



**YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARA
AİT ÖKC TSM MERKEZLERİNİN
BAŞVURU, TEST, DENETİM VE ONAY
TEKNİK KILAVUZU**

Sürüm 2.0

23 Eylül 2016

İÇİNDEKİLER

1. Amaç ve Kapsam	5
-------------------------	---

BÖLÜM I

YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARA AİT ÖKC TSM MERKEZLERİ GÜVENLİK GEREKSİNİMLERİ

2. Kritik Varlıklar ve Aktörler	7
2.1 Kritik Varlıklar	7
2.1.1 Birincil Varlıklar	7
2.1.2 İkincil Varlıklar	10
2.2 Aktörler.....	10
2.2.1 Yetkili Kullanıcılar.....	10
2.2.2 Yetkisiz Kullanıcılar (Hacker, Siber Terörist, vb.)	10
2.2.3 Teçhizat ve Yazılımlar	11
2.2.4 Çevresel Koşullar	11
3. Sistem Güvenliği, İş Sürekliliği, Felaket Kurtarma ve Olay Müdahale	11
4. Kullanılan Donanımların Güvenliği.....	11
5. Kullanılan Yazılımların Güvenliği.....	11
6. Güvenlik Denetimi.....	12

BÖLÜM II

YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARA AİT ÖKC TSM MERKEZİ SİSTEM GEREKSİNİMLERİ

7. ÖKC TSM Merkezlerinin Desteklemesi Gereken Standartlar.....	13
7.1 Uluslararası Standartlar:	13
7.2 Ulusal Standartlar:	14
8. ÖKC TSM Merkezi Başvuru, Test , Denetim ve Onay Süreçleri.....	14
9. Sistemlerin Münhasırlığı.....	14
10. ÖKC TSM Merkezleri Sorumluluk Dağılımı	18
11. Mükellef, ÖKC, TSM Merkezleri ve GİB İletişimi.....	19
12. Yeni Nesil ÖKC Yaşam Döngüsü Yönetimi	20
13. Yeni Nesil ÖKC Mesajlarının (ÖKC Durum Verisi ve GİB Hassas ÖKC Verisi) Yönetimi.....	23

14. Risk Yönetimi Esasları.....	24
15. Değişiklik Yönetimi.....	25
16. Denetim İzlerinin Oluşturulması.....	26
17. Anahtar Yönetim Süreçleri ve Hassas Veri Güvenliği	28
18. Yazılım Güvenliği ve Sorumluluğu	28
19. ÖKC TSM Merkezi İş Sürekliliği Yönetimi.....	29
20. Dış Hizmet Alımı.....	32
21. TSM Merkezi Personel Gereksinimleri	33
21.1. Network & Network Güvenlik Grubu:	33
21.2. Sistem ve Database Grubu:	33
21.3. Sistem ve Terminal Operasyon Grubu:.....	34
21.4. Uygulama Geliştirme Grubu:.....	34
22. ÖKC TSM Merkezlerinin Denetimi	34
23. GİB Uyarı Mekanizmaları	35
24. ÖKC TSM Merkezlerinin Harici Donanım ve Yazılım Bilgisi Tutma ve Bildirme Yükümlülüğü	36

BÖLÜM III

YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARA AİT ÖKC TSM MERKEZLERİ ONAY VE TEST BAŞVURU AKIŞLARI

25. Onay ve Test Başvuru Yönetimi.....	37
25.1. ÖKC TSM Merkezi Başvurusunda Sağlanacak Belgeler	37
25.2. ÖKC TSM Merkezi Denetim ve Onay Süreçleri	38
25.3. Dış Hizmet Sağlayıcılı TSM Merkezi Denetim ve Onay Süreçleri	40
25.4. Onay Denetimi Sonrasında Test Başvuruları ve Gerçek Ortama Geçiş	41

BÖLÜM IV

ÖKC TSM MERKEZLERİNDE GERÇEKLEŞTİRİLECEK DENETİM FAALİYETLERİ

26. ÖKC TSM Merkezlerinde Gerçekleştirilecek Onay Denetiminin Kapsamı.....	42
26.1. ÖKC TSM Merkezleri Bilgi Sistemleri Denetimi	42
26.2. ÖKC TSM Merkezleri Güvenli Haberleşme Denetimi	44
27. ÖKC TSM Merkezlerinde Gerçekleştirilecek Yıllık Denetiminin Kapsamı	46
28. ÖKC TSM Merkezi Denetimine İlişkin Düzenlenen Raporların Formatı	46
29. KILAVUZ EKLERİ.....	48

EK-1: Denetim Mektubu Oluřturulurken Metinde Deęiřtirilmesi Gereken Hususlar:	48
EK-2: ÖKC TSM Merkezi Bařvuru Formu	49
EK-3 : “ÖKC TSM Merkezi Onay Denetim Raporu Formatı.....	53
EK-4A : “ÖKC TSM Merkezi Yıllık Denetim Raporu Formatı	54
EK-4B: “ÖKC TSM Merkezi Güncelleme Denetimi Rapor Formatı	55
EK-5 – ÖKC TSM Merkezi Onay Denetimi ve Yıllık Denetim Süreçleri Akıřı	56
30. REFERANSLAR	57

1. Amaç ve Kapsam

Bu Kılavuz Gelir İdaresi Başkanlığının (GİB) Yeni Nesil ÖKC (YN ÖKC) projesine dahil olan ve ÖKC TSM Merkezi kurmak isteyen ya da ÖKC TSM Merkezi hizmetini bir Dış Hizmet Sağlayıcı (DHS)'dan temin etmek isteyen ÖKC üreticileri için hazırlanmıştır. Kılavuzda ÖKC TSM Merkezleri (TSM) ibaresi kullanıldığında DHS'yi de kapsamakta ve TSM ile DHS birlikte kastedilmektedir.

ÖKC TSM Merkezi hizmeti kurarak ya da bir dış hizmet sağlayıcıdan alarak cihazlarını yönetmek ve GİB BS ile iletişim kurmak isteyen ÖKC üreticileri bu kılavuzu rehber edinerek teknik konularını yönetebilecektir. Bu Kılavuz, ÖKC TSM Merkezi kurmak, işletmek, yönetmek ve denetlemek isteyenler için hazırlanan “Yeni Nesil Ödeme Kaydedici Cihazlara Ait ÖKC TSM Merkezleri Teknik Kılavuzu Sürüm 2.0” esas alınarak hazırlanmıştır. ÖKC TSM Merkezleri Teknik Kılavuzu'nda yer almayan bazı detayları açıklamak amacıyla yazılmış olan bu kılavuz, tek başına kullanılmamalı konu ile ilgili diğer dokümanlarla birlikte kullanılmalıdır.

ÖKC TSM Merkezinin gerekli şartları haiz olup olmadığının tespiti için gerekli Onay Denetimi, 13/01/2010 tarihli ve 27461 sayılı Resmi Gazete'de yayımlanan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik (BSDHY) kapsamında yetkilendirilmiş veya izin verilmiş bağımsız denetim kuruluşlarınca veya TÜBİTAK tarafından yerinde yapılmak zorundadır.

Onay Denetimi, bu Kılavuzda açıklanan; “Bilgi Sistemi Denetim Adımları” ve “Güvenli Haberleşme Denetim Adımları” aşamalarından oluşur.

TSM Merkezi'nin onay aldığı durumda; onay yazısını takip eden 1 yıllık süre sonunda ve takip eden her yıl 1 defa olmak üzere; “Bilgi Sistemi Denetim Adımları”, Bilgi Sistemi Denetimi ismi altında tekrar edilir. Bilgi Sistemi Denetimi esasları bu kılavuzda detaylı olarak belirtilmektedir.

“Güvenli Haberleşme Denetim Adımları” onay sürecine münhasıran uygulanır ancak GİB, GMP dokümanlarında gerçekleştirilecek değişikliklere istinaden bu denetimlerin tekrar edilmesini talep edebilir.

Bu Kılavuzun I. bölümünde ÖKC TSM Merkezlerinin sahip olması gereken **Güvenlik Gereksinimleri** açıklanmaktadır. Bu bölümde yer alan gereksinimler TSM topolojilerinden bağımsız olarak TK-1, TK-2, GMP-1 ve GMP-2 dokümanları temel alınarak hazırlanmıştır. Bu bölümde hassas verinin yetkisiz kişilerin eline geçmesini engellemeyi, verinin hem bilgisayar sistemlerinde, hem saklama ortamlarında, hem de ağ üzerinde gönderici ve alıcı arasında taşınırken yetkisiz erişimlerden korunması, gizliliği, bütünlüğü ve sürekliliği ile alakalı hususlar için güvenlik gereksinimlerinin belirlenmesi amacı ile oluşturulmuştur.

Bu Kılavuzun II. Bölümünde ÖKC TSM Merkezlerinin kurması gereken veri merkezlerinin, uygulama ve süreçlerin sahip olması gereken **Sistem Gereksinimleri** detaylandırılmaktadır. Bu bölümde GİB, ÖKC üreticileri, TSM Merkezleri, DHS hizmeti veren Kuruluşlar ve TÜBİTAK arasındaki sorumluluklar anlatılmaktadır.

Kılavuzun III. Bölümünde TSM Merkezini kendi kurmak ya da bir DHS'den temin etmek isteyen ÖKC üreticisi kurumların başvuru süreçleri ve formlarla iş akışları tarif edilmektedir.

Kılavuzun IV. Bölümünde ÖKC TSM Merkezlerinde gerçekleştirilecek onay denetimi ve yıllık bilgi sistemleri denetim faaliyetlerine ilişkin detaylar, iş akışları ve denetim faaliyeti sonucunda düzenlenen raporların formatları belirtilmektedir.

Bu kılavuz ÖKC üreticileri, ÖKC TSM Merkezi hizmeti verecek kuruluşları (ÖKC üreticisi ÖKC TSM Merkezi veya ÖKC TSM Merkezi hizmeti ile ilgili tüm Dış Hizmet Sağlayıcıları) ve ÖKC TSM Merkezi Denetçileri için bağlayıcıdır.

BÖLÜM I

YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARA AİT ÖKC TSM MERKEZLERİ GÜVENLİK GEREKSİNİMLERİ

2. Kritik Varlıklar ve Aktörler

Sistemde var olan ve ifşa olması veya değişikliğe uğraması durumunda sistemin gizliliğini, bütünlüğünü, kaynak/kimlik doğruluğunu ve erişilebilirliğini olumsuz yönde etkileyecek varlıklar aşağıda listelenmiştir. İlerleyen bölümlerde belirtilen gereksinimlere uyulmazsa aşağıda listelenen varlıkların biri veya birkaçı ifşa olabilir, bütünlüğü bozulabilir veya kullanılamaz/erişilemez duruma gelebilir.

2.1 Kritik Varlıklar

2.1.1 Birincil Varlıklar

Birincil varlıklar GİB-BS'nin TSM Merkezi'nden yönlendirilirken ya da TSM Merkezi'nde bulunurken korumasını istediği varlıklardır.

2.1.1.1 Z Raporu

Yeni Nesil ÖKC'den GİB BS'ye GMP dokümanlarında tanımlandığı gibi gizliliği ve bütünlüğü korunacak şekilde gönderilmektedir. Gizlilik ve bütünlüğün korunması Yeni Nesil ÖKC ve GİB BS arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır.

ÖKC TSM Merkezi bu varlık için yönlendirme işlemini yürütmektedir.

2.1.1.2 Yeni Nesil ÖKC Fiş Bilgisi

Yeni Nesil ÖKC'den GİB BS'ye GMP dokümanlarında tanımlandığı gibi gizliliği ve bütünlüğü korunacak şekilde gönderilmektedir. Gizlilik ve bütünlüğün korunması Yeni Nesil ÖKC ve GİB BS arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır.

ÖKC TSM Merkezi bu varlık için yönlendirme işlemini yürütmektedir.

2.1.1.3 Yeni Nesil ÖKC Fiş İptal Bilgisi

Yeni Nesil ÖKC'den GİB BS'ye GMP dokümanlarında tanımlandığı gibi gizliliği ve bütünlüğü korunacak şekilde gönderilmektedir. Gizlilik ve bütünlüğün korunması Yeni Nesil ÖKC ve GİB arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır.

ÖKC TSM Merkezi bu varlık için yönlendirme işlemini yürütmektedir.

2.1.1.4 Para Birimi Çevrim Oranları

GİB BS'den TSM Merkezi'ne GMP dokümanlarında tanımlandığı gibi bütünlüğü ve inkâr edilemezliği korunacak şekilde gönderilebilmektedir. Bütünlüğün korunması GİB tarafından sunulan MPLS hat üzerinde, GİB BS ve ÖKC TSM Merkezi arasında kurulan güvenli kanallar (VPN tünel) vasıtasıyla yapılmaktadır. İnkâr edilemezliğin korunması GİB'in imzası ile sağlanmaktadır.

Yeni Nesil ÖKC, ÖKC TSM Merkezi'nden GMP dokümanlarında tanımlandığı gibi bütünlüğü korunacak şekilde almaktadır. Bütünlüğün korunması ÖKC TSM Merkezi ve Yeni Nesil ÖKC arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır.

ÖKC TSM Merkezi bu varlığı açık olarak görebilmektedir.

2.1.1.5 Olay Kayıtları

Olay kayıtları, ÖKC TSM Merkezi üzerinden Yeni Nesil ÖKC ile GİB BS arasında paylaşılmaktadır.

Yeni Nesil ÖKC'den GİB BS'ye GMP dokümanlarında tanımlandığı gibi gizliliği ve bütünlüğü korunacak şekilde gönderilmektedir. Gizlilik ve bütünlüğün korunması Yeni Nesil ÖKC ve GİB arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır.

ÖKC TSM Merkezi bu varlık için yönlendirme işlemini yürütmektedir.

2.1.1.6 Haberleşme Tablosu

Yeni Nesil ÖKC, ÖKC TSM Merkezi'nden GMP dokümanlarında tanımlandığı gibi gizliliği ve bütünlüğü korunacak şekilde almaktadır. Gizliliğin ve bütünlüğün korunması ÖKC

TSM Merkezi ve Yeni Nesil ÖKC arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır.

ÖKC TSM Merkezi bu varlığı oluşturmaktadır.

2.1.1.7 Parametre Tablosu

GİB BS'den ÖKC TSM Merkezi'ne GMP dokümanlarında tanımlandığı gibi gizliliği, bütünlüğü ve inkâr edilemezliği korunacak şekilde gönderilmektedir. Gizliliğin ve bütünlüğün korunması GİB tarafından sağlanan MPLS hat üzerinden, GİB BS ve ÖKC TSM Merkezi arasında kurulan güvenli kanallar (VPN tünel.) vasıtasıyla yapılmaktadır. İnkâr edilemezliğin korunması GİB'in imzası ile sağlanmaktadır.

Yeni Nesil ÖKC, ÖKC TSM Merkezi'nden GMP dokümanlarında tanımlandığı gibi bütünlüğü korunacak şekilde almaktadır. Bütünlüğün korunması ÖKC TSM Merkezi ve Yeni Nesil ÖKC arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır.

ÖKC TSM Merkezi bu varlığı açık olarak görebilmektedir.

2.1.1.8 İstatistik Verileri

Yeni Nesil ÖKC'den GİB BS'ye GMP dokümanlarında tanımlandığı gibi gizliliği ve bütünlüğü korunacak şekilde gönderilmektedir. Gizlilik ve bütünlüğün korunması Yeni Nesil ÖKC ve GİB arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır.

