Ödeme Kartları Endüstrisi (PCI)
Veri Güvenliği Standardı
Kendini Değerlendirme Anketi

Talimat ve Kılavuzlar

Sürüm 3.2.1

Haziran 2018

Belge Değişiklikleri

Tarih	Sürüm	Açıklama
1 Ekim 2008	1.2	İçeriği, yeni PCI DSS v1.2 ile uyumlu hale getirmek ve orijinal v1.1'den bu yana kaydedilen küçük değişiklikleri uygulamak için.
28 Ekim 2010	2.0	İçeriği, yeni PCI DSS v2.0 ile uyumlu hale getirmek ve SAQ platform türleri ile uygunluk kriterlerini netleştirmek için. Web tabanlı Sanal Terminali olan üye işyerleri için SAQ C-VT'nin eklenmesi
Haziran 2012	2.1	Kart sahibi verilerini yalnızca doğrulanmış ve PCI SSC listesinde bulunan PCI Noktadan Noktaya Şifreleme (P2PE) çözümünde yer alan donanım ödeme terminalleri üzerinden işleyen üye işyerleri için SAQ P2PE-HW eklenmesi. İşbu belge, PCI DSS sürüm 2.0 ile kullanılmak üzere oluşturulmuştur.
Nisan 2015	3.1	SAQ'lar A-EP ve B-IP'nin eklenmesi de dahil olmak üzere, içeriği PCI DSS v3.1 ile uyumlu hale getirmek ve mevcut SAQ'lara uygunluk kriterlerini netleştirmek için.
Mayıs 2016	3.2	PCI DSS v3.2 ile uyumlu hale getirmek ve mevcut SAQ'lara uygunluk kriterlerini netleştirmek için güncellendi.
Haziran 2018	3.2.1	PCI DSS v3.2.1 ile uyumlu hale getirmek için küçük güncellemeler.

SORUMLULUK REDDİ: Bu belgenin, PCI SSC web sitesinde yer alan İngilizce sürümü, tüm amaçlar için, bu belgelerin resmi sürümü olarak kabul edilir ve bu metin ile İngilizce metnin yazımı arasında herhangi bir belirsizlik veya tutarsızlık olması durumunda, bahsedilen konumda bulunan İngilizce sürüm geçerli olacaktır.

İçindekiler

Bu Belge Hakkında

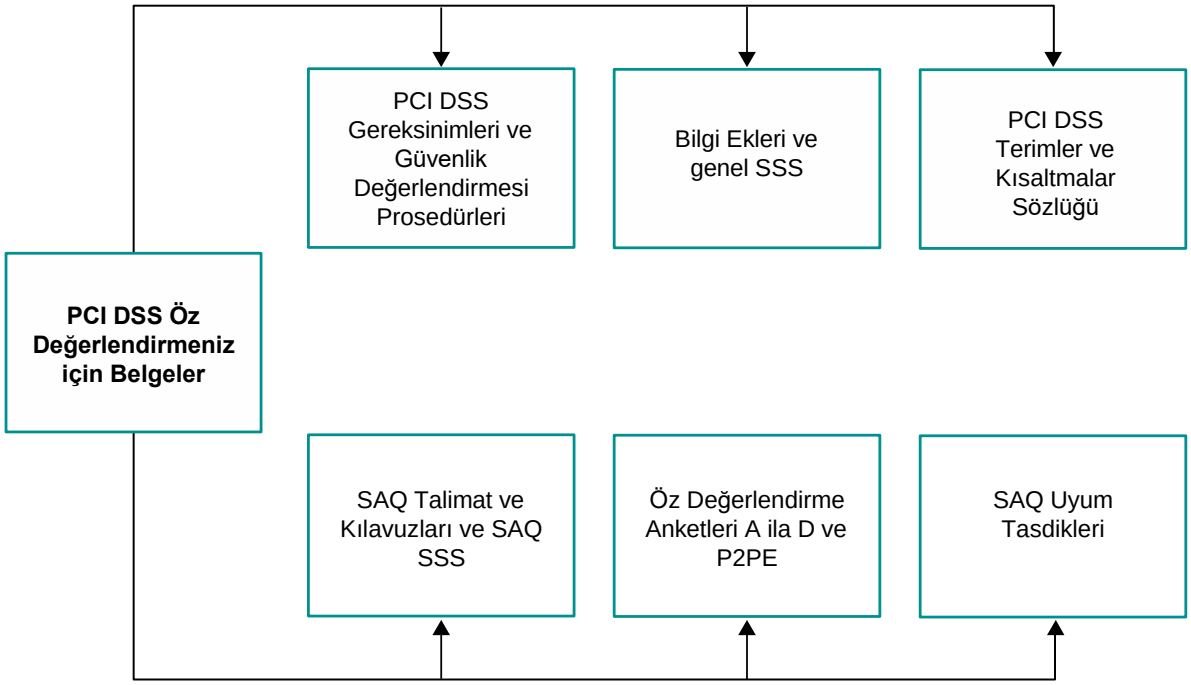
İşbu belge, üye işyerleri ile hizmet sağlayan firmaların, Ödeme Kartları Endüstrisi Veri Güvenliği Standardı (PCI DSS) Öz Değerlendirme Anketlerini (SAQ'lar) anlamalarına yardımcı olmak amacıyla oluşturulmuştur. PCI DSS'nin kuruluşunuz açısından neden önemli olduğunu, kuruluşunuzun PCI DSS uyum onayını kolaylaştırmak için hangi stratejileri kullanabileceğinizi ve kuruluşunuzun daha kısa SAQ'lardan birini tamamlamaya uygun olup olmadığını anlamak için işbu Talimat ve Kılavuzlar belgesinin tamamını incelemenizi tavsiye ederiz

PCI DSS Öz Değerlendirme: Her Şey Nasıl Yerine Oturur

PCI DSS ile destekleyici belgeler, kart sahiplerinin verilerinin güvenli bir şekilde kullanılmasını sağlamak amacını taşıyan endüstri araçlarının genel dizinini temsil eder. Standardın kendisi, güvenlik olaylarını önleme, bunları tespit etme ve bu olaylara tepki vermek de dahil olmak üzere sağlam bir güvenlik süreci geliştirmek için işlemeye uygun bir çerçeve sunar. Veri ihlali riskini azaltmak ve veri ihlali olması halinde etkisini azaltmak açısından, kart sahiplerinin verilerini depolayan, işleyen veya aktaran tüm kuruluşlar için uyumlu olması önem taşımaktadır.

Aşağıdaki tabloda, PCI DSS uyumu ve öz değerlendirme konusunda kuruluşlara yardımcı olmada kullanılan araçlar açıklanmaktadır.

Bunlara ve diğer ilgili belgelere www.pcisecuritystandards.org adresinden erişilebilir.



