e-BELGE ÖZEL ENTEGRATÖRLERİ BİLGİ SİSTEMLERİ DENETİMİ KILAVUZU

Kasım 2019

Versiyon	Yayım Tarihi	Açıklama
1.0	19.11.2019	Kılavuzun ilk yayımı

İçindekiler

1. Tanımlar

a) Bağımsız denetim: Bankacılık ve Sermaye Piyasası Mevzuatı çerçevesinde bilgi sistemlerine yönelik bağımsız denetim faaliyetini,
b) Bağımsız denetim kuruluşu: Bankacılık ve Sermaye Piyasası Mevzuatı çerçevesinde bilgi sistemleri denetimi yapma yetkisine haiz bağımsız denetim kuruluşlarını,
c) Hizmet: 213 sayılı Vergi Usul Kanunu ve 509 Sıra Nolu VUK GT uyarınca elektronik ortamda oluşturulmasına imkan verilen belgelerin (e-Belgeler) oluşturulma, imzalanma, iletilme veya saklanmasına ilişkin hizmetleri (Özel entegratörler, bu hizmetlerin bir kısmını veya tamamını veriyor olabilir),
d) BİS Raporu: Özel entegratör olmak için yapılan başvuruda hazırlanan Bilgi İşlem Sistemleri raporunu,
e) COBIT: Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) Bilgi Sistemleri Yönetişim Enstitüsü (ITGI) tarafından yayınlanmış olan Bilgi Teknolojilerine İlişkin Kontrol Hedefleri'nin (COBIT) denetim döneminin başlangıcı itibariyle güncel versiyonunu (en az 4.1 veya 5 versiyonu),
f) Denetçi: Bilgi sistemleri süreçlerinin denetimini yapmak üzere bağımsız denetim kuruluşları tarafından görevlendirilmiş denetçiyi,
g) Denetlenen: Özel entegratör kuruluşlarını,
h) Denetim izi: Bilgi sistemlerinde işlenen bir verinin bir sürecin başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtları,
i) Elektronik imza (e-İmza): 15/01/2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu'nda tanımlanan elektronik imzayı,
j) GİB: Gelir İdaresi Başkanlığını,
k) Güvenlik duvarı: Farklı güvenlik hassasiyet düzeylerine sahip ağlar arasında kontrollü geçişe imkân tanıyan yazılım ya da donanım temelli çözümleri,
l) 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 cihazı,
m) Kontrol: Bilgi sistemlerinin hedeflerinin gerçekleştirilmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli derecede güvenceyi oluşturma amacı güden politikalar, prosedürler, uygulamalar ve organizasyonel yapıların tamamını,
n) Kontrol hedefi: Belirli bir bilgi sistemleri aktivitesi içinde kontrol prosedürleri oluşturarak istenen bir sonucun veya bir amacın gerçekleştirilmesini sağlayan COBIT'teki kontrol hedeflerini,
o) ISO/IEC 20000: Bilgi Teknolojileri Servis Yönetimi Standardını,
p) ISO 22301: Uluslararası İş Sürekliliği Yönetimi Standardını,
q) ISO/IEC 27001: Bilgi Güvenliği Yönetim Sistemi Standardını,
r) Özel entegratör: 509 Sıra No.lu VUK GT uyarınca elektronik ortamda oluşturulmasına imkan verilen belgelerin (e-Belgeler) oluşturulma, imzalanma, iletilme veya saklanmasına ilişkin hizmeti vermek üzere GİB'den yetki almış kuruluşları,
s) ÖEBSD: Özel entegratör kuruluşları bilgi sistem süreçleri denetimini,
t) Sızma testi: Sistemin güvenlik açıklarını istismar edilmeden önce tespit etmek ve düzeltmek amaçlı gerçekleştirilen atakları,

İfade eder.

2. Amaç ve Kapsam

Bu Kılavuz, 509 Sıra No.lu Vergi Usul Kanunu Genel Tebliğinde belirtilen e-Belge uygulamaları kapsamında, GİB'den izin alan/alacak olan Özel Entegratör kuruluşlarının e-Belge uygulamaları ile ilgili özel entegratörlük faaliyet ve süreçlerine ilişkin bilgi sistemlerinin Başkanlıkça bu Kılavuzda belirtilen isteklerin karşılanıp karşılanmadığına yönelik bilgi sistemleri bağımsız denetim faaliyetinin gerçekleştirilmesine ve özel entegratör kuruluşlar nezdindeki sonuçlarına ilişkin usul ve esasları belirlemek üzere hazırlanmıştır.

Kılavuz, özel entegratörlerin bugüne kadar kullandıkları ve kullanmaya devam edecekleri veri standardı ve yazılım altyapısına ilişkin düzenlemeleri değiştirmemekte veya herhangi birisinin yerini almamaktadır. Özel entegratörler yenileri yayınlanıncaya kadar aynı veri standartlarında ve yazılım altyapılarında mevcut düzenlemelere uymaya devam edecektir.

ÖEBSD sonucuna göre özel entegratör için uygulanacak yaptırımlar bu Kılavuzun ilerleyen bölümlerinde açıklanmıştır.

3. Denetim ve Onay Süreci

Bu Kılavuzun yayım tarihinden itibaren yapılacak Özel entegratörlük başvurularında, özel entegratör kuruluş adaylarının bu Kılavuzda belirtilen ÖEBSD'yi yaptırmış olması ve başvuru dosyasına "ÖEBSD Görüş Yazısı ve Raporunu" eklemiş olması zorunludur.

Ayrıca hali hazırda bu Kılavuzun yayım tarihi itibariyle özel entegratör kuruluş yetkisi almış olanlar ile test ve değerlendirme süreçleri devam edenler; ÖEBSD'yi yaptırmaları için bu Kılavuzun yayım tarihinden başlamak üzere ilk denetimlerini yaptırmak üzere 31/12/2020 tarihine kadar süre verilmiştir.

Başkanlıkça özel entegratörlük izni verilen firmalar tarafından kurulan sistemlerin bağımsız denetimi bu Kılavuza uygun olarak bağımsız denetim kuruluşlarınca yerine getirilecektir.

Bakanlık ya da Başkanlık gerek görmesi durumunda, bu Kılavuz kapsamında e-Belge Özel Entegratörlerinin kurmuş olduğu altyapı sistemlerini dilediği anda ve dilediği şekilde denetleyebilir ya da denetletebilir.

Özel entegratör kuruluşları, bilgi sistemleri denetimini (ÖEBSD), bu Kılavuzda açıklanan özel entegratör bilgi sistemleri gereksinimlerine göre bu bölümün ilk iki paragrafında belirtilen ilk denetim haricinde, ilk denetim tarihini takip eden 2 yılda bir yaptırmak zorundadır. Bu çerçevede, tanzim olunan bağımsız denetim raporları rapor tarihinden itibaren en fazla 2 yıl süre ile geçerli olup, söz konusu sürenin bitiminden önce yeni bağımsız denetim raporunun GİB'e ibrazı zorunludur.

Özel entegratör kuruluşlar veya adayları, denetim tarihinden en az 1 ay önce güncellenmiş BİS raporunu üzerinde tarih ve güncel sürüm numarası olmak kaydıyla, GİB'e ve denetimi gerçekleştirecek bağımsız denetim kuruluşuna gönderir.

Bağımsız denetim kuruluşları tarafından gerçekleştirilen ÖEBSD'nin sonuçları, "**ÖEBSD Görüş Yazısı ve Raporuyla**" kayıt altına alınır.

ÖEBSD'nin sonucu (görüş yazısı ve raporu), rapor tarihinden itibaren en geç 15 gün içinde GİB'e yazılı olarak gönderilir. Denetçi, olumlu, şartlı veya olumsuz görüş bildirebileceği gibi, görüşten kaçınabilir. ÖEBSD raporunda bir sonraki denetime kadar tamamlanması gereken eksiklikler, veyadaha kısa süre içerisinde ve ancak ek bir denetimle tamamlandığı teyit edilmesi gereken eksiklikler bulunması halinde ilgili rapora açıkça yazılır.

GİB, yetkilendirilmiş özel entegratörler veya ilk başvuru aşamasında olanlara ilişkin denetim sonuçlarını ebelge.gib.gov.tr adresinde yayınlayabilir.

