Payment Card Industry (PCI)

Veri Güvenliği Standardı

PCI DSS Sürüm 2.0'dan 3.0'a Değişiklikler Özeti

Kasım 2013

Giriş

Bu belge, PCI DSS v2.0'dan PCI DSS v3.0'a olan değişikliklerin bir özetini sağlar. Tablo 1, PCI DSS v3.0'da bulunan değişikliklerin türlerine bir genel bakış sunar. Tablo 2, PCI DSS v3.0'da bulunan malzeme değişikliklerinin bir özetini sağlar.

Tablo 1: Değişiklik Türleri

Değişiklik Türü	Tanım
Açıklama	Gerekliliğin amacını açıklar. Standarttaki kısa ifadenin, gereksinimlerin istenen amacını tanımlamasını sağlar.
Ek kılavuz	Anlaşılırlığı artırmak veya belirli bir konuda daha fazla bilgi ya da kılavuz sağlamak için açıklama, tanım ve/veya talimat.
Gelişen Gereksinim	Standartların, ortaya çıkan tehditlerle ve pazardaki değişikliklerle güncel olmasını sağlamak için değişir.

Tablo 2: Değişiklik Özeti

Kısım		Değişiklik	Tür
PCI DSS v2.0	**PCI DSS v3.0**		
PCI DSS Uygulanabilirlik Bilgileri	PCI DSS Uygulanabilirlik Bilgileri	Ortamda hiç PAN olmasa da, yetkilendirmeden sonra SAD'nin saklanmaması gerektiği açıklandı.	Açıklama
PCI DSS ve PA-DSS arasındaki ilişki	PCI DSS ve PA-DSS arasındaki ilişki	PA-DSS doğrulanmış olsa da, kart sahibi verilerini saklayan, işleyen ya da ileten tüm uygulamaların, bir kuruluşun PCI DSS değerlendirmesinin kapsamında olduğu açıklandı. PCI DSS'nin ödeme uygulaması sağlayıcılarına uygulanabilirliği açıklandı.	Açıklama
PCI DSS Gereksinimleriyle Uyum İçin Değerlendirme Kapsamı	PCI DSS Gereksinimlerinin Kapsamı	Sistem bileşenleri örnekleri ile değerlendirme kapsamının nasıl doğru biçimde belirleneceği konusunda kılavuz eklendi. Bölümlemenin amacı açıklandı. PCI DSS gereksinimlerinin kapsamına yönelik hem üçüncü tarafın hem de müşterilerinin sorumluluklarına ve üçüncü tarafların, müşterilerinin üçüncü tarafın PCI DSS değerlendirmesinin kapsamını doğrulayabilmesi için sağlamalarının beklendiği kanıt açıklandı.	Ek Kılavuz
	PCI DSS'yi Olağan İşletme İşlemlerine Uygulama	Devam eden PCI DSS uyumunu sürdürmek amacıyla güvenliği olağan işletme (BAU) etkinliklerine uygulamaya yönelik "işin olağan akışı" kılavuzu sağlayan yeni kısım. Bu kısmın, yeni PCI DSS gereksinimleri değil, yalnızca öneriler ve kılavuz içerdiğine dikkat edin.	Ek Kılavuz
	Değerlendirme Prosedürleri	PCI DSS kapsam kısmını örnekleme kısmından ayırmak için yeni başlık eklendi.	Açıklama
Ticari Tesislerin/Sistem Bileşenlerinin Örneklemesi	Denetçiler için: Ticari Tesislerin/Sistem Bileşenlerinin Örneklemesi	Denetçiler için örnekleme kılavuzu iyileştirildi.	Ek Kılavuz
Uyumluluk Konusunda Rapor İçin Talimatlar ve İçerik	Uyumluluk Konusunda Rapor İçin Talimatlar ve İçerik	Önceki içerik, PCI DSS ROC Şablonu ve PCI DSS ROC Raporlama Talimatları belgelerini ayırmak için yeniden konumlandırıldı.	Açıklama
PCI DSS Uyumu – Tamamlama Adımları	PCI DSS Değerlendirme İşlemi	Belgeler yerine değerlendirme işlemine odaklanmak için kısım güncellendi.	Açıklama
Ayrıntılı PCI DSS Gereksinimleri ve Güvenlik Değerlendirme Prosedürleri	Ayrıntılı PCI DSS Gereksinimleri ve Güvenlik Değerlendirme Prosedürleri	Bu kısmın başlangıcında, bu kısmın sütun başlıklarını tanımlamak için dil eklendi ve "Yürürlükte", "Yürürlükte Değil" ve "Hedef Tarih/Yorumlar" sütunlarına olan başvurular kaldırıldı.	Açıklama

