güvenliğinin Yönetilmesi			
6.6.1	10.6.1	Ağ kontrolleri	Ağ yöneticileri, ağlardaki verinin güvenliği ve bağlı		

		(idari + teknik)	<p>bulunan servislere yetkisiz erişimi engellemek için gerekli tedbirleri almış mı?</p> <p>a) Ağların işletme sorumluluğu mümkün olan yerlerde bilgisayar işletmenlerinden ayrılmış mı?</p> <p>b) Uzaktan erişim donanımının/donanımlarının yönetimi için sorumluluklar ve prosedürler belirlenmiş mi?</p> <p>c) Halka açık ağlardan ve telsiz ağlardan geçen verinin bütünlüğünü ve gizliliği korumak, ağa bağlı sistemleri ve uygulamaları korumak için özel tedbirler alınmış mı? (VPN, erişim kontrolü ve kriptografik önlemler gibi)</p> <p>d) Ağ servislerini optimize etmek ve bilgi işlem altyapısı ile ilgili kontrollerin koordinasyonunu ve kuruluşun tamamında uygulanmasını sağlamak üzere yönetim faaliyetleri gerçekleştiriliyor mu?</p>		
6.6.2	10.6.2	Ağ hizmetlerinin güvenliği (idari + teknik)	<p>Kurumun içinden sağlanacak veya dışarıdan alınacak ağ hizmetlerinin her birinin yönetilmesi ve güvenliği ile ilgili ihtiyaçlar belirleniyor mu? Bu ihtiyaçlar hizmet sağlayıcıları ile yapılan anlaşmalarda yer alıyor mu?</p> <p>Ağ hizmetleri sağlayıcısının, üstünde anlaşma sağlanan servislerin güvenli olarak verilmesi ve yönetilmesi ile ilgili imkân ve kabiliyetlere sahip olduğu tespit edilmiş mi?</p> <p>Alınan hizmetin kuruluş tarafından izlenmesi ve denetlenmesi konusunda anlaşmaya varılmış mı?</p>		

6.7	10.7	Bilgi ortamı yönetimi ve güvenlik			
6.7.1	10.7.1	Taşınabilir depolama ortamlarının yönetimi (idari)	<p>Teyp, disk, disket, kaset, hafıza kartları ve yazılı raporlar gibi sökülebilir bilgisayar ortamlarının yönetilmesi ile ilgili prosedürler var mı?</p> <p>Tüm prosedürler ve yetki seviyeleri açıkça tanımlanmış ve belgelenmiş mi?</p> <p>a) Daha fazla gerekmediği için kurum dışına çıkarılacak yeniden kullanılabilir ortamlar (disket vs.) okunamaz hale getiriliyor mu?</p> <p>b) Organizasyondan çıkarılan tüm ortam malzemeleri için yetkilendirme gereklidir ve bu işlemlerin hepsi için resmi kayıtların tutulması gerekir. Bu kayıtlar tutuluyor mu?</p> <p>c) Ortam malzemelerinin güvenliği sağlanıyor mu?</p> <p>d) Taşınabilir hafıza ortamlarını destekleyen ara yüzler gerçekten gerekmedikçe kapalı tutuluyor mu?</p>		
6.7.2	10.7.2	Depolama ortamının imhası (idari + teknik)	<p>Daha fazla kullanılmayacak bilgi ortamı resmi prosedürler uyarınca emniyetli bir biçimde imha ediliyor mu?</p> <p>a) Emniyetli imhaya tabii tutulacak varlığı belirlemek için prosedür var mı?</p> <p>b) Emniyetli imha işi dışarıdan bir firmaya yaptırılıyorsa gereken güvenlik önlemlerini uygulayan bir firmanın seçilmesine dikkat edildi</p>		

			mi? c) İmha edilen ortamların kaydı tutuluyor mu?		
6.7.3	10.7.3	Bilgi depolama ve işleme prosedürleri (idari)	Bilginin yetkisiz olarak açıklanmasına veya yanlış kullanımına engel olmak için bilginin yönetilmesi ve saklanması ile ilgili prosedürler oluşturulmuş mu? a) Tüm ortamlar gizlilik dereceleri uyarınca etiketleniyor ve yönetiliyor mu? b) Yetkisiz kişilerin bilgiye erişimine engel olmak için erişim kısıtlaması uygulanıyor mu? c) Bilgiye erişim yetkisi olan kişiler resmi ve güncellenmekte olan bir belgede belirtilmiş mi? d) Veri girdisinin eksiksiz olduğu, işlemin hatasız tamamlandığı ve çıktı onayından geçtiği kontrol ediliyor mu? e) Veri dağıtımının en alt düzeyde tutulması sağlanıyor mu?		
6.7.4	10.7.4	Sistem dokümantasyonu güvenliği (idari + teknik)	İşlemler, prosedürler, veri yapıları, yetkilendirme işlemlerinin uygulama tanımları gibi bir dizi duyarlı bilgiyi içeren sistem dokümantasyonu yetkisiz erişimden korunuyor mu? a) Sistem dokümantasyonu güvenli bir ortamda bulunduruluyor mu? b) Sistem dokümantasyonuna erişim listesi asgari düzeyde tutulmuş mu? Yetkilendirme sistemin sahibi tarafından yapılmış mı?		

6.8	10.8	Bilgi ve Yazılım Değiş Tokuşu			
6.8.1	10.8.1	<p>Bilgi deęiş tokuşu ile ilgili politika ve prosedürler.</p> <p>(idari + teknik)</p>	<p>Her türlü iletişim ortamında bilginin güvenliğini sağlamak için resmi bir deęiş tokuş politikası veya prosedürü uygulanıyor mu?</p> <p>Elektronik iletişim araçları ile ilgili prosedür ve kontroller aşığıdaki durumları düzenliyor mu?</p> <ul style="list-style-type: none"> a) Bilginin kopyalanması, tahribi, içeriğinin veya yolunun deęiştirilmesinden korunma. b) Elektronik iletişim aracılığı ile alınabilecek kötü niyetli yazılımların tespiti ve bertaraf edilmesi. c) Mesajlara eklenmiş hassas bilgilerin korunması. d) Elektronik iletişim yöntemlerinin kullanımı ile ilgili rehber ve politikalar. e) Telsiz veri iletişiminin içerdiği riskler de göz önüne alınarak kullanılması. f) Bilginin bütünlüğünü ve gizliliğini korumak için kriptografik tekniklerin kullanılması. g) İş ile ilgili yazışmaların saklanması ve imhası. h) Fotokopi makinesi, yazıcı ve faks cihazlarında hassas bilgi içeren belgelerin bırakılmaması. i) Elektronik mesajların harici posta kutularına iletilmemesi için yapılacak düzenlemeler. j) Personelin telefon konuşmaları sırasında hassas bilgilerin açığa çıkmaması için tedbirli davranması. k) Cevap verme makinelerine hassas bilgi içeren mesajlar bırakılmaması. 		

			l) Faks cihazlarının kullanılması ile ilgili risklerin personele anlatılması. m) Gizli görüşmelerin halka açık yerlerde yapılmaması.		
6.8.2	10.8.2	Bilgi ve yazılım değişim anlaşmaları (idari)	Kurum ile diğer taraf arasında bilgi ve yazılım değişiminin şartlarını düzenleyen anlaşma yapılmış mı? Bu anlaşmada iş bilgilerinin duyarlılığı ile ilgili güvenlik konularına değinilmiş mi?		
6.8.3	10.8.3	Nakil esnasındaki bilgi ortamının güvenliği (idari + teknik)	Nakil halindeki bilgi, yetkisiz erişime, bilinçsiz kötü kullanıma veya değiştirilmelere karşı korunuyor mu? a) Güvenilir araç veya kuryeler kullanılıyor mu? b) Kuryelerin kimliğini kontrol etmek için prosedür geliştirilmiş mi? c) Nakil esnasında varlığı fiziksel hasardan koruyacak paketleme yapılıyor mu?		
6.8.4	10.8.4	Elektronik mesajlaşmanın güvenliği (idari + teknik)	Elektronik olarak taşınan bilgi gerektiği gibi korunuyor mu? a) Mesajlar yetkisiz erişimden korunuyor mu? b) Mesajın doğru adrese gitmesi sağlanıyor mu? c) Elektronik posta hizmetinin sürekliliği ve güvenilirliği yüksek mi? d) Elektronik imza gibi yasal yükümlülükler var mı?		