Belirlenen süreler içerisinde ÖEBSD sonucu Başkanlığa ulaşmamış olan özel entegratörler ile özel entegratör adaylarının izinleri/başvuruları önce askıya alınır ve bu durum ebelge.gib.gov.tr

adresinden duyurulur. Bunun üzerine özel entegratöre denetim raporlarını teslim etmesi için 6 ay ek süre verilir. Bu süre zarfında da denetim raporlarını teslim etmeyen ya da edemeyen özel entegratörün izni iptal edilir.

Bu Kılavuzun; 4. Bölümünde özel entegratör bilgi sistemlerindeki "**Kritik Varlıklar ve Aktörler**", 5. Bölümünde "**Fiziki Güvenlik Şartları ve Tedbirleri**", 6. Bölümünde "**Sızma Testleri**", 7.Bölümünde "**Risk Yönetimi**", 8.Bölümünde "**İş Sürekliliği ve FKM Yönetimi**", 9. Bölümünde "**Değişiklik Yönetimi**", 10. Bölümünde "**Denetim İzlerinin Oluşturulması ve Saklanması**", 11.Bölümünde "**Dış Hizmet Alımı**", 12. Bölümünde "**Personelin Niteliğine İlişkin Gereksinimler**", 13. Bölümünde "**Uluslararası Standartlara İlişkin Sertifikasyonlar**", 14. Bölümünde "**Özel EntegratörünÖEBSD'ye İlişkin Sorumlulukları**", 15. Bölümünde "**ÖEBSD Raporunun İçeriği ve Oluşturulması**", 16. Bölümünde "**ÖEBSD Raporuna Bağlı Olarak GİB Tarafından Uygulanacak Yaptırımlar**", 17. Bölümünde "**ÖEBSD Değerlendirme Sınıfları**" yer almıştır. Kılavuz ekleri olan; EK-1'de "ÖEBSD Değerlendirme Sınıfları Kontrol Tabloları", EK-2'de "**Denetçinin Görüşünü Oluşturması İçin Kılavuz**", EK-3'de "**ÖEBSD Rapor Formatı**", EK-4'de "**Olumlu, Şartlı, Görüşten Kaçınma ve Olumsuz Görüş Yazısı Şablonları**" bulunmaktadır.

4. Kritik Varlıklar ve Aktörler

Sistemde var olan ve ifşa olması veya değişikliğe uğraması durumunda sistemin gizliliğini, bütünlüğünü, kaynak/kimlik doğruluğunu veya 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.

4.1. Kritik Varlıklar

Sistemde var olan ve ifşa olması veya tahrif edilmesi durumunda sistemin gizliliğini, bütünlüğünü, kaynak/kimlik doğruluğunu veya erişilebilirliğini olumsuz yönde etkileyecek varlıklardır. Aşağıda birincil veya ikincil düzeyde sayılmamış dahi olsa, burada tanımlanan sonuca yol açabilecek her türlü nitelik kritik varlık kapsamında değerlendirilir.

4.1.1. Birincil Varlıklar

Birincil varlıklar, özel entegratör tarafından üretilen veya saklanan ve GİB ile paylaşılan ve en az 10 yıl süreyle korunması gereken varlıklardır. Birincil varlıkların bu süre sonunda sistemden silinmeleri ancak silme kayıtlarının tutulmasıyla mümkündür.

4.1.1.1. Mükellef/Kullanıcı Bilgileri

Mükellefler/kullanıcılara ait her türlü özel bilginin gizliliği ve bütünlüğü 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 213 Sayılı Vergi Usul Kanununun 5 inci maddesi ile 509 sıra no.lu VUK Genel Tebliği kapsamında yapılan düzenlemelere uygun olarak korunmalıdır.

4.1.1.2. İşlem Kayıtları

Özel entegratör, GİB ile arasında çalışan Veri Aktarım Protokolü ve mükellef ile arasında çalışan güvenli haberleşme protokolüne dair tüm işlem kayıtlarını, bütünlüğünü de koruyacak biçimde 10 yıl süreyle saklar.

4.1.1.3. Güvenli Haberleşmeye Dair Parametreler

Özel entegratör, GİB ile arasında çalışan Veri Aktarım Protokolü ve mükellef ile arasında çalışan haberleşme protokolüne dair tuttuğu güvenlik parametrelerini, bu parametrelere erişim yetkilerini ve bunların (parametrelerin görüntülenmesi, güncellenme sıklığı vb.) korunmasını sağlar.

4.1.1.4. Verilen Hizmetlere Ait Bilgiler

4.1.1.4.1. e-Fatura Bilgileri

Düzenlenen her e-Fatura ve uygulama yanıtında yer alan bilgilerin tamamının gizliliği ve bütünlüğü korunmalıdır. GİB'e gönderilen zarf ve belgede yer alan verilerle özel entegratörde ayrıştırılmış dahi olsa tutulan veriler bir ve aynı olmalıdır.

4.1.1.4.2. e-Arşiv Bilgileri

Düzenlenen her e-Arşiv Fatura, e-SMM, e-MM, e-Bilet vb. altyapıda işleyen elektronik belgeler ve oluşturulan her e-Arşiv raporunda yer alan bilgilerin tamamının gizliliği ve bütünlüğü korunmalıdır. GİB'e gönderilen belgede yer alan verilerle özel entegratörde ayrıştırılmış dahi olsa tutulan veriler bir ve aynı olmalıdır.

4.1.1.4.3. e-İrsaliye Bilgileri

Düzenlenen her e-İrsaliye ve irsaliye yanıtında yer alan bilgilerin tamamının gizliliği ve bütünlüğü korunmalıdır. GİB'e gönderilen zarf ve belgede yer alan verilerle özel entegratörde ayrıştırılmış dahi olsa tutulan veriler bir ve aynı olmalıdır.

4.1.1.4.4. e-Belge Saklama

GİB tarafından saklama hizmeti verme izni almış firma, mükellefin e-Belge uygulamaları kapsamında oluşturulan belgelerinin BİS raporuna uygun olarak saklanmasını sağlamalıdır. e-Belgelerin muhafazasının Türkiye Cumhuriyeti sınırları içinde yapılması zorunludur.

4.1.2. İkincil Varlıklar

Birincil varlıkları korumak için özel entegratör tarafından kullanılan varlıklardır. Buna göre, her türlü kriptografik anahtar, kullanıcı adı ve erişim şifresi, bunları tutan HSM gibi özelleşmiş cihazlar, aktif ağ cihazları, sunucular, özel entegratör personelinin kullandığı bilgisayarlar ve bilgi sistemlerinde kullanılan her türlü yazılım ikincil varlıktır.

Bilgi sistemleri ağ ve uygulama topolojileri ile varlıklara erişim için yetkilendirilmiş tüm kullanıcıların isimleri güncel biçimde tutulur. Bu veri için yeterli gizlilik önlemleri alınır. Bu biçimde saklanan liste, çizim, resim ve benzeri her türlü elektronik dosya da ikincil bir varlık olarak değerlendirilir.

4.1.2.1. Aktif Güvenlik Cihazları, Güvenlik Duvarları ve 3. Parti Yazılımlar

Bilgi sistemlerinde kullanılan aktif ağ cihazları, güvenlik duvarları ve sunucu veya kişisel bilgisayarlarda kullanılan her türlü 3. parti yazılımın denetçi tarafından kabul edilebilir sürümleri kullanılmalıdır. Bu kapsamda uygulama bütünlüğü açısından son/güncel sürüm olma şartı aranmaz.

Söz konusu donanım ve yazılımların ilk kurulumunda, güvenlik ayarları yapılmalı, kullanıcı adı ve erişim şifreleri değiştirilmelidir. Söz konusu sistemlerin arıza veya bakım nedeniyle 3. kişilerin erişimine açılması halinde, işlem süresince yeterli gözetimin yapılması ve olay kayıtlarının tutulması gerekir.

4.1.2.2. Kriptografik Donanımların ve Hassas Verilerin Güvenliği

Bilgi sistemlerinde kriptografik anahtarlar ancak özel donanım güvenlik modüllerinde (HSM) bulundurulabilir. Bu cihazlar en az FIPS 140-2 Düzey 3 veya EAL 4+ sertifikası sahibi olmalıdır.

