YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARA AİT

TSM MERKEZLERİNİN

BİLGİ SİSTEMLERİ DENETİMİ ADIMLARI

TEKNİK KILAVUZU

Sürüm 1.0

23 Eylül 2016

İÇİNDEKİLER

1. Tanımlar ve Kısaltmalar

1.1. Tanımlar

Kavram	Tanımı
HSM	Hassas anahtar ve verileri koruyan fiziksel, yan kanal ataklarına dirençli, mantıksal ve çevresel güvenlik mekanizmalarına sahip, kendisine dışarıdan yapılacak saldırılara (fiziksel atak, ısı ve gerilim değişimi, vb) karşı dirençli olan, 3DES, AES, RSA gibi algoritmaları kullanarak kripto işlemlerini gerçekleştirebilen cihazdır.
ÖKC TSM MERKEZİ	Yeni Nesil Ödeme Kaydedici Cihazlara yazılım-parametre yükleme, yazılım güncelleme, bu cihazları ve bu cihazlar ile birlikte veya üzerinde gerçekleştirilen kartlı işlemleri yönetme, cihazlar ile ilgili güvenli anahtar yönetimini gerçekleştirme, ön kontrol işlemlerini yapma, banka uygulaması yazılım ve parametrelerini cihaza yükleme, cihaz yaşam döngüsünü kontrol etme ve yönetme, YN ÖKC mesajlarının GİB BS'ye ve üye işyeri anlaşması yapan kuruluşlara GMP dokümanlarında belirlenen iletişim protokolleri çerçevesinde aktarılmasını sağlama amacıyla Yeni Nesil ÖKC üreticileri tarafından veya bir Dış Hizmet Sağlayıcısı tarafından kurulmuş terminal yönetim merkezini ifade eder.
GMP (GİB Mesajlaşma Protokolü)	Yeni Nesil Ödeme Kaydedici Cihazlar (YN ÖKC), çevre birimleri, ÖKC TSM Merkezi ve GİB BS arasındaki güvenli haberleşmeyi ve mesajlaşma yapısını içeren haberleşme protokolleri.
Yetkilendirilmiş ESHS	ESHS (Elektronik Sertifika Hizmet Sağlayıcısı) Yeni Nesil ÖKC'lere, ÖKC TSM Merkezlerine ve GİB BS'ye yüklenecek sertifikaların üretimi, dağıtımı ve sonrasında yönetimini ve denetimini gerçekleştirecek kurum (TÜBİTAK Kamu SM) ya da GİB tarafından yetkilendirilmiş sertifika otoritesi olan kurum.
YN ÖKC Üreticisi	Maliye Bakanlığı'ndan onay alan ve YN ÖKC ile TSM Merkezinden sorumlu olan üretici firma
ISO/IEC 20000	Bilgi Teknolojileri Servis Yönetimi Standardı
ISO 22301	Uluslararası İş Sürekliliği Yönetimi Standardı
ISO/IEC 27001	Bilgi Güvenliği Yönetim Sistemi Standardı

1.2. Kısaltmalar

Kısaltma	Karşılığı
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange (Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi)
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BCD	Binary Coded Decimal
EFT	Elektronik Fon Transferi
ESHS	Elektronik Sertifika Hizmet Sağlayıcısı
GİB	Gelir İdaresi Başkanlığı
GİB BS	Gelir İdaresi Başkanlığı Bilgi Sistemleri
GMP	Gelir İdaresi Başkanlığı Mesajlaşma Protokolü
HSM	Hardware Security Module
LRC	Longitudinal Redundancy Check
OCSP	Online Certificate Status Protocol
YN ÖKC	Yeni Nesil Ödeme Kaydedici Cihaz
PCI DSS	Payment Card Industry Data Security Standard
POS	Point of Sale (Satış Noktası)
SİL	Sertifika İptal Listesi
TLV	Tag Length Value
TPDU	Transport Protocol Data Unit
TSM	Trusted Service Manager
SSL	Secure Socket Layer (TLS v1.2)

2. Amaç

Bu Kılavuz, GİB tarafından yayınlanan "Yeni Nesil Ödeme Kaydedici Cihazlara Ait TSM Merkezi Teknik Kılavuzu Sürüm 2.0" ve "Yeni Nesil Ödeme Kaydedici Cihazlara Ait TSM Merkezi Başvuru, Test, Denetim ve Onay Teknik Kılavuzu Sürüm 2.0" Kılavuzlarında açıklanan ÖKC TSM Merkezlerinin Onay Denetimi ve Yıllık Denetim süreçleri kapsamında gerçekleştirilecek Bilgi Sistemleri Denetimlerinin kapsamı ve yürütülmesi gereken değerlendirme adımlarının belirlenmesi amacı ile hazırlanmıştır.

3. Kapsam ve Dayanak

ÖKC TSM Merkezlerine yönelik gerçekleştirielcek Bilgi Sistemleri Denetim Adımlarını belirten bu Kılavuz, GİB tarafından yayınlanmış "Yeni Nesil Ödeme Kaydedici Cihazlara Ait TSM Merkezi Teknik Kılavuzu Sürüm 2.0" ve "Yeni Nesil Ödeme Kaydedici Cihazlara Ait TSM Merkezi Başvuru, Test, Denetim ve Onay Teknik Kılavuzu Sürüm 2.0" Kılavuzları kapsamına girmiş gereksinimlerden oluşturulan değerlendirme sınıflarını içermektedir.

4. Değerlendirme Sınıfları

ÖKC TSM Merkezi değerlendirmelerinin sağlıklı ve takip edilebilir olarak yapılabilmesi için Bilgi Sistemi özelinde gerçekleştirilecek değerlendirmeler özelliklerine göre gruplandırılmıştır. Gruplandırılan her bir test kümesi, birer Değerlendirme Sınıfı olarak tanımlanmış ve içeriğine uygun isimler verilmiştir.

Her bir ***Değerlendirme Sınıfı***, ***Değerlendirme Alt Bileşenlerinden*** oluşmaktadır. ***Değerlendirme Alt Bileşenleri*** için yapılacak kontroller ile ilgili ek açıklayıcı bilgiler ilgili bileşenkontrol tablosu altında ***Uygulama Notu*** olarak verilmiştir.

Değerlendirme neticesinde; her bir ***Değerlendirme Alt Bileşeni*** özelinde ilgili denetçi tarafından doldurulacak kontrol tablolarının ve bu Kılavuzun 5.2 başlığında yer alan Değerlendirme Sonuç Raporu Formatına uygun olarak değerlendirme özetinin, Onay Denetimi veya Yıllık Denetim Raporu ekinde yer alması temin edilmelidir.

Doküman aşağıda verilen ***Değerlendirme Sınıflarından*** oluşmaktadır;

1. TSM_SER : Uluslararası Sertifikasyon Raporları ve Denetim Talepleri Değerlendirme Sınıfı
2. TSM_SIS : Sistem ve Güvenlik Değerlendirme Sınıfı
3. TSM_ILT : Paydaş İletişimi ve İş Kurgusu Değerlendirme Sınıfı
4. TSM_OKC : Güvenli Yazılım Yükleme ve Mesaj Yönetim Değerlendirme Sınıfı

4.1. Uluslararası Sertifikasyon Raporları ve Denetim Talepleri Değerlendirme Sınıfı (TSM_SER)

Bu değerlendirme sınıfı, ÖKC TSM Merkezlerinin sağlaması gereken Uluslararası Standartlara ait sertifikasyon süreçlerinin çıktıları ile ÖKC TSM Merkezlerinin rutin olarak sağlaması gereken denetim süreçlerinim varlığının ve uygunluğunun kontrol edilmesini amaçlamaktadır.