PCI DSS gereksinimleri boyunca genel değişiklikler uygulandı	Tür
Önceki PCI DSS kılavuzu belgesinden elde edilen içerikle, her gereksinimin amacını açıklamak için yeni sütun. Bu sütundaki kılavuzun, gereksinimlerin anlaşılmasına yardımcı olması amaçlanır ve PCI DSS Gereksinimleri ve Test Prosedürlerini değiştirmez ya da genişletmez.	Ek Kılavuz
Güvenlik politikaları ve günlük operasyonel prosedürler için (önceki gereksinim 12.1.1 ve 12.2) yeni bir güvenlik numarası atandı ve gereksinimler ile test prosedürleri Gereksinim 1-11'in her birine taşındı.	Açıklama
Uyum ve tutarlılık için, gereksinimler ve/veya karşılık gelen test prosedürlerinde dil güncellendi.	Açıklama
Anlaşılırlık için karmaşık gereksinimler / test prosedürleri ayrıldı ve fazla ya da örtüşen test prosedürleri kaldırıldı.	Açıklama
Her gereksinim için beklenen doğrulama düzeyine açıklık getirmek için test prosedürleri iyileştirildi.	Açıklama
Diğer genel düzenleme değişiklikleri şunlardır: • Aşağıdaki sütunlar kaldırıldı: “Yürürlükte”, “Yürürlükte Değil” ve “Hedef Tarih/Yorumlar”. • Değişikliklere uyum sağlamak için gereksinimler ve test prosedürleri yeniden numaralandırıldı. • Gereksinimler ve test prosedürleri, okunabilirlik için yeniden biçimlendirildi; örneğin, paragraftaki içerik madde işaretli olarak yeniden biçimlendirildi. • Okunabilirlik için, baştan sona küçük ifade değişiklikleri yapıldı. • Baskı hataları düzeltildi	

Gereksinim		Değişiklik	Tür
PCI DSS v2.0	PCI DSS v3.0		
Gereksinim 1			
1.1.x	1.1.x	Hem güvenlik duvarı hem de yönlendirici standartlarının belgelenmesi ve uygulanması gerektiği açıklandı.	Açıklama
1.1.2	1.1.2 1.1.3	Ağ şemasının ne içermesi gerektiği açıklandı ve kart sahibi verileri akışlarını gösteren bir güncel şema için 1.1.3'te yeni gereksinim eklendi.	Gelişen Gereksinim
1.1.5	1.1.6	SNMP v1 ve v2'yi belirlemek için güvenli olmayan hizmetler, protokoller ve bağlantı noktalarının örnekleri açıklandı.	Açıklama
1.2.2	1.2.2	Yönlendirici yapılandırma dosyalarının güvenli kılınması amacının, dosyaları yetkisiz erişimden korumak olduğu açıklandı.	Açıklama
1.2.3	1.2.3	Kablosuz ağlar ve CDE arasındaki trafiği kontrol etme amacının “yalnızca yetkilendirilmiş trafiğe izin vermek” olduğu açıklandı.	Açıklama