Sistemlerde bulunan ve veri gizliliği amacıyla şifreli tutulan veriler için simetrik şifreleme yönteminde AES 256, asimetrik şifrelemede RSA2048 ve hash algoritmasında SHA-2 kullanılmalıdır. Bu amaçla tutulan kriptografik anahtarlar da HSM cihazlarında tutulmalı ve şifreleme işlemi cihaz üzerinde gerçekleştirilmelidir.

4.1.2.3. Erişim Güvenliği

Bilgi sistemlerinde kullanılan varlıklara elektronik veya fiziki yolla erişim kontrollü sağlanır. Varlığın risk durumuna göre, en az iki yetkili kişinin aynı anda erişimi gerekebilir. En az iki yetkili kişinin aynı anda erişimi, bu amaçla yetkilendirilmiş iki personelin bir arada olması ve ancak art arda doğrulama yapmasıyla varlığa erişim sağlamasıdır. Elektronik erişim için kullanılan şifreler için özel entegratör, tüm kullanıcıların güvenli şifre/parola belirlemesini sağlar. Bir kullanıcının şifresinin en geç 90 günde bir değiştirilmesi sağlanır.

4.2. Aktörler

4.2.1. Yetkili Kullanıcılar

Sisteme veya sistemin herhangi bir bileşenine erişim amacıyla yetkilendirilmiş (kullanıcı adı/parola veya akıllı kartı olan) herkes kullanıcıdır. Yetkili 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 haline dönüşebilir. Yetersiz eğitilmiş, hoşnutsuz, ihmalci, kötü amaçlı, sahtekâr, işine son verilmiş veya işinden ayrılmış olabilirler. Bu kişiler; şantaj yapmak, özel bilgilere erişmek, bilgisayarları bozmak, sahtekârlık veya hırsızlık yapmak, bilgi rüşvetçiliği yapmak, tahrif edilmiş veya sahte 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.

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

Yetkisiz kullanıcılar, sisteme herhangi bir noktadan (kablolu veya kablosuz ağlar üzerinden, kullanıcı bilgisayarlarından, aktif veya pasif yöntemlerle veya fiziki yollarla) 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, yabancı ülke çıkarlarına hizmet etme, özel veya kamu kuruluşlarına, altyapılara veya doğrudan vatandaşlara zarar verme gibi. Saldırganlar amaçlarına erişmek için sosyal mühendislik, sistem açıkları, kriptografik saldırılar, yan kanal saldırıları, üretim sırasında müdahale gibi birçok farklı tekniği kullanabilirler.

5. Fiziki Güvenlik Şartları ve Tedbirleri

Özel entegratörün bilgi sistemleri için, fiziki erişim, uygun iklimlendirme ortamımın sağlanması, yangın, sel ve benzeri doğal afetler için makul uyarı ve korunma tedbirlerinin alınmış olması gerekir. Olaya kısa sürede müdahale için gerekli hazırlıklar yapılmış olmalıdır.

Özel entegratör, bilgi sistemlerinin çalıştığı tüm odalarda asgari ISO standartlarını sağlaması gerekmektedir.

Özel entegratörün bilgi sistemlerinin tamamı veya bir bölümü için dışarıdan hizmet alması, burada sayılan tedbirlerin alınmasına engel teşkil etmez.

6. Sızma Testleri

Özel entegratör aşağıdaki liste kapsamda sızma testi yaptırır:

- Ağ ve İletişim Altyapısı Testleri
- İşletim Sistemi ve Platform Testleri
- Uygulama Testleri
- Veri Tabanı Testleri
- Web uygulamaları testleri
- Mobil uygulama testleri

Sızma testi; bu Kılavuzda tanımlanan varlıkları ve bilgi sistemlerinin genelini kapsayacak şekilde yaptırılır. Sızma testleri yılda en az bir kez olmak üzere tekrarlanır. Sızma testinde varsa tespit edilen açıklara ilişkin alınan tedbirleri, bir takvime bağlanmış eylem planı biçiminde özel entegratör tarafından kayıt altına alınır.

Özel entegratör, bu kılavuzun 3 üncü bölümünde belirtilen ilk denetim haricinde, ÖEBSD sırasında son iki sızma testi raporlarını ve alınan tedbirlerin yer aldığı kayıtları denetçiye ibraz eder.

7. Risk Yönetimi

Özel entegratör, bilgi sistemlerindeki varlıkların tamamı için risk değerlendirmesi yapar. Buna göre, her varlık için olası riskler, risklerin niteliklerine göre sınıflandırılması, risklerin oluşması halinde doğacak zararın derecesi "Risk Değerlendirme Tablosunda" belirlenir.

Risk işleme planı ISO 27001 ve ISO 22301 standartları kapsamında uygulanır. Yönetim Gözden geçirme kapsamında Üst Yönetimin görüş ve onayına sunulur.

- Risk metodolojisi
- Kabul edilebilir risk seviyesi
- Artık riskler
- Risk işleme planı

Onaylanan Risk İşleme Planı'nın ardından, ilgili aksiyonların alınması için Aksiyon Sorumluları faaliyetlerini gerçekleştirir. Her yıl ya da önemli değişikliklerden sonra bir önceki Risk İşleme Planındaki aksiyonların uygulanma durumları ve etkinliği değerlendirilir ve YGG de Üst Yönetime sunulur.

Özel entegratör, YGG raporlarını 10 yıl süreyle saklar. Bu raporlar istenildiğinde GİB'e ibraz edilmek zorundadır.

8. İş Sürekliliği ve FKM Yönetimi

Özel entegratör, verdiği hizmetin kesintisiz ve etkin biçimde yürümesini sağlar. Bu amaçla, İş Sürekliliği ve Acil Durum Prosedürünü hazırlar ve işletir. Bu prosedürün, risk yönetim esasları ve Risk Değerlendirme Tablosuyla ilişkisi kurulmuş olmalıdır.

Bilgi sistemleri planlı yapılan bakımlar hariç aylık %99,75 kullanılabilirlik ile hizmet sunulmasını temin edecek altyapıda olmalıdır. Prosedüre göre, sistemlerin ayakta kalma süreleri izlenir ve kayıt altına alınır. Sistemin performansının 2 ay üst üste veya yılda en az 3 kez hedefin altında kalması durumunda, iyileştirme planı yapılır ve en geç 3 ay içinde devreye alınır. Bu faaliyetlerle ilgili tüm kayıtlar tutulur ve en az 10 yıl süreyle saklanır.

Bilgi sistemlerinde veri tabanı, uygulama sunucuları, aktif ağ cihazları, güvenlik duvarları gibi kritik önemdeki altyapılar aktif yedekli çalıştırılır. Bu durum bilgi sistemleri ağ ve uygulama topolojileri dokümanında açıkça gösterilmiş olmalıdır.

İş sürekliliğin sağlanması amacıyla, önceden belirlenmiş senaryolara göre risklerin gerçekleştiğinin varsayıldığı tatbikatlar yapılır. Yılda bir kez en az iki farklı senaryo için tatbikat yapılır ve kayıt altına alınır. Bu senaryolarda risklerin oluşması, etkileri, dış bağımlılıklar dikkate alınmalı, riskin oluşması durumunda uygulanacak prosedür açık ve uygulanabilir olmalıdır.

Hizmetin kesintiye uğramasının ivedilikle tespiti için acil uyarı sistemleri kurulmalıdır. Mümkün olan her durumda bu sistemler otomatik çalışmalı, e-posta, SMS, acil otomatik çağrı yöntemlerini kullanmalı ve her hâlükârda 7x24 esasına göre işlemelidir.

İş sürekliliğinin ayrılmaz parçası felaket kurtarma merkezidir (FKM). Buna göre özel entegratör, aşağıdaki özellikleri sağlayan bir felaket kurtarma merkezini işletmek zorundadır:

- FKM, coğrafi yönden özel entegratörün merkezinden farklı bir ilde olmalıdır.
- Özel entegratörün veri tabanının en fazla 30 dakika gecikmeyle alınan bir yedeği FKM'de bulunmalıdır.
- FKM, diğer sistem odalarıyla aynı nitelikte fiziksel ve elektronik koruma tedbirleriyle donatılmış olmalıdır.
- Ana sistemlerde kesinti olması halinde özel entegratör hizmeti FKM üzerine alabilecek biçimde FKM'yi yapılandırmış olmalıdır. FKM üzerinden hizmetin verilmesi, bir kesinti başladıktan sonra 6 saati aşmamalı ve ISO 223012'e uygun bir altyapı kurulmuş olmalıdır.