ÖKC TSM Merkezi bu varlık için yönlendirme işlemini yürütmektedir.

2.1.1.9 Yeni Nesil ÖKC Yazılımı

Yeni Nesil ÖKC, TSM Merkezinden GMP dokümanlarında tanımlandığı gibi gizliliği, bütünlüğü ve inkâr edilemezliği korunacak şekilde almaktadır. Gizliliğin, bütünlüğün korunması ÖKC TSM Merkezi ve Yeni Nesil ÖKC arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır. İnkâr edilemezliği OKTEM Laboratuvarının YN ÖKC yazılımının özetine uyguladığı imza veya üretici imzası ile sağlanmaktadır.

ÖKC TSM Merkezi bu varlığı açık olarak görebilmektedir.

2.1.2 İkincil Varlıklar

Birincil varlıkları korumak için ÖKC TSM Merkezi'nin kullandığı varlıklardır.

- Kriptografik Anahtarlar
- ÖKC TSM Merkezi sistem bileşenleri erişim denetim verisi (ÖKC TSM Merkezibileşenlerine yetkili kullanıcıların erişim izleri)
- Sunucular
- HSM Cihazları
- ÖKC TSM MerkeziOlay Kayıtları (ÖKC TSM Merkeziİz Kayıtları)
- Yazılımlar (TSM Merkezinde kullanılan yazılımlar)

2.2 Aktörler

2.2.1 Yetkili Kullanıcılar

Sistemin tüm alt bileşenlerinde yer alan yetkilendirilmiş (kullanıcı adı /parola veya akıllı kartı olan) kullanıcılardır. Bu kullanıcılar, sadece normal veri akış senaryosunda yer alan kullanıcılarla sınırlı değildir. Kurulumcu, bakım/onarımcı, denetçi gibi farklı kullanıcılar da potansiyel tehdit kaynağı olarak görülmelidir.

Kullanıcılar farklı motivasyonlarla tehdit unsuru olabilir. Yetersiz eğitilmiş, hoşnutsuz, ihmalcı, kötü amaçlı, sahtekâr, işine son verilmiş veya işinden ayrılmış olabilirler. Bu kişiler; şantaj yapmak, özel bilgilere erişmek, bilgisayarları bozmak, sahtekârlık ve hırsızlık yapmak, bilgi rüşvetçiliği yapmak, tahrif edilmiş ve bozulmuş ya da yanlış veri girişi yapmak, kötü amaçlı kod (virüs, truva atı, vb.) yüklemek, kişisel bilgileri satmak, sistemi sabote etmek, kurum itibarını zedelemek veya yetki yükseltmek gibi çeşitli vesilelerle tehdit oluşturabilirler.

2.2.2 Yetkisiz Kullanıcılar (Hacker, Siber Terörist, vb.)

Sisteme herhangi bir atak yüzeyinden (örn: cihazlar, ağ üzeri) saldıran, genellikle sistem tarafından yetki verilmemiş kişi veya organizasyonlardır. Sistemi alt etme teşebbüslerinde farklı motivasyonlar olabilir: Maddi kazanç, şöhret, otoriteye karşı verilen mücadeleden keyif alma, farklı bir ülke çıkarlarını koruma, vb. operatörlere ve vatandaşlara yönelik sosyal mühendislik saldırıları, sistem açıklıkları, kriptografik saldırılar, yan kanal saldırıları, üretim sırasında müdahale gibi birçok tekniği kullanabilirler.

2.2.3 Teçhizat ve Yazılımlar

Ağ ve veri tabanı sunucusuna bağlanılmasını sağlayan teçhizat ve yazılımlar (bilgisayar, işletim sistemleri vb.) arızalandıklarında, kusurları olduğunda ya da güncel tutulmadıklarında çeşitli saldırılara maruz kalabilirler.

Teçhizat ve yazılımlar sahaya ilk çıktıklarında saldırmaya elverişli açıklık barındırabilirler. Bir diğer tehlike, teçhizat ve yazılımların sahada kullanıma çıktıklarında veya güncelleme, bakım/onarım aşamalarında saldırganlar tarafından kötücül yazılım (malware, trojan vb.) araçları vasıtasıyla saldırıda kullanılmalarıdır. Dolayısıyla, teçhizat ve yazılımlar bilgi kaçağı, yetkisiz erişim ya da hizmet engellemesine neden olabilirler.

2.2.4 Çevresel Koşullar

Bulundukları konumlarda nem, ısı, ışık, sıcaklık vb. hava şartlarından kaynaklı olarak birçok farklılık olacaktır. Ortam sıcaklığının değişmesiyle güvenlik fonksiyonlarının aksamaması nedeniyle cihazlardan bilgi kaybı, cihazın bozulmasıyla sistemin aksamaması vb. durumlar meydana gelebilir.

3. Sistem Güvenliği, İş Sürekliliği, Felaket Kurtarma ve Olay Müdahale

✓ TSM Merkezi'nin ISO/IEC 27001 [1] sertifikasının bulunduğu görülmelidir. Sertifikanın Bölüm 2'de belirtilen kritik varlıkları işleyen ve kullanan süreçleri kapsadığı kontrol edilmelidir.

✓ TSM Merkezi'nin ISO/IEC 22301 [2] sertifikasının bulunduğu görülmelidir.

4. Kullanılan Donanımların Güvenliği

ÖKC TSM Merkezleri; GİB BSve Yeni Nesil ÖKC ile haberleşmek için kriptografik anahtarlar kullanılması ve bu anahtarların ÖKC TSM Merkezleri'nde FIPS 140-2 Level 3 ve üzeri için sertifika almış ürünler ile saklanması gerekmektedir.

5. Kullanılan Yazılımların Güvenliği

Yapılacak test ve değerlendirmeler sonucunda TSM Merkezi'nin aşağıdaki görevleri yerine getirdiği anlaşılan yazılımlarının, PCI DSS denetim kapsamında olduğu görülmelidir.

Yazılımın Güvenlik ile İlgili Görevleri;

➤ Yeni Nesil ÖKC ile haberleşmeyi sağlamak

- Yeni Nesil ÖKC'lere mali uygulama yazılımını yüklemek
- Yeni Nesil ÖKC'lere mali parametreleri yüklemek
- GİB BS ile haberleşmeyi sağlamak
- Yeni Nesil ÖKC'lere yükleyeceği parametreleri GİB BS'den almak
- Yeni Nesil ÖKC ile GİB BS'nin haberleşmesini sağlamak
- Mali bilgilerin gönderilmesi
- Olay kayıtlarının gönderilmesi
- İstatistik verilerinin gönderilmesi
- Yeni Nesil ÖKC'den Olay Kayıtlarının alınması

6. Güvenlik Denetimi

TSM Merkezi'nin aşağıda listelenen kapsamda Sızma Testi Raporunun bulunduğu ve her yıl yenilendiği görülmelidir. Sızma testinin Bölüm 2'deki tüm kritik varlıkları ve sistemin genelini kapsayacak şekilde yapıldığı kontrol edilmelidir. Sızma testinde açıklık tespit edilmişse, tespit edilen açıklığın giderilmesine yönelik müdahale planının olduğu bir raporda görülmelidir.

- ✓ Sosyal Mühendislik Testleri
- ✓ Ağ ve İletişim Altyapısı Testleri
- ✓ İşletim Sistemi ve Platform Testleri
- ✓ Uygulama Testleri
- ✓ Veri Tabanı Testleri

BÖLÜM II

YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARA AİT ÖKC TSM MERKEZİ SİSTEM GEREKSİNİMLERİ

7. ÖKC TSM Merkezlerinin Desteklemesi Gereken Standartlar

ÖKC TSM Merkezlerinin aşağıdaki sertifikasyonlar için denetlemelerden geçmiş ve bu sertifikaları almaya hak kazanmış olmalıdır. 13/01/2010 tarihli ve 27461 sayılı Resmi Gazete’de yayımlanan “Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmeliği”nde açıklandığı şekilde ÖKC TSM Merkezi yılda bir kez denetlenmiş ve denetim mektubu ile güncellenmiş sertifikaların Üye İşyeri Anlaşması yapan kuruluşlara gönderilmiş olmalıdır.

İlki başvuru sürecinde olmak üzere yılda bir kez ÖKC TSM Merkezi bağımsız denetim kuruluşları tarafından gerçekleştirilecek Bilgi Sistemleri Denetimi ile proje genelinde hedeflenen bilgi güvenliği standardına ulaşıp ulaşılmadığı sınanmış olmalıdır. Tespit edilen açıklıkların kapatılmasına yönelik ÖKC TSM tarafından alınan aksiyonlar kontrol edilmelidir.

7.1 Uluslararası Standartlar:

Uluslararası bilgi sistemleri ve ödeme sistemlerine ait aşağıdaki temel standartlar sağlanmalıdır. Bu standartların sağlandığı alınan sertifikalarla ispatlanmalıdır. Sertifikalar düzenli olarak yenilenmelidir. Sertifikalar ile ilgili detaylı bilgiye Referanslar bölümünde yer alan linklerden ulaşılabilmelidir.

a. PCI-DSS Payment Card Industry Data Security Standard Onay Belgesi AOC (Attestation of Compliance for Onsite Assessments) Belgesi üzerinde ÖKC TSM Merkezi hizmetlerinin verildiği uygulamaların denetim kapsamında olduğunun, sertifikanın Bölüm 2’de belirtilen kritik varlıkları işleyen ve kullanan süreçleri kapsadığının kontrol edilmesi gerekmektedir.

Sertifikasyon asgari olarak *Infrastructure/Network, Payment Gateway/Switch, Backoffice Services ve POS/Card Present* için alınmış olmalıdır. AOC (Attestation of Compliance for Onsite Assessments) Dokümanında bu başlıklardan onay alındığı görülmelidir.

Ayrıca AOC içerisinde *Other Processing (specify)* alanında "*Trusted Service Manager Services*" ibaresi bulunmalıdır veya *Description* alanında ÖKC TSM Merkezi Hizmetlerinin kapsamda olduğu ifade edilmiş olmalıdır.

Yeni Nesil ÖKC'ler, ÖKC TSM Merkezleri ve üye işyeri anlaşması yapmış kurumlar arasındaki iletişim güvenliği için PCI DSS onaylı bir anahtar yönetim mekanizması kurulmuş olmalıdır.

- b. ISO/IEC 20000 Bilgi Teknolojileri Hizmet Yönetim Sistemi Belgesi
- c. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi
- ç. ISO 22301 İş Sürekliliği Yönetim Sistemi Belgesi

7.2 Ulusal Standartlar:

Ulusal Ödeme Sistemleri Kural Koyucuları (BDDK) ve Mali Kural Koyucular (GİB) tarafından belirlenen ve güncellenen standartlara uyulması gerekmektedir.

8. ÖKC TSM Merkezi Başvuru, Test , Denetim ve Onay Süreçleri

ÖKC TSM Merkezlerinin başvuru, test, denetim ve onay süreçleri Bölüm III'te detaylı olarak anlatılmaktadır. ÖKC TSM Merkezleri'nde ÖKC Üreticileri için münhasıran kurulmuş bir donanım, yazılım ve işletim sistemi olup olmadığı incelenecek ve sertifikalar bu sistem için alınmış olacaktır.

9. Sistemlerin Münhasırlığı

✓ ÖKC TSM Merkezi alt yapısı için kullanılan uygulama sunucuları her ÖKC üreticisi için ayrı bir fiziki ve/veya sanal ortamlarda kurulabilir. Kurulan bu fiziki ve/veya sanal ortamlar sadece Yeni Nesil ÖKC alt yapısına hizmet veren sanal ve/veya fiziksel sunucular üzerlerindeki görevler (Servisler, uygulamalar vb.) PCI-DSS kriterlerine uygun şekilde yapılandırılmalıdır.

✓ ÖKC TSM Merkezi altyapısında kullanılan veri tabanı sunucuları her ÖKC üreticisi için ayrı bir fiziksel ve/veya sanal sunucularda kurulmalıdır. Veri tabanı sunucularına ait veriler her üretici için kendine ait disk gruplarında barındırılmalıdır.

✓ Sanallaştırma sistemlerine ait fiziksel sunucular (Vmware, Hyper-V vb.) üzerinde ÖKC TSM Merkezi sistemleri dışında sanal sunucular varsa, ÖKC TSM Merkezi sistemleri diğer sunuculardan ağ bazında tamamen izole olarak ayrı sanal lokal ağlarda (VLAN) kurulmalıdır. ÖKC TSM Merkezi sistemleri kendi içinde de PCI-DSS kriterlerine uygun olarak rol bazında da (Web sunucu, uygulama sunucu, veri tabanı sunucusu gibi) ayrı sanal lokal ağlarda (VLAN) izole edilmelidir.

✓ ÖKC TSM Merkezi ve İkincil Merkez’de bulunan ağlar, ÖKC TSM Merkezi sistemlerini varsa diğer tüm sistemlerden izole edecek şekilde (Sanal lokal ağlar kullanılarak) yapılandırılmalıdır. ÖKC TSM Merkezi omurgasında ortak olarak kullanılan tüm cihazlar (Firewall, Load Balancer, Switch, Storage, vs) üzerindeki konfigürasyonlar mantıksal seviyede izole edilerek hazırlanmalıdır.

✓ Veri tabanı sunucuları ayrı bir ağ altında bulunmalı ve sanal lokal ağlarla (VLAN) diğer uygulamalardan ayrılmalıdır. Bu VLAN’lara erişim, sadece kontrolsüz ağlara erişimi olmayan uygulama sunucularından ve en az mantıksal seviyede sağlanmalıdır.

✓ HSM cihazları ve sunucuları farklı ÖKC üreticileri için farklı kriptografik anahtarlar olmak üzere ortak olarak kullanılabilir.