			Eğer varsa gereği yerine getirilmiş mi? e) Halka açık sistemler (“Instant Messaging” gibi) kullanılmadan önce yönetimden onay alınıyor mu?		
6.8.5	10.8.5	Ofis bilgi sistemleri (idari + teknik)	Elektronik ofis sistemlerinin birbirine bağlanması ile ilgili olarak burada bulunan bilginin korunması için politika ve prosedürler geliştirilmiş ve kullanılmış mı? a) İdari sistemdeki ve muhasebe sistemindeki açıklar dikkate alınmış mı? b) Bilgi paylaşımının yönetilmesi için politika ve tedbirler mevcut mu? c) Sistemde gerekli koruma yoksa gizli belgeler ve hassas iş bilgileri sistem dışında tutulmuş mu?		
6.9	10.9	Elektronik Ticaret Hizmetleri			
6.9.1	10.9.1	Elektronik ticaret güvenliği (idari + teknik)	Halka açık ağlar vasıtası ile taşınan elektronik ticaret bilgileri, hileli kazanç faaliyetleri, anlaşma itilafları ya da bilginin değişikliğe maruz kalması gibi bir dizi ağ şebekesi tehdidine karşı korunmuş mu? Kriptografik önlemler alınmış mı? (Elektronik ticaret ile ilgili risklerin çoğu kriptografik tedbirlerin uygulanması ile bertaraf edilebilmektedir). Ticaret ortakları arasındaki elektronik ticaret düzenlemeleri,		

			iki tarafı bilgilendiren, yetkilendirme detaylarının dahil olduğu, üzerinde anlaşma sağlanan ticari şartların yazılı olduğu bir belge ile tespit edilmiş midir?		
6.9.2	10.9.2	“On-line” işlemler (idari + teknik)	“On-line” işlemlerle ilgili bilgi hatalı gönderme, hatalı yönlendirme, mesajın yetkisiz kişiler tarafından ifşa edilmesi, değiştirilmesi, kopyalanması veya tekrar gönderilmesine karşı korunuyor mu?		
6.9.3	10.9.3	Halka açık bilgi (idari + teknik)	Halka açık bilginin bütünlüğü yetkisiz kişilerin değişiklik yapmaması için korunuyor mu? Sistem üstünde teknik açıklık testleri yapılıyor mu? Halka açık sisteme konmadan önce bilginin onaylanmasını sağlayan belgelenmiş bir süreç var mı?		
6.10	10.10	Sistem Erişiminin Gözlenmesi ve Kullanımı			
6.10.1	10.10.1	Olay kayıtlarının tutulması (idari + teknik)	Erişimi gözlemek ve gerektiği takdirde soruşturmalarda kullanmak üzere gerekli sistemlerde kullanıcı faaliyetleri ve güvenlik ile ilgili olay kayıtları tutuluyor ve bu kayıtlar belirli bir süre boyunca saklanıyor mu? a) Kullanıcı kimlikleri, b) Oturuma giriş ve çıkış tarihleri ve zamanları, c) Eğer mümkünse terminal kimliği, d) Başarılı ve reddedilmiş sistem erişim denemeleri,		

			<p>e) Sistem konfigürasyonunda yapılan değişiklikler, f) Ayrıcalıkların kullanılması, g) Hangi dosyalara erişimin gerçekleştiği ile ilgili kayıtlar tutuluyor mu?</p> <p>h) Sistem yöneticilerinin kendi faaliyetlerini silme yetkisine sahip olmaması gerekir.</p>		
6.10.2	10.10.2	Sistem kullanımının gözetlenmesi (idari + teknik)	<p>Bilgi işlem araçlarının kullanımının gözlenmesi ile ilgili prosedürler geliştirilmiş mi? Bu prosedürler uygulanıyor mu?</p> <p>Sistem kullanımı kayıtları düzenli olarak gözden geçiriliyor mu?</p> <p>Bilgi işlem araçlarında yapılan işlemlerin hangi düzeyde kaydedileceği risk değerlendirme çalışması sonucunda belirlenmiş mi?</p>		
6.10.3	10.10.3	Kayıt bilgilerinin muhafazası (idari + teknik)	Kayıt alma araçları ve kayıt bilgileri yetkisiz erişim ve değiştirmeye karşı korunuyor mu?		
6.10.4	10.10.4	Yönetici ve işletmen kayıtları (idari + teknik)	<p>Yönetici ve işletmen faaliyetlerinin kaydı tutuluyor mu?</p> <p>a) Başarılı veya başarısız faaliyetin tarihi ve zamanı, b) Faaliyetle ilgili bilgi (örneğin sistemde oluşan hata ve alınan tedbir), c) İşlemin hangi kullanıcı hesabı üstünde ve hangi</p>		

			yönetici tarafından yapıldığı, d) Hangi süreçlerin etkilendiği kaydediliyor mu? İşletmen kayıtları, düzenli olarak inceleniyor mu?		
6.10.5	10.10.5	Hata kayıtları (idari + teknik)	Hatalar rapor edilip düzeltici tedbirler alınıyor mu? Bilgi işlem ya da iletişim sistemleri ile ilgili olarak kullanıcılar tarafından rapor edilen hataların kaydı tutuluyor mu? Hataların tatmin edici bir şekilde giderildiğinden emin olmak için hata kayıtları gözden geçiriliyor mu?		
6.10.6	10.10.6	Saat senkronizasyonu (teknik)	Sistem bilgisayarları veya diğer bilgi sistemi cihazlarının saatleri standart bir zaman bilgisine göre ayarlanmış mı? Bilgisayar saatlerinin doğru ayarlanmış olması farklı bilgisayarlardan alınmış olay kayıtlarının birlikte incelenebilmesi açısından büyük önem arz etmektedir. Bu iş için NTP protokolü kullanılabilir.		