Merkez ile FKM arasında açıklandığı gibi hizmetin geçişini sağlamak üzere hazırlanmış "Acil Durum Eylem Planına" iş sürekliliği prosedüründe yer verilir. Acil Durum Eylem Planında, hangi durumda, kim tarafından, neyin ve nasıl yapılacağını ayrıntılı biçimde açıklanmış olmalıdır.

Özel entegratör, güncel BİS raporunda, burada sayılan şartların üzerinde taahhütlerde bulunmuş ise BİS raporundaki şartları sağlamak zorundadır.

9. Değişiklik Yönetimi

Özel entegratör, hizmetlerinde kullandığı, mükellef ve GİB ile entegrasyonu sağlayan yazılımların değişiklik yönetimini yapar. Buna göre, bu yazılımların geliştirme ortamı, yazılım ve bileşenlerinin tamamını tüm geçmiş sürümlerinin yönetilmesine izin verecek biçimde yapılandırılmalıdır. Yazılım ve bileşenlerinin geçmiş sürümleri ile bunlar üzerinde yapılan değişikliklerin tarihçesi, değişikliğin ne amaçla, kim tarafından ve ne zaman yapıldığı bilgileri mutlaka bulunmak kaydıyla erişilebilir olmalı ve 5 yıl süreyle saklanmalıdır.

Yazılım geliştirme ve test ortamı ve canlı ortam aynı alt ağda yer almamalıdır. Test ortamında kullanılan verilerin, gizlilik haklarına halel getirmeyecek biçimde canlı ortamdan farklılaştırılmış olması gerekir. Test prosedürlerine göre testi tamamlanmış yazılım veya bileşenlerinin canlı ortama aktarılması ancak yetkilendirilmiş personelce yapılabilmelidir. Bu işleme dair kayıtlar, canlı ortama neyin alındığı, işlemin kim tarafından ve ne zaman yapıldığı bilgileri mutlaka bulunmak kaydıyla erişilebilir olmalı ve 5 yıl süreyle saklanmalıdır.

Canlı ortamda çalışan yazılım ve bileşenlerinin bütünlüğünü korumak üzere gerekli tedbirler alınır. Bütünlüğün bozulduğu anlık tespit edilebilmeli ve uyarı verilerek müdahale edilebilmesi mümkün olmalıdır.

10. Denetim İzlerinin Oluşturulması ve Saklanması

Özel entegratör, bilgi sistemlerinde kullandığı her türlü sunucu, veri tabanı, güvenlik duvarı, aktif ağ cihazı ve işletim sistemi kayıtları ile mükellef ve GİB ile haberleşmesinde kullanılan yazılım uygulamalarının veri tabanı motorları ve uygulama kayıtlarını tutar.

Bu kayıtlarda, işleme ilişkin ağ trafiği bilgisine ek olarak asgari aşağıdaki bilgiler bulunur:

a) İşlemi gerçekleştiren uygulama,

b) İşlemi gerçekleştiren ve varsa onaylayan yetkili kişiler veya yetkisiz erişim kayıtları,

c) İşlemin açıklaması,

ç) Yapılan işlemin zaman bilgisi,

d) İşlemin olumlu veya olumsuz olmak üzere sonucu,

e) Etkilenen veri ve sistemlerin bilgisi.

Özel entegratör denetim izi kayıtlarının bütünlüğünü korumak üzere tedbir alır. Bu amaçla, bir defa yazma, birden fazla kez okuma özelliği olan cihazlar kullanılabileceği gibi, zaman damgası da kullanılabilir. Kayıtlar en az 10 yıl süreyle saklanır ve istenildiğinde GİB yetkililerinin veya denetçilerin

erişimine açılır.

Denetim izi kayıtlarını alan sistemlerin durması halinde acil ve otomatik uyarı mekanizmaları tesis edilmiş olmalıdır.

Denetim izi kayıtlarını; bilgi sistemlerine izinsiz erişim denemeleri, yetkisiz kullanımlar, aşırı veri yüklemeleri, olağan olmayan trafik verileri, izinsiz müdahaleler ve benzeri her türlü olağan dışı hareket bakımından gerçek zamanda analiz ve gerektiğinde otomatik uyarılar üreten bir sistem kurar. Bu sistemin işleyişi, ilgili personel tarafından ayda bir kez gözden geçirilip 3 ayda bir yapılan toplantılarda değerlendirilir. Bu kayıtlar da en az 10 yıl süreyle saklanır.

11. Dış Hizmet Alımı

Özel entegratör, bilgi sistemlerinin temini, işletimi veya bakımı için dış hizmet alımı yapabilir. Dış hizmet alımı taraflar arasında bir sözleşmeyle yapılır.

Bu sözleşmede alınan hizmetin türü, konusu, kapsamı, işin süresi, tarafların açık unvan ve adresleri ile hak ve sorumlulukları açıkça belirtilmelidir.

Dış hizmet alımı sözleşmesinin, yürürlüğe girdiği tarihten itibaren en geç 15 gün içinde özel entegratör tarafından GİB'ebildirilmesi gerekmektedir. Bu bildirimde, sözleşmenin yürürlük tarihi, süresi, tarafların açık unvan ve adresleri ile hizmetin konusu ve kapsamına yerverilir. Aynı şekilde, süresi sonunda biten veya süresinden önce sona erdirilen sözleşmeler de işlem tarihinden itibaren en geç 15 gün içinde GİB'e bildirilir.

Özel entegratör, dış hizmet alımı yaptığı tedarikçide kriptografik anahtarlar için kullanılan özel donanım güvenlik modülleri (HSM) de bulunduruyorsa, bu cihazların münhasıran kendisine adanmış olması şartının da sözleşmede açıkçabulunması gerekir.

Dış hizmet alımı nedeniyle özel entegratörün işbu Kılavuzda tanımlanan yükümlülükleri değişmez. Talep edilen kalite belgeleri, fiziki ve elektronik şartlar, personele ilişkin nitelikler ve alınması gereken eğitimler taşeronda da aranır. Denetim faaliyetleri dış hizmet alımı yapılan taşeronda gerçekleştirilir. Taşeronun bu sorumluluğu yapılan sözleşmede açıkça yer almalıdır. Denetçinin dış hizmet alımı yapılan taşeronun, alıma konu olan tesis, teçhizat ve mekanlarına erişiminin engellenmesi, denetim görüşünün "olumsuz" olması için yeterlidir.

Özel entegratör dış hizmet alımı sözleşmelerini, istenildiğinde ibraz etmek üzere, 10 yıl süreyle saklar.

12. Personelin Niteliğine İlişkin Gereksinimler

Özel entegratör, verdiği hizmete uygun nitelikte ve sayıda personel istihdam etmekle veya dış hizmet alımı yoluyla işgücü sağlamakla sorumludur. Buna göre, ağ ve ağ güvenliği uzmanı, veri tabanı uzmanı, sistem uzmanı, kalite sistemleri uzmanı, yazılım geliştirme uzmanı, konfigürasyon yöneticisi ve test uzmanı rollerinde personel istihdamı zorunludur. Bu rollerde ikiz görev kabul edilmez. Bununla birlikte dış hizmet alımı yapılıyor olması durumunda, yukarıda sayılan personellerin bir kısmının sözleşme kapsamında dış hizmet sağlayıcı tarafından temin edilmesi yeterlidir. Bu konuda nihai karar denetçiye aittir.

Sistemlerin yönetiminde, veri tabanı ve uygulamaların geliştirilmesinde, test edilmesinde ve işletilmesinde görev ve sorumlulukların ayrılığı prensibi uygulanır. Buna göre bu roller aynı kişiler tarafından yerine getirilemez. Süreçler ve sistemler, kritik bir işlemin tek bir personel veya tek bir kaynağın doğrulanmasıyla gerçekleşmesine imkân vermeyecek şekilde tasarlanır.