** Bilgi Eklerinin, yalnızca ek bilgi ve kılavuzluk sağladığı, PCI DSS'nin gereksinimlerinin yerine geçmediği ya da bunları hükümsüz kılmadığını unutmayın.*

* ***Not:*** *Bilgi Ekleri, yalnızca ek bilgi ve kılavuzluk sağlar, PCI DSS'nin gereksinimlerinin yerine geçmez ya da bunları hükümsüz kılmaz.*

SAQ'ya Genel Bakış

PCI DSS Öz Değerlendirme Anketleri (SAQ'lar), üye işyerleri ve hizmet sağlayan firmaların PCI DSS uyumlarını kendi kendilerine değerlendirmelerine yardımcı olmada kullanılan doğrulama araçlarıdır. Farklı senaryolara uygun birçok PCI DSS SAQ sürümü mevcuttur. İşbu belge, kuruluşunuzun sisteminize en uygun SAQ'nın/SAQ'ları belirlemesine yardımcı olmak için oluşturulmuştur.

PCI DSS SAQ, ilgili POS hizmeti veren bankalarının veya kredi kartı firmasının/firmalarının PCI DSS Uyum Raporu (ROC) ibraz etmelerini gerektirmediği üye işyerleri ve hizmet sağlayan firmalara yönelik bir doğrulama aracıdır.. PCI DSS doğrulama gereksinimleriyle ilgili ayrıntılar için lütfen POS hizmeti veren bankanıza veya kredi kartı firmanıza danışın.

Her bir PCI DSS SAQ, aşağıdaki bileşenlerden oluşur:

1. Farklı sistemlere uygun olduğu şekilde PCI DSS gereksinimlerine ilişkin sorular: Bu belgedeki “Kuruluşunuz için En Uygun SAQ ve Tasdik Seçme” konusuna bakın. Bu bölümde ayrıca, PCI DSS kapsamındaki test prosedürlerine dayanan “Beklenen Test” için ayrılmış bir sütun da bulunmaktadır.
2. Uygunluk Tasdiki: Tasdik, ilgili SAQ'yu tamamlamaya uygun olduğunuza ilişkin beyanınızı ve bunu izleyen PCI DSS öz değerlendirmesinin sonuçlarını içerir.

PCI DSS'nin Önemi

PCI Veri Güvenliği Standartları Konseyi'nin (American Express, Discover, JCB, Mastercard ve Visa) kurucu üyeleri, hesap verisi ihlallerinin yaşandığı durumları sürekli olarak izler. Bu veri ihlalleri, çok küçükten çok büyük üye işyerleri ve hizmet sağlayan firmalara kadar tüm kuruluş yelpazesini kapsar.

Güvenlik ihlali ve bunun ardından gelen ödeme kartı verilerinin ihlal edilmesi, etkilenen kuruluşlarda aşağıdakiler de dahil olmak üzere geniş kapsamlı sonuçlar doğurur:

1. Düzenleyici makamlara bildirim gereksinimleri,
2. İtibar kaybı,
3. Müşteri kaybı,
4. Olası mali sorumluluklar (örneğin düzenleyici makamlara ödenecek olan ve başka ücret ve para cezaları) ve
5. Dava.

Veri ihlallerinin adli analizi, PCI DSS kontrollerinin ele aldığı genel güvenlik zaaflarının, veri ihlali gerçekleştiği anda PCI DSS kontrolleri uygulanmadığı ya da kötü uygulandığı için sıklıkla istismar edildiğini göstermiştir. PCI DSS, tam da bu nedenle, yani veri ihlali olasılığını ve veri ihlali olması halinde ortaya çıkacak etkileri en aza indirmek için tasarlanmış olup ayrıntılı gereksinimler içermektedir.

Yaygın PCI DSS kontrol hatalarının örnekleri arasında, bunlarla sınırlı olmamak üzere aşağıdakiler sayılabilir:

- Provizyon sonrası manyetik şerit verileri gibi hassas olan kimlik doğrulama verilerinin (SAD) depolanması (Gereksinim 3.2). Veri ihlali yaşanan kuruluşların çoğu, sistemlerinin bu verileri depoladığından bihaberdi.
- Kötü niyetli kullanıcıların POS satıcıları için tasarlanmış yollar üzerinden girmesine izin veren yanlış kurulmuş satış noktası (POS) sistemleri nedeniyle yetersiz erişim kontrolleri (Gereksinimler 7.1, 7.2, 8.2 ve 8.3).
- Sistem kurulduğunda değiştirilmeyen, varsayılan sistem ayarları ve parolaları (Gereksinim 2.1).
- Sistem kurulduğunda kaldırılmayan veya güvenli hale getirilmeyen gereksiz ve güvenliksiz hizmetler (Gereksinimler 2.2.2 ve 2.2.3).
- SQL enjeksiyonu ve diğer güvenlik açıklarıyla sonuçlanan ve kart sahibinin verilerini doğrudan web sitesinden depolayan veri tabanına erişim sağlayan kötü kodlanmış web uygulamaları (Gereksinim 6.5).
- Eksik ve eski güvenlik yamaları (Gereksinim 6.2).
- Günlük kaydı eksikliği (Gereksinim 10).
- İzlemenin olmaması (günlük incelemeleri, sızıntı tespiti/önleme, üç aylık güvenlik açığı taramaları ve değişiklik algılama mekanizmaları üzerinden) (Gereksinimler 10.6, 11.2, 11.4 ve 11.5).
- Kapsam tespitine ilişkin kötü kararların verilmesi; örneğin, etkili olduğu doğrulanmamış ağ segmentasyonu yetersizliğinden dolayı ağın bir kısmının PCI DSS kapsamı dışında tutulması (Gereksinim 11.3.4). Bu, kart sahibi verilerinin depolandığı ortamın, ağın PCI DSS uyarınca güvenli hale getirilmemiş diğer kısımlarında (örneğin, güvenli olmayan kablosuz erişim noktalarından ve çalışanların e-postaları ve web'de gezinmeleriyle karşılaşılan güvenlik açıklarından) farkında olmayarak güvenlik zaaflarına maruz kalmasına neden olur (Gereksinimler 1.2, 1.3 ve 1.4).

Uyum ve güvenlik arasındaki farkı anlama

Uyumlu olma ve güvenli olma arasındaki farkı anlamak önemlidir. Bir noktada PCI DSS ile uyumlu olmak sisteminizdeki durumların değişmesini engellemez; bu da uygun kontrollerin olmadığı hallerde güvenliğinizi etkileyebilir. Bu nedenle, PCI DSS kontrollerinin olağan iş (BAU) faaliyetlerinin bir parçası olarak ve genel güvenlik stratejinizde tanımlandığı şekilde uygulanmaya devam etmesini sağlamalısınız. Bu sayede kuruluşunuzun güvenlik kontrollerinin etkinliğini sürekli olarak izleyebilir ve PCI DSS değerlendirmeleri arasında sisteminizin PCI DSS'ye uygunluğunu sürdürebilirsiniz. PCI DSS'nin BAU faaliyetlerine nasıl dahil edileceğinin örnekleri, PCI DSS'deki “PCI DSS'yi Olağan İş Süreçlerine Uygulamada En İyi Uygulamalar” bölümünde verilmiştir.