ERİŞİM DENETİMİ						
Referans		Denetim alanı, hedefi ve sorusu			Sonuçlar	
Kontrol listesi	Standart	Bölüm	Denetim sorusu	Bulgular	Uyumluluk	
7.1	11.1	Erişim Denetimi Gereksinimleri				
7.1.1	11.1.1	Erişim denetimi politikası (idari)	<p>Erişimle ilgili iş ve güvenlik ihtiyaçları göz önünde bulundurularak erişim denetimi politikası oluşturulmuş ve belgelenmiş mi?</p> <p>Erişim denetimi hem fiziksel, hem işlevsel boyutları ile değerlendirilmiş mi?</p> <p>Erişim denetimi politikası bütün kullanıcılar veya kullanıcı grupları için erişim kurallarını ve haklarını açıkça belirtiyor mu?</p> <p>Kullanıcılara ve servis sağlayıcılarına erişim denetimiyle hangi iş gereksinimlerinin karşılanacağı iyice açıklanmış mı?</p> <p>Politika belgesi aşağıdaki konuları içeriyor mu?</p>			

			<ul style="list-style-type: none"> a) Her bir iş sürecinin güvenlik ihtiyaçları, b) İş süreçleri ile ilgili tüm bilgiler ve bu bilgilerin yüz yüze olduğu riskler, c) Bilginin yayılması ve yetkilendirme ile ilgili politikalar, bilginin sınıflandırılması, güvenlik seviyeleri ve “gerektiği kadar bilme” prensibi. d) Farklı sistem ve ağlardaki bilginin sınıflandırılması ve erişim denetimine ilişkin politikaların tutarlı olması, e) Bilgiye erişimle ilgili olarak kontratlardan ve yasal yükümlülüklerden kaynaklanan şartların yerine getirilmesi, f) Kurumun yaygın kullanıcı profilleri ile ilgili erişim hakları ve g) Erişimin talep edilmesi, yetkilendirilmesi ve yönetilmesi görevlerinin birbirinden ayrılması. <p>Erişim haklarının “Yasaklanmadıkça her şey serbesttir” değil “İzin verilmedikçe her şey yasaktır” prensibine göre verilmesine dikkat edilmelidir.</p>		
7.2	11.2	Kullanıcı Erişiminin Yönetilmesi			
7.2.1	11.2.1	Kullanıcı kaydı (idari + teknik)	<p>Bilgi sistemlerine ve servislerine erişim hakkı vermek için resmi bir kullanıcı kaydı girme ve kullanıcı kaydı silme prosedürü var mı?</p> <ul style="list-style-type: none"> a) Sistem kayıtları ile ilişkilendirme ve sorumlu tutulabilme açısından kullanıcı kimliklerinin her kullanıcı için farklı olmasına dikkat ediliyor mu? 		

			<p>b) Bilgi sistemini ve servisini kullanabileceğine dair sistem sahibi kullanıcıya yetki vermiş mi?</p> <p>c) Verilen erişim hakkı kurumsal güvenlik politikasına ve görevler ayrılığı ilkesine uygun mu?</p> <p>d) Kullanıcılara erişim hakları ile ilgili yazılı belge veriliyor ve kullanıcılardan erişim şartlarını anladıklarına ilişkin imzalı belge alınıyor mu?</p> <p>e) Görevi değişen veya kuruluştan ayrılan personelin erişim hakları derhal güncelleniyor mu?</p>		
7.2.2	11.2.2	Ayrıcalık yönetimi (idari + teknik)	<p>Ayrıcalıkların kullanımı sınırlandırılmış mı ve denetleniyor mu?</p> <p>Ayrıcalıklar “kullanması gereken” prensibine göre ve resmi bir yetkilendirme süreci sonunda mı verilmiş?</p>		
7.2.3	11.2.3	Kullanıcı parola yönetimi (idari + teknik)	<p>Kullanıcı parolalarının atanması ya da değiştirilmesi resmi bir prosedür uyarınca yapılıyor mu? a</p> <p>Kullanıcılara parolalarını saklı tutacaklarına dair bir anlaşma imzalatılıyor mu? b</p>		
7.2.4	11.2.4	Kullanıcı erişim haklarının gözden geçirilmesi	<p>Kullanıcı erişim haklarının düzenli aralıklarla kontrol edilmesini sağlayan resmi bir süreç var mı?</p>		

		(idari)			
7.3	11.3	Kullanıcı Sorumlulukları			
7.3.1	11.3.1	Parola kullanımı (idari + teknik)	<p>Kullanıcı parolalarının seçilmesi ve kullanılması ile ilgili güvenlik tedbirleri uygulanıyor mu?</p> <p>a) Sistem tarafından geçici olarak verilen parolaların kullanıcı tarafından sisteme ilk girişte değiştirilmesi sağlanıyor mu?</p> <p>b) Kullanıcılar zor kırılacak parolalar seçmeleri konusunda bilinçlendirilmiş mi?</p> <p>c) Kişisel parolaların hiç kimse ile paylaşılmamasına, yazılı veya elektronik ortamlarda kaydedilmemesine dikkat ediliyor mu?</p> <p>d) Kullanıcılar düzenli aralıklarla veya sistem güvenliği ile ilgili bir kuşku oluştuktan sonra parolalarını değiştirmeye zorlanıyor mu?</p> <p>e) Kullanıcılar kişisel işlerinde kullandıkları parolaları kuruluşun iş süreçlerinde kullanmamaları gerektiği konusunda bilinçlendirilmiş mi?</p>		
7.3.2	11.3.2	Başboş kullanıcı ekipmanı (idari + teknik)	<p>Atıl cihazlara ait güvenlik gereksinimlerinden, bu cihazları koruma prosedürlerinden ve bu cihazları korumak için üzerlerine düşen sorumluluklardan kullanıcıların ve iş ortaklarının haberleri var mı? (İşi biten kullanıcıların bilgisayarını kapatması ve şifreli ekran koruyucuların kullanılması gibi)</p>		

7.3.3.	11.3.3	Temiz masa ve temiz ekran politikası (idari + teknik)	<p>Kuruluş kağıt ve taşınabilir elektronik depolama ortamları ile ilgili olarak temiz masa politikası uyguluyor mu?</p> <p>Kuruluş bilgi veya bilgi işlem araçları ile ilgili olarak temiz ekran politikası uyguluyor mu?</p> <p>a) Hassas bilgileri içeren kağıt ve elektronik depolama ortamlarının kullanılmadığı zaman kilitlemesi, b) Bilgisayar başından kalkarken personelin oturumunu kapaması veya ancak parola ile açılabilen ekran koruyucu vb. önlemleri devreye sokması, c) Gelen/giden postaya erişim noktalarının ve faks cihazlarının denetlenmesi, d) Fotokopi makinesi, tarayıcı, sayısal fotoğraf makinesi gibi kopyalama teknolojilerinin yetkisiz olarak kullanılmaması ve e) Hassas bilgi içeren dokümanların yazıcı üstünde bırakılmaması</p> <p>konularına özen gösterilmelidir.</p>		
7.4	11.4	Ağ Erişimi Denetimi			
7.4.1	11.4.1	Ağ hizmetlerinin kullanılması ile ilgili politikalar (idari)	<p>Kullanıcıların sadece kullanma yetkisine sahip oldukları ağ servislerine erişebilmesi sağlanmış mı?</p> <p>Ağlar ve ağ servisleri ile ilgili olarak aşağıdaki konuları düzenleyen politikalar uygulanıyor mu?</p>		

			<p>a) Kimin hangi ağlara ve ağ servislerine erişebileceğini belirlemek için yetkilendirme prosedürü tanımlanmış mı?</p> <p>b) Ağ bağlantılarını korumak ve ağ servislerine erişimi engellemek için yönetim denetimleri ve süreçleri belirlenmiş mi?</p>		
7.4.2	11.4.2	Harici bağlantılar için kullanıcı kimliği doğrulaması (idari + teknik)	Sisteme dışardan yapılacak kullanıcı bağlantıları için kullanıcı kimliği doğrulama mekanizmaları uygulanıyor mu? (Kripto tabanlı teknikler veya klasik “challenge-response” mekanizmaları ile çözülebilir. VPN çözümleri de bu teknikleri kullanmaktadır.)		
7.4.3	11.4.3	Ağlarda cihaz kimliği belirleme (idari + teknik)	Bağlantının belli bir cihaz kullanılarak yapıldığından emin olmak için otomatik cihaz kimliği belirleme yöntemleri kullanılıyor mu?		
7.4.4	11.4.4	Uzak yönetim ve yapılandırma portlarının korunması (idari + teknik)	Yönetim ve yapılandırma portlarına fiziksel ve işlevsel erişimi denetleyen bir güvenlik mekanizması var mı?		