Gereksinim		Değişiklik	Tür
PCI DSS v2.0	PCI DSS v3.0		
1.3.4	1.3.4	Gerekliliğin amacının, sahte kaynaklı IP adreslerini algılamak ve ağa girmelerini engellemek için sahtekârlığa karşı önlemler olduğu açıklandı.	Açıklama
1.4	1.4	Tutarlılık için, gereksinim ve test prosedürleri arasında dil uyumu sağlandı.	Açıklama
Gereksinim 2			
2.1	2.1	Sağlayıcının varsayılan şifrelerinin değiştirilmesine yönelik gereksinimin, sistemler, uygulamalar, güvenlik yazılımı, terminaller vb. unsurları da içermek üzere tüm varsayılan şifrelere uygulandığına ve gereksiz varsayılan hesapların kaldırıldığına ya da devre dışı bırakıldığı açıklandı.	Açıklama
2.1.1	2.1.1	Gerekliliğin amacının, tüm kablosuz sağlayıcı varsayılanlarının kurulumda değiştirilmesine yönelik olduğu açıklandı.	Açıklama
2.2	2.2	Sistem yapılandırma standartlarının, sağlayıcı tarafından sunulan tüm varsayılanların ve gereksiz varsayılan hesapların değiştirilmesine yönelik prosedürler içerdiği açıklandı.	Açıklama
2.2.2	2.2.2 2.2.3	2.2.2'deki gereksinim, *gerekli* hizmetler, protokoller ve bağlantı noktalarına (2.2.2) ve *güvenli* hizmetler, protokoller ve bağlantı noktalarına (2.2.3) ayrı ayrı odaklanmak için iki gereksinime ayrıldı.	Açıklama
	2.4	Yapılandırma standartlarının gelişimini desteklemek amacıyla PCI DSS'ye yönelik kapsamda sistem bileşenlerinin bir envanterini tutmak için yeni gereksinim.	Gelişen Gereksinim
Gereksinim 3			
3.1 3.1.1	3.1	Açıklık getirmek ve fazlalığı gidermek için, gereksinim 3.1.1 ve test prosedürleri gereksinim 3.1'de birleştirildi.	Açıklama
3.2	3.2	Hassas kimlik doğrulama verileri alınması durumunda, yetkilendirme işleminin tamamlanması üzerine kurtarılamaz hale getirildiği açıklandı. Şirketlere yönelik test prosedürlerinin, verme hizmetlerini desteklediğine ve hassas kimlik doğrulama verilerini sakladığı açıklandı.	Açıklama
3.3	3.3	Önceki not gereksinimin gövdesiyle birleştirilerek ve test prosedürleri iyileştirilerek, PAN'ların maskelenmesine yönelik gereksinimin amacı açıklandı.	Açıklama

Gereksinim		Değişiklik	Tür
PCI DSS v2.0	PCI DSS v3.0		
3.4.1	3.4.1	Disk şifreleme için mantıksal erişimin, yerel işletim sistemi *kimlik doğrulama* ve erişim kontrolü mekanizmalarından *ayrı* ve bağımsız olarak yönetilmesi ve şifre çözme anahtarlarının kullanıcı hesaplarıyla *ilişkilendirilmemesi* gerektiği açıklandı.	Açıklama
3.5	3.5	Anahtar yönetimi prosedürlerinin hem uygulanması hem de belgelenmesi gerektiği açıklandı.	Açıklama
3.5.2	3.5.2 3.5.3	Gereksinim 3.5.2, kriptografik anahtarların güvenli bir biçimde (3.5.2) ve olası en az konumda (3.5.3) saklanmasına ayrı ayrı odaklanmak için iki gereksinime ayrıldı. Gereksinim 3.5.2, kriptografik anahtarların güvenli saklanmasına yönelik daha fazla seçenekle esneklik de sağlamaktadır.	Açıklama
3.6.x	3.6.x	Kriptografik anahtar yönetimi prosedürlerinin uygulanmasını doğrulamak için test prosedürleri eklendi.	Açıklama
3.6.6	3.6.6	Bölünmüş bilgi ve ikili kontrol ilkeleri açıklandı.	Açıklama
Gereksinim 4			
4.1	4.1	Tutarlılık için, gereksinim ve test prosedürleri arasında dil uyumu sağlandı. Açık, kamusal ağların örnekleri de genişletildi.	Açıklama
Gereksinim 5			
Gereksinim 5 - Genel		Gerekliliğin amacını yansıtmak için başlık güncellendi (*tüm sistemleri kötücül yazılımlara karşı korumak amacıyla).*	Açıklama
	5.1.2	Kötü amaçlı yazılımlardan yaygın olarak etkilendiği düşünülmeyen sistemlere yönelik gelişen kötücül yazılım tehditlerini değerlendirmek için yeni gereksinim.	Gelişen Gereksinim
5.2	5.2	Tutarlılık için, gereksinim ve test prosedürleri arasında dil uyumu sağlandı.	Açıklama
	5.3	Virüsten koruma çözümlerinin etkin biçimde çalışmasını (daha önce 5.2'de) ve olay temelinde yönetimce özel olarak yetkilendirilmediği sürece kullanıcılar tarafından devre dışı bırakılamamasını ya da değiştirilememesini sağlamak için yeni gereksinim.	Gelişen Gereksinim
Gereksinim 6			