Ayrıca, PCI DSS güvenlik gereksinimleri ödeme kartı verilerinin korunması için tasarlanmış olup kuruluşunuzda, PCI DSS kapsamı dışında olabilecek korunması gereken başka hassas veriler ve varlıklar da olabilir. Bu nedenle, gerektiği gibi sürdürülmesi koşuluyla PCI DSS uyumu güvenliğin geneline katkıda bulunabileceği kesin olsa da, sağlam, kuruluş çapında bir güvenlik programının ikamesi olarak görülmemelidir.

PCI DSS Uyumu için Genel İpuçları ve Stratejiler

Aşağıda, PCI DSS uyumuna yönelik çalışmalarınızı başlatmanız için bazı genel ipuçları ve stratejiler verilmiştir. Bu ipuçları, ihtiyacınız olmayan kart sahibi verilerinin depolanmasını durdurmanıza ve ihtiyacınız olan verileri tanımlanmış ve kontrollü merkezi alanlara izole etmenize yardımcı olabilir ve PCI DSS uyumluluk doğrulama çalışmalarınızın kapsamını sınırlamanızı da sağlayabilir. Örneğin, ihtiyacınız olmayan kart sahibi verilerini kaldırarak ve/veya ihtiyacınız olan verileri tanımlanmış ve kontrollü merkezi alanlara izole ederek, kart sahibi verilerini depolamayan, işlemeyen veya iletmeyen ve aynı zamanda bunları yapan sistemlere bağlantısı olmayan sistem ve ağları öz değerlendirmenizin kapsamından çıkarabilirsiniz.

1. **Hassas Olan Kimlik Doğrulama Verileri (manyetik şeridin bant içeriğinin tamamını veya bir çipteki eşdeğer verileri, kart doğrulama kodlarını ve değerlerini, PIN'leri ve PIN bloklarını içerir):**

   Provizyon sonrasında ***bu verileri*** asla depolamadığınızdan emin olun:

2. **Aşağıda önerdiğimiz soruları kullanarak POS satıcınıza sisteminizin güvenliği hakkında sorular sorun:**

   a. POS sisteminin bir parçası olan sistemlerde ve veri tabanlarında varsayılan ayarlar ve parolalar değiştirildi mi?

   b. POS sistemime uzaktan erişiminiz var mı? Uzaktan erişiminiz varsa başkalarının POS sistemime erişmesini önlemek için güvenli uzaktan erişim yöntemleri kullanmak ve genel ya da varsayılan parolalar kullanmamak gibi uygun kontrolleri uyguladınız mı? POS cihazıma uzaktan ne sıklıkta ve neden erişiyorsunuz? POS cihazıma uzaktan erişim yetkisi kimlerde var?

   c. Gereksiz ve güvenli olmayan hizmetlerin hepsi POS sisteminin bir parçası olan sistemlerden ve veri tabanlarından kaldırıldı mı?

   d. POS yazılımım Ödeme Uygulamaları Veri Güvenliği Standardına (PA-DSS) göre doğrulandı mı? (PCI SSC'nin Onaylanmış Ödeme Uygulamaları listesine bakınız.)

   e. POS yazılımım, manyetik şerit verileri veya PIN blokları gibi hassas olan kimlik doğrulama verilerini depoluyor mu? Depoluyorsa bu işlem yasak bir işlemdir: bu verileri silip işlemi durdurmama ne kadar çabuk yardımcı olabilirsiniz?

f. POS yazılımım, kart numaralarını (PAN) depoluyor mu? Depoluyorsa, bu depolama işleminin güvenli olması gerekir: POS cihazı bu verileri nasıl koruyor?

g. Yukarıda belirtilen yasaklanmış verilerin depolanmadığını doğrulamak için uygulamanın yazdığı dosyaların listesini, her dosyanın içeriğinin özetini de içerecek şekilde belgeler misiniz?

h. POS yazılımım tüm kullanıcı erişimi için karmaşık ve benzersiz parolalar uyguluyor mu?

i. Sistemime ve desteklediğiniz diğer üye işyerlerinin sistemlerine erişmek için genel veya varsayılan parolalar kullanmadığınızı teyit edebilir misiniz?

j. POS sisteminin bir parçası olan sistem ve veri tabanlarının hepsinde güvenlik güncelleştirmelerinin tamamını içeren yamalar yapıldı mı?

k. POS sisteminin bir parçası olan sistemlerde ve veri tabanlarında günlük tutma özelliği açık mı?

l. POS yazılımımın önceki sürümleri hassas olan kimlik doğrulama verilerini depoluyorsa bu özellik, POS yazılımında yapılan son güncellemelerde kaldırıldı mı? Bu verileri kaldırırken güvenli silme yardımcı yazılımı kullanıldı mı?

3. Kart sahiplerinin verileri—ihtiyacınız yoksa depolamayın!

a. Kredi kartı firmalarının kurallarına göre kart numarası (PAN), son kullanma tarihi, kart sahibinin adı ve hizmet kodu depolanabilir.

b. Bu verileri depolamanızın tüm nedenlerini ve depoladığınız yerlerin tamamını değerlendirin. Verilerin depolanması işinizle ilgili meşru bir amaca hizmet etmiyorsa bu verileri silmeyi düşünün.

c. Bu verilerin depolanmasının ve desteklediği iş sürecinin aşağıdakilere değer olup olmadığını düşünün:

i. Verilerin veri ihlaliyle karşı karşıya olması riski.

ii. Bu verileri korumak için uygulanması gereken ek PCI DSS kontrolleri.

iii. Zaman içinde PCI DSS uyumunu sürdürmek için gerekecek sürekli bakım çabaları.

4. Kart sahiplerinin verileri—ihtiyacınız varsa birleştirin ve izole edin!

PCI DSS değerlendirmesinin kapsamını, veri depolamayı tanımlı bir ortamda birleştirerek ve doğru ağ segmentasyonu kullanıp verileri izole ederek sınırlandırabilirsiniz. Örneğin, çalışanlarınız, kart sahiplerinin verilerinin bulunduğu makine ya da ağ segmenti ile aynı makine veya ağ segmentini kullanarak İnternet'te geziniyor ve e-posta alıyorsa kart sahiplerinin verilerini kendilerine özel makineye veya ağ segmentine segmentlemeyi (izole etmeyi) (örneğin, routerler veya güvenlik duvarları ile) düşünün. Kart sahiplerinin verilerini etkili bir şekilde izole edebilirseniz PCI DSS çalışmalarınıza makinelerinizin tamamını dahil etmek yerine çalışmalarınızı yalnızca izole edilmiş kısma odaklayabilirsiniz.