7.4.5	11.4.5	Ağlardaki ayırım (idari + teknik)	Bilgi sistemi üstündeki kullanıcı ve servisler gruplara ayrılmış mı? Kurumun ağı dahili ve harici etki alanlarına bölünmüş mü? Etki alanları kurumun erişim kontrol politikası ve erişim ihtiyaçları uyarınca oluşturulmuş mu? Etki alanları sınır güvenliği sistemleri ile korunuyor mu? Telsiz ağların diğer ağlardan ayrılması ile ilgili olarak çalışma yapılmış mı?		
7.4.6	11.4.6	Ağ bağlantısı kontrolleri (idari + teknik)	Kurum sınırlarının dışına taşan ağlar ve ağ bağlantılarının kullanımı kurumun erişim kontrol politikası uyarınca kısıtlanmış mı? a) Elektronik mesaj, b) Tek veya çift yönlü dosya aktarımı, c) İnteraktif erişim, d) Bağlantı zamanı ve süresi ile ilgili kısıtlamalar getirilmiş mi?		
7.4.7	11.4.7	Ağ yönlendirme kontrolleri (idari + teknik)	Ağ yönlendirme kontrolleri, bilgisayar bağlantılarının ve bilgi akışının erişim politikasına uygun gerçekleşmesini sağlayacak şekilde tanımlanmış mı? Ağ iletişimi kaynak adres ve hedef adreslere bağlı olarak		

			güvenlik duvarı vb. cihazlar aracılığı ile kontrol ediliyor mu?		
7.5	11.5	İşletim Sistemi Erişim Denetimi			
7.5.1	11.5.1	Terminal oturum açma işlemleri (idari + teknik)	<p>Oturum açma işlemleri yetkisiz erişim olasılığını asgari düzeye indirecek şekilde düzenlenmiş mi?</p> <p>a) Sistem ve uygulamaya ilişkin olarak yetkisiz kullanıcıya yardımcı olabilecek bilgiler oturuma giriş başarıyla tamamlanana kadar gizleniyor mu?</p> <p>b) Bilgisayarda sadece yetkili personel tarafından erişilebileceğini bildiren uyarı mesajı gösteriliyor mu?</p> <p>c) Oturuma giriş sadece tüm girdi verilerinin doğrulanmasından sonra mı sağlanıyor? Bir hata durumu varsa sistem verinin hangi kısmının doğru veya yanlış olduğu bilgisini gizliyor mu?</p> <p>d) Sistem tarafından izin verilen başarısız giriş denemelerine sınırlama getirilmiş mi? Oturuma giriş işlemi için zaman sınırı var mı?</p> <p>e) Başarısız giriş denemeleri kaydediliyor mu?</p> <p>f) Ağ üstünden şifrenin açık olarak gönderilmemesi sağlanıyor mu?</p>		
7.5.2	11.5.2	Kullanıcı tanımlaması ve	Gerektiğinde sistem kayıtlarının incelenmesi ve bir işlemin sorumlusunun bulunabilmesi açısından her bir kullanıcıya		

		doğrulaması (idari + teknik)	kendine özgü bir kullanıcı kimliği verilmiş mi? Sistem yöneticilerine ait kullanıcı kimlikleri birbirinden farklı mı? Kurum bünyesinde kullanılan kullanıcı tanımlama ve yetkilendirme mekanizmaları iş gereklerine uygun mu?		
7.5.3	11.5.3	Parola yönetim sistemi (idari + teknik)	Kurum bünyesinde kullanılan belirli bir parola yönetim sistemi var mı? Parola yönetim sistemi aşağıdaki özelliklere sahip mi? a) Kullanıcıları bireysel parolaların kullanımına zorluyor mu? b) Kullanıcıların kendi parolalarını seçmelerine ve değiştirmelerine izin veriyor mu? c) Kullanıcıyı kuvvetli parola seçmeye zorluyor mu? d) Kullanıcıyı belli zamanlarda parolasını değiştirmeye zorluyor mu? e) Sisteme ilk girişte geçici parolayı değiştirmeye zorluyor mu? f) Eski parolaları hatırlayarak tekrar kullanılmalara engel oluyor mu? g) Parolalar ağ üstünden gönderilirken ve saklanırken kriptolama gibi yöntemlerle korunuyor mu?		
7.5.4	11.5.4	Yardımcı sistem	Sistem araçlarının sistem özelliklerini ve uygulama		

		programlarının kullanılması (idari + teknik)	programlarının yetkilerini aşarak ekstra işlemler yapmadığı kontrol ediliyor mu?		
7.5.5	11.5.5	Oturum zaman aşımı (idari + teknik)	Kullanılmayan oturumlar tanımlı bir süre sonunda kapatılıyor mu?		
7.5.6	11.5.6	Bağlantı süresinin sınırlandırılması (idari + teknik)	Kurum dışından veya halka açık alanlardan yüksek riskli uygulamalara erişim durumunda a) Bağlantı süresi kısıtlanmış mı? b) Kullanıcı belli aralıklarla kimliğini tekrar doğrulamaya zorlanıyor mu?		
7.6	11.6	Uygulama Erişimi Denetimi			
7.6.1	11.6.1	Bilgi erişimi kısıtlaması (teknik)	Erişim kontrolü politikası uyarınca kullanıcılar ve destek personeli için bilgi sistemleri fonksiyonları ve bilgilerine erişim kısıtlanmış mı? Kullanıcıların bilgiyi yazma, okuma, silme veya çalıştırma hakları düzenleniyor mu?		
7.6.2	11.6.2	Duyarlı sistem yalıtımı	Uygulamanın duyarlılığı uygulama sahibi tarafından açıklanmış ve belgelenmiş mi?		

		(idari + teknik)	Duyarlı bilgilerin bulunduğu sistemler diğer sistemlerden izole edilmiş mi? (Kendisine ait bilgisayarda çalıştırılması, ayrı ağ bölmesine yerleştirilmesi, ağ kaynaklarının ayrılması, sadece gerekli uygulamalar ile iletişim kurulması vb. İzolasyon fiziksel veya işlevsel olarak gerçekleştirilebilir.)		
7.7	11.7	Mobil Bilgi İşlem ve Uzaktan Çalışma			
7.7.1	11.7.1	Mobil bilgi işlem ve iletişim (idari + teknik)	Dizüstü bilgisayar, cep bilgisayarı, cep telefonu, akıllı kartlar vb. mobil bilgi işlem ve iletişim araçlarının kullanılmasından kaynaklanan risklerden korunmak için benimsenmiş bir politika ve uygulanmakta olan güvenlik önlemleri var mı? Mobil bilgi işlem politika belgesi fiziksel koruma, erişim denetimi, kriptografik denetimler, yedekleme ve virüs koruması konularını içeriyor mu? Mobil bilgi işlem araçlarının halka açık yerler, toplantı odaları gibi korumasız ortamlarda kullanılması sırasında yetkisiz erişime ve bilginin açığa çıkmasına karşı kriptografik tekniklerin kullanılması gibi önlemler alınıyor mu?		