Değerlendirme Sınıfı Alt Bileşenleri;

Bu değerlendirme sınıfı, 2 alt bileşenden oluşmaktadır;

TSM_SER.1 Bu değerlendirme alt bileşeninde değerlendiriciden;

4.1.1. PCI-DSS (Payment Card Industry Data Security Standard) Onay Belgesinin
4.1.2. ISO/IEC 20000 Bilgi Teknolojileri Hizmet Yönetim Sistemi Belgesinin
4.1.3. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesinin
4.1.4. ISO 22301 İş Sürekliliği Yönetim Sistemi Belgesinin

varlığının ve belgelendirmenin ÖKC TSM Merkezi özelinde gerekli isterleri içerip içermediğinin kontrolü beklenmektedir.

TSM_SER.2 Bu değerlendirme alt bileşeninde değerlendiriciden, ÖKC TSM Merkezlerinin rutin olarak gerçekleştirmesi gereken iç kontrol ve denetim süreçlerinin varlığının ve çıktılarının uygunluğunun kontrolü beklenmektedir.

TSM_SER.1 Kontrol Tablosu

ÖKC TSM Merkezi'nin aşağıda yer alan "Uluslararası Sertifikasyon" kurallarına uygunluğu kontrol edilmelidir.

☐	PCI-DSS sertifikası mevcut ve denetim tarihinde geçerli mi?
☐	Infrastructure/Network, alınan PCI-DSS sertifikası kapsamına dahil mi?
☐	Payment Gateway/Switch, alınan PCI-DSS sertifikası kapsamına dahil mi?
☐	Backoffice Services, alınan PCI-DSS sertifikası kapsamına dahil mi?
☐	POS/Card Present, alınan PCI-DSS sertifikası kapsamına dahil mi?
☐	PCI-DSS sertifikası Other Processing (specify) alanında "Trusted Service Manager Services" ibaresi bulunmakta mı?
☐	PCI-DSS sertifikası Description alanında ÖKC TSM Merkezi hizmetlerinin kapsamda olduğu ifade edilmiş mi?
☐	PCI-DSS - AOC (Attestation of Compliance for Onsite Assessments) Belgesi üzerinde TSM hizmetlerinin verildiği uygulamaların denetim kapsamında olduğu ve sertifikanın bu Kılavuzun 5.1 bölümünde belirtilen kritik varlıkları işleyen ve kullanan süreçleri kapsadığı kontrol edildi mi?
☐	ISO/IEC 20000 sertifikası mevcut ve denetim tarihinde geçerli mi?
☐	ISO 22301 sertifikası mevcut ve denetim tarihinde geçerli mi?
☐	ISO/IEC 27001 sertifikası mevcut ve denetim tarihinde geçerli mi?
☐	ISO/IEC 27001 sertifikası bu Kılavuzun 5.1 bölümünde belirtilen kritik varlıkları işleyen ve kullanan süreçleri kapsıyor mu?

Değerlendirme Sonucu: ***Olumlu*** ☐ ***Olumsuz*** ☐ ***Belirsiz*** ☐

Ek Açıklama:

*Bu kutu, Değerlendirme Sonucunun "**Belirsiz**" olarak işaretlenmesi durumunda mutlaka doldurulmalıdır.*

Uygulama Notu 1: TSM'e ait sertifikalar 5.2. bölümünde yeralan Değerlendirme Sonuç Raporu ekinde yer almalıdır.

TSM_SER.2 Kontrol Tablosu

ÖKC TSM Merkezi'nin aşağıda yer alan "Denetim" kurallarına uygunluğu kontrol edilmelidir.

☐	İç kontrol ve iç denetim dokümanı oluşturulmuş ve uygulanıyor mu?
☐	İç ve dış denetimde kullanılmak üzere iç kontrol sonuçlarının nasıl raporlanacağı tarif edilmiş mi?
☐	İç kontrol dokümanları ile iş süreklilik dokümanları birbiriyle uyumlu mu?
☐	ÖKC TSM Merkezi için Bilgi Sistemleri Denetimi yılda en az bir kez yapılacak şekilde süreç oluşturulmuş ve uygulanıyor mu?
☐	ÖKC TSM Merkezi güvenli oda kontrolleri TÜBİTAK tarafından sağlanmış mı?
☐	Onay almış ÖKC TSM Merkezleri için; yılda bir kez bağımsız denetim kuruluşları tarafından sızma testleri gerçekleştiriliyor mu?
☐	Onay almış ÖKC TSM Merkezleri için; en son yapılan denetim sonucunda düzenlenen raporda tespit edilen sorun ve eksiklikler ÖKC TSM Merkezi tarafından giderilmiş mi?

Değerlendirme Sonucu: ***Olumlu*** ☐ ***Olumsuz*** ☐ ***Belirsiz*** ☐

Ek Açıklama:

*Bu kutu, Değerlendirme Sonucunun "**Belirsiz**" olarak işaretlenmesi durumunda mutlaka doldurulmalıdır.*

Uygulama Notu 2: Belirtilen denetim ve kontrollere ilişkin süreç, test ve/veya rapor dokümanları 5.2. bölümünde yer alan Değerlendirme Sonuç Raporu ekinde yer almalıdır.

4.2. Sistem ve Güvenlik Değerlendirme Sınıfı (TSM_SIS)

Bu değerlendirme sınıfı, ÖKC TSM Merkezlerinin 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.

Değerlendirme Sınıfı Alt Bileşenleri;

Bu değerlendirme sınıfı, 5 alt bileşenden oluşmaktadır;

TSM_SİS.1 Bu değerlendirme bileşeninde değerlendiriciden; TSM Merkezinin kurup işlettiği sistem alt yapısının uygunluğunun kontrol edilmesi, gerekli münhasırlık kurallarının uygulandığının tespiti beklenmektedir.

TSM_SİS.2 Bu değerlendirme bileşeninde değerlendiriciden, ÖKC TSM Merkezlerinin Yeni Nesil ÖKC'ler üzerinden sunduğu hizmetin sürekliliğini ve kesinti halinde faaliyetlerinin sürdürülebilmesini amaçlayan İş Süreklilik ve Acil Durum Yönetim Süreci ile YN ÖKC Mesajlarına dair işlemlerde kullandığı bilgi sistemlerine ve tüm operasyon süreçlerine ilişkin bir Risk Yönetim Planının mevcudiyeti ve uygulandığının kontrolü beklenmektedir.

TSM_SİS.3 Bu değerlendirme bileşeninde değerlendiriciden, ÖKC TSM Merkezlerinin bünyesindeki bilgi sistemleri üzerinde, YN ÖKC mesajlarını yöneten donanım ve yazılımlarda gerçekleştirilen her türlü yama, bakım ve değişikliğe yönelik gereklilikleri sağlayan prosedürel bir yönetim sürecinin uygulandığının kontrolü beklenmektedir.

TSM_SİS.4 Bu değerlendirme bileşeninde değerlendiriciden, ÖKC TSM Merkezlerinin YN ÖKC Mesajlarının yönetildiği sistemlere ve yazılımlara gerçekleştirilen mantıksal veya fiziksel erişimlerde, işlem altyapısını kullanan yetkisiz erişim teşebbüslerinde gerekli denetim izlerini sağlayan süreçlerin mevcudiyeti ve uygulandığının kontrolü beklenmektedir.