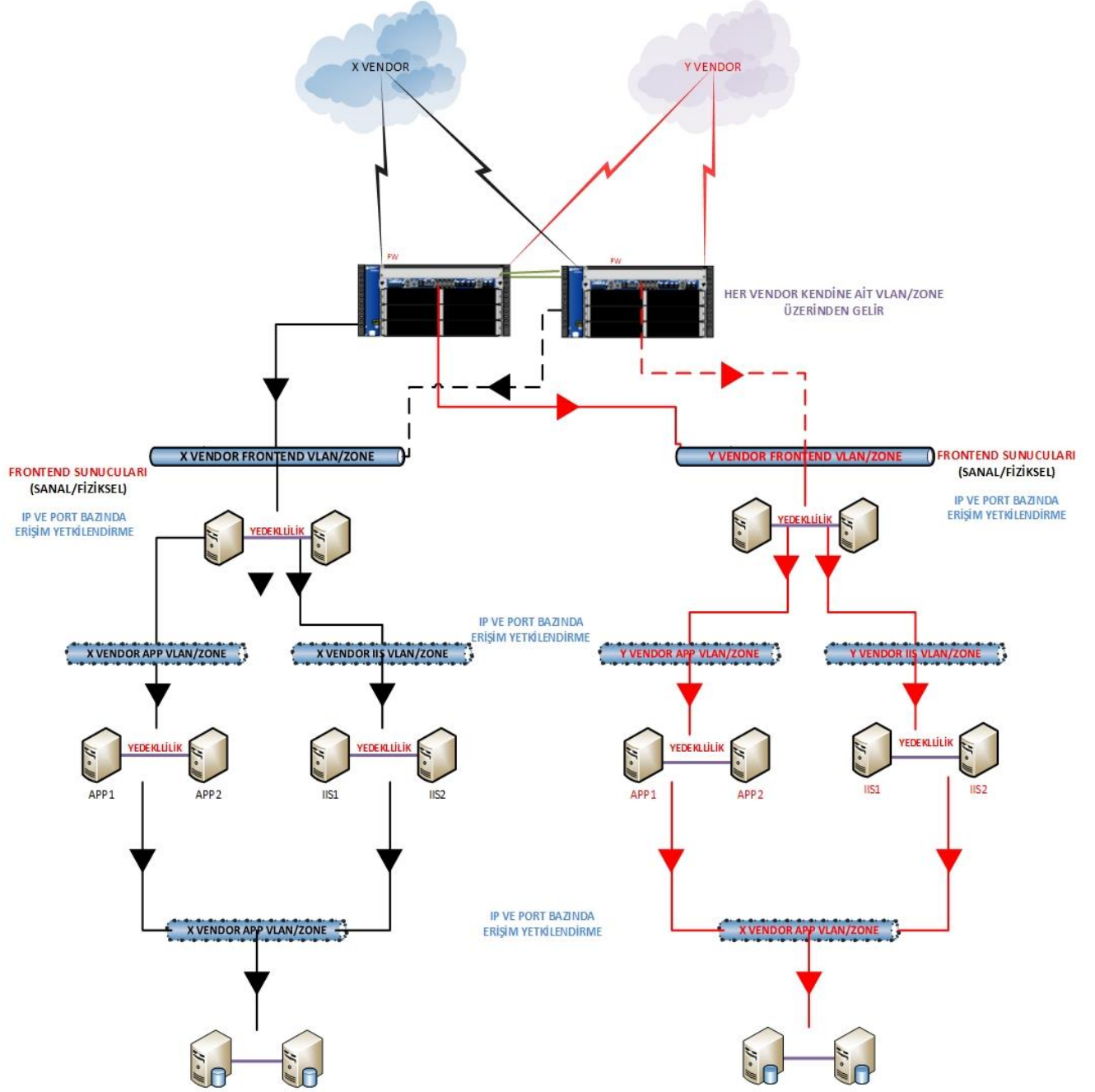
✓ Tüm sistemlerde erişim yetkileri PCI-DSS standartlarına göre belirlenmeli, uygulanmalı ve dokümanite edilmelidir. Ayrıca PCI-DSS standartları gereği yıllık olarak bağımsız firmalar tarafından denetlenmelidir.

✓ Yukarıda bahsedilen münhasırlık maddeleri ÖKC TSM Merkezlerinin ikincil merkezleri için de geçerlidir.

Birden fazla ÖKC üreticisine hizmet veren örnek bir TSM Merkezi’nin sistemlerinin münhasırlığına ilişkin topoloji aşağıdaki şekilde gösterilmektedir. Bu şekil doğrudan

uygulanması gereken bir zorunluluk değildir. Ancak yukarıdaki münhasırlık prensiplerinin uygulanabileceği örnek bir şekildir.

ÖRNEK DHS TSM TOPOLOJİSİ



1. Her üreticiye ait terminaller, gerekli izolasyon sağlanmış (APN, İp tanımı, Tunnel vs) çeşitli bağlantı yöntemleri ile TSM güvenlik duvarına gelir.
2. Güvenlik duvarları üzerinde her bir üretici için ayrı olarak tanımlanmış ZONE/ VLAN'lar gelen trafikleri karşılar ve sadece ilgili Frontend alanına gönderir.
3. Frontend alanında bulunan donanımlarda işleme tabi tutulan trafik, yine güvenlik duvarı üzerinden (L3 seviyesinde) kendisine ait Core Application ya da IIS makinalarına yönlendirilirler.
4. Core alanlarda bulunan donanımlar dışında veri tabanına hiç bir erişim bulunmamaktadır. Veri tabanlarına sadece Core alanlardaki sunucu/donanımlar erişebilir. Veritabanına yapılacak network erişimleri için trafik, güvenlik duvarı üzerinden (L3 seviyesinde) geçer.

10. ÖKC TSM Merkezleri Sorumluluk Dağılımı

Yeni Nesil ÖKC'lerin yaşam döngüsü yönetimi (ayrı bir başlık ile kapsamı belirlenmiştir) ÖKC TSM Merkezi üzerinden yapılacaktır. ÖKC TSM Merkezinin yönetim, yetki ve sorumluluğu ise ÖKC üreticilerindedir. Burada kastedilen, ÖKC üreticilerinin bir Dış Hizmet Sağlayıcısından TSM Merkezi'ne ilişkin hizmet temin etmesi durumunda ÖKC üreticisinin, ÖKC TSM Merkezi hizmetlerine ilişkin sorumluluklarının ortadan kalkmayacağıdır. ÖKC üreticileri ÖKC TSM Merkezleri'ne ilişkin hizmetlerin sunumunda DHS'lerden de hizmet temin edebilir. GİB açısından muhatap ÖKC üreticisidir. ÖKC üreticilerinin dış hizmet alımlarında riskini yönetebilmek adına DHS'lerle yaptığı anlaşmaları bu kılavuzu dikkate alarak yönetmesi önerilmektedir.

ÖKC üreticileri, kendi kuracakları ÖKC TSM Merkezlerine ait birincil merkezinin donanım altyapısı ile tüm işletim ve operasyon süreçlerini dış kaynak kullanımı veya barındırma hizmeti şeklinde başka bir alt yükleniciden/taşerondan sağlayamaz. Birincil merkezin tüm işletim ve operasyon süreçlerini ÖKC üreticisi 7/24 kendi personeli ile yürütmek zorundadır. İstihdam edilecek personel nitelik ve niceliği ile ilgili "ÖKC TSM Merkezi Personel Gereksinimleri" başlığında detaylı bilgi verilmektedir. Söz konusu donanım, tüm işletim ve operasyon süreçlerinin herhangi bir kısmının ÖKC üreticisi dışında bir dış kaynaktan temin edilmesi halinde söz konusu ÖKC TSM Merkezi Dış Hizmet Sağlayıcısının verdiği bu hizmetler bakımından da test, değerlendirme, denetim ve onay süreçlerine tabi tutulacaktır.

ÖKC üreticileri kendi kuracakları ÖKC TSM Merkezleri'ne ait ikincil merkezinin; sadece donanım alt yapısının barındırılması hizmetini taşeron ya da alt yükleniciden temin edebilir. Ancak, ikincil merkeze ait donanım alt yapısının yönetimi ile tüm işletim ve operasyon süreçlerinin ÖKC üreticisine ait kendi personeli ile yürütmek zorundadır.

Yeni Nesil ÖKC'ler üzerinde veya Yeni Nesil ÖKC'ler ile birlikte çalışacak cihazlar (EFT-POS, PinPad) yoluyla Üye İşyeri Anlaşması Yapan Kuruluşun uygulamalarının çalıştırılmasına ilişkin sahada yapılması gereken tüm servis ve saha operasyonlarının yetki ve sorumluluğu ÖKC üreticilerindedir.

ÖKC TSM Merkezleri ve DHS'ler vereceği hizmetlerden doğabilecek zararları karşılamak amacıyla mesleki sorumluluk sigortası yaptırmak zorundadır.

11. Mükellef, Yeni Nesil ÖKC, ÖKC TSM Merkezleri ve GİB İletişimi

Yeni Nesil ÖKC'ler GİB BS'ye ÖKC TSM Merkezleri üzerinden bağlanacak olup, cihazların doğrudan veya ÖKC TSM Merkezleri haricinde başka bir hat üzerinden GİB BS'ye bağlanması mümkün değildir. ÖKC TSM Merkezleri ile Yeni Nesil ÖKC'ler ve GİB BS arasındaki kurulacak olan güvenli alt yapı, ağların sorumluluğu ve sahipliği (tasarrufu) ÖKC üreticilerinde olacaktır. Yeni Nesil ÖKC'lerin ÖKC TSM Merkezlerine erişimleri için gereken alt yapı, erişim hatlarının sorumluluğu ve sahipliği ise Yeni Nesil ÖKC kullanan mükelleflere aittir.

Yeni Nesil ÖKC GMP Mesajı ağ iletim seviyesi, ÖKC TSM Merkezinde sonlandırılacak olup, GMP Mesajı üzerinde gerekli ön kontroller yapıldıktan sonra GİB BS'ye GMP Mesaj formatında iletilecektir.

ÖKC TSM Merkezleri, Yeni Nesil ÖKC'leri yönetme, ayakta tutma, her işlemde cihazdan gelen GMP Mesaj bilgilerinin format ve doğruluğunu değerlendirme, bu mesaj bilgilerinin içerisindeki hassas mali verilerin kaynağının doğruluğunu kontrol etmekle yükümlüdür. Bu kontrol işlemi sırasında GİB hassas ÖKC verisinin ve Üye İşyeri Anlaşması Yapan Kuruluşlara ait hassas verilerin ÖKC TSM Merkezi tarafından açılmaması ve saklanmaması gerekmektedir.

GİB BS'nin cihazları yönetme, ayakta tutma veya Yeni Nesil ÖKC'lerin durumu ile ilgili üreticiye veya ÖKC TSM Merkezlerine geri bildirim yapma görevi bulunmamaktadır. Bu sorumluluk ÖKC üreticileri ile birlikte ÖKC TSM Merkezlerine aittir. ÖKC Üreticileri, cihazda oluşturularak ÖKC TSM Merkezleri üzerinden GİB BS'ye gönderilen GİB ÖKC mesajlarının kaynağının doğruluğundan, değişmezliğinden ve bütünlüğünden sorumludur. GİB ÖKC mesajlarının teknik kılavuzlarda ve protokollerde öngörülen zaman ve sıralamaya uygun olarak GİB BS'ye gönderilmesi gerekmekte olup, hata içeren mesajların gönderilmesi halinde sorumluluk ÖKC Üreticilerine aittir.

ÖKC'lerin ÖKC TSM Merkezleri üzerinden GİB BS'ye gönderecekleri mesajların sadece GİB BS tarafından kayıt ve analiz edilebilecek mahiyette olması ve ilgili mesajlaşma protokollerine uygun şekilde gönderilmesi esastır.

ÖKC TSM Merkezleri ve DHS'ler, EFT-POS özellikli Yeni Nesil ÖKC'ler ve EFT-POS cihazları ile entegre çalışan Yeni Nesil ÖKC'ler de dahil, üzerlerinden bankacılık mesajlarının da

geçecek olması nedeniyle BDDK ve PCI SSC'nin gerektirdiği düzenleme ve standartlarını karşılaması zorunludur.

Üye İşyeri Anlaşması Yapan Kuruluşlara ait olanlar da dahil olmak üzere Yeni Nesil ÖKC'ler üzerinde çalışan tüm uygulamalar ÖKC TSM Merkezi üzerinden banka ya da diğer uygulama sistemlerine bağlanacaktır. (Kurum ERP programlarına GMP3 ile kablolu bağlanabilir). Üye İşyeri Anlaşması Yapan Kuruluşun yetkilendireceği kişi ve/veya kurumlar, Yeni Nesil ÖKC ile birlikte çalışacak bankacılık uygulamaları ve bunlara ilişkin parametre, anahtar yazılım yükleme ve ihtiyaç duyulan diğer işlemleri yerine getirmek için taleplerini ÖKC TSM Merkezlerine bildireceklerdir. Bu işlemler ÖKC TSM Merkezleri aracılığıyla gerçekleştirilecektir. Yeni Nesil ÖKC'ler parametre veya yazılımları ÖKC TSM Merkezi üzerinden geçmek kaydıyla doğrudan talep ederek de alabilirler. Tüm parametre veya yazılım yüklemeler esnasında, GMP3 dokümanının 4.4.1 bölümünde belirtilen Header yapısındaki bilgilerin doldurulmuş olması ve taşınan bilgilerin TSM Merkezi tarafından kaydedilip ve takip edilmesi gereklidir. Yeni Nesil ÖKC parametre yönetiminde, cihazın genel işlevine etki eden parametreler (cihazın açılması, kapanması, işlevsel olarak devre dışı kalması gibi diğer uygulamaların çalışmasını etkileyecek genel cihaz parametreleri) sadece ÖKC TSM Merkezleri tarafından yönetilmeli, diğer uygulamalara bırakılmamalıdır. Yeni Nesil ÖKC, TSM Merkezleri ve üye işyeri anlaşması yapmış kurumlar arasındaki güvenli iletişim için kullanılacak anahtarların yönetim mekanizmaları PCI DSS'nin kabul ettiği mekanizmalar olmalıdır. Yeni Nesil ÖKC'lerde oluşabilecek sorunlardan (sahada yaşanacak cihaz ya da tüm uygulamalardaki manipülasyonlar, alınan ödeme ile kesilen mali fiş mutabakatsızlıkları, fonksiyonel arızalar, usulsüz banka/sadakat uygulama anahtar yüklemeleri, saha operasyonel sıkıntıları vb.) ÖKC üreticileri sorumludur.

12. Yeni Nesil ÖKC Yaşam Döngüsü Yönetimi

- İçeriğinden bağımsız olarak Yeni Nesil ÖKC üzerinden başlatılacak olan her işlem ÖKC TSM Merkezi üzerinden yönlendirilmelidir. Bu yönlendirme işlemi öncesinde alınan tüm mali ve GMP-3 ile haberleşilen mesajlarla ilgili kontrollerin yapılması gerekmektedir.
- ÖKC TSM Merkezi tarafından, belirtilen mesajlar için yapılması gereken minimum kontroller aşağıda verilmiştir.

- Yeni Nesil ÖKC seri numarası kontrolü
 - Yeni Nesil ÖKC sistemde kayıtlı bir Yeni Nesil ÖKC olmalıdır.
 - Yeni Nesil ÖKC kurulumu tamamlanmış ve aktive edilmiş bir Yeni Nesil ÖKC olmalıdır.
 - Yeni Nesil ÖKC seri numarası daha önceden arıza veya şirket kapanması sebebi ile hurdaya ayrılmamış bir Yeni Nesil ÖKC olmalıdır.
- Yeni Nesil ÖKC uygulama kontrolü
 - Yeni Nesil ÖKC üzerinden mesajı gönderen uygulama, daha önceden Yeni Nesil ÖKC'ye ÖKC TSM Merkezi üzerinden yüklenildiğinden emin olunan bir uygulama olmalıdır.
 - Yeni Nesil ÖKC üzerinden mesaj gönderen uygulama sürümü ile sistemde görünen ÖKC'ye yüklü uygulama sürümü aynı olmalıdır.
- Mesaj tip kontrolü
 - Gönderilen mesaj sistemde tanımlı bir mesaj olmalıdır.
 - Gönderilen mesaj, Yeni Nesil ÖKC'nin sisteme gönderme izni olan mesajlardan biri olmalıdır. Sistemde tanımlı olsa bile Yeni Nesil ÖKC'nin yetkisi yoksa mesaj ÖKC TSM Merkezi tarafından iletilmemelidir.
 - Hiçbir Yeni Nesil ÖKC'den kendi yetkisi dışında bir sisteme ÖKC TSM Merkezi aracılığı ile mesaj gönderilemez.
- Yeni Nesil ÖKC ve İşyeri Tanım kontrolleri
 - Yeni Nesil ÖKC tarafından gönderilen her mesaj içinde ÖKC TSM Merkezi'nde o seri numaralı Yeni Nesil ÖKC'nin bir işyerine atanmış olması zorunludur.
- Yeni Nesil ÖKC Bilgi Parametreleri
 - Yeni Nesil ÖKC'nin gönderdiği mesaj grup numarası, aksi operasyon birimleri tarafından söylenmediği sürece geriye gidemez. Bu GİB için Z raporu numarasıdır (Header bulunan mesajlarda).
 - Yeni Nesil ÖKC'nin gönderdiği işlem numarası, aynı grup içindeyken geriye gidemez. Grup numarasının arttığı durumda 1 değerine geri dönülebilir (Header bulunan mesajlarda). Yeni Nesil ÖKC'den gelen işlem saati, ülke saatinin geri alındığı günler hariç geriye gidemez. Yeni Nesil ÖKC son yaptığı işlemde muhakkak daha ileri bir tarih ve saatte işlem yapabilir.