İstihdam edilen personelin öğrenimi ve sertifikasyonları rolüyle uygun olmalıdır. Genel kabul görmüş makul ölçülerin dışında düşük nitelikli personelin istihdam edilmesi halinde gereksinim karşılanmamış sayılır.

Özel entegratör, yönetim kurulu kararıyla belirlemiş olduğu organizasyon şemasını ve bağlı kadro planını, yönetim kurulu karar tarihinden itibaren en geç 15 gün içinde GİB'e bildirir. İstihdam edilmiş personelin TCKN'si, ismi, öğrenim durumu ve kadro planındaki yeri, işe giriş tarihinden itibaren en geç 15 gün içinde GİB'e bildirilir. Benzer biçimde işten ayrılan personelin bildiriminin ise ilişiğinin kesilmesinde sonraki hafta içinde yapılması gerekmektedir..

Mevcut özel entegratörler, organizasyon şemasının ve kadro planının belirlendiği yönetim kurulu kararını ve mevcut personel bildirimini bu Kılavuzun yayın tarihinden itibaren en geç 1 ay içinde GİB'e yapar.

13. Uluslararası Standartlara İlişkin Sertifikasyonlar

Özel entegratör, bilgi sistemlerinin tamamını içerecek bir kapsamdan daha dar olmamak üzere, aşağıdaki sertifikasyon belgelerine sahip olmalıdır:

a) ISO/IEC 20000:1 2011 Bilgi Teknolojileri Hizmet Yönetim Sistemi Belgesi
b) ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Belgesi
c) ISO 22301 İş Sürekliliği Yönetim Sistemi Belgesi

14. Özel Entegratörün ÖEBSD'ye İlişkin Sorumlulukları

ÖEBSD, özel entegratörün faaliyetin gerektirdiği bilgi sistemleri altyapısına sahip olup olmadığının ve altyapıyı beklendiği gibi işlettiğinin tespit edilmesi amacıyla yapılır. Denetimleri başarıyla tamamlamak, özel entegratörün aldığı yetkiye bağlı olarak mükelleflerine, GİB'e ve kamuya karşı sorumluluklarını yerine getirmesi bakımından gerek şarttır.

ÖEBSD 2 yılda bir gerçekleştirilir. GİB dilediği zaman kendi personeliyle yerinde denetim yapabileceği veya yazıyla bilgi talep edebileceği gibi, son denetimin üzerinden 2 yıl geçmemiş olmasına karşın özel entegratörden ÖEBSD yaptırmasını isteyebilir.

Özel entegratör, denetim süresince, her türlü bilgi ve belgenin denetçilerce erişebilmesine zaman yitirmeden olanak sağlar. Denetçilerin rahat çalışması için gerekli fiziki mekân, bilgisayar, yazıcı, ağ bağlantısı, kırtasiye malzemeleri gibi ihtiyaçları eksiksiz biçimde karşılanır.

Denetim sonuçları "Denetim Görüş Yazısı ve Rapor Ekiyle" açıklanır. "Denetim Görüş Yazısı ve Rapor Eki", denetçi tarafından GİB'e, rapor tarihinden itibaren en geç 15 gün içinde gönderilir.

Özel entegratör, denetim hizmetini aynı denetçiden sıralı en fazla 2 kez üst üste alabilir. Aynı özel hukuk tüzel kişisinden, denetim ekibinin değişmiş olması kaydıyla 5 defaya kadar üst üste denetim hizmeti alınabilir. Hiçbir şart altında özel entegratör, denetim sonuçlarını içerecek bir beyanat veremez veya reklam amaçlı kullanamaz.

15. ÖEBSD Raporunun İçeriği ve Oluşturulması

ÖEBSD raporu, önemlilik kavramı da dikkate alınarak, denetçinin özel entegratörün bilgi sistemlerini değerlendirdiği ve kanaatinin net bir dille yazılı olarak açıklandığı metindir. Denetçinin görevi, bilgi sistemleri süreçleri üzerindeki kontroller hakkında denetim kanıtlarını toplayıp incelemek, değerlendirmek ve bu kanıtlar üzerinden denetim görüşünü oluşturmaktır.

Denetçi, denetimi, denetim görüşüne makul güvence oluşturacak olgulara ve kanıtlara dayandırarak gerçekleştirir. Bu amaçla, bilgi toplamak, gözlem yapmak, sorgulamak, yeniden gerçekleştirmek veya hesaplamak ve analitik akıl yürütmek denetim faaliyetinin esasını oluşturur.

Denetçi ÖEBSD'yi bu Kılavuzda tanımlanan kontrollere göre yapar. Bu Kılavuzda yer almayan

veya yorumunda tereddüt duyulan bir hususla karşılaşılması halinde, uluslararası kabul görmüş bilgi teknolojileri kontrol hedefleri sunan ISO standartları ya da COBIT dokümanlarında yer alan usul ve esasları uygulanır. Bu durumda kullanılan kontrol, gerekçesi ve değerlendirmesiyle birlikte denetim raporu ekinde açıkça belirtilir.

ÖEBSD Raporu, "Denetim görüş yazısı" ve "Rapordan" oluşur. "Denetim görüş yazısında", denetimin yeri, tarihi, denetlenen özel entagratörün unvanı, denetçi veya denetçilerin isimleri ve unvanları ile denetim görüşü, "olumlu", "şartlı", "olumsuz" veya "görüşten kaçınma" biçimde yer alır. ÖEBSD rapor formatı ve denetim görüş yazısı şablonları eklerde verilmiştir.

"Olumlu görüş" kontrollerin uygulanmasında kayda değer bir eksiklik veya uygulama sorunuyla karşılaşmadığında verilir. Denetim görüşünün doğru biçimde oluşturulması için yeterli kanıt bulunamadığında "şartlı görüş", bir kontrolün tamamen eksik olması veya birden fazla kontrolde, bilgi sistemlerinin işleyişini veya güvenliğini tehlikeye atacak nitelikte kayda değer uygulama eksiklikleriyle karşılaşılması halinde "olumsuz görüş" bildirilir. Denetçi, bir görüş oluşturmasına imkân vermeyecek biçimde denetimi faaliyetini yerine getirememiş ise, "görüşten kaçınabilir".

Denetçinin görüşünü oluşturmasında ve özel entegratörün bu Kılavuzda aranan şartları yeterli düzeyde taşıyıp taşımadığını belirlemesine yardımcı olmak üzere ÖEBSD değerlendirme sınıfları ilerleyen bölümlerde, bunlara ilişkin ayrıntılı kontrol tabloları ise eklerde verilmiştir. Ayrı bir ekte, kontrol tablolarının değerlendirme sonuçlarına göre denetçinin görüşünü oluşturmasına ilişkin kurallar da yer verilmiştir.

Denetim raporunda, denetim bulguları, denetim faaliyetinin nasıl gerçekleştirildiği, denetim görüşüne esas oluşturan kanıtlar ve olgular ile değerlendirmesi yapılmış kontrol tabloları yer alır. Saptanan eksikliklerin ve gözlemlerin, varsa bir sonraki denetime kadar veya daha kısa bir süre içinde tamamlanması hususundaki görüşler ile denetim görüşüne dayanak oluşturan tespitler raporda açıkça yazılır. Denetim raporu şablonu eklerde verilmiştir.

16. ÖEBSD Raporuna Bağlı Olarak GİB Tarafından Uygulanacak Yaptırımlar

GİB, ÖEBSD raporunun sonuçlarına göre farklı yaptırımlar uygulayabilir. Buna göre;

a) Rapor sonucunun olumlu olması halinde özel entegratör, varsa kendisine tebliğ edilen eksikliklerin veya iyileştirmelere ilişkin alacağı tedbirleri içeren eylem planını ve buna ilişkin faaliyetleri ve tamamlama sürelerini GİB'e 15 gün içinde bildirir. Buna uymayan özel entegratör bir yazıyla uyarılır. GİB, eylem planına ilişkin tamamlama sürelerinde değişiklik yapmaya yetkilidir.

b) Şartlı görüş veya görüşten kaçınma halinde, özel entegratör ivedilikle bir yazıyla uyarılır ve denetimi en geç 90 gün içinde tekrarlaması istenir. Üst üste 2 kez şartlı görüş veya görüşten kaçınma olması durumunda, özel entegratörün faaliyeti, olumlu görüş alacağı yeni bir denetim sonucuna kadar askıya alınır. Faaliyetin askıya alınması nedeninin 2 kez üst üste görüşten kaçınma olması durumunda, faaliyetin askıya alınma süresi 3 aydan daha kısa olamaz.

c) Rapor sonucunun olumsuz olması halinde özel entegratörün faaliyeti ivedilikle geçici süreyle durdurulur. 6 ay içinde olumlu görüş bildiren yeni bir denetim raporunun GİB'e ibraz edilmemesi halinde özel entegratörün yetkisi iptal edilir. Özel entegratör, 6 ay içinde yaptıracağı her yeni denetime ilişkin, denetim öncesinde ve sonrasında GİB'i bilgilendirmekle mükelleftir.