TSM_SİS.5 Bu değerlendirme bileşeninde değerlendiriciden, ÖKC TSM Merkezinin Dış Hizmet sağlayıcı olması durumunda, Dış Hizmet Sağlayıcı olmanın hususi gerekliliklerini sağladığının kontrolü beklenmektedir.

TSM_SİS.1 Kontrol Tablosu

ÖKC *TSM Merkezi'nin aşağıda yer alan "Alt Yapı ve Münhasırlık" kurallarına uygunluğu kontrol edilmelidir.*

- ☐ TSM Merkezinde her üretici için ayrı bir veritabanı tutulmuş mu?
- ☐ Ayrı veritabanlarının birbiriyle iletişimi hem network hem de sistem konfigürasyonu olarak izole mi?
- ☐ Veritabanlarının çalıştığı makina ve porta sadece ilgili uygulama mı erişebiliyor?
- ☐ Veritabanları üzerinde linkserver kurgusu olmadığı kontrol edildi mi?
- ☐ ÖKC TSM Merkezi ile GİB BS arasında ve ÖKC TSM Merkezi ile cihazlar arasındaki anlık iletişim kuran uygulamalar farklı sanal/fiziksel sunucularda çalışıyor mu?
- ☐ Üreticiye özel olarak ayrılmış fiziksel/sanal alanda başka üreticiye ait veri bulunmadığı kontrol edildi mi?
- ☐ GİB BS ve YN ÖKC ile haberleşmek için kullanılan kriptografik anahtarlar, FIPS 140-2 Level 3 ve üzeri için sertifika almış ürünler ile saklanmakta mı?
- ☐ Loglamalar ayrı sanal/fiziksel sunuculara kaydediliyor mu?
- ☐ Log ve verilerin yedeklenmesi üreticiye özel olarak yapılmış mı?
- ☐ Log ve verilerin arşivlemesi üreticiye özel olarak yapılmış mı?
- ☐ YÖKCYN ÖKC'den ÖKC TSM Merkezine'ye ulaşmak için gerekli APN – GSM bağlantıları sağlanmış mı?
- ☐ ÖKC TSM Merkezi, GİB BS erişimi için gereken altyapı sağlanmış ve erişim hatları binaya kadar ulaştırılmış mı?
- ☐ GMP Mesajı ağ (network) iletim seviyesi, TSM Merkezinde sonlandırılmakta mı?
- ☐ YN ÖKC mali olmayan mesajları (GMP kapsamı haricindeki) TSM'de kabul edilip, ilgili sisteme iletilip alınabiliyor ve denetim izi bırakıyor mu?
- ☐ YN ÖKC ile ilgili güvenli anahtar yönetimi başarılı gerçekleştirilebiliyor mu?
- ☐ ÖKC TSM Merkezi kontrollerin sonucuna bağlı uyarı mekanizmaları gerçekleştirilmiş mi?
- ☐ ÖKC TSM Merkezi, GİB ile olan iletişimine bağlı olarak oluşturalacak uyarı mekanizmalarını gerçekleştirmiş mi?
- ☐ YN ÖKC'lerden hatalı veri gelmesi ya da beklenmeyen bir mesaj gelmesi

durumunda mesajların kaydedilmesi ve GİB BS'e iletilmemesi sağlanıyor mu?

☐ YN ÖKC'den ÖKC TSM Merkezine gelen ve GİB BS'e gönderilmemesi gereken mesajlar eşik değere ulaştığında cihaza saha hizmetleri ile müdahale edilmesi için ÖKC TSM Merkezinde akıllı bir mekanizma bulunuyor mu?

☐ YN ÖKC'den ÖKC TSM Merkezine gelen ancak GİB BS'e gönderilmemesi gereken mesajlar eşik değere ulaştığında cihaza saha hizmetleri yoluyla müdahale talimatı iletildiği loglardan izlenebiliyor mu?

☐ ÖKC TSM Merkezi, kendi sistemsel kontrollerini gerçekleştirirerek arıza ya da şüpheli durumlarda kontrollerin sağlanması için uyarı mekanizmaları gerçekleştirmiş mi?

☐ ÖKC TSM Merkezinde, GİB Hassas ÖKC verisinin açılmaması ve saklanmaması sağlanmakta mı?

☐ ÖKC TSM Merkezinde, Üye İşyeri Anlaşması Yapan Kuruluşlara ait hassas verilerin açılmaması ve saklanmaması sağlanmakta mı?

Değerlendirme Sonucu: ***Olumlu*** ☐ ***Olumsuz*** ☐ ***Belirsiz*** ☐

Ek Açıklama:

*Bu kutu, Değerlendirme Sonucunun "**Belirsiz**" olarak işaretlenmesi durumunda mutlaka doldurulmalıdır.*

Uygulama Notu 3: ÖKC TSM Merkezi sistem topolojisi 5.2. bölümünde yer alan Değerlendirme Sonuç Raporu ekinde yer almalıdır.

Uygulama Notu 4: GİB BS ve YN ÖKC ile haberleşmek için kullanılan kriptografik anahtarların saklandığı HSM lere ait sertifikalar 5.2. bölümünde yer alan Değerlendirme Sonuç Raporu ekinde yer almalıdır.

TSM_SİS.2 Kontrol Tablosu

ÖKC TSM Merkezi'nin aşağıda yer alan "Veri Merkezi Hizmet Sürekliliği ve Risk Yönetimi" kurallarına uygunluğu kontrol edilmelidir.

- ☐ ÖKC TSM Merkezi, YN ÖKC mesajlarına dair işlemlerde kullandığı bilgi sistemlerine ve tüm operasyon süreçlerine ilişkin riskleri tespit ve analiz ederek, ölçme, izleme, kontrol etme ve raporlama işlemlerini yerine getirebilecek durumda mı?
- ☐ ÖKC TSM Merkezi, YN ÖKC Mesajlarına dair işlemlerde kullandığı bilgi sistemlerine ve tüm operasyon süreçlerine ilişkin bir risk yönetim planı tarif edilmiş, oluşturmuş ve dokümante edilmiş mi?
- ☐ ÖKC TSM Merkezi altyapısının bir parçası olan veya herhangi bir noktada YN ÖKC Mesajlarını yöneten donanım, yazılım, uygulama geliştirme, değişim yönetim süreçleri, iletişim alt yapıları ve operasyon süreçleri risk yönetim planına dahil edilmiş, tarif edilmiş ve dokümante edilmiş mi?
- ☐ YN ÖKC üreticisi, ÖKC TSM Merkezinin uyguladığı risk yönetim planı çerçevesinde, faaliyetlerinde kullandığı bilgi teknolojisi varlıklarının risk analizini, Dış Hizmet Sağlayıcılarından kaynaklanabilecek riskleri de dikkate alarak gerçekleştirmesine yönelik yapılacak çalışmalar tarif edilmiş ve dokümante edilmiş mi?
- ☐ ÖKC TSM Merkezi (Dış Hizmet Sağlayıcılar dahil) tarafından vereceği hizmetlerden doğabilecek zararları karşılamak amacıyla mesleki sorumluluk sigortası yaptırılmış mı?
- ☐ ÖKC üreticisi varlık envanteri, varlıklara yönelik tehditler, tehditlerin risk seviyeleri ve uygulanacak eylemleri belirleyerek yazılı hale getirmiş, tanımlamış, tarif etmiş ve dokümante edilmiş mi?
- ☐ Bilgi sistemlerine ilişkin risk analizleri, hizmetleri etkileyen önemli güvenlik olayları sonrasında, önemli bir değişiklik öncesinde ve yeni tehditlerin tespiti halinde gözden geçirilmesi adına alınacak aksiyonlar tarif edilmiş ve dokümante edilmiş mi?
- ☐ Bilgi sistemlerine ait risk analizlerini, yılda en az 1 defa olmak üzere güncellenmeye yönelik gerçekleştirilecek çalışmalar tarif edilmiş mi?
- ☐ Yılda 4 defa olmak üzere, tüm sistemlere ait iş sürekliliği iç testleri gerçekleştirilerek kayıt altına alınmakta mı?
- ☐ Veritabanı sistemsel bakım planları tarif edilmiş ve sunulmuş mu?
- ☐ Veritabanı performans iyileştirici indeksleme ve rotasyonlar oluşturulmuş, yeni isteklerin oluşması durumunda izlenecek işlemler tarif edilmiş mi?
- ☐ İşlem performansları sürekli kontrol edilebilir ve proaktif önlem alınmaya elverişli mi?