Gereksinim		Değişiklik	Tür
PCI DSS v2.0	PCI DSS v3.0		
6.2	6.1	Gereksinimler 6.1 ve 6.2'nin sırası değiştirildi. Artık, gereksinim 6.1 yeni güvenlik açıklarının belirlenmesi ve risk derecelendirmesi, 6.2 de, önemli güvenlik açıklarına yama uygulanması için kullanılmaktadır. Risk derecelendirme işleminin (6.1), yama uygulama işlemiyle (6.2) nasıl uyumlu olduğu açıklandı.	Açıklama
6.1	6.2	6.1 için yukarıdaki açıklamaya bakın. Ayrıca, bu gereksinimin, "uygulanabilir" yamalara da uygulandığı açıklandı.	Açıklama
6.3	6.3	Yazılı yazılım geliştirme işlemlerine yönelik gereksinimin, tüm dahili olarak geliştirilen yazılımlara ve sipariş edilen yazılımlara uygulandığına açıklık getirmek için bir not eklendi.	Açıklama
6.3.1	6.3.1	Gerekliliğin amacına açıklık getirmek için, "ön üretim" ifadesi "geliştirme/test" olarak değiştirildi	Açıklama
6.4	6.4	6.4.1 ila 6.4.4 arasındaki tüm gereksinimlere yönelik belge gözden geçirmeleri içermek için test prosedürleri iyileştirildi.	Açıklama
6.4.1	6.4.1	Üretim/geliştirme ortamlarının ayrımının erişim kontrolleriyle uygulandığına açıklık getirmek için, gereksinimle test prosedürleri arasında dil uyumu sağlandı.	Açıklama
6.5	6.5	Yaygın kodlama güvenlik açıklarının nasıl engellendiğini içermek ve hassas verilerin bellekte nasıl işlendiğini anlamak için geliştirici eğitimi güncellendi.	Açıklama
6.5.x	6.5.x	Geçerli ve ortaya çıkan kodlama güvenlik açıklarını ve güvenli kodlama kılavuzlarını yansıtmak için gereksinimler güncellendi. Kodlama tekniklerinin güvenlik açıklarını nasıl ele aldığına açıklık getirmek için test prosedürleri güncellendi.	Açıklama
	6.5.10	Bozuk kimlik doğrulama ve oturum yönetimine karşı koruma sağlamak için kodlama uygulamalarına yönelik yeni gereksinim. *Yürürlük tarihi 1 Temmuz 2015*	Gelişen Gereksinim
6.6	6.6	"Web uygulaması güvenlik duvarı" yerine, *web tabanlı saldırıları algılayan ve önleyen otomatik teknik çözüm belirlenerek* esneklik artırıldı. Bu değerlendirmenin, 11.2'de zorunlu kılınan güvenlik açığı taramalarıyla aynı olmadığına açıklık getirmek için not eklendi.	Açıklama
Gereksinim 7			
7.1	7.1	Gereksinim 7.1.1 ila 7.1.4'teki değişiklikler esas alınarak, politikanın ne içerdiğine açıklık getirmek için test prosedürü başka şekilde ifade edildi.	Açıklama