			Hırsızlığa karşı önlemler alınıyor mu? Hassas bilgi içeren araçların başıboş bırakılmamasına özen gösteriliyor mu?		
7.7.2	11.7.2	Uzaktan çalışma (idari + teknik)	Uzaktan çalışma faaliyetleri için organizasyonun güvenlik politikasına uygun plan ve prosedürler geliştirilmiş mi? Uzaktan çalışmanın yapılacağı yerde ekipman ve bilginin çalınmasına, bilgiye yetkisiz erişim yapılmasına, kuruluşun dahili sistemlerine uzaktan yetkisiz erişime ve bilgi işlem araçlarının kötüye kullanılmasına engel olmak için uygun önlemler alınmış mı?		

BİLGİ SİSTEMİ TEDARİĞİ, GELİŞTİRİLMESİ VE BAKIMI							
Referans		Denetim alanı, hedefi ve sorusu			Sonuçlar		
Kontrol listesi	Standart	Bölüm	Denetim sorusu	Bulgular	Uyumluluk		
8.1	12.1	Bilgi Sistemlerinin Güvenlik Gereksinimleri					
8.1.1	12.1.1	Güvenlik gereksinimlerinin analizi ve özelleştirilmesi (idari + teknik)	Yeni sistemlerin geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınıyor mu? a) Ortaya konan güvenlik gereksinimleri bilgi varlıklarının değerini ve bir güvenlik açığı dolayısıyla oluşabilecek zararı yansıtıyor mu? b) Sistem geliştirilirken işin başından itibaren güvenlik ihtiyaçları göz önünde bulunduruluyor mu? c) Satın alınan ürünler için resmi bir test ve tedarik süreci işletiliyor mu?				
8.2	12.2	Uygulamaların Doğru Çalışması					
8.2.1	12.2.1	Girdi verilerinin	Uygulama sistemlerinin girdilerinin doğru ve uygun				

		kontrolü (teknik) <i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi uygulamalar" arasında gösterilmiştir)</i>	olduğuna dair kontrol yapılıyor mu? Ne tür kontroller yapılıyor? İş hareketlerinin daimi veri (isim, adres, vb) ve parametre tabloları (döviz kurları, vergi oranları gibi) girişlerine kontroller uygulanıyor mu?		
8.2.2	12.2.2	İç işleğin kontrolü (teknik) <i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi uygulamalar" arasında gösterilmiştir)</i>	Doğru girilmiş bilginin işlem sırasında hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmiş mi? Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmış mı?		
8.2.3	12.2.3	Mesaj bütünlüğü (teknik) <i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi uygulamalar" arasında gösterilmiştir)</i>	Mesaj bütünlüğü gereksinimini belirlemek için güvenlik ihtiyaçları değerlendirilmiş ve gereken önlemler alınmış mı? Mesaj doğrulama yöntemi olarak kriptografik teknikler kullanılıyor mu?		
8.2.4	12.2.4	Çıktı verilerinin kontrolü (teknik)	Saklanan bilgilerin üstünde gerçekleştirilen işlemlerin doğru ve şartlara uygun olduğundan emin olmak için uygulama çıktılarının denetimi yapılıyor mu?		

		<i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi uygulamalar" arasında gösterilmiştir)</i>	<p>Bu çerçevede</p> <ul style="list-style-type: none"> a) Çıktı verilerin makul değerler alıp almadığı, b) Tüm verinin işlenip işlenmediği, c) Çıktı veriyi işleyen sisteme verinin bütünlüğünü ve doğruluğunu sınamasını sağlayacak bilginin verilip verilmediği <p>kontrol edilebilir.</p>		
8.3	12.3	Kriptografik Kontroller			
8.3.1	12.3.1	<p>Kriptografik kontrollerin kullanımına ilişkin politika</p> <p>(idari + teknik)</p>	<p>Bilginin korunması için kriptografik kontrollerin kullanılmasını düzenleyen politika geliştirilmiş ve uygulamaya alınmış mı?</p> <p>Politika oluşturulurken</p> <ul style="list-style-type: none"> a) Bilginin korunması ile ilgili genel prensipler ve yönetimin konuya yaklaşımı göz önünde bulundurulmuş mu? b) Kullanılacak güvenlik seviyesine karar vermek için risk değerlendirmesi yapılmış mı? c) Taşınabilir ortamlar ve iletişim kanallarındaki hassas bilginin korunması için kriptografik kontrollerin uygulanması düşünülmüş mü? d) Anahtar yönetimi ile ilgili güvenlik hususları düzenlenmiş mi? (anahtarın saklanması, anahtarın kaybolması durumunda şifrelenmiş bilginin kurtarılması vb) e) Roller ve sorumluluklar tanımlanmış mı? 		

8.3.2	12.3.2	Kriptografik anahtar yönetimi (idari + teknik)	Kurumun kriptografik teknikleri kullanmasına imkân sağlamak için anahtar yönetimi gerçekleştiriliyor mu? Anahtar yönetim sistemi tanımlı standartlar, prosedürler ve güvenli yöntemler esas alınarak oluşturulmuş mu? Algılanan risk ve kullanım şartları uyarınca anahtarların sınırlı bir süre boyunca kullanılabilmesi için gereken düzenlemeler yapılmış mı? c		
8.4	12.4	Sistem Dosyalarının Güvenliği			
8.4.1	12.4.1	Çalışmakta olan yazılımın denetimi (idari + teknik)	Çalışan sistemlere yazılım yüklenmesini -bozulma riskini asgariye indirmek için- düzenleyen prosedürler var mı? a) Yazılım yükleme, eğitimli sistem yöneticileri tarafından ve sadece yönetim yetkilendirmesi ile yapılıyor mu? b) Çalışan sistemde geliştirilmekte olan yazılım ve derleyici bulunmaması sağlanmış mı? c) İşletim sistemi ve uygulama yazılımlarının iyice test edilmeden yüklenmemesine dikkat ediliyor mu? d) Konfigürasyon kontrol sistemi aracılığı ile eski ve yeni yazılım sürümleri, yazılımla ilgili dokümantasyon ve konfigürasyon bilgileri ve sistem dokümantasyonu saklanıyor mu? e) Üçüncü taraflardan alınmış yazılımın kullanılması, güvenliği ve bakımı ile ilgili riskler göz önünde		

			bulunduruluyor mu?		
8.4.2	12.4.2	Sistem test verilerinin korunması (idari + teknik)	Sistem testi için kullanılan veri dikkatle oluşturuluyor ve korunuyor mu? (Kişisel bilgiler ve diğer hassas bilgileri içeren aktif veri tabanının sistem testi için kullanılmasından kaçınılmalı, canlı sistem bilgileri test sırasında kullanılacaksa içindeki gizli bilgiler çıkarılmalıdır.)		
8.4.3	12.4.3	Program kaynak kütüphanesine erişimin kontrolü (idari + teknik)	Program kaynak kodlarının bulunduğu kütüphanelere erişim sıkı bir şekilde denetleniyor mu? (Bu önlem yetkilendirilmemiş, kontrolsüz değişikliklere engel olmak içindir).		
8.5	12.5	Geliştirme ve Destek Süreçlerinde Güvenlik			
8.5.1	12.5.1	Değişim kontrol prosedürleri (idari + teknik)	Bilgi sistemleri üzerinde yapılacak değişiklikler resmi kontrol prosedürleri aracılığı ile denetleniyor mu? Yeni sistem ilaveleri ve büyük değişiklikler resmi bir belgeleme, tarif, test ve kalite kontrol süreci uyarınca gerçekleştiriliyor mu?		
8.5.2	12.5.2	İşletim sistemi	İşletim sisteminde yapılan değişikliklerin ardından kritik		