- ☐ ÖKC TSM Merkezi, YN ÖKC'ler üzerinden sunduğu hizmetin sürekliliğini ve kesinti halinde faaliyetlerinin sürdürülebilmesini amaçlayan üst yönetim tarafından onaylanmış "İş Süreklilik ve Acil Durum Yönetim Süreci" oluşturulup dokümante edilmiş mi?
- ☐ İş sürekliliği planı ve planının bir parçası olan bilgi sistemleri süreklilik planı hazırlanmış mı ?
- ☐ ÖKC TSM Merkezi tarafından, iş sürekliliği planlamasına yönelik olarak iş etki analizi yapılarak, kurtarma stratejilerini belirlenmiş ve dokümante edilmiş mi?
- ☐ ÖKC TSM Merkezi tarafından iç ve dış bağımlılıklar belirlenmiş ve dokümante edilmiş mi?
- ☐ ÖKC TSM Merkezi tarafından, meydana gelebilecek bir kesinti durumunda gereken faaliyet düzeyini ve çerçevesini ortaya koymak üzere operasyonlar önem düzeyi açısından sınıflandırılmış ve dokümante edilmiş mi?
- ☐ Farklı kesinti senaryolarının faaliyetler üzerinde yaratabileceği muhtemel riskler ve bunların potansiyel etkileri ÖKC TSM Merkezi tarafından değerlendirilmiş, ve dokümante edilmiş mi?
- ☐ Kurtarma ve iletişim prosedürleri geliştirilmiş ve dokümante edilmiş mi?
- ☐ İş sürekliliği yönetimi sürecinde, bilgi sistemleri varlıklarının ve tutulan verilerin önem düzeyleri dikkate alınarak iş etki analizi çerçevesinde kabul edilebilir kesinti süreleri verilen hizmet bazında (ödeme sistemleri / GİB BS bağlantısı vb.) belirleyerek ve bu süreler içinde servislerin tekrar erişime açılabilmesini sağlamak amacıyla, alternatifli kurtarma prosedürleri ile yetki ve sorumlukları içeren iletişim prosedürleri ÖKC TSM Merkezi tarafından geliştirilmiş ve dokümante edilmiş mi?
- ☐ Performans takip teknikleri kullanılarak, kapasite planlaması yapılarak, işlem hacmi tahminleri doğrultusunda stres testleri gerçekleştirilerek, ağ ve iletişim altyapısından kaynaklanabilecek kesintilere karşı uygun alternatif kanallar oluşturulmuş ve dokümante edilmiş mi?
- ☐ Servis dışı bırakma atakları göz önünde bulundurularak ve buna karşı gerekli önlemler ÖKC TSM Merkezi tarafından alınmış mı?
- ☐ ÖKC TSM Merkezi tarafından, yurtiçinde bir İkincil Merkez tesis edilmiş mi?
- ☐ Veri ve sistem yedekleri kurulan İkincil Merkezde kullanıma hazır bulundurulmakta mı?
- ☐ ÖKC TSM Merkezi bilgi sistemleri sürekliliğini etkileyecek olay ya da değişikliklerden sonra iş sürekliliği planını gözden geçirirerek ve güncellemeleri gerçekleştirmekte mi?
- ☐ Mevcut planın etkinliğini ve güncelliğini temin etmek üzere, yılda en az 1 defa

günlük operasyonlarının tamamını İkincil Merkez üzerinden gerçekleştirecek şekilde testler yaparak, test sonuçlarını ve hizmet sürekliliğini etkileyen olayları üst yönetime ve GİB'e raporlayacak şekilde süreç oluşturmuş mu?

☐ ÖKC TSM Merkezi, bilgi sistemlerine ilişkin beklenmedik olayları yönetmek ve bunların etkilerini en aza indirmek üzere acil ve beklenmedik durum planı oluşturarak gerekli önlemleri almış mı?

☐ Faaliyetlerin güvenilir bir şekilde sürdürülmesini sağlayan hızlı, etkili ve düzenli bir tepki süreci ile beklenmedik olayları erken haber almayı sağlayacak mekanizmaları tesis etmiş mi?

☐ Acil ve beklenmedik durum planı kapsamında, bilgi sistemlerine ilişkin olayın kaynağını hızlı bir şekilde bulma, hasarı tespit etme, olayın potansiyel boyutunu ve etkisini gösterme, yetkili yönetim birimine ulaştırılmasını sağlama ve etkilenen müşterileri tespit etme süreçlerini planlamış ve işletmekte mi?

☐ Bilgi sistemlerine ilişkin beklenmedik olayların sonradan incelenmesine imkân tanıyacak, yetkili merciler tarafından talep edildiğinde kullanılabilecek nitelikte kayıt ve bilgileri toplayan bir mekanizma oluşturmuş mu?

☐ ÖKC TSM Merkezi, Bilgi Sistemleri servislerinin, aylık %99,75 kullanılabilirlik ile hizmet sunmasını temin edecek şekilde, mimari tasarımın ve testlerin yapıldığına dair güvence sunmuş mu?

☐ Sunulacak güvence ve raporlamalar asgari olarak Uptime Institute Tier 2 standartlarına uyumlu mu?

☐ Raporlar aylık olarak denetimlerde sunulmak üzere hazır bulundurmak için plan hazırlanmış mı?

☐ ÖKC TSM Merkezi, kesinti süresince yapılan işlemlerde kayıp oluşmayacağını garanti altına almış mı?

☐ Sistem işlem performansları sürekli kontrol edilebilir ve proaktif önlem alınmaya elverişli mi?

Değerlendirme Sonucu: ***Olumlu*** ☐ ***Olumsuz*** ☐ ***Belirsiz*** ☐

Ek Açıklama:

*Bu kutu, Değerlendirme Sonucunun "**Belirsiz**" olarak işaretlenmesi durumunda mutlaka doldurulmalıdır.*

Uygulama Notu 5: Geçerli mesleki sorumluluk sigortası poliçe nüshası 5.2. bölümünde yeralan Değerlendirme Sonuç Raporu ekinde yer almalıdır

Uygulama Notu 6: Risk Yönetim Planı, İş Süreklilik ve Acil Durum Yönetim Süreci, 5.2. bölümünde yeralan Değerlendirme Sonuç Raporu ekinde yer almalıdır

TSM_SİS.3 Kontrol Tablosu

ÖKC TSM Merkezi'nin aşağıda yer alan "Değişiklik Yönetimi" kurallarına uygunluğu kontrol edilmelidir.