5. Telafi Edici Kontroller

Kuruluşun bir gereksinimin teknik şartnamesini karşılayamadığı, ancak alternatif kontroller kullanarak ilişkili riski yeterince azalttığı durumlarda çoğu PCI DSS gereksinimleri için telafi edici kontroller göz önünde bulundurulabilir. Kuruluşunuzun tam olarak PCI DSS'de belirtilen kontrole sahip olmaması, ancak PCI DSS'nın telafi edici kontroller tanımını karşılayan başka kontrollerinin olması halinde (bkz. PCI DSS Ek B'deki ve ayrıca *PPCI DSS ve PA-DSS Terimler ve Kısaltmalar Sözlüğündeki* “Telafi Edici Kontroller”), kuruluşunuz aşağıdakileri yapmalıdır:

a. PCI DSS Ek B'de özetlendiği şekilde telafi edici kontroller prosedürlerini izlemelidir.

b. Telafi edici kontrol yardımıyla karşılanan tüm gereksinimler için, SAQ sorusuna "CCW sütununda EVET" işaretleyerek yanıt verin.

c. SAQ Ek B'deki Telafi Edici Kontroller Çalışma Sayfası doldurarak her telafi edici kontrolü belgeleyin.

> Telafi edici bir kontrolle karşılanan her gereksinim için bir Telafi Edici Kontroller Çalışma Sayfası doldurulmalıdır.

d. Doldurulan Telafi Edici Kontroler Çalışma Sayfalarını, tamamlanmış SAQ ve/veya Uyum Tasdikiniz ile birlikte, POS hizmeti veren bankanızın veya kredi kartı firmanızın talimatlarına göre ibraz edin.

6. Profesyonel Destek ve Eğitim

a. Öz değerlendirmenizde size yardımcı olması için bir güvenlik uzmanı işe almak isterseniz bir Nitelikli Güvenlik Denetmeni (QSA) ile iletişime geçmeyi düşünmenizi öneririz. QSA'lar PCI DSS tarafından, PCI SSC değerlendirmelerini yapmak üzere eğitilmiş olup PCI SSC web sitesi üzerinde listeleri bulunmaktadır.

b. PCI SSC web sitesi, aşağıdakiler de dahil olmak üzere ek kaynaklara ulaşabileceğiniz birincil kaynaktır:

- *PCI DSS Terimler ve Kısaltmalar Sözlüğü*
- Sıkça Sorulan Sorular (SSS)
- Web Seminerleri
- Bilgi Ekleri ve Kılavuzlar
- SAQ formları ve Uyum Tasdikleri

Not: *Bilgi Ekleri, PCI DSS'yi tamamlayıcı nitelikte olup PCI DSS gereksinimlerinin karşılanmasına ilişkin ek hususları ve tavsiyeleri tanımlar—PCI DSS'yi veya herhangi bir gereksinimini değiştirmez, ortadan kaldırmaz ya da bunların yerine geçmez.*

c. PCI SSC ayrıca bir kuruluşun personellerinde farkındalık oluşturmaya yardımcı olmak amacıyla bir dizi eğitim programı sağlamaktadır. Bunların örnekleri arasında PCI Farkındalığı, PCI Profesyoneli (PCIP) programı ve Dahili Güvenlik Denetmeni (ISA) programı sayılabilir.

Daha fazla bilgi almak için lütfen www.pcisecuritystandards.org adresine gidin.

d. Ödeme ile ilgili eğitim programları ve kaynakları, kredi kartı firmalarından ve/veya ye işyerine POS hizmeti veren bankadan da edinilebilir.

Kuruluşunuz için En Uygun SAQ ve Tasdiki Seçme

Tüm üye işyerleri ve hizmet sağlayan firmaların, kendi sistemleri için geçerli olan PCI DSS'e her zaman uymaları gerekmektedir. Aşağıdaki tabloda kısaca gösterilen ve sonraki sayfalarda daha ayrıntılı olarak ele alınan bir dizi SAQ türü mevcuttur. Kuruluşunuz için geçerli olan SAQ'yu belirlemenize yardımcı olması için tabloyu kullanın ve sonrasında bu SAQ'nın tüm gereksinimleri karşıladığınızdan emin olmak için ayrıntılı açıklamaları inceleyin.

SAQ D haricindeki tüm SAQ'lar için not: Bu SAQ'lar, ilgili SAQ uygunluk kriterlerinde tanımlandığı şekilde üye işyerindeki belirli bir sistem türü için geçerli olan soruları içerir. Belirli bir SAQ kapsamında olmayan sisteminiz için geçerli PCI DSS gereksinimleri varsa bu SAQ, sizin sisteminiz için uygun olmayabilir. Ayrıca, PCI DSS uyumlu olabilmek için geçerli tüm PCI DSS gereksinimlerine uymanız gerekmektedir.

SAQ	Açıklama
A	Kart sahiplerinin verilerine ilişkin tüm işlevlerin yürütülmesini PCI uyumlu üçüncü taraf hizmet sağlayan firmalara dış kaynaklı olarak yaptıran, kart sahiplerinin bilgilerini üye işyeri sistemleri veya tesislerinde elektronik olarak depolama ortamı olmayan, işlemeyen veya aktarmayan kartın satış esnasında fiziksel olarak okutulmadığı üye işyerleri (e-ticaret ya da posta/telefon yoluyla sipariş). *Yüz yüze kanallarda geçerli değildir.*
A-EP	Tüm ödeme işlemini dış kaynaklı olarak PCI DSS onaylı üçüncü taraflara yaptıran ve kart sahiplerini verilerini doğrudan almayan ancak ödeme işleminin güvenliğini etkileyebilecek web sitesi/siteleri olan e-ticaretle uğraşan üye işyerleri. Kart sahiplerinin bilgilerini, üye işyeri sistemleri veya tesislerinde elektronik olarak depolama ortamı yoktur, bunları buralarda işlemez veya aktarmaz. *Sadece e-ticaret kanalları için geçerlidir.*
B	Sadece aşağıdakileri kullanan üye işyerleri: ▪ Kart sahiplerinin verilerini tutacak elektronik depolama ortamına sahip olmayan imprinter ve/veya ▪ Kart sahiplerinin verilerini tutacak elektronik depolama ortamına sahip olmayan bağımsız, telefon hatlı terminaller. *E-ticaret kanalları için geçerli değildir.*
B-IP	Yalnızca kart sahiplerinin verilerini tutacak elektronik depolama ortamına sahip olmayan, ödeme işleyiciye IP bağlantılı bağımsız, PTS onaylı ödeme terminalleri kullanan üye işyerleri. *E-ticaret kanalları için geçerli değildir.*
C-VT	PCI DSS onaylı bir üçüncü taraf hizmet sağlayan firma tarafından sunulup barındırılan İnternet tabanlı sanal ödeme terminali çözümüne manüel olarak klavye ile her seferde tek bir işlem giren üye işyerleri. Kart sahiplerinin verilerini tutacak elektronik depolama ortamı yok. *E-ticaret kanalları için geçerli değildir.*
C	Internet bağlantılı, kart sahiplerini tutacak elektronik ortama sahip olmayan ödeme uygulaması sistemleri olan üye işyerleri. *E-ticaret kanalları için geçerli değildir.*

SAQ	Açıklama
P2PE	Yalnızca kart sahiplerini tutacak elektronik ortama sahip olmayan, onaylı, PCI SSC listesinde bulunan Noktadan Noktaya Şifreleme (P2PE) çözümü üzerinde bulunan ve burada yönetilen donanım ödeme terminalleri kullanan üye işyerleri. *E-ticaret kanalları için geçerli değildir.*
D	***Üye İşyerleri için SAQ D:*** Yukarıdaki SAQ türlerinin açıklamalarına dahil edilmemiş tüm üye işyerleri.
	Hizmet Sağlayan Firmalar için SAQ D: Bir kredi kartı firması tarafından SAQ doldurmaya uygun olduğu tanımlanan tüm hizmet sağlayan firmalar.