- ÖKC TSM Merkezleri GİB BS ile zaman senkronizasyonunu sağlamakla yükümlüdür. ÖKC TSM Merkezleri Yeni Nesil ÖKC'lerden gelen mesajlarda saat farkından dolayı hata alıyorsa parametrik bir sayıdan sonra aynı hatayı alacak mesajların gönderilmesine izin vermeyecektir. ÖKC TSM Merkezleri Yeni Nesil ÖKC'nin senkronize olması için otomatik ya da manuel süreçlerini başlatabilir.

- Kritik Mesaj Güvenliği

- Uygulama ve parametre yükleme işlemlerinde ÖKC TSM Merkezi gönderdiği mesajları imzalar. Yeni Nesil ÖKC, TSM Merkezi imza kontrolünü yapmak durumundadır.

- İstatistik

- Yeni Nesil ÖKC sistemsel arızalarını gün sonlarında raporlar. Bu raporlar sistem tarafından alarm oluşturabilir, arıza bildirimlerinde önemli bir bilgi kaynağı olduğu için kontrol edilir. Bu raporlar Yeni Nesil ÖKC'den GİB BS'ye GMP dokümanlarına uygun gönderilen ve bu kılavuzun 2.1.1.8 başlığında açıklanan istatistik verilerinden ayrıca temin edilmelidir.

- Yeni Nesil ÖKC günlük işlemlerine ilişkin sorunlu ve başarılı durum istatistiklerini gönderir. Bu raporlar her Yeni Nesil ÖKC için oluşturulur. Ortalamanın üstündeki başarısız durumlar TSM Merkezinde incelenir. TSM Merkezinde incelenen verilerden yola çıkılarak bazı zamanlarda bu Kılavzun 23. maddesinde açıklanan GİB BS'ye uyarı mekanizmalarını kullanarak bilgi verir. GİB BS'ye bildirmesi gerekmeyen teknik arızaları ÖKC TSM Merkezi saha operasyonları yoluyla ya da uzaktan çözer.

- ÖKC TSM Merkezi, mesaj ile ilgili kontrolleri yaparken, Yeni Nesil ÖKC üzerinden gelen mesajların içeriğindeki hassas verileri açamamalı, ancak mesajı ilgili sunucuya doğru bir şekilde yönlendirebilecek alt yapıya sahip olmalıdır. ÖKC TSM Merkezi mesaj üzerinde kendi kontrollerini yapmasını sağlayacak olan alanları bu şifreli mesajların yapısını bozmadan eklemek sureti ile tek bağlantıda gönderebilmelidir.

- Cihazların yönetilmesi, ayakta tutulması, gelen bilgilerin doğruluğunun değerlendirilmesi, Yeni Nesil ÖKC'nin durumu gibi bilgilerin cihaz üzerinden alınıp ÖKC TSM Merkezi içerisinde değerlendirilmesi ya da gerekliyse GİB'e iletilmesi görevi ÖKC TSM Merkezi sorumluluğundadır.

- Yeni Nesil ÖKC'lerin ÖKC TSM Merkezleri üzerinden GİB BS'ye gönderecekleri mesajların doğrudan GİB BS tarafından kayıt ve analiz edilebilecek mahiyette olması esas olup, bu mesajlar üzerinde GİB BS'nin ilave bir çalışma yapılmasına ihtiyaç gerektirmeyecek yapıda ve ilgili mesajlaşma protokollerine uygun şekilde olması esastır.
- Yeni Nesil ÖKC'ler, ÖKC TSM Merkezi ile GMP'lerde belirtilen güvenli ilklendirme yapılmadan yaşam döngüsüne başlayamaz.
- ÖKC TSM Merkezleri, GİB ve yasalarca yetkili kılınmış diğer kurumlardan gelen talimatlar doğrultusunda Yeni Nesil ÖKC'lerin fonksiyonlarının tümünü veya belli bir kısmını uygun denetim izleri bırakarak tamamen ya da geçici süreyle durdurabilir veya değiştirebilir.
- ÖKC üreticileri ve bunlara ait ÖKC TSM Merkezleri kural koyuculardan gelen talimatlar doğrultusunda veya ÖKC üreticilerinin oluşturduğu sahtekârlık senaryolarına göre otomatik izleme mekanizmalarını ve raporlamalara uygun şekilde sahtekârlık önleme ve izleme sistemini kurmakla yükümlüdür. Oluşan sahtekârlıkları GİB uyarı mekanizmalarını kullanarak GİB'e iletir.
- Üye İşyeri Anlaşması Yapan Kuruluşlara ait kural koyucular tarafından hassas veri olarak kabul edilen veriler ÖKC TSM Merkezi üzerinden iletilirken hiç bir durumda (Banka ve kurumlara kredi kartı, banka kartı, POS, sanal POS, elektronik ticaret, ATM işletimi vb. ödeme sistemleri hizmetleri verilmesi hariç) açılmamalı veya saklanmamalıdır. ÖKC TSM Merkezlerinin, müşteriler (kart hamilleri) ile ilişkilendirilebilecek hiçbir veriye ve kural koyucular tarafından hassas veri olarak tanımlanan verilere erişebilme kabiliyeti bulunamaz.

13. Yeni Nesil ÖKC Mesajlarının (ÖKC Durum Verisi ve GİB Hassas ÖKC Verisi) Yönetimi

Yeni Nesil ÖKC'ler, ÖKC TSM Merkezi ile GMP'lerde belirtilen güvenli ilklendirme yapıldıktan sonra yaşam döngüsüne başlamış olur. ÖKC Durum Verisi, Yeni Nesil ÖKC'den gelen her bir mesaj için ÖKC TSM Merkezinde tutarlılık ve yaşam döngüsü kontrollerinden geçirildikten sonra, GİB hassas ÖKC verisi ise ÖKC TSM Merkezi üzerinden GİB BS'ye GMP'lere uygun olarak iletilir.

ÖKC TSM Merkezleri Yeni Nesil ÖKC ilklendirilmesiyle birlikte her mesaj için mesaj işlem kontrolleri yapılmalıdır. Mesaj işlem kontrollerinin; mesajların sıralamalarında, formatlarında, geliş kaynaklarında, zamanlarında vb. unsurlarda tutarsızlıkları ve atakları önlemek için yapılması şarttır. Bu tutarsızlıkları ve atakları analiz ederek gerekli düzeltmeleri sağlamak ve problemleri çözmek ÖKC TSM Merkezleri ile birlikte ÖKC üreticilerinin görevidir.

Tutarsızlık ve atak içeren mesajlar ÖKC TSM Merkezleri tarafından geçersiz mesaj kabul edilecek olup bu mesajlar gerekli araştırmaya tabi tutulmadan ve ÖKC Üreticilerince Yeni Nesil ÖKC üzerinde düzeltme işlemleri yapılmadan GİB BS'ye iletilmeyecektir. Bazı finansal kayıp oluşabilecek durumlarda mesajın iletilmesi ve akışın devamı gerekebilir, bu durumlarda kılavuzlarda belirlenen gerekli loglama ve bildirimde bulunma yöntemlerinden biri kullanılarak ilgili taraflar bilgilendirilir. Kritik durumlarda düzeltme yapılarak gönderilmesi gereken mesajlar, durumun olduğu tarihten itibaren en geç Yeni Nesil ÖKC onarım süresi içerisinde düzeltilip GİB BS'ye düzeltilmiş mesaj formatında aktarılacaktır.

ÖKC TSM Merkezleri tarafından yapılan hassas veri kontrolleri ve sürüm, onay, marka, fiş numarası, Yeni Nesil ÖKC numarası, işlem tarihi ve saati vb. mesaj (ÖKC TSM Merkezleri tarafından görülebilen) kontrolleri sırasında karşılaşılan tüm tutarsızlıklar ve GİB uyarı mekanizmaları çerçevesinde GİB BS'ye bildirilmek zorundadır.

Yeni Nesil ÖKC'ler GMP dokümanlarına uygun olarak, sadece ÖKC TSM Merkezlerine bağlı olarak çalışmak ve ÖKC TSM Merkezleri üzerinden GİB BS ve Üye İşyeri Anlaşması Yapan Kuruluşlar ile haberleşmek zorundadırlar.

14. Risk Yönetimi Esasları

- ÖKC TSM Merkezi bilgi teknolojilerindeki riskler kurumdaki tüm risklerin bir parçası olarak belirlenmeli, ölçülmeli ve yönetmelidir. Risk yönetim çerçevesi, BT genel risk seviyelerini, risk oluştuğunda karşılama stratejilerini belirlemelidir. Bu amaçla bir Risk Komitesi oluşturulmuş olmalıdır.

- Mevcut yapının hedefleri üzerinde herhangi bir potansiyel etkinin oluřturacađı beklenmedik durumlar önceden tespit edilmeye çalıřılmalıdır. Artakalan riskleri kabul edilebilir bir seviyeye ulařtırmak için risk karřılama stratejileri uygulanmalıdır. Risk analizi sonrası riskler tanımlanmalı, sınıflandırılmalı ve derecelendirilmelidir. Tanımlama, sınıflandırma ve derecelendirme sonrasında sonuç raporlanmalıdır. Tanımlanan riskler önceliklendirilmeli ve uygun risk karřılama stratejisi belirlenmelidir.

- Önemli deđiřikliklerden önce risk analizi yapılmalı ve analizlere iliřkin yazılı politikalar belirlenmelidir. Yapılan deđiřiklik sonrası durum raporlanmalıdır.

- Risk analizi belirlenmesi, analiz edilmesi ve izlenebilmesi için risk yönetim politikaları belirlenmeli ve politikaların destekleneceđi dokümanlar oluřturulmalıdır. Riskleri yönetebilmek için önceliklerin ve risklerin neler olduđunun bilinmesi gerekmektedir. Bu sebeple, önem dereceleri ve riskler gerçekteřtiđinde oluřan etkiler göz önüne alınarak, kabul edilebilir risk toleransı ve bu duruma uygun kontroller tanımlanmalıdır. Rollerin ve sorumlulukların tanımlanması ve rehberlik ve talimatların sađlanması için politika, prosedür, kılavuzlar ve standartlar geliřtirilmelidir ve yılda en az bir kez bunları kontrol ederek güncellemelidir. ÖKC TSM Merkezi kendi iř süreçlerini oluřturan teknik raporu ÖKC TSM Merkezi Onay bařvuru sırasında teslim etmelidir.

- Eriřim, kimlik dođrulama, yetkilendirme kontrolü belli aralıklarla kontrol edilmeli ve tekrarlanmalıdır. Sistemlere eriřimler kayıt altında tutulmalı ve farklı bir ortamda saklanmalıdır.

15. Deđiřiklik Yönetimi

- ÖKC TSM Merkezi, bünyesindeki bilgi sistemleri üzerinde gerçekteřtirilen ve Yeni Nesil ÖKC Mesajlarını yöneten donanım ve yazılımlara iliřkin her türlü bakım, yama ve deđiřikliđin uygun bir řekilde planlanmasını, yetkilendirilmesini, test edilmesini, gerçekteřtirilmesini, belgelendirilmesini ve sonrasında denetlenebilirliđini sađlayacak yazılı ve etkin bir deđiřiklik yönetimi süreci iřletmelidir.

- ÖKC TSM Merkezi, Yeni Nesil ÖKC mesajını yöneten yazılımlar için, yazılım geliřtirilen ortamların ve geliřtirilen yazılımların canlı ortama aktarılmadan önce test edildiđi

ortamların canlı ortamlardan ayrılmasını ve bu ortamların herhangi birinde deęişiklik yapma yetkisine sahip personelin dięerlerinde deęişiklik yapma yetkisinin bulunmamasını saęlar, test ve geliştirme ortamlarında kullanılan verilerin canlı ortam verileri ile eşleřtirilemez nitelikte olmasını temin eder.

- ÖKC TSM Merkezi, Yeni Nesil ÖKC Mesajını yöneten sistemlere ilişkin deęişikliklerde etki analizi yapılmasını, deęişiklięin yetkili kiři veya kiřilerce onaylanmasını ve deęişiklięi geri çekme prosedürünün oluřturulmasını saęlar.

16. Denetim İzlerinin Oluřturulması

- ÖKC TSM Merkezleri, GİB ÖKC Mesajlarının yönetildięi sistemlere ve yazılımlara gerçekteřtirilen mantıksal veya fiziksel erişimlere, iřlem altyapısını kullanan yetkisiz erişim teřebbüslerine ilişkin etkin bir denetim izi mekanizması tesis eder.

Denetim izi, kullanıcılara sorumluluk atayan, yeterli detay içeren ve řüpheli bir olayı izleme imkânı sunan nitelikte tutulur.

- Denetim izleri asgari olarak ařaęıdaki bilgileri içeriř:
 - İřlemi gerçekteřtiren uygulama ve/veya iřlemi gerçekteřtiren ve varsa onaylayan kiřiler,
 - İřlemin açıklaması,
 - Yapılan iřlemin zaman bilgisi,
 - İřlemin olumlu veya olumsuz sonucu,
 - Etkilenen veri ve sistemlerin bilgisi.

- Yeni Nesil ÖKC'lere ÖKC Denetim izi oluřturulmadan bir yazılım veya parametre yükleme emri oluřturulamaz. Bu emrin oluřturulması için emrin sisteme kaydedildięi ilk andan itibaren tüm ařamaların iz kaydı oluřturulur ve saklanır.

- Söz konusu emrin bir dıř sistem tarafından alındıęı durumda, bu emrin hangi dıř sistem tarafından ne zaman ve ne řekilde alındıęı sorgulanabilmeli ve görüñtölenebilmelidir.

- ÖKC TSM Merkezinde bulunan sistemlere erişimlerin, denetim izlerinin prosedürlerde belirtilen sistemler için, prosedürlerde belirtildięi řekilde tutulduęu ve düzenli

olarak gözden geçirme ve izlemeye tabi tutulduğu incelenmelidir. Denetim izi olarak hangi parametrelerin (örneğin başarılı ya da başarısız giriş denemeleri, bilgi sistemleri üzerinde yapılan faaliyetler, vb.) tutulacağının belirlendiği kontrol edilmelidir.

- ÖKC TSM Merkezi bünyesinde, kullanıcıların bilgi kaynaklarına erişimleri ile ilgili denetim izlerinin tutulmasına dair bir politika ya da prosedürün olması gerekmektedir.

- Yeni Nesil ÖKC sisteminin altyapısına ait sistem/güvenlik izleme araçlarının kullanıldığı ve bu araçlar tarafından üretilen kayıtların tutulduğu ve takip edildiği gözlemlenmelidir.

- Yedeklemelere ilişkin denetim izleri yedekleme periyodlarına uygun bir aralıkta (log) tutulmalı ve bu logların geçerliliği kontrol edilmelidir.

- ÖKC TSM Merkezinde bulunan sistemler üzerinde, sistem ve kullanıcı işlemlerinin denetim izlerinin (log) ne şekilde ve nasıl saklandığı öğrenilmeli ve ilgili personel tarafından düzenli olarak gözden geçirildiğine ilişkin kanıtlar temin edilerek incelenmelidir.

- Denetim izleri asgari 5 yıl süreyle denetime hazır bulundurulacak şekilde ÖKC ÖKC TSM Merkezleritarafından saklanır.