Gereksinim		Değişiklik	Tür
PCI DSS v2.0	PCI DSS v3.0		
	7.1.1	Gereksinim 7.1.2 ila 7.1.4'ü desteklemek amacıyla, her role yönelik erişim gereksinimlerinin tanımını dâhil etmek için yeni 7.1.1.	Açıklama
7.1.1	7.1.2	Ayrıcalıklı kullanıcı kimliklerinin gerekli olan en az ayrıcalıkla kısıtlanması konusundaki gereksinime yeniden odaklanıldı ve test prosedürleri iyileştirildi.	Açıklama
7.1.2	7.1.3	Bağımsız iş sınıflandırması ve işlevi temelinde erişim ataması konusundaki gereksinime yeniden odaklanıldı.	Açıklama
7.1.4		Önceki gereksinim 7.1.4 kaldırıldı (Gereksinim 7.2'de ele alındı)	Açıklama
Gereksinim 8			
Gereksinim 8 - Genel		Gerekliliğin amacını (sistem bileşenlerine tüm erişimi belirleme ve kimliklerini doğrulama) yansıtmak için başlık güncellendi. Kullanıcı kimlik doğrulamasına ve tanımlamasına daha bütünsel bir yaklaşım sağlamak için gereksinimler güncellendi ve yeniden düzenlendi: • Kullanıcı tanımlaması konusunda 8.1'e odaklanıldı • Kullanıcı kimlik doğrulaması konusunda 8.2'ye odaklanıldı • Şifreler dışındaki kimlik doğrulama yöntemlerini göz önünde bulundurmak için gereksinimler güncellendi • Gerekliliğin yalnızca şifrelere/parolalara uygulandığı yerlerde, “şifreler” ifadesi “şifreler/parolalar” olarak değiştirildi • Gerekliliğin, herhangi bir kimlik doğrulama bilgileri türüne uygulandığı yerlerde, “şifreler” ifadesi “kimlik doğrulama bilgileri” olarak değiştirildi • Şifre güvenliği gereksinimlerinin, üçüncü taraf sağlayıcılarca kullanılan hesaplara uygulandığı açıklandı	Açıklama
8.5.6	8.1.5	Uzak sağlayıcı erişimine yönelik gereksinimin, sistem bileşenlerine erişen, destekleyen ya da sürdüren sağlayıcılara uygulandığına ve kullanımda değilken devre dışı bırakılması gerektiği açıklandı.	Açıklama
8.4.2	8.2.1	İletim ve depolama sırasında kimlik doğrulama bilgilerinin okunamaz hale getirilmesi için güçlü kriptografi kullanılması gerektiği açıklandı.	Açıklama
8.5.2	8.2.2	Kimlik doğrulama bilgilerinin düzenlenmesinden önce kullanıcı kimliğinin doğrulanması gerektiği açıklandı ve düzenleme örnekleri olarak yeni andaçlar tedarik etme ve yeni anahtarlar oluşturma eklendi.	Açıklama