SAQ A — Kartın Satış Esnasında Fiziksel Olarak Okutulmadığı Üye İşyerleri, Tüm Kart Sahibi Verilerinin İşlevleri Tamamen Dış Kaynaklı

SAQ A, üye işyerinin kart sahiplerinin verilerini içeren matbu raporları veya makbuzları tuttuğı, kart sahiplerinin verilerine ilişkin işlevlerin tamamen dış kaynaklı olarak gerçekleştirildiği üye işyerleri tüccarlar için geçerli gereksinimleri ele almak üzere geliştirilmiştir.

18. sayfadaki "Sistemime En Uygun SAQ Hangisi?" bölümünde SAQ türünüzü seçmenize yardımcı olarak grafik kılavuzu görebilirsiniz.

SAQ A üye işyerleri, e-ticaret ile uğraşan veya posta/telefon yoluyla sipariş alan üye işyerleri (kartın satış esnasında fiziksel olarak okutulmadığı) olabilir ve kart sahiplerinin verilerini sistem veya tesislerinde elektronik olarak depolamaz, işlemez ve aktarmaz.

SAQ A üye işyerleri, bu ödeme kanalına ilişkin aşağıdaki uygunluk kriterlerini karşıladıklarını teyit edecektir:

- Şirketiniz yalnızca kartın satış esnasında fiziksel olarak okutulmadığı (e-ticaret ya da posta/telefon yoluyla sipariş) işlemleri kabul ediyor;
- Kart sahiplerinin verilerin işlenmesi tamamen dış kaynaklı olarak PCI DSS onaylı üçüncü taraf hizmet sağlayan firmalara yaptırılıyor;
- Şirketiniz, kart sahiplerinin verilerini sistemlerinizde veya tesislerinizde kart elektronik ortamda depolamıyor, işlemiyor veya aktarmıyor, ancak bu işlevlerin tamamını yerine getirmesi için tamamen üçüncü taraflara güveniyor;
- Şirketiniz, kart sahiplerinin verilerinin depolanması, işlenmesi ve/veya aktarımını gerçekleştiren üçüncü tarafların tamamının PCI DSS uyumlu olduğunu onaylamıştır **ve**
- Şirketinizin sakladığı kart sahiplerinin verilerinin tamamı kağıt üzerinde olup (örneğin, matbu raporlar veya makbuzlar) bu belgeler elektronik ortamda alınmaz.

Ayrıca e-ticaret kanalları için:

- Tüketicinin tarayıcısına gönderilen ödeme sayfalarının tüm unsurları, yalnızca ve doğrudan PCI DSS onaylı üçüncü taraf hizmet sağlayan firma(lar) tarafından oluşturulur.

Bu SAQ, yüz yüze kanallar için geçerli değildir.

SAQ A-EP – Kısmen Dış Kaynaklı Ödeme İşlemesi için Üçüncü Taraf Web Sitesi Kullanan E-Ticaretle Uğraşan Üye İşyerleri

SAQ A-EP, kendisi kart sahiplerinin verilerini almayan ancak ödeme işleminin güvenliğini ve/veya tüketicilerin kart sahibi verilerini kabul eden sayfanın bütünlüğünü etkileyen bir web sitesi/web siteleri olan e-ticaretle uğraşan üye işyerleri için geçerli gereksinimleri ele almak üzere geliştirilmiştir.

SAQ A-EP üye işyerleri, e-ticaret ödeme kanalı işlemlerinin gerçekleştirilmesini kısmen dış kaynaklı olarak PCI DSS onaylı üçüncü taraflara yaptıran ve kart sahiplerinin bilgilerini kendi sistemleri veya tesislerinde elektronik olarak depolamayan, işlemeyen veya aktarmayan e-ticaretle uğraşan üye işyerleridir.

18. sayfadaki "Sistemime En Uygun SAQ Hangisi?" bölümünde SAQ türünüzü seçmenize yardımcı olarak grafik kılavuzu görebilirsiniz.

SAQ A-EP üye işyerleri, bu ödeme kanalına ilişkin aşağıdaki uygunluk kriterlerini karşıladıklarını teyit edecektir:

- Şirketiniz yalnızca e-ticaret işlemleri kabul ediyor;
- Ödeme sayfası hariç olmak üzere kart sahiplerinin verilerin işlenmesi tamamen dış kaynaklı olarak PCI DSS onaylı üçüncü taraf ödeme işleyiciye yaptırılıyor;
- E-ticaret web siteniz kart sahiplerinin verilerini almıyor, ancak tüketicilerin veya kart sahiplerinin verilerinin PCI DSS onaylı üçüncü taraf ödeme işleyiciye nasıl yönlendirileceğini kontrol ediyor;
- Üye işyerinin web sitesi, üçüncü taraf bir hizmet sağlayan firmada barındırılıyorsa bu firma, geçerli tüm PCI DSS gereksinimlerine göre doğrulanır (örneğin, hizmet sağlayan firma, ortak hosting hizmeti sağlayan bir firmaysa PCI DSS Ek A dahil);
- Tüketicinin tarayıcısına gönderilen ödeme sayfası(ları)nın her unsuru, üye işyerinin web sitesi ya da PCI DSS uyumlu hizmet sağlayan firma(lar) tarafından oluşturulur.
- Şirketiniz, kart sahiplerinin verilerini sistemlerinizde veya tesislerinizde kart elektronik ortamda depolamıyor, işlemiyor veya aktarmıyor, ancak bu işlevlerin tamamını yerine getirmesi için tamamen üçüncü taraflara güveniyor;
- Şirketiniz, kart sahiplerinin verilerinin depolanması, işlenmesi ve/veya aktarımını gerçekleştiren üçüncü tarafların tamamının PCI DSS uyumlu olduğunu onaylamıştır **ve**
- Şirketinizin sakladığı kart sahiplerinin verilerinin tamamı kağıt üzerinde olup (örneğin, matbu raporlar veya makbuzlar) bu belgeler elektronik ortamda alınmaz.

İşbu SAQ, yalnızca e-ticaret kanalları için geçerlidir.

Not: *SAQ A-EP amaçları doğrultusunda, "kart sahiplerinin verilerinin tutulduğu platforma" atofta bulunan PCI DSS gereksinimleri, üye işyerlerinin web sitesi/siteleri için geçerlidir. Bunun nedeni, üye işyerlerinin web sitesinin, kart sahiplerinin verilerini kendisi almasa da, kart sahiplerinin verilerinin nasıl aktarıldığını doğrudan etkilemesidir.*

SAQ B – Yalnızca İmprinter ya da Yalnızca Bağımsız, Telefon Hatlı Terminalleri olan Üye İşyerleri. Kart Sahiplerinin Verilerini Tutacak Elektronik Depolama Ortamı Yok

SAQ B, kart sahiplerinin verilerini yalnızca imprinterler ya da bağımsız, telefon bağlantılı terminaller ile işleyen üye işyerleri için geçerli gereksinimleri ele almak üzere geliştirilmiştir.