- Denetim izlerinin bütünlüğünün sağlanması ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli teknikler kullanılır.

- Denetim izlerinin güvenli ortamlarda saklanması gerekmektedir.

- ÖKC üreticisi, denetim izlerinin düzenli olarak gözden geçirilmesine, değerlendirilmesine ve raporlanmasına ilişkin iç süreçlerini oluşturur.

- Denetim izi oluştururken GİB hassas ÖKC Verilerinin ve Ödeme Sistemi hassas verilerinden herhangi birinin tamamının (örneğin kart numarasının tamamının yazılmaması gibi) kullanılmaması esastır.

17. Anahtar Yönetim Süreçleri ve Hassas Veri Güvenliği

- Yeni Nesil ÖKC ile ÖKC TSM Merkezi arasındaki tüm mesajlar ilgili teknik kılavuzlara uygun GMP dokümanlarında belirtildiği şekilde şifrelenmelidir.

- Yeni Nesil ÖKC ile ÖKC TSM Merkezi arasındaki tüm anahtar yönetim mesajlarında kimlik doğrulama, veri bütünlüğünü sağlama, gizlilik ve mahremiyeti temin etme ve inkâr edememe şartlarını sağlama amaçlarıyla kullanılabilen, literatürde kabul görmüş ve güvenilirliğini yitirmemiş güçlü bir algoritma kullanılmalıdır.

- Tüm kriptolojik anahtarlar güvenliği uluslararası standartlarca belirlenmiş şifreleme donanımlarında veya bu anahtarları saklayabilecek şifreleyebilme seviyesine sahip olduğu bilinen algoritma ve anahtarların kullanımı ile güvenli saklama ortamlarında korunmalıdır. Söz konusu anahtar şifreleme anahtarları muhakkak güvenliği uluslararası standartlarca belirlenmiş şifreleme donanımlarında saklanmalıdır.

18. Yazılım Güvenliği ve Sorumluluğu

- ÖKC TSM Merkezinde çalışan yazılımların güvenliğinden TSM Merkezi, ÖKC Üreticisine karşı sorumludur.

- Yazılım geliştirme esnasında tüm geliştirme süreçlerinin ve tarihçesinin gözlemlenebildiği ve tüm geliştirici adımlarının takip edilebildiği denetlenebilir kaynak kod kontrol / sürüm yönetim sistemleri kullanılmalıdır.

- Geliştirilmiş olan yazılımın tüm tarihçesi ve hangi geliştirmenin kim tarafından hangi sürüm için yapılmış olduğu bu sistemler tarafından izlenebilir olmalıdır.

- Cihazlar üzerinde yüklenecek olan tüm uygulamaların kaynağının doğrulanması sağlanmalıdır. Sadece kaynağı doğrulanmış ve güvenilir kaynaklardan gelen uygulamalar yüklenmelidir.

- ÖKC TSM Merkezleri aracılığıyla cihazlara yüklenecek yazılımlara ilişkin sürüm, tarih ve açıklama bilgilerinin TSM Merkezine bildirilmesi ve ÖKC TSM Merkezleri tarafından kontrol edilerek kaydedilmesi gerekir.

19. ÖKC TSM Merkezi İş Sürekliliği Yönetimi

- ÖKC TSM Merkezi İş Süreklilik ve Acil Durum Prosedürlerini hazırlamış ve işletiyor olmalıdır.
- ÖKC TSM Merkezi, iş sürekliliği standartlarına uygun olacak şekilde Bilgi Sistemleri servislerinin, aylık %99,75 kullanılabilirlik ile hizmet sunmasını temin edecek sistem mimarisini tasarlamış ve işletiyor olmalıdır.
- Kullanılan uygulamalar birbirlerini yedekleyecek şekilde kurulmuş sunucular üzerinde yedekli olarak barındırılmalı ve yayınlanmalıdır.
- Yılda 4 defa tüm sistemlere ait iş sürekliliği iç testleri gerçekleştirilerek kayıt altına alınmalıdır. Testlerden ortaya çıkan tüm sonuçlar risk yönetimi prosedürlerine ya da iş sürekliliği eğitimlerine dahil edilmelidir.
- ÖKC TSM Merkezi, iş sürekliliği planlamasına yönelik olarak iş etki analizi yapmalı ve kurtarma stratejilerini belirlemelidir. Bu kapsamda, iç ve dış bağımlılıklar belirlenmeli ve meydana gelebilecek bir kesinti durumunda gereken faaliyet düzeyini ortaya koymak üzere operasyonlar önem düzeyi açısından sınıflandırılmalıdır. Farklı kesinti senaryolarının faaliyetler üzerinde yaratabileceği muhtemel riskler ve bunların potansiyel etkileri ÖKC TSM Merkezi tarafından değerlendirilmelidir.
- İş Sürekliliği Dokümanı ile belirlenmiş süreçlerle sürekliliği etkileyebilecek durumlar oluşmadan, sırasında ve sonrasında kullanılacak yöntemler belirlenmeli ve dokümante edilmelidir.
- Süreç kapsamında sistemlerin performans takibi ve uyarı mekanizmaları için bir alt sistem ya da uygulama kullanılmalıdır. Bu ürün ile sunucular, işletim sistemleri, işletim sistemi servisleri, veri hatları, network aktif cihazları vb. sistem bileşenleri, her cihaza özel parametreler ve eşik değerleri ile 7x24 esasına göre işletim ekipleri tarafından izlenmelidir. Aynı zamanda bu uygulama, sistem bileşenlerinin belirlenmiş herhangi bir eşik değerinin aşılması

durumunda sisteme tanımlanmış personele uyarı mesajlarını SMS ve/veya e-mail yolu ile göndererek gerektiğinde yine önceden belirlenmiş otomatik prosedürler ile müdahale edilmelidir.

- İletişim kanalları ve veri hatları yedekli olarak çalışmalı ve sonlandırılmalıdır.
- ÖKC TSM Merkezi felaket durumunda sistemin çalışırılığını sağlayabilmek için aşağıdaki şartları sağlayan bir İkincil Merkez oluşturmalıdır;
 - İkincil Merkez, ÖKC TSM Merkezi'nden coğrafi olarak aynı riskleri taşımayan en az 300 km uzaklıkta bir lokasyonda kurulmalıdır.
 - İkincil Merkezde tüm elektrik ve soğutma sistemleri yedekli olarak bulunmalı, ayrıca yangın, su baskını, sel vb. doğal afetlerden de korunma sağlanmalıdır.
 - İkincil Merkezde kurulan altyapı ÖKC TSM Merkezi'ne gelen işlem kapasitesini karşılayacak seviyede olmalıdır.
 - İkincil Merkez felaket durumunda en geç 60 dakika içinde, en fazla 30 dakikalık veri kaybı ile ayağa kaldırılabilmelidir.
 - Birincil Merkezin olağanüstü bir durum nedeniyle hizmet veremez duruma gelmesi halinde İkincil Merkeze geçilmesine yönelik acil durum planı yapılmalı, 6 aylık periyodlar ile kontrol edilmeli ve gerektiğinde güncellenmelidir. İkincil sistemin çalışırılığı yıllık olarak test edilmeli ve yıllık testler raporlanmalıdır.
 - Acil Durum Planı hazırlanırken;
 - Kimin, nereye, nasıl müdahale edeceğini belirleyen prosedürler ve süreçler tanımlanmalıdır. Bu prosedür ve süreçler sistemi izleyen işletim personelinin elektronik ve basılı ortamda kolayca ulaşabileceği şekilde bulundurulmalıdır.

▪ Beklenmedik olay meydana geldiğinde “ilk tespit, tespitin sorumlusuna atanması, kesin tespit, çözüm önerisi ve çözüm aksiyonunun alınması” yetkileri belirlenmiş ve dokümante edilmiş personellere atanmalı ve aksiyonlar takip edilerek raporlanmalıdır.

• ÖKC TSM Merkezi Sistem Odası asgari olarak aşağıdaki kriterlerde Uptime Institue Tier 2 standartlarında belirtilen kriterlere uyumlu olacaktır.

- Yedekli Klima – İklimlendirme
- Yedekli Kesintisiz Güç Kaynağı (2 UPS)
- Sistem Odası Yedekli Jeneratör
- Yükseltilmiş Döşeme
- Sistem Operasyon Vardiya Düzeni
- Otomatik Yangın Söndürme Sistemi
- Sistem Odası Erişim Kontrolü
- Sistem Odası CCTV

• ÖKC TSM Merkezi tarafından plansız kesintiler Olay İnceleme Raporu ile belgelendirilmiş olmalıdır.

• ÖKC TSM Merkezi, ÖKC TSM Merkezi Bilgi Sistemleri servislerinin, aylık %99,75 kullanılabilirlik ile hizmet sunmasını temin edecek şekilde, mimari tasarımın ve testlerin yapıldığına dair güvence sunar. Kesinti süreleri yıllık plansız toplam 18 saati ve planlı bir defada 1,5 saati aşmayacak şekilde yılda 4 defadan (toplam 6 saatten) fazla olamaz. Planlı kesintilerin ÖKC TSM Merkezinden hizmet almakta olan Üye İşyeri Anlaşması Yapan Kuruluşlara en az 5 gün önceden gerekçeleri ile birlikte bildirilmesi zorunlu olup planlı kesintilerin günün yoğun olmayan saatlerinde gerçekleştirilmesi gerekmektedir. ÖKC TSM Merkezi aylık olarak

kullanılabilirlik raporunu hazırlayacak ve GİB'e ve ÖKC TSM Merkezi hizmeti almakta olan Üye İşyeri Anlaşması Yapan Kuruluşlara sunacaktır. Bu rapor aylık olarak denetimlerde sunulmak üzere hazır bulundurulur. Kullanılabilirlik raporlarının incelenmesinde ve ÖKC TSM Merkezleri'nin kullanılabilirlik aylık oranının hesaplanmasında GİB BS kaynaklı ve ÖKC TSM Merkezi harici kaynaklardan gelen problemler tespit edilmiş olmalı ve ÖKC TSM Merkezleri'nin kullanılabilirlik değerlerine (oranlarına) negatif etki ettirilmemelidir.

20. Dış Hizmet Alımı

ÖKC Üreticisi TSM Merkezi hizmetini tamamen kendisi sağlayabileceği gibi, bu hizmetlere ilişkin dış hizmet sağlayıcıdan da hizmet alabilir. ÖKC üreticileri, DHS'lerin bu dokümanda belirlenen temel koşullar ile uyumlu olduğuna ve sistem altyapısının güvenlik seviyesini düşürmediğine ilişkin, Dış Hizmet Sağlayıcısı nezdinde gerçekleştirdiği denetimlerle veya başka taraflarca gerçekleştirilen yerinde denetimler sonucunda oluşturulan onay belgelerinden faydalanarak emin olur. Ayrıca buna ilişkin belgelendirme dokümanlarını kendisinde muhafaza eder ve talep edilmesi halinde GİB'e sunar. ÖKC üreticisi, TSM Merkezi'ne ilişkin DHS'den temin ettiği hizmetler için de asıl sorumlu olup, DHS'den temin edilen hizmetler de, hizmetin niteliğine bağlı olarak bu Kılavuzda belirlenen güvenlik ve sistem gereksinimlerine haiz olmalıdır.

TSM Merkezi'ne ilişkin Dış Hizmet Sağlayıcıdan temin edilen TSM hizmetlerinin, bu Kılavuz Bölüm 9'da Sistemlerin Münhasırlığı ilkesine uygun olarak verildiğinden emin olunmalıdır. ÖKC Üreticisi; TSM hizmetini sunduğu sistemiyöneten ve 7/24 takip eden bir ekibi kendi sorumluluğu altında görevlendirilmesini sağlamalıdır.

TSM Merkezlerinin birincil ve ikincil sistemleri (Dış Hizmet Sağlayıcıdan temin edilenler dahil) yurtiçinde olmak zorundadır. TSM Merkezlerine ilişkin ikincil sistemler; birincil sistemden farklı bir il sınırları içinde ve aralarında en az 300 km mesafe bulunacak şekilde kurulmuş olması zorunludur.

ÖKC üreticileri, kendi kuracakları ÖKC TSM Merkezlerine ait birincil merkezinin donanım alt yapısı ile tüm işletim ve operasyon süreçlerini dış kaynak kullanımı veya barındırma hizmeti şeklinde başka bir alt yükleniciden/taşerondan sağlayamaz. Birincil merkezin tüm işletim ve operasyon süreçlerini ÖKC üreticisi 7/24 kendi personeli ile yürütmek zorundadır. İstihdam edilecek personel nitelik ve niceliği ile ilgili "ÖKC TSM Merkezi Personel

Gereksinimleri” başlığında detaylı bilgi verilmektedir. Söz konusu donanım, tüm işletim ve operasyon süreçlerinin herhangi bir kısmının ÖKC üreticisi dışında bir dış kaynaktan temin edilmesi halinde söz konusu ÖKC TSM Merkezi Dış Hizmet Sağlayıcısının verdiği bu hizmetler bakımından da test, değerlendirme, denetim ve onay süreçlerine tabi tutulacaktır.

ÖKC üreticileri kendi kuracakları ÖKC TSM Merkezlerine ait ikincil merkezinin; sadece donanım alt yapısının barındırılması hizmetini taşıron ya da alt yükleniciden temin edebilir. Ancak, ikincil merkeze ait donanım alt yapısının yönetimi ile tüm işletim ve operasyon süreçlerinin ÖKC üreticisine ait kendi personeli ile yürütmek zorundadır.

Dış Hizmet Sağlayıcı, ÖKC TSM Merkezlerine ait ikincil merkezinin; sadece donanım alt yapısının barındırılması hizmetini taşıron ya da alt yükleniciden temin edebilir. Ancak, ikincil merkeze ait donanım alt yapısının yönetimi ile tüm işletim ve operasyon süreçlerinin yönetiminin ilgili DHS/ ÖKC üreticisine ait personel tarafından yürütülmesi zorunludur.

21. ÖKC TSM Merkezi Personel Gereksinimleri

TSM Merkezleri’nde, ÖKC TSM Merkezi Teknik Kılavuzu’nun Madde 4/j ve Madde 6/8 bendinde belirtilen sistemlerin münhasırlığı prensibine göre TSM Merkezi’nin yönetim ve sürekliliği için ÖKC üreticisine veya ÖKC üreticisinin sorumluluğu altında dış hizmet sağlayıcıya ait yeterli düzeyde personel istihdam edilmelidir. İstihdam edilmesi tavsiye edilen personelin görevleri ve nitelikleri aşağıda belirtilmiştir.

Aşağıdaki rollerin her birini yapabilecek en az bir kişi görevlendirilmelidir. Aynı kişi birden fazla konuda görevlendirilebilir.

21.1. Network & Network Güvenlik Grubu:

(Grupta en az 3 kişi olmalıdır.)

- Network Uzmanı (Admin) & Mühendisi
- Network Güvenlik Mühendisi
- Bilgi Güvenliği Uzmanı

21.2. Sistem ve Database Grubu:

(Grupta en az 3 kişi olmalıdır.)

Sistem, Veritabanı ve Sistem Operasyon birimlerinin prosedürlere uygun bir şekilde yönetimini sağlamaktadır.

- **Sistem Yöneticisi:** TSM Merkezi'nde bulunan ve sistemlerin/donanımların bakımı, işletilmesini sağlayan birimlerden sorumludur.