Gereksinim		Değişiklik	Tür
PCI DSS v2.0	PCI DSS v3.0		
8.5.10 8.5.11	8.2.3	En az şifre karmaşıklığı ve gücü gereksinimleri tek bir gereksinimte birleştirilerek eşdeğer karmaşıklığı ve gücü karşılayan alternatifler için esneklik artırıldı.	Gelişen Gereksinim
8.3	8.3	İki faktörlü kimlik doğrulamaya yönelik gereksinimin kullanıcılara, yöneticilere ve destek ya da bakım için üye iş yeri erişimi de dahil olmak üzere tüm üçüncü taraflara uygulandığı açıklandı.	Açıklama
8.5.7	8.4	Şifre/parola yeniden kullanımını ve tehlikede olduğundan şüphelenildiğinde şifre/parola değiştirmeyi de dâhil etmek üzere, kullanıcıların kimlik doğrulama bilgilerini nasıl korumaları gerektiğine yönelik belgelendirme ve iletme kılavuzunu dâhil etmek için gereksinim güncellendi.	Açıklama
	8.5.1	Her müşteri için benzersiz kimlik doğrulama bilgilerini kullanmak amacıyla, müşteri tesislerine uzaktan erişime sahip hizmet sağlayıcılara yönelik yeni gereksinim. *Yürürlük tarihi 1 Temmuz 2015*	Gelişen Gereksinim
	8.6	Diğer kimlik doğrulama mekanizmalarının kullanıldığı yerlerde (örneğin, fiziksel ya da mantıksal güvenlik andaçları, akıllı kartlar, sertifikalar vb.) mekanizmaların bireysel bir hesaba bağlanması gerektiğine ve o mekanizmayla yalnızca amaçlanan kullanıcının erişim hakkına sahip olacağının sağlanmasına yönelik yeni gereksinim.	Gelişen Gereksinim
8.5.16	8.7	Tutarlılık için, gereksinim ve test prosedürleri arasında dil uyumu sağlandı.	Açıklama
Gereksinim 9			
9.1.2	9.1.2	Gerekliliğin amacının, genel olarak erişilebilen ağ girişlerini korumak için fiziksel ve/veya mantıksal erişim kontrolleri uygulamak olduğu açıklandı.	Açıklama
9.2.x	9.2.x	Tesis içi personel ve ziyaretçileri belirlemek, aralarında ayrım yapmak ve erişim vermek için gereksinimin amacına ve yaka kartlarının seçeneklerden yalnızca biri olduğu (gerekli değillerdir) açıklandı.	Açıklama
	9.3	Erişimi yetkilendirmek amacıyla bir işlem dahil olmak üzere, tesis içi personel için hassas alanlara fiziksel erişimi kontrol etmeye ve sonlandırmanın hemen ardından erişimi iptal etmeye yönelik yeni gereksinim.	Gelişen Gereksinim
9.3.x	9.4.x	Tutarlılık ve ziyaretçilere her zaman eşlik edilmesi, ziyaretçi etkinliğinin denetim izinin, tesise, bilgisayar odasına ve/veya veri merkezine erişimi içermesi gerektiğine açıklık getirmek için gereksinim ve test prosedürleri arasında dil uyumu sağlandı.	Açıklama

Gereksinim		Değişiklik	Tür
PCI DSS v2.0	PCI DSS v3.0		
9.5 – 9.10	9.5 – 9.8	Önceki gereksinim 9.6 taşındı ve 9.5 olarak yeniden numaralandırıldı; önceki gereksinim 9.5, alt gereksinim 9.5.1 olarak yeniden numaralandırıldı. Önceki gereksinim 9.7, 9.6 olarak yeniden numaralandırıldı; önceki gereksinim 9.8, alt gereksinim 9.6.3 olarak yeniden numaralandırıldı. Önceki gereksinim 9.9, 9.7 olarak yeniden numaralandırıldı; önceki gereksinim 9.10, 9.8 olarak yeniden numaralandırıldı.	Açıklama
	9.9.x	Kartla doğrudan fiziksel etkileşimle ödeme kartı verilerini alan cihazları kurcalamaya ve değiştirmeye karşı korumak için yeni gereksinimler. *Yürürlük tarihi 1 Temmuz 2015*	Gelişen Gereksinim
Gereksinim 10			
10.1	10.1	Denetim kılavuzlarının, yalnızca bir işlem oluşturmak yerine, her bağımsız kullanıcı için sistem bileşenlerine erişime bağlamak amacıyla uygulanması gerektiği açıklandı.	Açıklama
10.2.1	10.2.1	Amacın, kart sahibi verilerine tüm bağımsız *kullanıcı* erişiminin denetim izlerine dâhil edilmesine yönelik olduğu açıklandı.	Açıklama
10.2.5	10.2.5	Belirleme ve kimlik doğrulama mekanizmalarındaki değişiklikleri (yeni hesapların oluşturulması, ayrıcalıkların yükseltilmesi dahil) ve kök ya da yönetici erişimine sahip hesaplardaki tüm değişiklik, ekleme ve silme işlemlerini dahil etmek için gereksinim iyileştirildi.	Gelişen Gereksinim
10.2.6	10.2.6	Denetim günlüklerinin durdurulmasını veya duraklatılmasını dahil etmek için gereksinim iyileştirildi.	Gelişen Gereksinim
10.6	10.6.x	Günlük gözden geçirmelerin amacının, anormallikleri ya da şüpheli etkinlikleri belirlemek olduğu açıklandı ve her günkü günlük gözden geçirmelerin kapsamı konusunda daha fazla rehberlik sağlandı. Kuruluşun risk yönetimi stratejisiyle tanımlandığı gibi, güvenlik olayları ve önemli sistem günlüklerinin günlük olarak ve diğer günlük olaylarının düzenli olarak gözden geçirilmesi için de daha fazla esneklik sağlandı.	Açıklama
Gereksinim 11			
11.1.x	11.1.x	Yetkisiz kablosuz cihazları taramayı desteklemek amacıyla, yetkili kablosuz erişim noktalarının envanterini ve bir ticari gerekçeyi (11.1.1) dahil etmek için gereksinim iyileştirildi ve yetkisiz kablosuz erişim noktaları algılandığında olay tepkisi prosedürleri için, zaten var olan test prosedürüyle uyum sağlamak amacıyla yeni gereksinim 11.1.2 eklendi.	Gelişen Gereksinim