SAQ B üye işyerleri, fiziksel (ödeme anında kartın fiziksel olarak okutulduğu) veya posta/telefon üzerinden sipariş alan (ödeme anında kartın fiziksel olarak okutulmadığı) üye işyerleri olabilir ve kart sahiplerinin verilerini herhangi bir bilgisayar sisteminde depolamaz. SAQ B üye işyerleri, bu ödeme kanalına ilişkin aşağıdaki uygunluk kriterlerini karşıladıklarını teyit edecektir:

18. sayfadaki "Sistemime En Uygun SAQ Hangisi?" bölümünde SAQ türünüzü seçmenize yardımcı olarak grafik kılavuzu görebilirsiniz.

- Şirketiniz, müşterinizin ödeme kartı bilgilerini almak için yalnızca imprinter ve/veya yalnızca bağımsız, telefon bağlantılı terminaller (bir telefon hattı üzerinden işleyicinize bağlı) kullanıyor;
- Bağımsız, telefon bağlantılı terminaller platformunuzdaki diğer sistemlere bağlı değildir;
- Bağımsız, telefon bağlantılı terminaller İnternet'e bağlı değildir;
- Şirketiniz kart sahiplerinin verilerini bir ağ üzerinden (dahili ağ veya İnternet) aktarmaz;
- Şirketinizin sakladığı kart sahiplerinin verilerinin tamamı kağıt üzerinde olup (örneğin, matbu raporlar veya makbuzlar) bu belgeler elektronik ortamda alınmaz **ve**
- Şirketiniz kart sahiplerinin verilerini elektronik formatta depolamaz.

Bu SAQ, e-ticaret kanalları için geçerli değildir.

SAQ B-IP – Bağımsız, IP Bağlantılı PTS Etkileşim Noktası (POI) terminalleri olan, Kart Sahiplerinin Verilerini Tutacak Elektronik Depolama Ortamı Olmayan Üye İşyerleri

SAQ B-IP, kart sahiplerinin verilerini yalnızca bağımsız, ödeme işleyiciye IP bağlantısı olan PTS onaylı etkileşim noktası (POI) cihazları ile işleyen üye işyerleri için geçerli gereksinimleri ele almak üzere geliştirilmiştir.

18. sayfadaki "Sistemime En Uygun SAQ Hangisi?" bölümünde SAQ türünüzü seçmenize yardımcı olarak grafik kılavuzu görebilirsiniz.

SAQ B-IP üye işyerleri, fiziksel (ödeme anında kartın fiziksel olarak okutulduğu) veya posta/telefon üzerinden sipariş alan (ödeme anında kartın fiziksel olarak okutulmadığı) üye işyerleri olabilir ve kart sahiplerinin verilerini herhangi bir bilgisayar sisteminde depolamaz.

SAQ B-IP üye işyerleri, bu ödeme kanalına ilişkin aşağıdaki uygunluk kriterlerini karşıladıklarını teyit edecektir:

- Şirketiniz, müşterilerinizin ödeme kartı bilgilerini almak için yalnızca bağımsız, ödeme işleyicinize IP bağlantısı olan PTS onaylı etkileşim noktası (POI) cihazlar (SCR'ler hariç) kullanıyor;
- Bağımsız, IP bağlantılı POI cihazlar, PCI SSC web sitesinde listelenen PTS POI programına göre doğrulanır (SCR'ler hariç);
- Bağımsız, IP bağlantılı POI cihazları platformunuzdaki diğer sistemlere bağlı değildir (bu, POI cihazlarını diğer sistemlerden izole etmek için ağ segmentasyonu yaparak sağlanabilir);
- Kart sahibi verilerinin tek aktarımı, PTS onaylı POI cihazlarından ödeme işleyici yönünedir.
- POI cihazı, ödeme işleyiciye bağlanmak için başka bir cihaza (örn. bilgisayar, cep telefonu, tablet vb.) güvenmez;
- Şirketinizin sakladığı kart sahiplerinin verilerinin tamamı kağıt üzerinde olup (örneğin, matbu raporlar veya makbuzlar) bu belgeler elektronik ortamda alınmaz **ve**
- Şirketiniz kart sahiplerinin verilerini elektronik formatta depolamaz.

Bu SAQ, e-ticaret kanalları için geçerli değildir.

SAQ C-VT – Web Tabanlı Sanal Terminalleri olan, Kart Sahiplerinin Verilerini Tutacak Elektronik Depolama Ortamı Olmayan Üye İşyerleri

SAQ C-VT, kart sahiplerinin verilerini yalnızca İnternet bağlantılı kişisel bir bilgisayarda izole edilmiş sanal ödeme terminalleri ile işleyen üye işyerleri için geçerli gereksinimleri ele almak üzere geliştirilmiştir.

Sanal ödeme terminali, üye işyerinin ödeme kartı verilerini güvenli bağlantısı olan web tarayıcısı üzerinden manuel olarak girdiği, ödeme kartı işlemlerinin provizyonu için POS hizmeti veren banka, işleyici veya üçüncü taraf hizmet sağlayan firma web sitesine web tarayıcı tabanlı erişimdir. Fiziksel terminallerin aksine sanal ödeme terminalleri verileri doğrudan bir ödeme kartından okumaz. Ödeme kartı işlemleri manuel olarak girilir.

18. sayfadaki "Sistemime En Uygun SAQ Hangisi?" bölümünde SAQ türünüzü seçmenize yardımcı olarak grafik kılavuzu görebilirsiniz.

SAQ C-VT üye işyerleri, kart sahiplerinin verilerini yalnızca sanal ödeme terminali ile okur ve kart sahiplerinin verilerini herhangi bir bilgisayar sistemi üzerinde depolamaz. Bu sanal terminaller, sanal terminal ödeme işleme işlevini barındıran üçüncü tarafa erişmek için İnternet bağlantısına sahiptir. Bu üçüncü taraf, üye işyerinin sanal terminal ödeme işlemlerinin provizyon ve/veya mutabakat işlemlerini yapmak için kart sahiplerinin verilerini depolayan, işleyen ve/veya aktaran bir işleyici, POS hizmeti veren banka veya başka bir üçüncü taraf hizmet sağlayan firma olabilir.

Bu SAQ seçeneği, yalnızca internet tabanlı bir sanal terminal çözümüne klavye kullanarak manuel olarak tek seferde tek bir işlem giren üye işyerleri için geçerli olmak üzere tasarlanmıştır. SAQ C-VT üye işyerleri, fiziksel (ödeme anında kartın fiziksel olarak okutulduğu) veya posta/telefon üzerinden sipariş alan (ödeme anında kartın fiziksel olarak okutulmadığı) üye işyerleri olabilir.