☐	TSM Merkezi, bünyesindeki bilgi sistemleri üzerinde gerçekleştirilen ve YN ÖKC Mesajlarını yöneten donanım ve yazılımlara ilişkin her türlü bakım, yama ve değişikliğin uygun bir şekilde planlanmasını, yetkilendirilmesini, test edilmesini, gerçekleştirilmesini, belgelendirilmesini ve sonrasında denetlenebilirliğini sağlayacak yazılı ve etkin bir değişiklik yönetimi süreci oluşturulmuş mu?
☐	Bu süreçler için uygun işlemlerin gerçekleştirilmesinin tarif edildiği yapı dokümante edilmiş mi?
☐	ÖKC TSM Merkezi, YN ÖKC Mesajını yöneten yazılımlar için, yazılım geliştirilen ortamların ve geliştirilen yazılımların canlı ortama aktarılmadan önce test edildiği ortamların canlı ortamlardan ayrılmasını sağlamış mı?
☐	ÖKC TSM Merkezi, bu ortamların herhangi birinde değişiklik yapma yetkisine sahip personelin diğerlerinde de değişiklik yapma yetkisinin bulunmamasını sağlamış mı?
☐	ÖKC TSM Merkezi, test ve geliştirme ortamlarında kullanılan verilerin canlı ortam verileri ile eşleştirilemez nitelikte olmasını temin etmiş ve edeceğini kabul etmış mı?
☐	ÖKC TSM Merkezi, YN ÖKC Mesajını yöneten sistemlere ilişkin değişikliklerde etki analizi yapılmasını, değişikliğin yetkili kişi veya kişilerce onaylanmasını ve değişikliği geri çekme prosedürünün oluşturulması ve yürütülmesini sağlamak için bu süreç yazılı hale getirilmiş mi?

Değerlendirme Sonucu: ***Olumlu*** ☐ ***Olumsuz*** ☐ ***Belirsiz*** ☐

Ek Açıklama:

*Bu kutu, Değerlendirme Sonucunun "**Belirsiz**" olarak işaretlenmesi durumunda mutlaka doldurulmalıdır.*

Uygulama Notu 7: Değişiklik Yönetim Süreci ve Değişiklik Geri Çekme Prosedürü, 5.2. bölümünde yer alan Değerlendirme Sonuç Raporu ekinde yer almalıdır.

TSM_SİS.4 Kontrol Toblosu ***TSM Merkezi'nin aşağıda yer alan "Denetim İzi Yönetimi" kurallarına uygunluğu kontrol edilmelidir.***	
☐	ÖKC TSM Merkezi tarafından, ÖKC Mesajlarının yönetildiği sistemlere ve yazılımlara gerçekleştirilen mantıksal veya fiziksel erişimlere, işlem altyapısını kullanan yetkisiz erişim teşebbüslerine ilişkin etkin bir denetim izi mekanizması oluşturulmuş mu?
☐	Oluşturulan denetim izi, kullanıcılara sorumluluk atayan, detay içeren ve şüpheli bir olayı izleme imkânı sunan nitelikte tutulmakta mı?
☐	Denetim izleri asgari bilgileri (işlemi gerçekleştiren uygulama, işlemi gerçekleştiren ve varsa onaylayan kişiler, işlemin açıklaması, yapılan işlemin zaman bilgisi, işlemin olumlu veya olumsuz sonucu, etkilenen veri ve sistemlerin bilgisi) içeriyor mu?
☐	Denetim izlerinin asgari 5 yıl süreyle denetime hazır bulundurulacak şekilde ÖKC TSM Merkezi tarafından saklanacak şekilde planlanmış ve gerekli otomasyon yedekleme sistemleri kurulmuş mu?
☐	Denetim izlerinin bütünlüğünün sağlanması ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için kullanılacak teknikler belirlenmiş ve kullanılmakta mı?
☐	Denetim izleri, yetkisiz değiştirilmeye karşı ayrıcalıklı yetkiye sahip kullanıcıların kendi faaliyetlerine ilişkin denetim izlerine müdahale edemeyeceği şekilde 5651 sayılı kanunda öngörülen elektronik imzalı ve zaman damgalı merkezi kayıt/log sistemi ile ÖKC TSM Merkezi tarafından koruma altına alınmış mı?
☐	Denetim izi mekanizmalarının geçici veya sürekli olarak durdurulmasını önlemeye ve durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılmakta mı?
☐	Bilgi Sistemleri faaliyetleri kapsamında dış hizmet alıyor olması durumunda; ÖKC üreticisi, dış hizmet sağlayıcısı tarafından tutulan denetim izlerinin kendi standartlarına uygunluğunu ve kendisinin bu denetim izlerine erişebilirliğini temin etmiş mi? Süreçler ve kullanılan teknik dokümante edilmiş mi?
☐	ÖKC üreticisi tarafından, denetim izlerinin düzenli olarak gözden geçirilmesine, değerlendirilmesine ve raporlanmasına ilişkin iş süreçleri oluşturulmuş mu?
☐	Denetim izi oluştururken GİB Hassas ÖKC Verilerinin ve Ödeme Sistemi hassas verilerinden herhangi bir kısmının ya da tamamının kullanılmadığı görülmekte mi?

Değerlendirme Sonucu:	***Olumlu*** ☐	***Olumsuz*** ☐	***Belirsiz*** ☐

Ek Açıklama:

*Bu kutu, Değerlendirme Sonucunun "**Belirsiz"** olarak işaretlenmesi durumunda mutlaka doldurulmalıdır.*

TSM_SİS.5 Kontrol Tablosu

ÖKC TSM Merkezi'nin DHS'si olması halinde; aşağıda yer alan "Dış Hizmet Sağlayıcı Olmanın Hususi Gereklilikleri" kurallarına uygunluğu kontrol edilmelidir.

☐	Dış Hizmet Sağlayıcının ISO/IEC 20000, ISO 22301, ISO/IEC 27001 ve PCI DSS belgelerine uyumluluk onay durumunun belgelendirildiği ÖKC üreticisi tarafından yılda 1 defa kontrol ediliyor mu?
☐	Dış Hizmet Sağlayıcısının merkezi (birincil) sistemi yurt içinde mi?
☐	Dış Hizmet Sağlayıcılarının ikincil sistemi de yurt içinde, birincil sistemden farklı bir il sınırları içinde ve aralarında en az 300 km mesafe bulunacak şekilde kurulmuş mu?
☐	Dış Hizmet Sağlayıcı, TSM birincil merkezinin donanım altyapısını, dış kaynak kullanımı ve barındırma hizmeti şeklinde başka bir alt yükleniciden/taşerondan sağlamamış durumda mı?
☐	Birincil merkezin tüm işletim ve operasyon süreçlerini Dış Hizmet Sağlayıcı kendi personeli ile yürütür durumda mı? Bu durum yazılı olarak belirtilmiş mi?
☐	İkincil merkezin tüm işletim ve operasyon süreçlerini Dış Hizmet Sağlayıcı kendi personeli ile yürütür durumda mı?
☐	ÖKC TSM Merkezi, ikincil merkezlerini taşerondan / alt yükleniciden temin ediyorsa, tüm işletim ve operasyon süreçlerini Dış Hizmet Sağlayıcı kendi personeli ile yürütür durumda olduğu belirtilmiş mi?