Gereksinim		Değişiklik	Tür
PCI DSS v2.0	PCI DSS v3.0		
11.2	11.2	Bir geçer sonuç elde etmek ve belgelemek için, birden fazla tarama raporunu birleştirme konusunda rehberlik eklendi.	Ek Kılavuz
11.2.1	11.2.1	Üç aylık dâhili güvenlik açığı taramalarının, tüm "yüksek" güvenlik açıkları (PCI DSS Gereksinim 6.1 ile belirlendiği gibi) çözülene kadar gerektiği biçimde tekrar taramalar içerdiğine ve yetkili personel tarafından gerçekleştirilmesi gerektiği açıklandı.	Açıklama
11.2.2	11.2.2	Harici güvenlik açığı taramalarının, geçer taramalar elde edilene kadar gerektiği biçimde tekrar taramalar içerdiği açıklandı ve ASV Program Kılavuzuna başvurmak için bir not eklendi.	Açıklama
11.2.3	11.2.3	Önemli değişikliklerden sonra gerçekleştirilen dahili ve harici taramaların, tüm "yüksek" güvenlik açıkları (PCI DSS Gereksinim 6.1 ile belirlendiği gibi) çözülene kadar gerektiği biçimde tekrar taramalar içerdiğine ve yetkili personel tarafından gerçekleştirilmesi gerektiği açıklandı.	Açıklama
	11.3	Sızma testine yönelik bir yöntem uygulamak için yeni gereksinim. *Yürürlük tarihi 1 Temmuz 2015. Sızma testine yönelik PCI DSS v2.0 gereksinimleri v3.0 yürürlükte olana kadar izlenmelidir.*	Gelişen Gereksinim
11.3	11.3.1 11.3.2	Önceki gereksinim 11.3, *harici* sızma testi gereksinimlerine yönelik 11.3.1 ve *dahili* sızma testi gereksinimlerine yönelik 11.3.2 olarak ayrıldı.	Açıklama
11.3	11.3.3	Sızma testi sırasında bulunan kötüye kullanılabilen güvenlik açıklarını düzeltmek ve düzeltmeleri doğrulamak için testi tekrarlamak üzere, önceki test prosedüründen (11.3.b) yeni gereksinim oluşturuldu.	Açıklama
	11.3.4	CDE'yi diğer ağlardan ayırmak amacıyla bölümleme kullanılması durumunda, bölümleme yöntemlerinin çalışır ve verimli olduğunu doğrulamaya yönelik olarak sızma testleri gerçekleştirmek için yeni gereksinim.	Gelişen Gereksinim
11.4	11.4	Ağdaki saldırıları algılamak ve/veya önlemek için *"saldırı algılama sistemleri ve/veya saldırı önleme sistemleri" yerine* saldırı algılama ve/veya saldırı önleme teknikleri belirlenerek esneklik artırıldı.	Açıklama
11.5	11.5	"Dosya bütünlüğü izleme" yerine *değişiklik algılama mekanizması* belirlenerek esneklik artırıldı.	Açıklama
	11.5.1	Değişiklik algılama mekanizması tarafından üretilen uyarılara yanıt vermek amacıyla bir işlem uygulamak için yeni gereksinim (11.5'i destekler)	Gelişen Gereksinim