		değişiklerinin ardından uygulamaların teknik olarak gözden geçirilmesi. (idari + teknik)	uygulamaların gözden geçirilip test edilmesini sağlayan süreç veya prosedürler geliştirilmiş mi? Değişiklik gerçekleştirilmeden belli bir zaman önce ilgili yerlere haber verilerek test ve gözden geçirmelerin yapılması sağlanıyor mu?		
8.5.3	12.5.3	Yazılım paketlerinde yapılacak değişikliklerin kısıtlanması (idari + teknik)	Yazılım paketleri üzerinde değişiklik yapılması gerçekten gerekli olduğu durumlar dışında engelleniyor mu? (Hazır yazılımlar mümkün olduğu sürece değiştirilmeden kullanılmalıdır.) Değişikliğin kaçınılmaz olduğu durumlarda <ul style="list-style-type: none">a) Programın gömülü kontrollerine ve bütünlüğüne ilişkin süreçlerin tahrip edilmemesine,b) Üreticiden izin almak gerekip gerekmediğinin düşünülmesine,c) Gerekli değişikliklerin üretici tarafından standart yazılım güncellemeleri çerçevesinde gerçekleştirilip gerçekleştirilemeyeceğinin soruşturulmasına,d) Değişiklik sonucunda yazılımın bakımının kuruluş tarafından sürdürülmesi gerekirse bu durumun kabul edilebilir olup olmadığının değerlendirilmesine		

			dikkat ediliyor mu?		
8.5.4	12.5.4	Bilgi kaçağı (idari + teknik)	<p>Bilgi kaçağına karşı denetim var mı?</p> <p>Kurum dışına çıkan ortamların denetlenmesi, personel ve sistem aktivitelerinin izlenmesi ve bilgisayar ortamındaki kaynak kullanımının izlenmesi gibi denetimler yapılıyor mu?</p> <p>Sistem ve yazılım bütünlüğü yönünden açıklığı düşük olan (ISO/IEC 15408 Ortak Kriterler standardına uygun) ürünlerin kullanılması tercih edilmiş mi?</p> <p>İzleme yapan kişi veya kurumların bilgi edinmesine engel olmak için sistem ve iletişim karakteristiği maskeleniyor mu?</p>		
8.5.5	12.5.5	Dış kaynaklı yazılım geliştirme (idari + teknik)	<p>Dış kaynaklı yazılım geliştirme faaliyetleri izleniyor ve denetleniyor mu?</p> <p>a) Lisans anlaşması, b) Fikri mülkiyet hakları, c) Kalite güvencesi, d) Denetleme için erişim hakkı, e) Kurulum öncesi “Trojan” kod araması için test hususları düşünülmüş mü?</p>		
8.6	12.6	Teknik Açıklık Yönetimi			

8.6.1	12.6.1	<p>Teknik açıklıkların denetimi</p> <p>(idari + teknik)</p> <p><i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi uygulamalar" arasında gösterilmiştir)</i></p>	<p>Kullanılan bilgi sistemlerinin teknik açıklıkları ile ilgili bilgiler zamanında toplanıyor, bunlara bağlı olarak kurumun nasıl etkileneceği değerlendiriliyor ve riski azaltmak için uygun tedbirler alınıyor mu?</p> <p>a) Varlık envanterinin güncel ve eksiksiz olarak tutulmasına özen gösteriliyor mu?</p> <p>b) Teknik açıklık yönetimi ile ilgili rol ve sorumluluklar belirlenmiş mi?</p> <p>(Yazılım şirketleri yama çıkarma konusunda zaman zaman büyük baskı altında kalmakta ve çıkardıkları yamalar problemlere çözüm getiremeyebilmektedir.</p> <p>Bu konuda "Değişiklik Yönetimi" başlığı altındaki prosedürler göz önünde bulundurulabilir)</p>		
-------	--------	---	--	--	--

BİLGİ GÜVENLİĞİ OLAYLARI YÖNETİMİ					
Referans		Denetim alanı, hedefi ve sorusu		Sonuçlar	
Kontrol listesi	Standart	Bölüm	Denetim sorusu	Bulgular	Uyumluluk
9.1	13.1	Bilgi Güvenliği Olaylarının ve Zafiyetlerin Rapor Edilmesi			
9.1.1	13.1.1	Bilgi güvenliği olaylarının rapor edilmesi (idari)	Güvenlik olaylarını mümkün olduğunca hızlı bir şekilde raporlamak için resmi bir prosedür var mı? a) Raporlama prosedürü ile birlikte olaya yanıt vermek için yapılacakları belirten bir prosedür var mı? b) Raporlama prosedürü ve başvuru noktası tüm personel tarafından biliniyor mu? c) Başvuru noktasındaki personel her zaman ulaşılabilir durumda ve olaya müdahale edebilecek yetkinlikte mi? d) Tüm personel ve üçüncü parti çalışanlarına karşılaştıkları bilgi güvenliği olaylarını hızla bildirme konusunda yükümlü oldukları açıklanmış mı?		
9.1.2	13.1.2	Bilgi güvenliği zafiyetlerinin	Kurum çalışanlarının sistem ve servislerdeki güvenlik zafiyetlerini ya da bunları kullanan tehditleri bildirmesi		

		rapor edilmesi (idari)	<p>için resmi bir raporlama prosedürü var mı?</p> <p>Raporlama prosedürü kolayca kullanılabilir şekilde hazırlanmış mı?</p> <p>(Personel ve üçüncü taraf çalışanları zafiyetlerin varlığını kanıtlamak için test ve girişimler yapmaktan kaçınmalıdır. Aksi halde sistemde hasar oluşabileceği gibi testi yapan personel de suçlu durumuna düşebilir).</p>		
9.2	13.2	Bilgi Güvenliği Olaylarının Yönetimi ve İyileştirmeler			
9.2.1	13.2.1	<p>Sorumluluklar ve prosedürler</p> <p>(idari)</p> <p><i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi uygulamalar" arasında gösterilmiştir)</i></p>	<p>Bilgi güvenliği olaylarına hızlı, etkili ve düzenli bir biçimde karşılık verebilmek için yönetime ait sorumluluk belirlenmiş, prosedürler oluşturulmuş mu?</p> <p>Bilgi güvenliği olaylarını ortaya çıkarmak için sistemler, sistemlerin açıklıkları ve üretilen alarmlar izleniyor mu?</p> <p>a) Aşağıdaki farklı olay tiplerini ele almak üzere prosedürler geliştirilmiş mi?</p> <ul style="list-style-type: none"> ○ Bilgi sisteminin çökmesi ○ Kötü niyetli yazılım ○ Servis dışı bırakma saldırısı ○ Eksik veya hatalı veri girişi ○ Gizlilik ve bütünlüğü bozan ihlaller ○ Bilgi sisteminin kötüye kullanılması <p>b) Denetim sonuçları ve deliller toplanıyor ve güvenli bir biçimde saklanıyor mu?</p> <p>c) Açığı kapatmak ve hataları düzeltmek için gereken</p>		