Değerlendirme Sonucu: ***Olumlu*** ☐ ***Olumsuz*** ☐ ***Belirsiz*** ☐

Ek Açıklama:

*Bu kutu, Değerlendirme Sonucunun "**Belirsiz"** olarak işaretlenmesi durumunda mutlaka doldurulmalıdır.*

4.3. Paydaş İletişimi ve İş Kurgusu Değerlendirme Sınıfı (TSM_ILT)

Bu değerlendirme sınıfı, ÖKC TSM Merkezlerinin YN ÖKC yönetimi çerçevesinde iletişim içerisinde olduğu, ÖKC Üreticisi, Üye İşyeri Anlaşması Yapan Kuruluşlar ve Katma Değerli Hizmet sağlayıcı kuruluşlar ile ilişki yönetiminin gerekliliklere uygunluğunun kontrol edilmesini amaçlamaktadır.

Değerlendirme Sınıfı Alt Bileşenleri;

Bu değerlendirme sınıfı, 2 alt bileşenden oluşmaktadır;

TSM_ILT.1 Bu değerlendirme bileşeninde değerlendiriciden; ÖKC TSM Merkezinin YN ÖKC üreticisi ile arasındaki yetki ve sorumluluk paylaşımının, gerekli yazılı kabul kurallarına uygun gerçekleştirildiğinin kontrolü beklenmektedir.

TSM_ILT.2 Bu değerlendirme bileşeninde değerlendiriciden, ÖKC TSM Merkezinin Üye İş yeri Anlaşması Yapan Kuruluşlar ve Katma Değerli Hizmet sağlayıcı kuruluşlar ile arasındaki anlaşma uyarınca, YN ÖKC yaşam döngüsü kapsamındaki yazılım geliştirme, yükleme, güncelleme, parametre yükleme, kartlı işlemlerin yönetimi, güvenli anahtar yönetimi, terminal güvenlik kontrolleri, işlemlerin yönlendirilmesi, çalıştırılması, sonuçlarının izlenmesi ile iş sürekliliği kapsamında rapor isterlerini gerekliliklere uygun sağladığının kontrolü beklenmektedir.

TSM_ILT.1 Kontrol Tablosu

TSM Merkezi'nin aşağıda yer alan "YN ÖKC Üreticisi ile İletişim" kurallarına uygunluğu kontrol edilmelidir.

☐	YN ÖKC üreticisi ve ÖKC TSM Merkezi arasındaki ilişkilerin yetki sorumluluklarının kabulü yazılı olarak mevcut mu?
☐	YN ÖKC'lerin yaşam döngüsünün (Terminal ve Mesaj Yönetim Sistemi) ve ÖKC TSM Merkezinin yönetim, yetki ve sorumluluğunun ÖKC üreticilerinde olduğu hakkında taahhütname alınmış mı?
☐	ÖKC TSM Merkezi hizmetlerini kısmen veya tamemen Dış Hizmet Sağlayıcıdan temin etmesi durumunda ÖKC üreticisinin, sağlanan DHS hizmetlerine ilişkin taahhütname alınmış mı?

Değerlendirme Sonucu: ***Olumlu*** ☐ ***Olumsuz*** ☐ ***Belirsiz*** ☐

Ek Açıklama:

*Bu kutu, Değerlendirme Sonucunun "**Belirsiz**" olarak işaretlenmesi durumunda mutlaka doldurulmalıdır.*

Uygulama Notu 8: Yetki, sorumluluk paylaşımına ilişkin taahhütname, sözleşme, anlaşma ve benzeri diğer yazılı kabuller 5.2. bölümünde yeralan Değerlendirme Sonuç Raporu ekinde yer almalıdır.

TSM_ILT.2 Kontrol Tablosu

TSM Merkezi'nin aşağıda yer alan "Üye İş Yeri Anlaşması Yapan Kuruluşlar ve Katma Değerli Hizmetler" kurallarına uygunluğu kontrol edilmelidir.

☐	YN ÖKC'ler Üye İşyeri Anlaşması Yapan Kuruluşlar ile ÖKC TSM Merkezi üzerinden haberleşmekte mi?
☐	ÖKC TSM Merkezinden hizmet almakta olan Üye İşyeri Anlaşması Yapan Kuruluşlara 15 gün önceden gerekçeleri ile birlikte bildirilmesi zorunluluğu ve planlı kesintilerin günün yoğun olmayan saatlerinde gerçekleştirilmesi için süreç oluşturulmuş mu?
☐	ÖKC TSM Merkezi aylık olarak kullanılabilirlik/erişlebilirlik/başarım raporunun hazırlanarak, GİB ve ÖKC TSM Merkezi hizmeti almakta olan Üye İşyeri Anlaşması Yapan Kuruluşlara sunulması için süreç oluşturulmuş mu?
☐	ÖKC TSM Merkezi aylık olarak SLA/KPI raporunun hazırlanarak, GİB'e ve ÖKC TSM Merkezi hizmeti almakta olan Üye İşyeri Anlaşması Yapan Kuruluşlara sunulması için süreç oluşturulmuş mu?
☐	Üye İşyeri Anlaşması Yapan Kuruluşun YN ÖKC yaşam döngüsü kapsamındaki yazılım geliştirme, yükleme, güncelleme, parametre yükleme, kartlı işlemlerin yönetimi, güvenli anahtar yönetimi, terminal güvenlik kontrolleri, işlemlerin yönlendirilmesi, çalıştırılması ve sonuçlarının sözleşmelere ve sözleşmelerde belirtilen kriterlere (SLA-Service Level Agreement) uygun şekilde iletilmesi vb. faaliyetlerinin yetki ve sorumluluğun ÖKC üreticilerinde olduğunun kabul edildiği anlaşmalar yapılmış mı?
☐	Üye İş yeri anlaşması yapan kuruluş, hizmet aldığı ÖKC TSM Merkezinin PCI DSS ile uyumlu olduğuna ve işlem altyapısının güvenlik seviyesini düşürmediğine ilişkin, gerçekleştirdiği denetimlerden veya geçerliliğini yitirmemiş denetim raporu, sertifika gibi belgelerden faydalanarak makul güvence oluşturmakta mı?
☐	Üye İşyeri Anlaşması Yapan Kuruluşlar tarafından, sahtecilik ve dolandırıcılık faaliyetlerinin önlenmesine yönelik olarak, anlaşması bulunan üye işyerleri ve YN ÖKC'ler için takip mekanizmaları tesis edilmiş mi?
☐	YN ÖKC üreticilerinin oluşturduğu sahtekârlık senaryolarına göre otomatik izleme mekanizmalarını ve raporlamalara uygun şekilde sahtekârlık önleme ve izleme sistemini kurulmuş mu?
☐	EFT-POS özellikli YN ÖKC'ler ile PinPad bağlanmış Basit/Bilgisayar Bağlantılı YN ÖKC'lerde terminal yönetim ve Üye İşyeri Anlaşması Yapan Kuruluşlar ile iletişim, YN ÖKC ve ÖKC TSM Merkezi üzerinden şifreli olarak, GMP'lerde belirtilen kurallara göre gerçekleştirilmekte mi?