Gereksinim		Değişiklik	Tür
PCI DSS v2.0	PCI DSS v3.0		
Gereksinim 12			
12.1.1 12.2	1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6	12.1.1'deki (tüm PCI DSS gereksinimlerini ele almak için bilgi güvenliği politikasına yönelik) ve 12.2'deki (operasyonel güvenlik prosedürlerine yönelik) önceki gereksinimler birleştirildi ve bunlar, her birinde bir gereksinim olarak Gereksinim 1 ila 11'e taşındı.	Açıklama
12.1.3	12.1.1	Önceki gereksinim 12.1.3, 12.1.1'e taşındı.	Açıklama
12.1.2	12.2	Yıllık risk değerlendirmesi işlemine yönelik önceki gereksinim 12.1.2, 12.2'ye taşındı ve risk değerlendirmesinin, en az yıllık olarak *ve ortamdaki önemli değişiklikler sonrasında gerçekleştirilmesi gerektiği açıklandı*.	Gelişen Gereksinim
12.3.4	12.3.4	"Etiketlemenin", kullanılacak bir yöntem örneği olduğu açıklandı.	Açıklama
12.3.8	12.3.8	Belirli bir süre etkinlik olmamasından sonra uzaktan erişim oturumlarının bağlantısını kesmeye yönelik olarak politikanın uygulandığını doğrulamak için yeni test prosedürü.	Açıklama
12.3.10	12.3.10	Personelin, uzaktan erişim teknolojileri aracılığıyla kart sahibi verilerine erişmek için yetkilendirilmiş bir ticari gereksinimi olduğunda, verilerin, tüm uygulanabilir PCI DSS Gereksinimlerine göre korunması gerektiğine açıklık getirmek amacıyla gereksinim ve test prosedürleri arasında dil uyumu sağlandı.	Açıklama
12.8	12.8	Amacın, kart sahibi verilerinin paylaşıldığı hizmet sağlayıcıları yönetmek amacıyla politikalar ve prosedürler uygulanıp sürdürüldüğüne, aksi halde kart sahibi verilerinin güvenliğini etkileyebileceği açıklandı.	Açıklama
12.8.2	12.8.2	Hizmet sağlayıcının yazılı sözleşmesine/kabulüne yönelik geçerli sorumluluklar açıklandı.	Açıklama
	12.8.5	Her bir hizmet sağlayıcı tarafından hangi PCI DSS gereksinimlerinin yönetildiği ve hangilerinin kuruluş tarafından yönetildiği konusunda bilgi tutmak için yeni gereksinim.	Gelişen Gereksinim
	12.9	Hizmet sağlayıcıların, gereksinim 12.8'de belirtildiği şekliyle müşterilerine yazılı sözleşme/kabul sağlamasına yönelik yeni gereksinim. *Yürürlük tarihi 1 Temmuz 2015*	Gelişen Gereksinim

Gereksinim		Değişiklik	Tür
PCI DSS v2.0	PCI DSS v3.0		
12.9.x	12.10.x	Gereksinim yeniden numaralandırıldı ve amacın, *güvenlik izleme sistemlerinden* gelen uyarıların olay tepkisi planına dahil edileceğine yönelik olduğunu açıklamak için 12.10.5 güncellendi.	Açıklama