SAQ C-VT üye işyerleri, bu ödeme kanalına ilişkin aşağıdaki uygunluk kriterlerini karşıladıklarını teyit edecektir:

- Şirketinizin tek ödeme işlemi İnternet bağlantılı bir web tarayıcısının erişebildiği bir sanal ödeme terminali üzerinden yapılıyor;
- Şirketinizin sanal ödeme terminali çözümü, PCI DSS onaylı bir üçüncü taraf hizmet sağlayan firma tarafından sunulup barındırılıyor;
- Şirketiniz PCI DSS uyumlu sanal ödeme terminali çözümüne tek bir konumda izole edilmiş ve platformunuzdaki diğer konum veya sistemlere bağlantısı olmayan bir bilgisayar üzerinden erişiyor (bu, bilgisayarı diğer sistemlerden izole etmek için bir güvenlik duvarı kullanarak veya ağ segmentasyonu yaparak gerçekleştirilebilir);
- Şirketinizin bilgisayarında kart sahiplerinin verilerinin depolanmasına neden olan yazılımlar yüklü değil (örneğin, toplu işleme veya sakla ve ilet kipi olan bir yazılım yoktur);
- Şirketinizin bilgisayarına, kart sahiplerinin verilerini elde etmek veya depolamak için kullanılan donanım aygıtları bağlı değildir (örneğin, kart okuyucu bağlı değildir);
- Şirketiniz kart sahiplerinin verilerini herhangi bir kanal üzerinden (dahili ağ veya İnternet üzerinden) elektronik olarak almaz ve aktarmaz;
- Şirketinizin sakladığı kart sahiplerinin verilerinin tamamı kağıt üzerinde olup (örneğin, matbu raporlar veya makbuzlar) bu belgeler elektronik ortamda alınmaz **ve**
- Şirketiniz kart sahiplerinin verilerini elektronik formatta depolamaz.

Bu SAQ, e-ticaret kanalları için geçerli değildir.

SAQ C – İnternete Bağlı Ödeme Uygulaması Sistemleri olan, ancak Kart Sahiplerinin Verilerini Tutacak Elektronik Depolama Ortamı Olmayan Üye İşyerleri

SAQ C, ödeme uygulama sistemleri (örneğin POS sistemleri) İnternet'e bağlı olan (örneğin, DSL, kablolu modem vb. ile) üye işyerleri için geçerli gereksinimleri ele almak üzere geliştirilmiştir.

SAQ C üye işyerleri, kart sahiplerinin verilerini bir satış noktası (POS) sistemi veya İnternet bağlantılı başka ödeme uygulama sistemleri aracılığıyla işler, kart sahiplerinin verilerini herhangi bir bilgisayar sisteminde saklamaz ve fiziksel (ödeme anında kartın fiziksel olarak okutulduğu) ya da posta/telefon üzerinden sipariş alan (ödeme anında kartın fiziksel olarak okutulmadığı) üye işyerleri olabilir.

18. sayfadaki "Sistemime En Uygun SAQ Hangisi?" bölümünde SAQ türünüzü seçmenize yardımcı olacak grafik kılavuzu görebilirsiniz.

SAQ C üye işyerleri, bu ödeme kanalına ilişkin aşağıdaki uygunluk kriterlerini karşıladıklarını teyit edecektir:

- Şirketinizin aynı cihaz ve/veya aynı yerel ağ (LAN) üzerinde bir ödeme uygulama sistemi ve İnternet bağlantısı mevcuttur;
- Ödeme uygulama sistemi/İnternet bağlantılı cihaz, platformunuzdaki diğer sistemlere bağlı değildir (bu, ödeme uygulama sistemini/İnternet bağlantılı cihazı diğer tüm sistemlerden izole etmek için ağ segmentasyonu yaparak sağlanabilir);
- POS platformunun fiziksel konumu diğer tesislere veya konumlara bağlı değildir ve her türlü LAN yalnızca tek bir satış noktası içindir;
- Şirketinizin sakladığı kart sahiplerinin verilerinin tamamı kağıt üzerinde olup (örneğin, matbu raporlar veya makbuzlar) bu belgeler elektronik ortamda alınmaz **ve**
- Şirketiniz kart sahiplerinin verilerini elektronik formatta depolamaz.

Bu SAQ, e-ticaret kanalları için geçerli değildir.

SAQ P2PE – Yalnızca PCI SSC Listesinde Bulunan Bir P2PE Çözümü Üzerindeki Donanım Ödeme Terminallerini Kullanan, Kart Sahiplerinin Verilerini Tutacak Elektronik Depolama Ortamı Olmayan Üye İşyerleri

SAQ P2PE, kart sahiplerinin verilerini yalnızca doğrulanmış ve PCI SSC listesinde bulunan Noktadan Noktaya Şifreleme (P2PE) çözümünde yer alan ödeme terminalleri üzerinden işleyen üye işyerleri için gereksinimleri ele almak üzere geliştirilmiştir.

18. sayfadaki "Sistemime En Uygun SAQ Hangisi?" bölümünde SAQ türünüzü seçmenize yardımcı olacak grafik kılavuzu görebilirsiniz.

SAQ P2PE üye işyerleri, herhangi bir bilgisayar sisteminde kripto ile şifrelenmemiş hesap verilerine erişemez ve hesap verilerini yalnızca PCI SSC onaylı P2PE çözümünden gelen donanım ödeme terminalleri üzerinden girer. SAQ P2PE üye işyerleri, fiziksel (ödeme anında kartın fiziksel olarak okutulduğu) ya da posta/telefon üzerinden sipariş alan (ödeme anında kartın fiziksel olarak okutulmadığı) üye işyerleri olabilir. Örneğin, posta/telefon yoluyla sipariş alan üye işyeri, kart sahiplerinin verilerini matbu olarak ya da telefon üzerinden alıp bu verileri doğrudan ve yalnızca P2PE onaylı bir donanım aygıtına giriyorlarsa SAQ P2PE için uygun olabilir.

SAQ P2PE üye işyerleri, bu ödeme kanalına ilişkin aşağıdaki uygunluk kriterlerini karşıladıklarını teyit edecektir:

- Tüm ödeme işlemleri, PCI SSC tarafından onaylanmış ve PCI SSC listesine dahil edilmiş doğrulanmış PCI P2PE çözümü kullanarak yapılır;
- Üye işyeri sisteminde hesap verilerini depolayan, işleyen veya aktaran sistemler yalnızca, doğrulanmış ve PCI listesine dahil edilmiş P2PE çözümü ile kullanımı onaylanmış Etkileşim Noktası (POI) cihazlarıdır;
- Şirketiniz kart sahiplerinin verilerini başka şekillerde elektronik olarak almaz veya aktarmaz.
- Sistemde kart sahiplerinin verilerinin elektronik olarak tutulduğu eski bir depolama yoktur;
- Şirketinizin sakladığı kart sahiplerinin verilerinin tamamı kağıt üzerinde olup (örneğin, matbu raporlar veya makbuzlar) bu belgeler elektronik ortamda alınmaz ve
- Şirketiniz, P2PE Çözümünü Sağlayan Kuruluş tarafından verilen *P2PE Kullanım Talimatları Kitapçığında (PIM)* bulunan tüm kontrolleri uygulamıştır.