☐	ÖKC TSM Merkezi, EFT-POS cihazı verilerini Üye İşyeri Anlaşması Yapan Kuruluşlara şifreli olarak iletiyor mu?
☐	İade ve İptal durumlarında işlemler EFTPOS cihazından (Harici EFT POS cihazları için) başlamakta ve EFTPOS cihazı kart veren banka ile ÖKC TSM Merkezi üzerinden haberleşmekte mi?
☐	ÖKC TSM Merkezi, GİB ve yasalarca yetkili kılınmış diğer kurumlardan gelen talimatlar doğrultusunda YN ÖKC'lerin fonksiyonlarını veya belli bir kısmını uygun denetim izleri bırakarak durdurabilir veya değiştirebilir durumda mı?
☐	Var ise, yönetilen Katma Değerli Hizmet uygulamaları YN ÖKC kullanan mükellefler (üye işyeri) adına ve bir sözleşmeye bağlı olmak koşulu ile mi geliştirilmiş?
☐	Üye İşyeri anlaşması yapan kuruluş ile ÖKC Üreticisi ve ÖKC TSM Merkezi hizmetini veren kuruluş arasında yapılacak olan sözleşmelerde; işlenecek, saklanacak ve raporlanacak olan verilerin içeriği, saklama süresi, gizlilik kuralları ile ilgili yetki ve kapsamın açıkça belirtilmiş mi?
☐	Sözleşmelerin elektronik ortamdaki bir örneğinin, sözleşmenin imzalandığı tarihten itibaren 15 gün içinde GİB'e elektronik ortamda aktarılması sağlanmakta mı?

Değerlendirme Sonucu: ***Olumlu*** ☐ ***Olumsuz*** ☐ ***Belirsiz*** ☐

Ek Açıklama:

*Bu kutu, Değerlendirme Sonucunun "**Belirsiz**" olarak işaretlenmesi durumunda mutlaka doldurulmalıdır.*

Uygulama Notu 9: Üye İşyeri anlaşması yapan kuruluş ve/veya Katma Değerli Hizmet sağlayıcı kuruluşun ÖKC Üreticisi ve ÖKC TSM Merkezinden hizmet satın almasına ilişkin taahhütname, sözleşme, anlaşma, süreç ve benzeri diğer yazılı kabuller 5.2. bölümünde yeralan Değerlendirme Sonuç Raporu ekinde yer almalıdır.

4.4. YN ÖKC Cihaz ve Mesaj Yönetim Değerlendirme Sınıfı (TSM_YOKC)

Bu değerlendirme sınıfı, ÖKC TSM Merkezlerinin YN ÖKC üzerinde çalışan mali uygulama, üye işyerleri anlaşması yapan kuruluşlara ait uygulama veya katma değerli hizmet sağlayıcıların uygulama yazılımlarının ayrıca YN ÖKC parametrelerinin cihaza yüklenmesi ve versiyon takibinin gerekliliklere uygun sağlandığının ve YN ÖKC mesajlarının isterlere uygun yönetildiğinin kontrol edilmesini amaçlamaktadır.

Değerlendirme Sınıfı Alt Bileşenleri;

Bu Değerlendirme Sınıfı, 2 alt bileşenden oluşmaktadır;

TSM_ILT.1 Bu değerlendirme bileşeninde değerlendiriciden; ÖKC TSM Merkezinin YN ÖKC cihazı yazılım ve parametre yönetiminin, gerekli iz kayıtları ile takip edilmek şartı ile sağlandığı ve cihaza yüklenen uygulama yazılım ve parametrelerin geriye dönük incelenebildiğinin diğer isterler ile birlikte kontrolünü sağlaması beklenmektedir.

TSM_ILT.2 Bu değerlendirme bileşeninde değerlendiriciden, ÖKC TSM Merkezlerinin YN ÖKC'den gelen her bir mesaj için gerekli tutarlılık kontrollerini sağladığı, tutarsızlık ve atak içeren mesajları yönetebildiğinin kontrolü beklenmektedir.

TSM_OKC.1 Kontrol Sınıfı

ÖKC TSM Merkezi'nin aşağıda yer alan "YN ÖKC Cihazı Yazılım ve Parametre Yönetimi" kurallarına uygunluğu kontrol edilmelidir.

☐	YN ÖKC cihazının her açılışta ve Z raporu sonrasında parametre ya da yazılım yükleme işlemi olup olmadığına ait sorgulama yaptığı ÖKC TSM Merkezi tarafında izlenebiliyor mu?
☐	ÖKC TSM Merkezi loglarında ya da işlem kayıtlarının gerçekleştirildiği alanlarda (veritabanı) mesajın alındığı ve işlendiğini gösteren kayıtların bulunduğu izlenebiliyor mu?
☐	Yazılım Yükleme Adımları ya da Parametre Yükleme Adımlarının başarılı bir şekilde takip edildiği ve ÖKC TSM Merkezi'nin terminale yüklenmesi gereken yazılım ve parametre listesini terminale ilettiği izlenebiliyor mu?
☐	ÖKC TSM Merkezinden gönderilen parametre ya da yazılım bilgilerinin iletildiği izlenebiliyor mu?
☐	YN ÖKC'nin hangi versiyon ile çalıştığı bilgisi ÖKC TSM Merkezi üzerinden izlenebiliyor mu?
☐	Üye İşyeri Anlaşması Yapan Kuruluşun, YN ÖKC ile birlikte çalışacak uygulamaları ve bunlara ilişkin parametre, anahtar yazılım yükleme ve ihtiyaç duyulan diğer işlemleri ÖKC TSM Merkezi üzerinden yapılmakta mı?
☐	Yükleme işlemine (YN ÖKC yazılım versiyonu veya Üye işyeri kuruluşa ait yazılım) ait bilgilerin log ve/veya ÖKC TSM Merkezi veritabanında tutulduğu ve işlemler ile güncellendiği izlenebiliyor mu?
☐	İşlemin kim (user, sysuser, application user vb.) tarafından gerçekleştirildiği bilgisi görülüyor mu?
☐	Yüklenen uygulama sürüm ve yükleme tarih ve saati bilgilerinin bu kayıtlarda bulunduğu izlenebiliyor mu?
☐	Yükleme işleminde tüm uygulamaların ÖKC TSM Merkezi tarafından imzalandığı izlenebiliyor mu?
☐	ÖKC TSM Merkezi üzerinden yapılmakta olan parametre, anahtar yazılım yükleme işlemlerine ilişkin işlem log ve yüklenen yazılım bilgileri kayıt altına alınmakta mı?
☐	Parametre yükleme isteğinin tetiklendiği ana birime (ÖKC üreticisi ya da GİB vb olabilir) ait parametre bloğunun, cihaza yüklendiğine ilişkin ana birime geri bildirim sağlanıyor mu ve/veya yükleme işlemine ait status bilgileri gerektiği zaman kontrol edilebiliyor mu?

Değerlendirme Sonucu:	***Olumlu*** ☐	***Olumsuz*** ☐	***Belirsiz*** ☐
Ek Açıklama:			
*Bu kutu, Değerlendirme Sonucunun "**Belirsiz"** olarak işaretlenmesi durumunda mutlaka doldurulmalıdır.*			

TSM_OKC.2 Kontrol Tablosu

ÖKC TSM Merkezi'nin aşağıda yer alan "YN ÖKC Mesajlarının Yönetimi" kurallarına uygunluğu kontrol edilmelidir.