- **Sistem ve Sanallaştırma Mühendisi:** İşletim sistemleri, IIS, Exchange vb. Microsoft sistemlerinin kurulması, yönetilmesi ve sürekliliğinin sağlanması, Vmware, Hyper-V vb. sanallaştırma sistemlerinin kurulması, yönetilmesi ve sürekliliğinin sağlanmasından sorumlu olup bu sistemlere bağlı Storage ve donanım altyapılarına da bakmakla, işletmekle sorumludur.

- **Veri Tabanı Uzmanı:** MS SQL, Oracle, MySQL vb. veri tabanlarının kurulması, yönetilmesi, sürekliliğinin sağlanmasından sorumludur.

21.3. Sistem ve Terminal Operasyon Grubu:

(Grupta en az 10 kişi olmalıdır.)

Sistem Operasyon Yöneticisi: Sistem operatörlerinden sorumlu olup, TSM Merkezi'nde yürütülen günlük operasyonel işlerin sürdürülmesinden ve takip edilmesinden sorumludur.

- *Sistem Operatörleri (Vardiyalı) :* TSM Merkezi'nde de kurulmuş olan tüm sistemlerin izlenmesi, operasyonel işlerin yürütülmesi ve ÖKC TSM Merkezi operasyonlarının sürekliliğinin sağlanmasından sorumludur.

Terminal Operasyonu

- Yönetici
- Terminal Operasyon Elemanları

21.4. Uygulama Geliştirme Grubu:

(Grupta en az 5 kişi olmalıdır.)

Uygulama geliştirme ve destek için dışarıdan hizmet alımı yöntemi benimsenmeli ya da biri teknik yönetici olmak üzere en az 5 kişilik yazılım geliştirme ekibi görevlendirilmelidir.

22. ÖKC TSM Merkezlerinin Denetimi

ÖKC TSM Merkezlerinin, bilgi sistemlerinin ve bu Kılavuzun gereksinimleri (bu Kılavuzun güvenlik ve sistem gereksinimleri bölümleri) bölümlerinde belirtilen hükümlere uyum

durumunun devamının tespit edilmesi amacıyla, düzenli olarak (yılda en az 1 defa) ya da GİB talebiyle istendiği zaman denetim yapılır.

GİB, TSM Merkezleri'nin onay almadan önce de bilgi sistemleri yönünden denetimden geçmesini beklemektedir.

ÖKC TSM Merkezlerinin bilgi sistemleri denetimi ve denetim sonuçlarının GİB'e raporlanması birinci fıkradaki tanımla sınırlı olmak üzere BSDHY ile belirlenen usul ve esaslar çerçevesinde, BSDHY kapsamında yetkilendirilmiş veya izin verilmiş bağımsız denetim kuruluşlarınca gerçekleştirilir.

BSDHY ile belirlenen usul ve esaslar bu Kılavuz çerçevesinde uygulanırken BSDHY'de geçen “banka” ve “denetlenen” ifadeleri ÖKC TSM Merkezleri'ni, “Bilgi Sistemleri Denetimi” ifadesi de ÖKC TSM Merkezleri üzerinde birinci fıkrada tanımlanan denetimi ifade eder.

ÖKC TSM Merkezleri'nde gerçekleştirilecek denetim faaliyetlerine ilişkin detaylar bu kılavuzun IV üncü bölümünde açıklanmıştır.

23. GİB Uyarı Mekanizmaları

ÖKC TSM Merkezleri'nden bazı durumlarda GİB BS'ye ulaşmak gerekebilir. Bu konuda aciliyet durumlarına göre yazılı, e-mail, telefon, faks veya SMS yoluyla iletişim kurmak mümkün olabildiği gibi otomatik işleyen bazı alt yapılar da mümkün olacaktır. Üretilen Yeni Nesil ÖKC'lerin kaydedilmesi, statülerinin (kullanıma hazır, aktif, kapalı, devir, hurdaya ayrılma vb) güncellenmesi, GİB tarafından yayımlanan Yeni Nesil ÖKC'lere Ait “Elektronik Kayıt, Aktivasyon Ve Yetkili Servis Listeleri Teknik Kılavuzu”na uygun olarak gerçekleştirilecektir. ÖKC TSM Merkezleri tarafından tespit edilen bir atak ya da önemli bir durumun GİB BS'ye bildirilmesi için erişim bilgileri GİB tarafından ayrıca duyurulacak olan İstihbarat Web Servisi kullanılacaktır. Aynı zamanda; GİB BS'den TSM Merkezleri'ne, cihazlar ve ÖKC TSM Merkezleri hakkında bilgilendirmeler de, Yeni Nesil ÖKC'lere Ait “Elektronik Kayıt, Aktivasyon Ve Yetkili Servis Listeleri Teknik Kılavuzu”na uygun olarak sağlanabileceği gibi GİB tarafından ilan edilecek farklı mekanizmalar da kullanılabilecektir.

Bu mekanizmalar online veya batch entegrasyon yöntemlerinden biri ile olabilecektir. Online ya da batch entegrasyon formatı ve kuralları daha sonra detaylı olarak iletilecektir.

24. ÖKC TSM Merkezlerinin Harici Donanım ve Yazılım Bilgisi Tutma ve Bildirim Yükümlülüğü

ÖKC TSM Merkezleri; ÖKC ile birlikte çalıştırılan harici EFT-POS cihazları, GMP3 dokümanı çerçevesinde eşleştirilecek harici donanım ve yazılımlara ilişkin olarak, üretici firma yazılım ve donanım sürümlerinin bilgilerini bünyelerinde geçmiş sürüm bilgileriyle birlikte güncel olarak tutar ve gerekli kontrolleri yaparlar. TSM Merkezleri'nden geçen mesajlarda TSM Merkezi'nde bilgisi bulunmayan üretici donanım, yazılımı veya yazılım sürümünü tespit edilirse TSM Merkezi'nin gerekli denetim ve müdahale aksiyonunu alması gerekmektedir. Yapılan kontrollerde bilgi verilmeyen bir durum tespit edilirse, ödemesi gerçekleşmiş işlemlerin GİB BS'ye iletilmesine engel olunmamalıdır. Ancak, tespit edilen durumun GİB BS'ye bildirilmesi için 23 numaralı başlıkta anlatılan GİB uyarı mekanizmaları kullanılmalıdır.

ÖKC TSM Merkezleri GİB tarafından talep edildiği takdirde, talep edilen yönetime uygun olarak harici donanımlara ait yazılım bilgilerini GİB'e bildirmekle yükümlüdür.

BÖLÜM III

YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARA AİT ÖKC TSM MERKEZLERİ ONAY VE TEST BAŞVURU AKIŞLARI

25. Onay ve Test Başvuru Yönetimi

Bu bölümde ÖKC TSM Merkezi başvurularına ilişkin olarak GİB’e yapılan başvuruların iş akışları anlatılacaktır.

Açıklanan iş akışları, EK-5 “ÖKC TSM Merkezleri Başvuru, Test, Denetim ve Onay İş Akışı” diyagramında da bütün olarak belirtilmiştir.

25.1. *ÖKC TSM Merkezi Başvurusunda Sağlanacak Belgeler*

ÖKC TSM Merkezi başvurularında aşağıdaki belgelerin teslim edilmesi zorunludur.

- a. ÖKC TSM Merkezi Başvuru Formu (EK-2)
- b. PCI-DSS Payment Card Industry Data Security Standard Onay Belgesi
AOC (Attestation of Compliance for Onsite Assessments).
- c. ISO/IEC 20000 Bilgi Teknolojileri Hizmet Yönetim Sistemi Belgesi
- ç. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi
- d. ISO 22301 İş Sürekliliği Yönetim Sistemi Belgesi
- e. Teknik Rapor Dokümanı (ÖKC TSM Merkezi Teknik Kılavuzu, madde 6/2)
- f. Güvence ve Denetim Rapor Dokümanı (ÖKC TSM Merkezi Teknik Kılavuzu, madde 10/8)

Daha önceden ÖKC TSM Merkezi hizmeti vermeye başlamış ve bankalara bütünleşik cihazlarından (EFT POS) mesaj göndermeye başlamış ÖKC TSM Merkezleri için geçmişe ait son 6 aya ait aylık bazda kullanılabilirlik oranı raporu. Tek bir banka için verilmesi yeterlidir.

- g. İş Sürekliliği Planı Dokümanı (ÖKC TSM Merkezi Teknik Kılavuzu, madde 10/1)
- ğ. **ÖKC Üreticisi – ÖKC TSM Merkezi Yetki Sorumluluk Anlaşma ve Dokümanları:** ÖKC üreticisi ile ÖKC TSM Merkezi arasındaki ilişkilerin yetki ve sorumlulukları anlaşması ve ekleri.
- h. **İç Kontrol ve İç Denetim Dokümanları:** Verileri yöneten yazılım, donanım ve kişiler (veya roller) arası iletişim ve süreçlerin uygunluğunun temini için yazılmış iç kontrol ve iç denetim prensipleri dokümanı.
1. **Güniçi ve Günsonu Süreçleri Dokümanları:** ÖKC Üreticisi için günüçinde ve günsonunda yapılan bütün işlerin (uygulamalar, dosya alışverişleri, entegrasyonlar vb) adım adım özetinin anlatıldığı tarif dokümanı.
- i. **İkincil Merkez Anlaşması:** ÖKC TSM Merkezi ikincil merkezi barındırma hizmeti olarak başka bir firmadan alıyorsa, alındığını gösteren kapsam, sözleşme tarihini, sözleşme başlama – bitiş tarihlerini ve süresini gösteren belgeler / sözleşme ön yüzü.
- j. **Diğer Anlaşmalar ve Dokümanlar:** ÖKC TSM Merkezi hizmeti faaliyetlerine ilişkin harici kurumlarla yapılan diğer mevcuttaki anlaşmalar veya sözleşmeleri tarif eden doküman. (Örneğin: VAS sözleşmesi vb.)

25.2. ÖKC TSM Merkezi Denetim ve Onay Süreçleri

ÖKC üreticileri cihazları için cihaz onayını aldıktan sonra cihazlarının yönetiminden sorumlu olacak ÖKC TSM Merkezi başvurusu için EK-2’de yer alan (**ÖKC ÜRETİCİ TSM MERKEZİ BAŞVURU FORMU**) ve 25.1 başlığında yer alan belgeleri tamamlayarak GİB’e yazılı olarak başvurur. GİB tarafından ön kontrolleri yapılan başvuru formu ve ekleri uygun görüldüğü takdirde, Onay Denetimi sürecinin başlatılabileceğine ilişkin ÖKC TSM Merkezi başvuru sahibine yazılı olarak bildirim sağlanır.

ÖKC TSM Merkezinin gerekli şartları haiz olup olmadığının tespiti için Onay Denetimi, BSDHY kapsamında yetkilendirilmiş veya izin verilmiş bağımsız denetim kuruluşlarınca veya TÜBİTAK tarafından gerçekleştirilir.

ÖKC üreticileri TSM Merkezleri'nin bu Kılavuza göre yapılacak test, denetim ve değerlendirme faaliyetlerini TÜBİTAK ya da GİB tarafından belirlenen Bağımsız Denetim Kuruluşlarından birine yaptırılmasını başvuru sırasında belirterek tercih edebilirler. GİB tarafından yetkilendirilen Bağımsız Denetim Kuruluşlarının listesi GİB'in resmi internet sitesinde yayınlanır.

TÜBİTAK Onay Denetimi'nin bir veya daha fazla bölümünü harici firmalara (Başkanlıkça TSM Merkezleri'nin denetimi hususunda yetkilendirilen Bağımsız Denetim Kuruluşları dahil) yaptırabilir.

Onay Denetiminin kapsamı bu Kılavuzun 4.Bölüm 26.Başlığında detaylı açıklanmaktadır. Onay Denetiminde gerçekleştirilecek test, değerlendirme ve denetim faaliyetlerine ilişkin tanzim edilecek raporun formatı EK-3'de yer almaktadır. Onay Denetimi raporu TÜBİTAK tarafından bu kılavuza uygunluk yönünden kontrol edilecek ve TÜBİTAK tarafından kontrolü sağlanmış şekilde GİB ile paylaşılacaktır.

TÜBİTAK, söz konusu Onay Denetim raporunun, bu Kılavuza uygun olarak hazırlandığını belirten dokümanla (yazı veya bir rapor şeklinde) birlikte GİB'e gönderir. Onay Raporu olumlu olarak kabul edilen başvurularda GİB olumlu değerlendirme yazısını firmaya bildirir. Onay Denetimi başarılı sonuçlanan firmalar ÖKC TSM Merkezi uçtan uca test işlemlerine başlayabilmek için GİB'e başvurur ve süreç 25.4 başlığında belirtilen şekilde devam eder.

GMP dokümanlarına uygun olarak hazırlanan Uçtan Uca Test Senaryoları GİB tarafından başvuru ön kabulü sonrasında paylaşılır.

GİB tarafından yayınlanan “Yeni Nesil Ödeme Kaydedici Cihazlara ait ÖKC TSM Merkezi Teknik Kılavuzu” nun 15 inci maddesinde belirtilen ve her yıl yapılması gereken Bilgi Sistemleri Denetiminin ilki Onay Denetimi kapsamında sağlanmaktadır.

GİB'e başvuru yapan ancak ön kabul verilmeyen firmalar Onay Denetimi süreçlerine başlayamazlar. Ancak bu durum, her yıl yapılması gereken Bilgi Sistemleri Denetiminin yapılmasına engel teşkil etmez. Bu statüde olan başvurularda; GİB tarafından yayınlanan “Yeni Nesil Ödeme Kaydedici Cihazlara ait ÖKC TSM Merkezi Teknik Kılavuzu” nun 15 inci

maddesine uygun şekilde Bilgi Sistemleri Denetimi temin edilmeli ve ilgili başlıkta belirtilen şekilde raporlama sağlanmalıdır. Başvurusuna ön kabul verilmeyen firmaların Bilgi Sistemleri Denetimi Raporunun da olumsuz olması durumunda GİB firma hakkında idari işlem başlatabilir.

ÖKC TSM Merkezi başvurularının; yetkili ÖKC firması ve ilgili ÖKC firmasına ait gerekli onayları almış bulunan veya onay başvurusu TÜBİTAK nezdinde devam eden Yeni Nesil ÖKC modelleri bazında yapılması gerekmektedir. Bir başvuruda, aynı ÖKC firmasına ait birden fazla Yeni Nesil ÖKC modeline de yer verilmesi mümkündür. ÖKC TSM Merkezi Onay denetiminde, Güvenli Haberleşme Denetim adımları her bir cihaz modeli için dokümanda belirtilen tekrar kurallarına uygun tatbik olunmalıdır.

25.3. Dış Hizmet Sağlayıcı ÖKC TSM Merkezi Denetim ve Onay Süreçleri

ÖKC üreticileri, TSM Merkezi'ne ait sunulması gereken hizmet altyapılarını kısmen veya tamamen bir dış hizmet sağlayıcıdan temin etmesi durumunda; ÖKC üreticisine ve dış hizmet sağlayıcıya ait ÖKC TSM Merkezi sistem unsurlarının niteliğine bağlı olarak bu kılavuzda belirtilen gereksinim unsurlarının (bilgi sistemleri ve güvenli haberleşme gereksinimleri) karşılandığını temin etmelidirler. Söz konusu unsurlara ilişkin sorumluluk müşterek ve müteselsil olup, dış hizmet sağlayıcı ile birlikte ÖKC üreticilerine ait olacaktır.