Bu SAQ, e-ticaret kanalları için geçerli değildir.

Üye İşyerlerine Yönelik SAQ D – SAQ'ya Uygun Olan Diğer Tüm Üye İşyerleri

Üye İşyerleri için SAQ D, diğer SAQ türlerinin kriterlerini karşılamayan SAQ'ya uygun üye işyerleri için geçerlidir.

SAQ D'yi kullanacak üye işyeri sistemlerinin örnekleri arasında aşağıdakiler sayılabilir, ancak bunlarla sınırlı değildir:

- Web siteleri üzerinde kart sahiplerinin verilerini kabul eden e-ticaretle uğraşan üye işyerleri;
- Kart sahiplerinin verilerini elektronik olarak depolayan üye işyerleri;
- Kart sahiplerinin verilerini elektronik olarak depolamayan ancak başka bir SAQ türünün kriterlerini karşılamayan üye işyerleri;
- Başka bir SAQ türünün kriterlerini karşılayabilecek sistemleri olan, ancak sistemleri için geçerli ek PCI DSS gereksinimleri olan üye işyerleri.

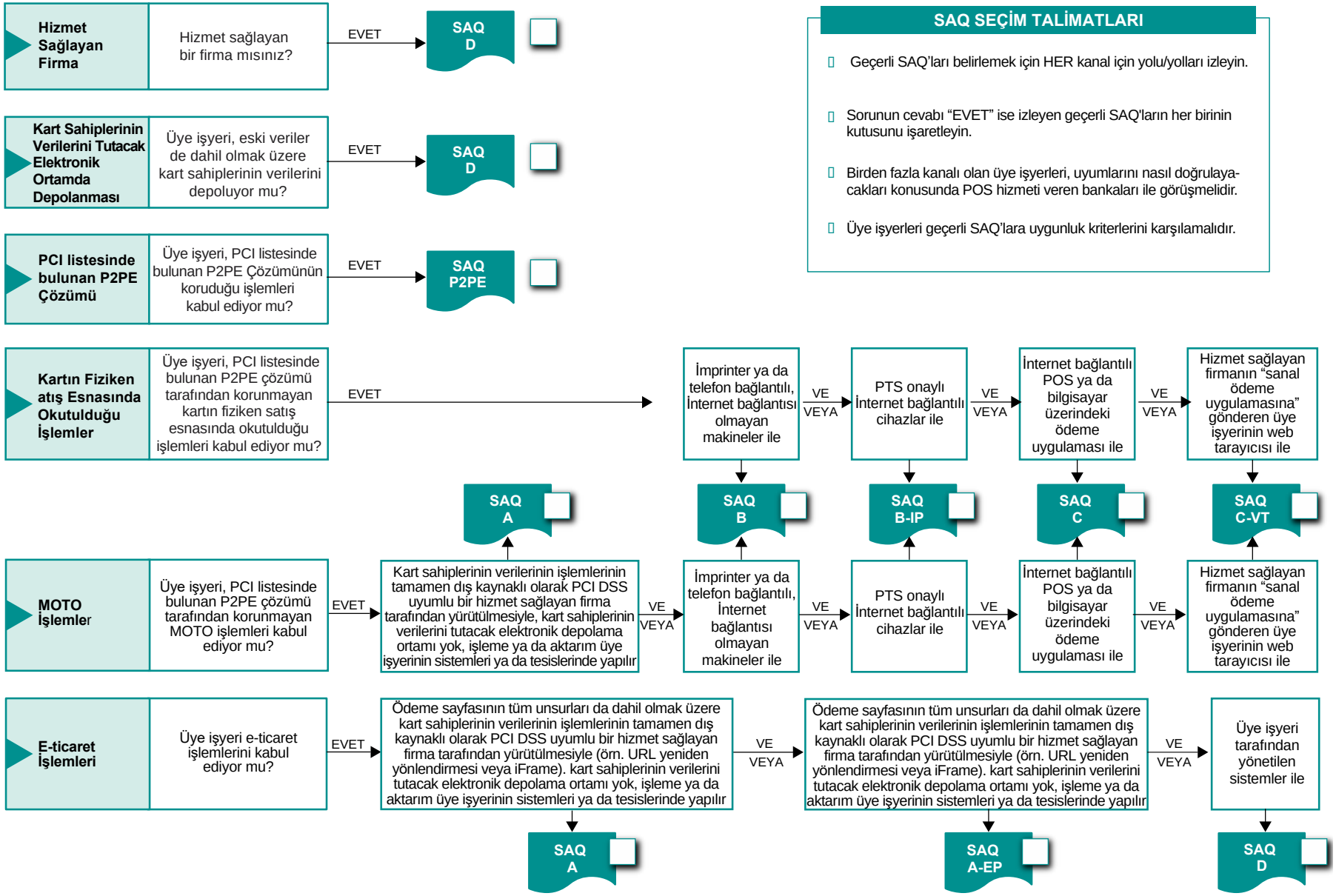
Hizmet Sağlayan Firmalara Yönelik SAQ D – SAQ'ya Uygun Hizmet Sağlayan Firmalar

Hizmet Sağlayan Firmalar için SAQ D, bir kredi kartı firması tarafından SAQ'ya uygun olduğu tanımlanan tüm hizmet sağlayan firmalar için geçerlidir.

Üye İşyerleri için SAQ D ve Hizmet Sağlayan Firmalar için SAQ D'ye ilişkin not: SAQ D'yi dolduran birçok kuruluşun her PCI DSS gereksinimine uyduğunu doğrulaması gerekirken, çok spesifik iş modelleri olan bazı kuruluşlar için gereksinimlerin bazıları geçerli olmayabilir. Örneğin, hiçbir surette kablosuz teknoloji kullanmayan bir şirketin, kablosuz teknoloji yönetimine özgü PCI DSS bölümlerine uyduklarını doğrulaması beklenmez. Diğer, spesifik gereksinimlerden muafiyet hakkında bilgi almak için ilgili SAQ D'deki spesifik kılavuza bakabilirsiniz.

18. sayfadaki "Sistemime En Uygun SAQ Hangisi?" bölümünde SAQ türünüzü seçmenize yardımcı olacak grafik kılavuzu görebilirsiniz.

Sistemime En Uygun SAQ Hangisi?



SAQ SEÇİM TALİMATLARI

- Geçerli SAQ'ları belirlemek için HER kanal için yolu/yolları izleyin.
- Sorunun cevabı "EVET" ise izleyen geçerli SAQ'ların her birinin kutusunu işaretleyin.
- Birden fazla kanalı olan üye işyerleri, uyumlarını nasıl doğrulayacakları konusunda POS hizmeti veren bankaları ile görüşmelidir.
- Üye işyerleri geçerli SAQ'lara uygunluk kriterlerini karşılamalıdır.