17. ÖEBSD Değerlendirme Sınıfları

17.1. Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu (ÖEBSD_SER)

Bu değerlendirme sınıfı, özel entegratörlerin sağlaması gereken uluslararası sertifikasyonların varlığı ve uygunluğu ile sızma testlerinin uygunluğunun kontrol edilmesini amaçlamaktadır. Bu sınıf altında iki alt bileşen tanımlanmıştır:

ÖEBSD_SER.1 Bu değerlendirme alt bileşeninde denetçiden özel entegartörün aşağıda uluslararası sertifikasyonları sahip olduğunu teyit etmesi istenmektedir:

a) ISO/IEC 20000 Bilgi Teknolojileri Hizmet Yönetim Sistemi Belgesi
b) ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi
c) ISO 22301 İş Sürekliliği Yönetim Sistemi Belgesi
d) Son yapılan sızma testi raporu
e) Güncel BİS Raporu

ÖEBSD_SER.2 Bu değerlendirme alt bileşeninde denetçiden, özel entegratörün iç kontrol ve denetim süreçlerinin varlığını ve çıktıların uygunluğunu kontrol etmesi beklenmektedir.

Değerlendirme alt bileşenlerine ilişkin kontrol tabloları eklerde verilmiştir.

17.2. Personelin Niteliği (ÖEBSD_PER)

Bu değerlendirme sınıfında, özel entegratörün, verdiği özel entegratörlük hizmetine uygun nitelikte ve sayıda personel istihdam edip etmediği kontrol edilecektir.

17.3. Sistem ve Güvenlik Değerlendirme Sınıfı (ÖEBSD_SIS)

Bu değerlendirme sınıfı, özel entegratörlerin bilgi sistemlerinde uyması gereken alt yapının, sistem mimarisi ve benzeri her türlü fiziki unsur ile iş sürekliliğinin temininin, gerekli güvenlik ve risk değerlendirme süreçlerinin oluşturulmasının, işletilmesinin, değişiklik yönetiminin, denetim izlerinin oluşturulmasının ve dışarıdan hizmet alınması durumundaki gerekliliklerin kontrol edilmesini amaçlamaktadır.

Bu değerlendirme sınıfının oluştuğu 7 alt bileşen aşağıda açıklanmıştır:

ÖEBSD_SIS.1 Fiziki Şartlar ve Güvenlik Tedbirleri: Özel entegratörün sağlaması gereken uluslararası sertifikasyonları varlığı ve uygunluğu ile sızma testlerinin uygunluğu kontrol edilecektir.

ÖEBSD_SIS.2 Erişim Güvenliği: Özel entegratörün bilgi sistemlerinin sağlaması gereken fiziki ve elektronik erişim güvenliği kontrol edilecektir.

ÖEBSD_SIS.3 İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları: Özel entegratörün "İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları" kurallarına uygunluğu kontrol edilecektir.

ÖEBSD_SIS.4 Değişiklik Yönetimi: Özel entegratörün "Değişiklik Yönetimi" kurallarına uygunluğu kontrol edilecektir.

ÖEBSD_SIS.5 Denetim İzleri Yönetimi: Özel entegratörün "Denetim İzleri Yönetimi" kurallarına uygunluğu kontrol edilecektir.

ÖEBSD_SIS.6 Dış Hizmet Sağlayıcılarının Yönetimi: Özel entegratörün "Dış Hizmet Sağlayıcılarının Yönetiminin" kurallara uygunluğu kontrol edilecektir.

ÖEBSD_SIS.7: Hizmet Yazılımlarına İlişkin Kontroller: Özel entegratörün hizmetlerinde kullandığı uygulama yazılımlarının, ilgili GİB kılavuzları, e-Fatura, e-Saklama, e-Arşiv, e-İrsaliye, e-Defter ve e-imza standartları ve hizmetin akışına uygun normları taşıyıp taşımadığı kontrol edilecektir.

Değerlendirme alt bileşenlerine ilişkin kontrol tabloları eklerde verilmiştir.

EK 1. ÖEBSD Değerlendirme Sınıfları Kontrol Tabloları

A. ÖEBSD_SER.1: Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu

Özel entegratörün sağlaması gereken uluslararası sertifikasyonların varlığı ve uygunluğu ile sızma testlerinin uygunluğu aşağıdaki tabloya göre kontrol edilecektir. Sertifika belgeleri Değerlendirme Raporu ekinde yer almalıdır. Dış hizmet alımı durumunda, ilgili kontrol ve testler, dış hizmet alımının yapıldığı lokasyonlarda da ,özel entegratörlük faaliyeti ile sınırlı olmak üzere, tekrarlanacaktır.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SER.1: Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu		
Kontrol No	***Kontrol Maddesi***	***Sonuç***
A1	*ISO / IEC 20000 Sertifikası mevcut ve denetim tarihinde geçerli mi?*	
A2	*ISO 22301 Sertifikası mevcut ve denetim tarihinde geçerli mi?*	
A3	*ISO / IEC 27001 Sertifikası mevcut ve denetim tarihinde geçerli mi?*	
A4	*ISO / IEC 27001 Sertifikası, bilgi sistemlerini ve bu kılavuzda belirtilen kritik varlıkları işleyen ve kullanan süreçleri kapsıyor mu?*	
A5	*Son yapılan sızma testi tarihinden itibaren geçen süre 1 yıldan kısa mıdır?*	
A6	*Sızma testinde veri tabanı sistemleri incelenmiş midir?*	
A7	*Sızma testinde ağ ve iletişim altyapısı güncel saldırı yöntemlerine göre test edilmiş midir?*	
A8	*Sızma testinde işletim sistemleri ve platformlar güvenlik açıkları açısından değerlendirilmiş midir?*	
A9	*Sızma testinde uygulamalar güncel saldırı yöntemlerine göre incelenmiş midir?*	
A10	*Sızma testi bulguları arasında bilgi sistemlerini güvenliğini tehdit eden kritik düzeyde bir açık olmadığını teyit ettiniz mi?*	

B. ÖEBSD_SER.2: İç Kontrol ve Denetim Mekanizmaları

Özel entegratörün iç kontrol ve denetimi bu tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama

olarak yazılmalıdır.