☐	YN ÖKC'den gelen her bir mesaj için ÖKC Durum Verisi, ÖKC TSM Merkezinde tutarlılık kontrollerinden geçirilmekte mi?
☐	GİB Hassas ÖKC verisi ÖKC TSM Merkezi üzerinden GİB BS'ye GMP'lere uygun olarak ve anahtarları korunarak iletilmekte mi?
☐	ÖKC TSM Merkezi YN ÖKC ilklendirilmesiyle birlikte her mesaj için mesaj işlem kontrolleri yapmakta mı? (Mesajların sıralamaları uyumlu ve tutarlı mı? Mesaj formatları uyumlu ve tutarlı mı? Mesajların geliş kaynakları bilgileri uyumlu ve tutarlı mı? Mesajların zaman bilgileri uyumlu ve tutarlı mı?)
☐	Tutarsızlık ve atak içeren (bilinmeyen anahtar ya da ömrü dolmuş anahtar ile gelen mesajlar vb.) mesajlar TSM Merkezi tarafından geçersiz mesaj kabul edilmekte mi?
☐	Tutarsız ve atak içeren mesajlar gerekli araştırmaya tabi tutulmadan ve ÖKC Üreticilerince YN ÖKC üzerinde düzeltme işlemleri yapılmadan GİB BS'ye iletilmeyeceği teyit edilmiş mi?
☐	Gerçekleştirilen işlem kayıtlarının status bilgileri hata kodlarını ve açıklamasını açık ve net şekilde belli ediyor mu?
☐	Gerçekleştirilen işlem kayıtlarında YN ÖKC bilgileri bulunuyor mu?
☐	Gerçekleştirilen işlemin kim (user, sysuser, application user)tarafından gerçekleştirildiği bilgisi görülüyor mu?

Değerlendirme Sonucu: ***Olumlu*** ☐ ***Olumsuz*** ☐ ***Belirsiz*** ☐

Ek Açıklama:

*Bu kutu, Değerlendirme Sonucunun "**Belirsiz**" olarak işaretlenmesi durumunda mutlaka doldurulmalıdır.*

5. EKLER

5.1. 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.

5.1.1. Kritik Varlıklar

5.1.1.1. Birincil Varlıklar

Birincil varlıklar GİB BS'nin ÖKC TSM Merkezinden yönlendirilirken ya da ÖKC TSM Merkezinde bulunurken korumasını istediği varlıklardır.

5.1.1.1.1. Z Raporu

YN ÖKC'den GİB BS'ye GMP dokümanlarında tanımlandığı gibi gizliliği ve bütünlüğü korunacak şekilde gönderilmektedir. Gizlilik ve bütünlüğün korunması YN ÖKC ve GİB BS arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır. ÖKC TSM Merkezi bu varlık için yönlendirme işlemini yürütmektedir.

5.1.1.1.2. YN ÖKC Fiş Bilgisi

YN ÖKC'den GİB BS'ye GMP dokümanlarında tanımlandığı gibi gizliliği ve bütünlüğü korunacak şekilde gönderilmektedir. Gizlilik ve bütünlüğün korunması YN ÖKC ve GİB arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır.TSM bu varlık için yönlendirme işlemini yürütmektedir.

5.1.1.1.3. YN ÖKC Fiş İptal Bilgisi

YN ÖKC'den GİB BS'ye GMP dokümanlarında tanımlandığı gibi gizliliği ve bütünlüğü korunacak şekilde gönderilmektedir. Gizlilik ve bütünlüğün korunması YN ÖKC ve GİB arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır. ÖKC TSM Merkezi bu varlık için yönlendirme işlemini yürütmektedir.

5.1.1.1.4. Para Birimi Çevrim Oranları

GİB BS'den ÖKC TSM Merkezine GMP dokümanlarında tanımlandığı gibi bütünlüğü ve inkâr edilemezliği korunacak şekilde gönderilebilmektedir. Bütünlüğün korunması GİB BS ve ÖKC TSM Merkezi arasında kurulan güvenli kanallar (VPN) vasıtasıyla yapılmaktadır.

İnkâr edilemezliğin korunması GİB'in imzası ile sağlanmaktadır.

YN ÖKC, ÖKC TSM Merkezinden GMP dokümanlarında tanımlandığı gibi bütünlüğü korunacak şekilde almaktadır. Bütünlüğün korunması ÖKC TSM Merkezi ve YN ÖKC arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır. ÖKC TSM Merkezi bu varlığı açık olarak görebilmektedir.

5.1.1.1.5. Olay Kayıtları

Olay Kayıtları, ÖKC TSM Merkezi üzerinden GİB BS ile paylaşılmaktadır. YN ÖKC'den GİB BS'ye GMP dokümanlarında tanımlandığı gibi gizliliği ve bütünlüğü korunacak şekilde gönderilmektedir. Gizlilik ve bütünlüğün korunması YN ÖKC ve GİB arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır. ÖKC TSM Merkezi bu haberleşmede varlığı sadece yönlendirmektedir.

5.1.1.1.6. Haberleşme Tablosu

YN ÖKC TSM'den GMP dokümanlarında tanımlandığı gibi gizliliği ve bütünlüğü korunacak şekilde almaktadır. Gizliliğin ve bütünlüğün korunması ÖKC TSM Merkezi ve YN ÖKC arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır. ÖKC TSM Merkezi bu varlığı oluşturmaktadır.

5.1.1.1.7. Parametre Tablosu

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

YN ÖKC, ÖKC TSM Merkezinden GMP dokümanlarında tanımlandığı gibi bütünlüğü korunacak şekilde almaktadır. Bütünlüğün korunması ÖKC TSM Merkezi ve YN ÖKC arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır. ÖKC TSM Merkezi bu varlığı açık olarak görebilmektedir.

5.1.1.1.8. İstatistik Verileri

YN ÖKC'den GİB BS'ye GMP dokümanlarında tanımlandığı gibi gizliliği ve bütünlüğü korunacak şekilde gönderilmektedir. Gizlilik ve bütünlüğün korunması YN ÖKC ve GİB arasında paylaşılan kriptografik anahtarlar vasıtasıyla yapılmaktadır. ÖKC TSM Merkezi bu haberleşmede varlığı yönlendirmektedir.

5.1.1.1.9. YN ÖKC Yazılımı

YN ÖKC, 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.

5.1.1.2. İkincil Varlıklar

Birincil varlıkları korumak için ÖKC TSM Merkezinin kullandığı varlıklardır.

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

5.2. Değerlendirme Sonuç Raporu Formatı

Değerlendirme Alt Bileşeni		Değerlendirme Sonucu		
TSM_SER	TSM_SER.1	*Olumlu* ☐	*Olumsuz* ☐	*Belirsiz* ☐
	TSM_SER.2	*Olumlu* ☐	*Olumsuz* ☐	*Belirsiz* ☐
TSM_SIS	TSM_SIS.1	*Olumlu* ☐	*Olumsuz* ☐	*Belirsiz* ☐
	TSM_ SIS.2	*Olumlu* ☐	*Olumsuz* ☐	*Belirsiz* ☐
	TSM_ SIS.3	*Olumlu* ☐	*Olumsuz* ☐	*Belirsiz* ☐
	TSM_ SIS.4	*Olumlu* ☐	*Olumsuz* ☐	*Belirsiz* ☐
	TSM_ SIS.5	*Olumlu* ☐	*Olumsuz* ☐	*Belirsiz* ☐
TSM_ILT	TSM_ILT.1	*Olumlu* ☐	*Olumsuz* ☐	*Belirsiz* ☐
	TSM_ILT.2	*Olumlu* ☐	*Olumsuz* ☐	*Belirsiz* ☐
TSM_OKC	TSM_OKC.1	*Olumlu* ☐	*Olumsuz* ☐	*Belirsiz* ☐
	TSM_OKC.2	*Olumlu* ☐	*Olumsuz* ☐	*Belirsiz* ☐