TSM Merkezi'ne ilişkin hizmetlerin kısmen veya tamamen bir Dış Hizmet Sağlayıcıdan temin edilmesi halinde; ÖKC TSM Merkezi Başvurusunda (Ek-2) Dış Hizmet Sağlayıcıdan temin edilen hizmet unsurları detaylı olarak belirtilmeli ve bu hizmetlerin niteliğine bağlı olarak gerekli ek ve tevsik edici bilgi ve belgeler başvuru formunda sunulmalıdır. TSM Merkezi'ne ilişkin test ve onay süreçlerinde Dış Hizmet Sağlayıcıdan temin edilen bu hizmet unsurları da test, denetim ve değerlendirmeye tabi tutulmalıdır.

Bu aşamadan sonra yapılması gereken iş ve işlemler ile sertifikasyon süreçleri bu Kılavuzun 25.2. bölümünde belirtilen şekilde tamamlanır.

Dış Hizmet Sağlayıcı ÖKC TSM Merkezi başvurularının; ÖKC üretici onayı almış üretici ve ilgili üreticinin gerekli onayları almış bulunan Yeni Nesil ÖKC modelleri (Bir başvuruda birden fazla Yeni Nesil ÖKC modeline yer verilmesi mümkündür.) bazında yapılması gerekmekte olup, ÖKC TSM Merkezi Onay denetiminde, Güvenli Haberleşme Denetim adımları her bir cihaz için dokümanda belirtilen tekrar kurallarına uygun tatbik olunmalıdır.

Dış hizmet sağlayıcılarınca sunulan ÖKC TSM Merkezi hizmet unsurları, sistemlerin münhasırlığı gereği; birlikte çalışacakları her farklı üretici firma için ayrı ayrı test, denetim ve değerlendirme süreçlerine tabi tutulması gerekmektedir.

25.4. Onay Denetimi Sonrasında Test Başvuruları ve Gerçek Ortama Geçiş

Onay Denetimi raporu ve TÜBİTAK format kontrolü sonrasında GİB tarafından olumlu değerlendirilen firmalar için TSM Merkezleri'nin uçtan uca test süreci, firmanın başvurusu akabinde GİB tarafından firmalara bildirilen test takvimine göre yürütülecektir.

Uçtan Uca Test Senaryolarının, firmanın başvurusunda belirtilen her bir Yeni Nesil ÖKC marka modeli için tekrar edilmesi gereklidir.

ÖKC TSM Merkezi uçtan uca test süreçlerini başarıyla tamamlayan firmalar GİB tarafından ÖKC TSM Merkezi olarak onaylanır, ÖKC TSM Merkezi onayı yazılı olarak ÖKC üreticisine bildirilir. GİB BS gerçek (canlı) ortamına bağlantı izni, GİB tarafından yazılı olarak ÖKC üreticisine bildirilir. ÖKC TSM Merkezi, söz konusu GİB yazısında belirtilen tarih itibari ile GİB BS'ye veri gönderme işlemine başlamak zorundadır. GİB, ÖKC üreticilerine ait sadece belli bir Yeni Nesil ÖKC kümesinin gerçek (canlı) ortama bağlanmasını (pilot süreci) tercih edebilir. Bu durumda pilot süreci tamamlandıktan sonra tüm Yeni Nesil ÖKC'ler gerçek ortama bağlanmaya başlayabilir.

BÖLÜM IV

ÖKC TSM MERKEZLERİNDE GERÇEKLEŞTİRİLECEK DENETİM FAALİYETLERİ

26. ÖKC TSM Merkezleri’nde Gerçekleştirilecek Onay Denetiminin Kapsamı

ÖKC TSM Merkezi olmak üzere GİB’e başvuruda bulunan ÖKC üreticilerinin kurmuş oldukları sistemin GİB tarafından talep edilen gerekli şartları haiz olup olmadığının tespiti için gerçekleştirilen denetim sürecidir.

ÖKC TSM Merkezleri’nde gerçekleştirilecek Onay Denetim faaliyetleri esas itibariyle “Bilgi Sistemleri Denetimi” ve “Güvenli Haberleşme Denetimi” olarak isimlendirilen iki kısımdan oluşmaktadır.

26.1. ÖKC TSM Merkezleri Bilgi Sistemleri Denetimi

ÖKC TSM Merkezleri’nde yürütülen işlemlerin; Başkanlıkça yayınlanan/paylaşılan ve TSM Merkezlerini doğrudan veya dolaylı olarak etki eden Teknik Kılavuzlar (TK-1, TK-2, TSM Teknik Kılavuzu, TSM Başvuru, Test, Denetim ve Onay Teknik Kılavuzu) ile 13/01/2010 tarihli ve 27461 sayılı Resmi Gazete’de yayımlanan “Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmeliği” nde belirtilen usul ve esaslar yönünden uygunluğuna yönelik yapılan denetim faaliyetleridir.

“Bilgi Sistemleri Denetimi” kapsamında; ÖKC Durum verisi ve GİB Hassas ÖKC verisini ve kural koyucular tarafından hassas veri olarak kabul edilen verileri yöneten kişiler, süreçler, yazılımlar, donanımlar ile bu kapsamda tesis edilen iş süreçleri ve iç kontrollerin değerlendirilmesinde, Başkanlık tarafından yayınlanan “Yeni Nesil Ödeme Kaydedici Cihazlara Ait ÖKC TSM Merkezi Bilgi Sistemleri Denetimi Adımları Kılavuzu Sürüm 1.0” da yer alan kontrol sınıfları çalıştırılmalıdır.

TSM Merkezi’nin, GİB isterleri olan Teknik Kılavuzlara uygunluk değerlendirmesinde çalıştırılacak kontrol sınıfları aşağıda belirtilmiştir.

1. TSM_SER: Uluslararası Sertifikasyon Raporları ve Denetim Talepleri Değerlendirme Sınıfı

Bu değerlendirme sınıfı, ÖKC TSM Merkezleri'nin sağlaması gereken Uluslararası Standartlara ait sertifikasyon süreçlerinin çıktıları ile ÖKC TSM Merkezleri'nin rutin olarak sağlaması gereken Denetim süreçlerinin varlığının ve uygunluğunun kontrol edilmesini amaçlamaktadır.

2. TSM_SIS : Sistem ve Güvenlik Değerlendirme Sınıfı

Bu değerlendirme sınıfı, ÖKC TSM Merkezleri'nin uyması gereken alt yapı, sistem mimarisi, münhasırlık kuralları ile veri merkezi iş sürekliliğinin temini, gerekli güvenlik ve risk değerlendirme süreçlerinin oluşturulması ve işletilmesi, yazılım değişikliklerinin yönetimi, gerçekleştirilen işlemlerin denetim izlerinin sağlanması, dış hizmet sağlayıcısı ile çalışılması durumunda sağlanması gereken hususi gerekliliklerin kontrol edilmesini amaçlamaktadır.

3. TSM_ILT : Paydaş İletişimi ve İş Kurgusu Değerlendirme Sınıfı

Bu değerlendirme sınıfı, ÖKC TSM Merkezleri'nin Yeni Nesil ÖKC yönetimi çerçevesinde iletişim içerisinde olduğu, ÖKC Üreticisi, Üye İşyeri Anlaşması Yapan Kuruluşlar ve Katma Değerli Hizmet sağlayıcılar ile ilişki yönetiminin gerekliliklere uygunluğunun kontrol edilmesini amaçlamaktadır.

4. TSM_OKC : Güvenli Yazılım Yükleme ve Mesaj Yönetim Değerlendirme Sınıfı

Bu değerlendirme sınıfı, ÖKC TSM Merkezleri'nin Yeni Nesil ÖKC üzerinde çalışan mali uygulama, üye işyerleri anlaşması yapan kuruluşlara ait uygulama veya katma değerli uygulama yazılımlarının ayrıca Yeni Nesil ÖKC parametrelerinin cihaza yüklenmesi ve versiyon takibinin gerekliliklere uygun sağlandığının ve ÖKC mesajlarının istelere uygun yönetildiğinin kontrol edilmesini amaçlamaktadır.

Söz konusu denetim adımları ile ilgili olarak, denetim faaliyetlerini yürütecek bağımsız denetim kuruluşlarının Gelir İdaresi Başkanlığı koordinatörlüğünde sunulan eğitim faaliyetine katılması zorunludur.

Gerçekleştirilen denetim sonucunda BSDHY'nin 5 inci, 7 nci ve 8 inci maddelerinde belirtilen hükümler çerçevesinde, BSDHY'nin 34 üncü maddesinde belirtilen şekilde denetim

mektubu düzenlenir. Denetim mektubu düzenlenirken metinde EK-1’de yer verilen ifade değişiklikleri uygulanır. Denetim mektubu, hazırlanan denetim raporu içerisinde yer alır.

26.2. ÖKC TSM Merkezleri Güvenli Haberleşme Denetimi

Yeni Nesil ÖKC TSM Merkezleri’nde yürütülen işlemlerin; Başkanlıkça yayınlanan/paylaşılan ve ÖKC TSM Merkezlerine doğrudan veya dolaylı olarak etki eden mesajlaşma protokolü dokümanlarının (GMP-1, GMP-2, GMP-3 vb.) isterlerine uygunluğuna yönelik yapılan denetim faaliyetleridir.

GİB isterleri olan mesajlaşma protokolü dokümanlarına uygunluk değerlendirmesinde çalıştırılacak kontrol sınıfları aşağıda belirtilmiştir.

Söz konusu denetim kılavuzunda belirtilen denetim işlem adımları ve detayları ile ilgili olarak, denetim faaliyetlerini yürütecek bağımsız denetim kuruluşlarının GİB tarafından sunulan eğitim faaliyetine katılması zorunludur.

Bu denetim kapsamında sınıflar itibariyle aşağıdaki denetim faaliyetleri yürütülecektir.

1. SSL_CON : ÖKC TSM Merkezi SSL Konfigürasyonu Değerlendirme Sınıfı (Münhasıran GMP TK-1 Dokümanı Kapsamındaki ÖKC TSM Merkezleri İçin)

Bu Değerlendirme sınıfı, Yeni Nesil ÖKC ile ÖKC TSM Merkezi arasındaki veri transferinin güvenliğini sağlamak için kurulan güvenli bağlantının (SSL CA) ÖKC TSM Merkezi yapılandırma özelliklerinin tespit edilmesini ve uygunluğunun kontrol edilmesini amaçlamaktadır.

2. SSL_COM : ÖKC TSM Merkezi - YN ÖKC SSL Haberleşmesi Değerlendirme Sınıfı (Münhasıran GMP TK-1 Dokümanı Kapsamındaki ÖKC TSM Merkezleri İçin)

Bu Değerlendirme sınıfı, Yeni Nesil ÖKC ile ÖKC TSM Merkezi arasında kurulacak güvenli bağlantının (SSL CA) haberleşme güvenliği özelliklerinin GMP TK1 dokümanına uygunluğunun kontrol edilmesini amaçlamaktadır.

3. SSL_CEV : SSL Sertifika Doğrulama Değerlendirme Sınıfı (Münhasıran GMP TK-1 Dokümanı Kapsamındaki ÖKC TSM Merkezleri İçin)

Bu Değerlendirme sınıfı, Yeni Nesil ÖKC ile ÖKC TSM Merkezi arasında kurulacak güvenli bağlantı esnasından kullanılan sertifikaların uygunluğunun kontrol edilmesini amaçlamaktadır.

4. TSM_SCOM : YN ÖKC – ÖKC TSM Merkezi Güvenli Haberleşmesi Değerlendirme Sınıfı (Münhasıran GMP TK-2 Dokümanı Kapsamındaki ÖKC TSM Merkezleri İçin)

Bu değerlendirme sınıfı Yeni Nesil ÖKC ile ÖKC TSM Merkezi arasında kurulacak güvenli bağlantının haberleşme güvenlik özelliklerinin GMP TK-2 dokümanına uygunluğunu amaçlamaktadır.

5. VPN_SCM : ÖKC TSM Merkezi - GİB BS Güvenli Haberleşme Değerlendirme Sınıfı (Tüm ÖKC TSM Merkezi Yapıları İçin)

Bu Değerlendirme sınıfı, ÖKC TSM Merkezi ile GİB BS arasında kurulacak güvenli bağlantının uygunluğunun kontrol edilmesini amaçlamaktadır.

6. PRA_CMS : ÖKC TSM Merkezi - GİB BS Haberleşme Mesajları Değerlendirme Sınıfı (Tüm ÖKC TSM Merkezi Yapıları İçin)

Bu Değerlendirme sınıfı, ÖKC TSM Merkezi ile GİB BS arasındaki haberleşme mesajlarının uygunluğunun kontrol edilip ve ilgili uygun aksiyonların alındığının kontrol edilmesini amaçlamaktadır.

7. FCR_CMS : YN ÖKC - ÖKC TSM Merkezi Haberleşme Mesajları Değerlendirme Sınıfı (Tüm ÖKC TSM Merkezi Yapıları İçin)

Bu Değerlendirme sınıfı, ÖKC TSM Merkezi ile Yeni Nesil ÖKC arasındaki haberleşme mesajlarının uygunluğunun kontrol edilip ve ilgili uygun aksiyonların alındığının kontrol edilmesini amaçlamaktadır.

8. FCR-MCF : GİB BS - YN ÖKC Haberleşme Mesajları Değerlendirme Sınıfı (Tüm ÖKC TSM Merkezi Yapıları İçin)

Bu değerlendirme sınıfı, GİB BS ile Yeni Nesil ÖKC arasındaki haberleşme mesajlarının uygunluğunun ÖKC TSM Merkezi tarafından kontrol edilip ve ilgili uygun aksiyonların alındığının kontrol edilmesini amaçlamaktadır.

ÖKC TSM Merkezlerinde gerçekleştirilecek Güvenli Haberleşme Denetimi adımlarına ilişkin GİB tarafından hazırlanan “Yeni Nesil ÖKC Güvenli Haberleşme Denetimi Adımları Kılavuzu”, gerekli eğitim faaliyetlerine katılmış ve GİB tarafından denetim faaliyetlerini yürütmeye yetkili kılınan Bağımsız Denetim Kuruluşları’na, taahhütname ile paylaşılacaktır.

27. ÖKC TSM Merkezlerinde Gerçekleştirilecek Yıllık Denetiminin Kapsamı

ÖKC TSM Merkezi’nin yıllık denetimi; GİB tarafından verilen ÖKC TSM Merkezi onayını takip eden 1 yılın sonuna kadar gerçekleştirilmesi gereken ve devam eden her yıl 1 yıllık süreçte de yapılması gereken denetim sürecini ifade eder. Yıllık denetimler takvim yılı esasında yapılacak olup, her bir takvim yılına ilişkin yıllık denetim raporları, izleyen takvim yılının 6’ncı ayının sonuna kadar GİB’e raporlanmak zorundadır. ÖKC TSM Merkezleri’nin onay denetimi sürecinde tanzim edilen ve GİB tarafından uygun bulunan raporlar, ilgili takvim yılına ait yıllık denetim raporu yerine geçer.

ÖKC TSM Merkezleri’nde gerçekleştirilecek yıllık denetim faaliyetleri, TSM Merkezi onay denetiminde de yer alan “Bilgi Sistemleri Denetimi” sürecini kapsamaktadır. Bu sürece ilişkin kapsam 26.1 başlığında detaylı olarak açıklanmaktadır. Süreç aynı şekilde işletilir.

Onay denetimi sonrasında, GMP dokümanlarında gerçekleştirilecek düzenlemelere bağlı olarak GİB, bu Kılavuzun 26.2 başlığında detaylı açıklanan “Güvenli Haberleşme Denetimi”nin tekrar edilmesini talep edebilir.