ÖEBSD_SER.2: İç Kontrol ve Denetim Mekanizmaları		
Kontrol No	***Kontrol Maddesi***	***Sonuç***
B1	*İç kontrol ve iç denetim dokümanı oluşturulmuş ve uygulanıyor mu?*	
B2	*İç ve dış denetimde kullanılmak üzere iç kontrol sonuçlarının nasıl raporlanacağı belirlenmiş mi?*	
B3	*İç kontrol dokümanları ile iş sürekliliği dokümanları birbiriyle uyumlu mu?*	
B4	*İç kontrol denetimleri periyodik biçimde yapılmış ve denetim sonuçları raporlanmış mı?*	
B5	*İç kontrol denetim sonuçlarının gereği yapılmış mı?*	

C. ÖEBSD_PER: Personelin Niteliği

Özel entegratörün iç kontrol ve denetimi bu tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_PER: Personelin Niteliği		
Kontrol No	***Kontrol Maddesi***	***Sonuç***
C1	*Bilgi sistemlerinde çalıştırılan personel sayısı yeterli midir?*	
C2	*Ağ ve ağ güvenliği uzmanı, veri tabanı uzmanı, kalite sistemleri uzmanı, yazılım geliştirme uzmanı, konfigürasyon yöneticisi ve test uzmanı rollerinin her birisi için ayrı bir kişi olmak üzere en az 1 personel bulunuyor mu?*	
C3	*Bilgi sistemleri organizasyon şeması ve bağlı kadro planı yönetim kurulu kararıyla belirlenmiş mi?*	
C4	*Son denetim tarihinden bugüne kadar istihdam edilen yeni personel ile işten ayılan personelin GİB'e zamanında bildirilmiş olduğu teyit edilebiliyor mu?*	

D. ÖEBSD_SIS.1: Fiziki Şartlar ve Güvenlik Tedbirleri

Özel entegratörün bilgi sistemlerinin sağlaması gereken fiziki ve güvenlik şartları aşağıdaki tabloya göre kontrol edilecektir. HSM'lere ilişkin sertifika belgeleri Değerlendirme Raporu ekinde yer almalıdır.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SIS.1: Fiziki Şartlar ve Güvenlik Tedbirleri		
Kontrol No	**Kontrol Maddesi**	**Sonuç**
D1	Özel entegratör münhasıran faaliyetine ayrılmış bir veri tabanı çalıştırıyor mu?	
D2	Veri tabanının çalıştığı sunucu kümesinin uygulama dışında erişime açık bırakılmadığı teyit edilebiliyor mu?	
D3	Veri tabanının çalıştığı sunucu kümesinin veri tabanı portları dışında erişime açık olmadığı teyit edilebiliyor mu?	
D4	Veri tabanı üzerinde “linked server” yapılanmasının olmadığı kontrol edildi mi?	
D5	Veri tabanının çalıştığı sunucu kümesi üzerinde başka servisler veya uygulamaların çalıştırılmadığı kontrol edildi mi?	
D6	Kriptografik anahtarlar, FIPS 140-2 Düzey 3 veya EAL 4+ sertifika sahibi sadece özel donanım güvenlik modüllerinde (HSM) mi barındırılıyor?	
D7	Hassas veriler (mükellef bilgileri, erişim şifreleri vb.) veri tabanında şifreli saklanıyor mu?	
D8	Hassas verilere herhangi bir personelin tek başına erişim yetkisi yoktur.	
D9	Sistemlerde bulunan ve veri gizliliği amacıyla şifreli tutulan verilen veriler için kullanılan şifreleme yöntemleri AES 256, RSA2048 ve hash algoritmasında SHA-2 olacak biçimde uygulanmış mıdır?	
D10	Denetim izi için tutulan kayıtlar, geçmişteki bir olayın izlenmesi için yeterli düzeyde veri içermekte midir?	
D11	Denetim izi için tutulan kayıtlar, ayrı bir sunucu kümesinde, veri bütünlüğü dikkate alınarak saklanıyor mu?	
D12	Denetim izi için tutulan kayıtlar için, olağan dışı hareketleri anında tespit edip otomatik uyarı üreten mekanizmalar kurulmuş mu?	
D13	Özel entegratör ile GİB arasında iletişim amacıyla kullanılan erişim hatları işin kapasitesi ve hattın yedeklenmesi bakımından yeterli düzeyde mi?	
D14	Bilgi sistemleri ağ ve uygulama topolojileri ile varlıklara erişim için yetkilendirilmiş tüm kullanıcıların isimleri güncel ve güvenli biçimde tutuluyor mu?	
D15	Veri tabanı, uygulama ve ağ erişim cihazları (güvenlik duvarı, aktif anahtarlama cihazları) katmanlarında tek noktadan arıza sonucu hizmetin durmasına izin verecek bir yapılanma olmadığı kontrol edildi mi?	
D16	Sunucuların veya aktif ağ cihazlarının yer aldığı sistem odaları ile kritik odalar, iklimlendirme, güç şebekesi, sel, yangın ve benzeri afetler için otomatik uyarı ve söndürme sistemleri gibi fiziksel altyapı gereklilikleri sağlanmış mıdır?	
D17	Sunucuların veya aktif ağ cihazlarının yer aldığı sistem odaları ile kritik odalarda, 7x24 görüntü kaydı yapılıyor mu?	
D18	Sunucuların veya aktif ağ cihazlarının yer aldığı sistem odaları ile kritik odalardaki görüntü kayıtları en az 6 ay süreyle saklanıyor mu?	
D19	Bilgi sistemlerinde kullanılan aktif ağ cihazları, güvenlik duvarları ve sunucu veya kişisel bilgisayarlarda kullanılan her türlü 3. parti yazılımın son güncel sürümleri kullanılıyor mu?	
D20	Bilgi sistemlerinde kullanılan aktif ağ cihazlarının, güvenlik duvarlarının, sunucu, kişisel bilgisayarların arızası veya bakımı nedeniyle 3. kişilerin erişimine açılması halinde, işlem süresince yeterli gözetimin yapılıp olay kayıtları tutuluyor mu?	

E. ÖEBSD_SIS.2: Erişim Güvenliği

Özel entegratörün bilgi sistemlerinin sağlaması gereken fiziki ve elektronik erişim güvenliği aşağıdaki tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SIS.2: Erişim Güvenliği		
Kontrol No	***Kontrol Maddesi***	***Sonuç***
E1	*Sistem odaları ve kritik odalara erişim yetkilendirmeleri ile personel kadro planındaki roller uyumlu mu?*	
E2	*Sistem odaları ve kritik odalara erişim yetkilendirmeleri ve değişikliklere ilişkin kayıtlar güvenli biçimde tutuluyor mu?*	
E3	*Sistem odaları ve kritik odalara erişim için iki faktörlü kimlik doğrulma mekanizması kullanılmış mı?*	
E4	*Sistem odaları ve kritik odalara erişimde en az iki yetkili ilkesi uygulanıyor mu?*	
E5	*Sistem odaları ve kritik odaların kapıları endüstri standartlarına uygun çelik kapılarla yapılıyor mu?*	
E6	*Sistem odaları ve kritik odalara her zaman en az iki yetkilendirilmiş kişinin bir arada olmasıyla erişimin mümkün olacağı mekanizma kurulmuş mu?*	
E7	*Fiziki erişim için kapı geçiş sistemlerinde yapılan yetkilendirme için ayrıştırılmış roller ve en az iki yetkili ilkesi uygulanıyor mu?*	
E8	*Veri tabanlarına, uygulamalara ve her türlü aktif cihaza (sunucular, aktif ağ cihazları, güvenlik duvarları vb.) erişimde kullanılan yönetici şifreleri ile kullanıcı şifreleri ayrıştırılmış mı?*	
E9	*Tek yönetici erişimiyle veri ve uygulama değişikliği yapılmasını engelleyecek mekanizmalar kurulmuş mu?*	
E10	*İşten ayrılan veya kötü niyetli bir yetkilinin tek başına, sistemlere erişimi ortadan kaldıracak veya yeniden çalıştırılamayacak biçimde bir sistemi durdurmasının engellenmesi için tedbirler alınmış mı?*	
E11	*Yönetici ve uygulama şifreleri, endüstriyel güvenli şifre standartlarını sağlayacak biçimde belirleniyor mu?*	
E12	*Yönetici ve uygulama şifreleri, endüstriyel güvenli şifre standartlarını sağlayacak biçimde belirlenen sürelerde yenileniyor mu?*	
E13	*Veri Aktarım Protokolü ve mükellef ile arasında çalışan haberleşme protokolüne dair tutulan güvenlik parametreleri, bu parametrelere erişim yetkileri ve bunların (parametrelerin görüntülenmesi, güncellenme sıklığı vb.) korunması sağlanıyor mu? Yönetici şifrelerinin yedekleri güvenli biçimde tutuluyor mu?*	