			<p>çalışmalar yapılırken</p> <ul style="list-style-type: none"> ○ Canlı sisteme sadece yetkili personelin erişmesine, ○ Acil düzeltme çalışmalarının dokümante edilmesine, ○ Çalışmaların düzenli olarak yönetime bildirilmesi ve yönetim tarafından gözden geçirilmesine ve ○ Bilgi sistemlerinin bütünlüğünün asgari gecikme ile sağlanmasına <p>dikkat ediliyor mu?</p>		
9.2.2	13.2.2	<p>Bilgi güvenliği olaylarından deneyim edinme</p> <p>(idari + teknik)</p> <p><i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi uygulamalar" arasında gösterilmiştir)</i></p>	<p>Bilgi güvenliği olaylarını teşhis eden, bunların sınıflandırılmasını, sayılmasını ve maliyetlerinin hesaplanmasını sağlayan bir mekanizma var mı?</p> <p>Geçmiş bilgi güvenliği olaylarından sağlanan tecrübe tekrarlanan veya büyük hasar meydana getiren olayların tespit edilmesinde kullanılıyor mu?</p>		
9.2.3	13.2.3	<p>Delil toplama</p> <p>(idari + teknik)</p> <p><i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi</i></p>	<p>Bilgi güvenliği olayının ardından şahıs veya kuruluşlarla ilgili yasal işlem yapılıyor mu?</p> <p>Olayla ilgili deliller toplanıyor, muhafaza ediliyor ve ilgili yargı organına sunuluyor mu?</p>		

		<i>uygulamalar” arasında gösterilmiştir)</i>			
--	--	--	--	--	--

İŞ SÜREKLİLİĞİ YÖNETİMİ					
Referans		Denetim alanı, hedefi ve sorusu		Sonuçlar	
Kontrol listesi	Standart	Bölüm	Denetim sorusu	Bulgular	Uyumluluk
10.1	14.1	İş Sürekliliği Yönetiminin Bilgi Güvenliği Boyutu			
10.1.1	14.1.1	<p>İş sürekliliği yönetim sürecinin bilgi güvenliğini içermesi (idari)</p> <p><i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi uygulamalar" arasında gösterilmiştir)</i></p>	<p>Kurum bünyesinde iş sürekliliği için geliştirilmiş bir süreç mevcut mu?</p> <p>Bu süreç bilgi güvenliği ihtiyaçlarına yer veriyor mu?</p> <p>Süreç iş sürekliliği ile ilgili olarak aşağıda belirtilen konulara değiniyor mu?</p> <ul style="list-style-type: none"> a) Kuruluşun yüz yüze olduğu riskler b) Kritik iş süreçleri ile ilgili varlıklar c) Bilgi güvenliği olayları yüzünden gerçekleşebilecek kesintilerin etkisi d) İlave önleyici tedbirlerin belirlenmesi ve uygulanması e) Bilgi güvenliğini de içeren iş sürekliliği planlarının belgelenmesi 		
10.1.2	14.1.2	İş sürekliliği ve	İş süreçlerinde kesinti yaratan veya yaratabilecek olaylar,		

		<p>risk analizi (idari)</p> <p><i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi uygulamalar" arasında gösterilmiştir)</i></p>	<p>kesintilerin yaratacağı etki, gerçekleşme olasılıkları ve bilgi güvenliği açısından sonuçları ile birlikte belirlenmiş mi?</p> <p>Bu tür kesintilerin etkisini belirlemek için risk analizi yapılmış mı?</p> <p>Risk analizi, bilgi güvenliği ile ilgili sonuçları içermekle birlikte sadece bilgi işlem değil tüm iş süreçlerini göz önünde bulundurarak ve tüm süreçlerin sahipleri ile birlikte gerçekleştirilmiş mi?</p> <p>Risk analizinin sonuçları uyarınca iş sürekliliği ile ilgili geniş kapsamlı strateji belirlenmiş mi?</p>		
10.1.3	14.1.3	<p>Bilgi güvenliğini içeren iş sürekliliği planlarının geliştirilmesi ve uygulanması</p> <p><i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi uygulamalar" arasında gösterilmiştir)</i></p>	<p>Kritik süreçlerin kesintiye uğramasının ardından kurum tarafından belirlenmiş zaman aralığı içinde iş sürecinin onarılması ve belli bir seviyedeki bilgiye ulaşılabilmesi için planlar geliştirilmiş mi?</p> <p>Plan, sorumlulukların belirlenmesi ve anlaşılması, kabul edilebilir hasarın belirlenmesi, onarım prosedürünün belirlenmesi, prosedürün düzenli aralıklarla test edilmesi ve belgelenmesine değiniyor mu?</p>		

		(idari)			
10.1.4	14.1.4	<p>İş sürekliliği planlama çerçevesi</p> <p>(idari)</p> <p><i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi uygulamalar" arasında gösterilmiştir)</i></p>	<p>Tüm planların tutarlı olması, bilgi güvenliği ihtiyaçlarının tutarlı olarak sağlanması, test ve bakımla ilgili önceliklerin belirlenmesi için iş sürekliliği planları tek bir çerçeve uyarınca hazırlanıyor ve güncelleniyor mu?</p> <p>İş sürekliliği planı</p> <p>a) Bilgi sistemleri erişilebilirliği ile ilgili yaklaşımını, b) Kurtarma planı ve planın harekete geçirilmesi için gereken şartları, c) Planın bölümlerini yerine getirmekle sorumlu kişileri d) Planın sahibini</p> <p>açıkça belirtiyor mu?</p> <p>Yeni ihtiyaçlar ortaya çıktığında prosedürler gerektiği gibi güncelleniyor mu?</p> <p>Prosedürlere kuruluşun değişiklik yönetimi programı içerisinde yer verilerek iş sürekliliği yönetiminin her zaman uygun şekilde ele alınması sağlanıyor mu?</p>		
10.1.5	14.1.5	<p>İş sürekliliği planlarının test edilmesi, bakımı</p>	<p>İş sürekliliği planları güncellik ve etkinliklerinin sınanması açısından düzenli olarak test ediliyor mu?</p> <p>Testler aracılığı ile onarım ekibinin üyeleri ve diğer ilgili</p>		

		<p>ve yeniden değerlendirilmesi</p> <p>(idari + teknik)</p> <p><i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında "umumi uygulamalar" arasında gösterilmiştir)</i></p>	<p>personelin</p> <p>a) Planlardan ve iş sürekliliği ile ilgili sorumluluklarından haberdar olduğu ve</p> <p>b) Plan devreye sokulduğu zaman üstlenecekleri rolün ne olduğunu bilip bilmedikleri</p> <p>sınıyor mu?</p>		
--	--	---	---	--	--

UYUM					
Referans		Denetim alanı, hedefi ve sorusu		Sonuçlar	
Kontrol listesi	Standart	Bölüm	Denetim sorusu	Bulgular	Uyumluluk
11.1	15.1	Yasal Gereklere Uyumluluk			
11.1.1	15.1.1	İlgili yasaların belirlenmesi (idari)	Her bir bilgi sistemi için ilgili bütün yasal, düzenleyici ve sözleşmeye bağlı gereksinimler ve gereksinimleri sağlamak için kullanılacak kurumsal yaklaşım açık şekilde tanımlanmış ve belgelenmiş mi? Bu gereksinimleri karşılamak amacıyla kontroller ve bireysel sorumluluklar tanımlanmış ve belgelenmiş mi?		
11.1.2	15.1.2	IPR (Fikri mülkiyet hakları) (idari + teknik) <i>(ISO 27002:2005 standardının "0.6 Bilgi güvenliğine giriş" başlığı altında kurumun kanuni yükümlülükleri</i>	Kullanılmakta olan yazılım ve diğer her türlü materyal ile ilgili olarak yasal kısıtlamalara uyulması açısından kopya hakkı, düzenleme hakkı, ticari marka gibi hakların kullanılmasını güvence altına alan prosedürler yürürlüğe sokulmuş mu?		