28. ÖKC TSM Merkezi Denetimine İlişkin Düzenlenen Raporların Formatı

ÖKC TSM Merkezleri’nde gerçekleştirilen denetim faaliyetleri sonucunda TÜBİTAK tarafından veya Başkanlıkça yetkilendirilen Bağımsız Denetim Kuruluşları tarafından düzenlenecek “YN ÖKC TSM MERKEZİ ONAY DENETİM RAPORU ” nun asgari formatı Ek-3’de belirtilmiştir. İlgili rapor TÜBİTAK tarafından gerekli format kontrolü yapıldığına ilişkin üst yazı ekinde GİB tarafından kabul edilecektir.

TSM Merkezi’nin GİB tarafından onayını takip eden 1 yılın sonunda ve devam eden her yıl 1 defa olmak kaydı ile gerçekleştirilecek “Bilgi Sistemleri Denetimi” ne ilişkin Başkanlıkça yetkilendirilen Bağımsız Denetim Kuruluşları tarafından düzenlenecek “YN ÖKC TSM

MERKEZİ BİLGİ SİSTEMİ DENETİM RAPORU ”nun asgari formatı EK-4A’da belirtilmiştir. GİB’e başvuru yapan ancak ön kabul verilmeyen firmalar için “Bilgi Sistemleri Denetimi” zorunlu olarak gerçekleştirilmeli ve EK-4A’ya uygun formatta denetim raporu tanzim edilmelidir. İlgili raporlar doğrudan GİB tarafından kabul edilecektir

GİB tarafından mesajlaşma protokollerinde gerçekleştirilecek düzenlemeler dolayısı ile “Güvenli Haberleşme Denetimi”nin tekrar edilmesinin talep edildiği durumda; “Güvenli Haberleşme Denetimi” ne ilişkin TÜBİTAK tarafından veya Başkanlıkça yetkilendirilen Bağımsız Denetim Kuruluşları tarafından düzenlenecek “YN ÖKC TSM MERKEZİ GÜVENLİ HABERLEŞME DENETİM RAPORU ” nun asgari formatı EK-4B’de belirtilmiştir. İlgili rapor TÜBİTAK tarafından gerekli format kontrolü yapıldığına ilişkin üst yazı ekinde GİB tarafından kabul edilecektir.

29. KILAVUZ EKLERİ

EK-1: Denetim Mektubu Oluşturulurken Metinde Değiştirilmesi Gereken Hususlar:

Denetim mektubu düzenlenirken "13.01.2010 tarih 27461 sayılı Resmi Gazete’de yayımlanan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik", "28.06.2012 tarih ve 28337 sayılı Resmi Gazete’de yayımlanan Bankaların İç Sistemleri Hakkında Yönetmelik ile 14.09.2007 tarih ve 26643 sayılı Resmi Gazete’de yayımlanan Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelerle İlişkin Tebliğ", "01.11.2006 tarih ve 26333 sayılı Resmi Gazete’de yayımlanan Bankalarda Bağımsız Denetim Gerçekleştirecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmelik ile 13.01.2010 tarih ve 27461 sayılı Resmi Gazete’de yayımlanan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik", "28.06.2012 tarih ve 28337 sayılı Resmi Gazete’de yayımlanan Bankaların İç Sistemleri Hakkında Yönetmelik’in “İç Kontrol Sistemi” başlıklı İkinci Kısım ile 14.09.2007 tarih ve 26643 sayılı Resmi Gazete’de yayımlanan Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelerle İlişkin Tebliğ" ifadeleri yerine **"Yeni Nesil Ödeme Kaydedici Cihazlara Ait ÖKC TSM Merkezi Teknik Kılavuzu"** ifadesi ve "(bilgi sistemleri ile)* bankacılık süreçleri", " bilgi sistemleri ile bankacılık süreçleri" ifadeleri yerine **"ÖKC TSM Merkezleri Bilgi Sistemleri"** ifadesi kullanılır.

EK-2: ÖKC TSM Merkezi Başvuru Formu

YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLAR TSM MERKEZİ BAŞVURU FORMU	
A. TSM MERKEZİ TÜRÜ	
ÜRETİCİ TSM MERKEZİ (Tüm alt yapı hizmetinin ÖKC üreticisine ait olması hali)	☐
DIŞ HİZMET SAĞLAYICILI TSM MERKEZİ (ÖKC TSM Merkezi alt yapılarına ilişkin kısmen veya tamamen bir dış hizmet sağlayıcıdan yararlanılması hali)	☐
B. ÖKC ÜRETİCİ KURUM BİLGİLERİ	
KURUM ÜNVANI	
İRTİBAT KURULACAK KİŞİ ADI-SOYADI	
BÖLÜM/GÖREV/ÜNVAN	
İrtibat Tel No	
İrtibat GSM No	
e-Mail	
Adresi	
C. DIŞ HİZMET SAĞLAYICISI BİLGİLERİ (Kısmen veya tamamen bir dış hizmet sağlayıcısından yararlanılması halinde)	
KURUM ÜNVANI	
İRTİBAT KURULACAK KİŞİ ADI-SOYADI	
BÖLÜM/GÖREV/ÜNVAN	
İrtibat Tel No	

İrtibat GSM No			
e-Mail			
Adresi			
D. TSM BİRİNCİL MERKEZ BİLGİLERİ			
İRTİBAT KURULACAK KİŞİ ADI-SOYADI			
BÖLÜM/GÖREV/ÜNVAN			
İrtibat Tel No			
İrtibat GSM No			
e-Mail			
ÖKC TSM BİRİNCİL MERKEZİN ADRESİ:			
E. TSM İKİNCİL MERKEZ BİLGİLERİ			
İRTİBAT KURULACAK KİŞİ ADI-SOYADI			
BÖLÜM/GÖREV/ÜNVAN			
İrtibat Tel No			
İrtibat GSM No			
e-Mail			
ÖKC TSM İKİNCİL MERKEZİN ADRESİ:			
F. TSM MERKEZİ HİZMETİ VERİLECEK YENİ NESİL ÖKC'LERE AİT BİLGİLER (*)			
SIRA NO	MARKA	MODEL	TÜRÜ (EFT POS ÖZELLİKLİ / BASİT-

			BİLGİSAYAR BAĞLANTILI)
1			
2			
(*) ÖKC TSM Merkezi Hizmeti Verilecek her marka ve model ÖKC için ilgili satırlar çoklanacaktır. ÖKC TSM Merkezi hizmetine daha sonradan dahil edilmesi talep edilen ÖKC Marka, Model ve Türüne ilişkin bildirimlerin yazılı olarak GİB'e yapılması gerekmektedir.			
G. BAŞVURU FORMU EKLERİ			
	ÖKC Üreticisine Ait	DHS'ye Ait	
1- PCI DSS	☐	☐	
2- ISO/IEC 20000	☐	☐	
3- ISO/IEC 27001	☐	☐	
4- ISO 22301	☐	☐	
5- TEKNİK RAPOR	☐	☐	
6- GÜVENÇE VE DENETİM RAPORU	☐	☐	
7- İŞ SÜREKLİLİĞİ DOKÜMANI	☐	☐	
8- ÖKC ÜRETİCİSİ TSM YETKİ SORUMLULUK ANLAŞMA VE DOKÜMANLARI	☐	☐	
9- İÇ KONTROL VE İÇ DENETİM DOKÜMANLARI	☐	☐	
10- GÜN İÇİ VE GÜN SONU SÜREÇLERİ DOKÜMANLARI	☐	☐	
11- DHS HİZMET SÖZLEŞMESİ	☐	☐	
12- İKİNCİL MERKEZ ANLAŞMASI	☐	☐	
13- ÜRETİCİ KURUM İMZA SİRKÜLERİ	☐	☐	
14- DHS KURUM İMZA SİRKÜLERİ	☐	☐	
H- DIŞ HİZMET SAĞLAYICIDAN TEMİN EDİLEN HİZMET UNSURLARINA İLİŞKİN BİLGİLER			
ÖKC üreticisinin; TSM Merkezine ilişkin hizmetlerden kısmen veya tamamen bir dış hizmet sağlayıcıdan yararlanması halinde; yararlanılan hizmet unsurları detaylı olarak açıklanacak ve hizmetin niteliğine bağlı olarak dış hizmet sağlayıcı tarafından temin edilen tevsik edici bilgi ve belgeler (sertifikalar, sözleşmeler vb.) başvuru formu ekinde Başkanlığa ibraz edilecektir.			

I. DİĞER ANLAŞMA VE DOKÜMANLARA İLİŞKİN AÇIKLAMALAR (Bölüm 25.1 /m)	
Bu form ve eklerinde kurumumuza ilişkin yer alan bilgi ve belgelerin doğruluğunu beyan ve taahhüt ederiz.	
ÖKC ÜRETİCİSİ KURUM UNVANI	DIŞ HİZMET SAĞLAYICI KURUM UNVANI
Yetkili Adı-Soyadı	Yetkili Adı-Soyadı
İmza	İmza
Tarih:	Tarih:

EK-3 : “ÖKC TSM Merkezi Onay Denetim Raporu Formatı

KAPAK

DİZİN

I- GENEL BİLGİ

Denetim faaliyeti gerçekleştirilen ÖKC TSM Merkezi'ne ilişkin genel bilgiler (ÖKC TSM Merkezi hizmeti verilecek ÖKC firmasının ünvanı, cihaz marka ve modeli, yazılacaktır.

II- ÖKC TSM MERKEZİ'NDE GERÇEKLEŞTİRİLEN BİLGİ SİSTEMLERİ DENETİMİ FAALİYETLERİ

III- ÖKC TSM MERKEZİ'NDE GERÇEKLEŞTİRİLEN GÜVENLİ HABERLEŞME DENETİMİ FAALİYETLERİ

IV- SONUÇ

Raporun önceki bölümlerinde elde edilen bulgular çerçevesinde, denetimi yürütülen ÖKC TSM Merkezi Başvurusunun onayını uygun olup olmadığı hakkında görüş bildirilecektir.

EK-4A : “ÖKC TSM Merkezi Yıllık Denetim Raporu Formatı

KAPAK

DİZİN

I- GENEL BİLGİ

Denetim faaliyeti gerçekleştirilen ÖKC TSM Merkezi'ne ilişkin genel bilgiler (ÖKC TSM Merkezi hizmeti verilecek ÖKC firmasının ünvanı, cihaz marka ve modeli, yazılacaktır.

II- ÖKC TSM MERKEZİNDE GERÇEKLEŞTİRİLEN BİLGİ SİSTEMLERİ DENETİMİ FAALİYETLERİ

III- SONUÇ

Raporun önceki bölümlerinde elde edilen bulgular çerçevesinde, denetimi yürütülen ÖKC TSM Merkezi Başvurusunun yıllık denetim değerlendirmesinin uygun olup olmadığı hakkında görüş bildirilecektir.

EK-4B: “ÖKC TSM Merkezi Güncelleme Denetimi Rapor Formatı

KAPAK

DİZİN

I- GENEL BİLGİ

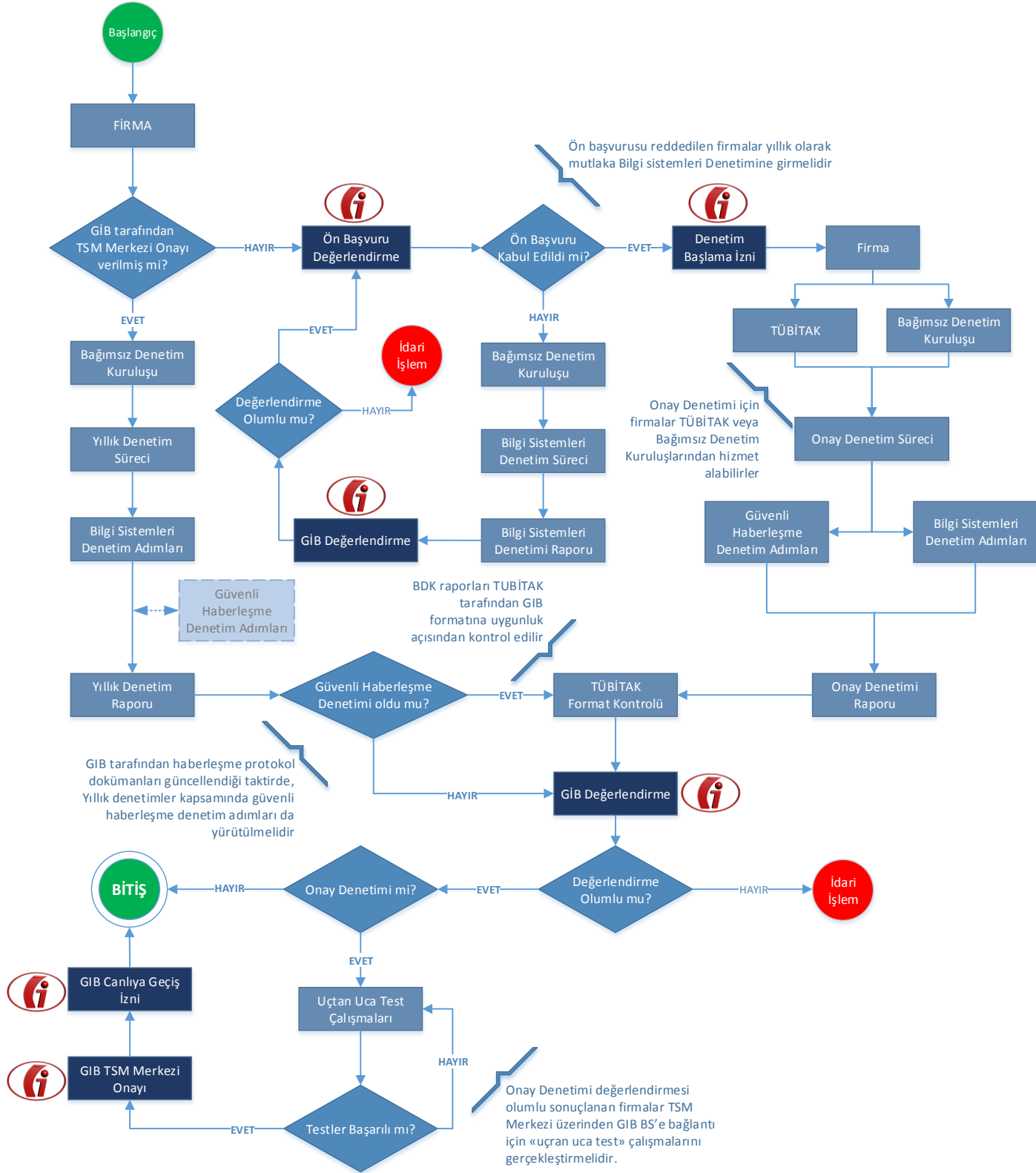
Denetim faaliyeti gerçekleştirilen ÖKC TSM Merkezi'ne ilişkin genel bilgiler (ÖKC TSM Merkezi hizmeti verilecek ÖKC firmasının ünvanı, cihaz marka ve modeli, yazılacaktır.

II- ÖKC TSM MERKEZİNDE GÜVENLİ HABERLEŞME DENETİMİ FAALİYETLERİ

III- SONUÇ

Raporun önceki bölümlerinde elde edilen bulgular çerçevesinde, denetimi yürütülen ÖKC TSM Merkezi Başvurusunun güncellenen mesajlaşma protokol dokümanlarına uygun denetim değerlendirmesinin uygun olup olmadığı hakkında görüş bildirilecektir.

EK-5 – ÖKC TSM Merkezi Onay Denetimi ve Yıllık Denetim Süreçleri Akışı



30. REFERANSLAR

[1] <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>

[2] http://www.iso.org/iso/catalogue_detail?csnumber=50038