		<i>açısından önemli olduğu belirtilmektedir)</i>	<p>Bu prosedürler uygulanıyor mu?</p> <p>Fikri mülkiyet olabilecek materyalin korunması için aşağıdaki hususlara özen gösteriliyor mu?</p> <p>a) Yazılım vb. diğer ürünlerin yasal olarak kullanılmasını öngören “Fikri Mülkiyet Haklarına Uyum” politikasının yayınlanması.</p> <p>b) Kullanım haklarının çiğnenmemesi için yazılımın sadece güvenilir kaynaklardan sağlanması.</p> <p>c) Mülkiyet haklarını ispatlamak için delil olarak kullanılacak lisans sözleşmesi, orijinal disk, kullanıcı rehberi vb. materyalin muhafaza edilmesi.</p> <p>d) Azami kullanıcı sayısının ihlal edilmemesini sağlamak için tedbirler alınması.</p> <p>e) Yazılım ve diğer ürünler için sadece lisanslı versiyonların kullanıldığının kontrollerle denetlenmesi.</p> <p>f) Film, müzik, kitap, makale ve diğer materyalin telif hakkı kanununun izin verdiği şartlar dışına çıkarak format dönüşümüne tabii tutulmaması, kısmen veya tamamen kopyalanmaması ve çoğaltılmaması.</p>		
11.1.3	15.1.3	<p>Kurumsal kayıtların korunması</p> <p>(idari + teknik)</p> <p><i>(ISO 27002:2005 standardının “0.6 Bilgi</i></p>	<p>Organizasyonun önemli kayıtları kanun, kontrat, anlaşma ve işin doğasından kaynaklanan gereksinimler uyarınca kaybolmaya ve bozulmaya karşı korunuyor mu?</p> <p>Kayıtların saklanması için kullanılan ortamın zaman içinde bozulabileceği göz önünde bulunduruluyor mu? b</p>		

		<i>güvenliğine giriş” başlığı altında kurumun kanuni yükümlülükleri açısından önemli olduğu belirtilmektedir)</i>	Veri saklama sistemi seçilirken belli bir süre sonra teknoloji değişikliği dolayısıyla kayıtların okunamaz hale gelmemesi için gerekli tedbirler alınmış mı? Donanımsal ve yazılımsal format uyumunu sağlamak için gerekli program ve teçhizat kayıtlarla birlikte saklanıyor mu?		
11.1.4	15.1.4	Verinin korunması ve kişisel bilginin mahremiyeti (idari) <i>(ISO 27002:2005 standardının “0.6 Bilgi güvenliğine giriş” başlığı altında kurumun kanuni yükümlülükleri açısından önemli olduğu belirtilmektedir)</i>	Yasalar veya mevcut kontratlar uyarınca veriyi ve kişisel bilgilerin gizliliğini korumak için kurumsal politika ve kontroller oluşturulmuş mu? Kişisel bilginin işlenmesi ile ilgisi olan tüm personel politikadan haberdar edilmiş mi?		
11.1.5.	15.1.5	Bilgi işlem birimlerinin yanlış kullanımının önlenmesi	Kullanıcıların bilgi işlem tesislerini yönetim tarafından yetkilendirilmemiş işler için kullanmasına engel olunuyor mu? a) Tüm kullanıcılara bilgi işlem tesisinin kullanımı ile ilgili yetkililerin ne olduğu yazılı olarak bildirilmiş ve bu belgeler kullanıcılara imzalatıldıktan sonra kurum tarafından muhafaza altına alınmış mı?		

		(idari + teknik)	<p>b) Tesislerin ve elektronik bilgi işlem ekipmanının yetkisiz kullanıma engel olmak için gözetim altında tutulduğu kullanıcılara bildirilmiş mi?</p> <p>c) Yetkisiz erişim tespit edildiği takdirde bu durum disiplin sürecinin veya yasal sürecin devreye sokulması için ilgili kullanıcının yöneticisine bildiriliyor mu?</p> <p>d) Oturum açıldığında bilgisayar ekranında “girilen sistemin kuruma ait olduğunu ve yetkisiz giriş izni verilmediğini” belirten uyarı mesajı çıkıyor mu?</p>		
11.1.6	15.1.6	<p>Kriptografik kontrollerin düzenlenmesi</p> <p>(idari + teknik)</p>	<p>Kriptografik kontroller sektörel ya da ulusal anlaşmalara ve kanunlara uygun olarak düzenlenmiş mi?</p> <p>Aşağıda belirtilen işlemler sırasında yasa ve anlaşmalara uyum göz önünde bulunduruluyor mu?</p> <p>a) Kriptografik işlemler yapan bilgisayar yazılım ve donanımının ihracat ve ithalatı ile ilgili kısıtlamalar</p> <p>b) Kriptografik işlemlerin eklenmesine hazır olarak tasarlanmış bilgisayar yazılım ve donanımının ihracat ve ithalatı ile ilgili kısıtlamalar,</p> <p>c) Kriptolama ile ilgili kısıtlamalar,</p> <p>d) Kriptolu bilgiye ulusal otoriteler tarafından erişilmek istenmesi durumunda kullanılacak yöntemler.</p>		
11.2	15.2	Güvenlik Politikası ile Uyum ve Teknik Uyum			

11.2.1	15.2.1	Güvenlik politikalarına ve standartlara uyum (idari + teknik)	<p>Yöneticiler kendi sorumluluk alanlarında –güvenlik politikalarına ve standartlara uyum açısından- güvenlik prosedürlerinin doğru olarak uygulanıp uygulanmadığını kontrol ediyor mu?</p> <p>Kontrol ya da gözden geçirme sonucunda bir uyumsuzluğun bulunması halinde yönetici</p> <ul style="list-style-type: none"> a) Uyumsuzluğun nedenini ve tekrar etmemesi için alınması gereken tedbirleri belirliyor mu? b) Tedbirin uygulanmasını sağlıyor ve sonuçları gözden geçiriyor mu? c) Gözden geçirme sonuçları ve tedbirler kayıt altına alınıyor mu? 		
11.2.2	15.2.2	Teknik uyum kontrolü (idari + teknik)	<p>Bilgi sistemleri, güvenlik uygulama standartları ile uyumun sağlanması için düzenli olarak kontrol ediliyor mu?</p> <p>Teknik uyumluluk testleri sadece yetkili personel eşliğinde yapılıyor mu?</p> <p>Sızma (Penetrasyon) testleri ve açıklık analizleri yapılıyorsa bu esnada sistem güvenliğinin sekteye uğramaması için gerekli tedbirler alınıyor mu?</p>		

11.3	15.3	Bilgi Sistemi Denetimi İle İlgili Hususlar			
11.3.1	15.3.1	Bilgi sistemleri denetim kontrolleri (idari + teknik)	Denetleme gereksinim ve aktiviteleri dolayısıyla çalışmakta olan sistemler üstünde kontroller yapılırken, iş sürecinin asgari düzeyde zarar görmesi için dikkatle planlama yapıldı mı? Denetim gereksinimleri ve kapsamı konusunda yönetim ile anlaşmaya varıldı mı? Yazılım ve veri ile ilgili kontroller salt okuma şeklinde gerçekleştiriliyor mu?		
11.3.2	15.3.2	Denetim araçlarının korunması (idari + teknik)	Yazılım ve veri dosyaları gibi sistem denetleme gereçlerine erişim, herhangi bir yanlış veya kötü niyetli kullanıma karşı korumaya alınmış mı? Sistem denetleme gereçleri -ilave koruma sağlanmadığıysa- geliştirme sisteminden ve çalışmakta olan sistemden ayrılmış mı?		