F. ÖEBSD_SIS.3: İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları

Özel entegratörün "İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları" kurallarına uygunluğu aşağıdaki tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SIS.3: İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları		
Kontrol No	**Kontrol Maddesi**	**Sonuç**
F1	İş sürekliliği prosedürü oluşturulmuş mu?	
F2	İş sürekliliği kapsam ve içerik yönünden amacına hizmet eder nitelikte mi?	
F3	Üst yönetim, iş sürekliliği prosedürünün çalıştırılmasından birinci derecede sorumlu tutulmuş ve bu sorumluluğunu yerine getirmiş mi?	
F4	Özel entegratör, bir risk yönetim planı oluşturmuş mu?	
F5	Risk yönetimi kapsam ve içerik yönünden amacına hizmet eder nitelikte mi?	
F6	Risk değerlendirme tablosunda olasılık ve etki değerlendirilmesi yapılmış mı?	
F7	Niceliksel olarak risklerin beklenen parasal değeri hesaplanmış mı?	
F8	Son denetim tarihinden bugüne kadar ki kayıtlara göre, hizmetin sürekliliği gerçekleşmesiyle güncel BİS raporu ve bu Kılavuzda verilen süreler uyumlu mudur?	
F9	Hizmetin sürekliliğinin gerçekleşmesine ilişkin kayıtlar Uptime Institute Tier 2 standartlarına uygun tutuluyor mu?	
F10	Varlık envanteri, varlıklara yönelik tehditler, tehditlerin risk seviyeleri ve uygulanacak eylemler risk yönetim planında yer alıyor mu?	
F11	Bilgi sistemleri ve tüm operasyonel süreçlere ilişkin riskleri tespit ve analiz edilerek, ölçme, izleme, kontrol etme ve raporlama işlemleri yerine getiriliyor mu?	
F12	Donanımlara, yazılımlara, uygulama geliştirme faaliyetine, iletişim alt yapılarına ve dış hizmet alımlarına bağlı olaylar risk yönetim planına dâhil edilmiş mi?	
F13	Özel entegratör 3. taraflara doğabilecek zararları karşılamak amacıyla mesleki sorumluluk sigortası yaptırmış mı?	
F14	Bilgi sistemlerine ilişkin hizmeti etkileyen olayların vuku bulması durumunda veya sistemlerde kayda değer bir değişiklik öncesinde veya yeni tehditlerin ortaya çıkması halinde, alınacak eylemler açıkça planlanmış mıdır?	
F15	Risk yönetim planı yılda en az bir kez olmak üzere üst yönetim tarafından gözden geçirilerek güncellenmeye yönelik çalışma yapılıyor mu?	

F16	Yılda 1 kez olmak üzere, bilgi sistemleri iş sürekliliği testleri ve acil durum planı tatbikatı gerçekleştirilerek kayıt altına alınmakta mı?	
F17	Veri tabanının etkin ve verimli çalışmasını temin etmek üzere, düzenli aralıklarla bakım, iyileştirici indeksleme yapılıyor mu?	
F18	Bilgi sistemlerinin çıktı performansı hedefi düzenli aralıklarla gözden geçirilip ihtiyaç halinde iyileştirici faaliyetler için kararlar alınıyor mu?	
F19	Bilgi sistemlerinin belirlenen süreleri aşan biçimde hizmet vermez hale gelmesi durumunda yapılacaklar için bir acil durum planı hazırlanmış mı?	
F20	Acil durum planında, olaylar, sistemler üzerindeki etkileri, aşamaya bağlı gelişimleri veya kök nedenlerine göre sınıflandırılmış mı?	
F21	Acil durum planında, olaya karşı alınacak tedbirler ve yapılacaklar, olay veya sınıf bazında ele alınmış mı?	
F22	Acil durum planında, olaya müdahale, kök nedeninin bulunarak ortadan kaldırılması, belirlenen sürenin aşılması halinde FKM'ye geçiş gibi acil durumun yönetim adımları, alt süreçler, süreç sorumluları, karar verici yetkililer, ulaşılamayan hallerde yedek aktörler tanımlanmış mı?	
F23	Acil durum planı, belirlenen süre içinde hizmetin özel entegratörün merkezinden veya felaket kurtarma merkezinden (FKM) yeniden verilmeye başlanmasına ilişkin eylem adımlarını yeterli ayrıntıda içeriyor mu?	
F24	Acil durum planında, hizmetin yeniden devreye alınmasından sonra, veri kaybı veya maddi kayıp olup olmadığı, olayın kök nedeni, iş sürekliliği, risk yönetimi, acil durum planları veya fiziki altyapıda önceden saptanamamış iyileştirilmesi gerekli görülen hususların tespitine yönelik ayrıntılı bir olay sonrası değerlendirme yapılması planlanmış mı?	
F25	Olay sonrası değerlendirme tutanakları ile olaya ilişkin sistemlerdeki her türlü denetim izi, denetçilere veya ihtiyaç halinde adli makamlara sunulmak üzere güvenli biçimde saklanıyor mu?	
F26	Olay halinde, GİB veya adli makamların bilgilendirilmesi konusuna acil durum planında yer verilmiş mi?	
F27	FKM, güncel BİS raporuyla uyumlu yeterli fiziki altyapıya ve özelliklere sahip mi?	
F28	FKM, güvenlik ve hizmetin çeşitliliği ve niteliği bakımlarından, merkez bilgi sistemleriyle aynı düzeyde mi?	
F29	FKM uygun bir yerde konumlandırılmış mı?	
F30	Veri yedekleri güncel BİS raporu ve bu Kılavuzla uyumlu biçimde FKM'ye alınıyor mu?	

G. ÖEBSD_SIS.4: Değişiklik Yönetimi

Özel entegratörün "Değişiklik Yönetimi" kurallarına uygunluğu aşağıdaki tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SIS.4: Değişiklik Yönetimi		
Kontrol No	**Kontrol Maddesi**	**Sonuç**
G1	Değişiklik yönetimi için bir prosedür oluşturulmuş mu?	
G2	Kullanıcı değişiklik kabul onayı var mı?	
G3	Değişiklik yönetimi prosedürü kapsam ve içerik yönünden amacına hizmet eder nitelikte mi?	
G4	Değişiklik yönetimi prosedüründe, bilgi sistemlerinde yer alan tüm donanım ve yazılımın her türlü bakım, yama ve değişikliği kapsamda yer alıyor mu?	
G5	Özel entegratör, yazılım geliştirme faaliyetinde, derlenmiş yazılım ve yazılımın tüm alt bileşenleri ile kaynak kodları geçmiş sürümleriyle birlikte yönetiyor mu?	
G6	Derlenerek bütüne dâhil edilen yazılım bileşenlerinin, ne zaman ve kim tarafından derlendiği ve bütüne dâhil edildiğinin tarihçesi tutuluyor mu?	
G7	Yazılım geliştirme ve sürüm yönetimi platformunda, geliştiriciler rollerine göre ayrıştırılmış yetkilerle tanımlanmış mı?	
G8	Derlenen yeni bir yazılım sürümü için, hangi testleri geçmesi gerektiği ve testin kimler tarafından yapılacağı önceden belirlenerek kayıt altına alınmış mı?	
G9	Test ortamı ile canlı ortam ağ erişimi düzeyinde birbirlerinden ayrılmış mı?	
G10	Test ortamında kullanılan veriler, gizlilik ve kişisel mahremiyete halel getirmeyecek nitelikte midir?	
G11	Testleri başarıyla geçtiği halde canlı ortamda doğru çalışmayan bir sürümden geri dönüşe ilişkin plan yapılmış mı?	
G12	Geri dönüş planında, doğru çalışmayan sürümün canlı ortamda bulunduğu süre içinde veri kaybı, hatalı veya eksik işlem gibi sorunlar yaratıp yaratmadığının tespit edilerek kayıt altına alınması dikkate alınmış mı?	

H. ÖEBSD_SIS.5: Denetim İzleri Yönetimi

Özel entegratörün "Denetim İzleri Yönetimi" kurallarına uygunluğu aşağıdaki tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SIS.5: Denetim İzleri Yönetimi		
Kontrol No	**Kontrol Maddesi**	**Sonuç**
H1	Denetim İzleri Yönetimi için bir prosedür oluşturulmuş mu?	
H2	Denetim İzleri Yönetimi prosedüründe, denetim izlerinin oluşturulması ve güvenli saklanmasına ilişkin yeterli ayrıntıya yer verilmiş mi?	
H3	Denetim İzleri Yönetimi prosedüründe, denetim izlerine bağlı şüpheli olarak nitelendirilecek olaylar yeterli ayrıntıda tanımlanmış mı?	
H4	Denetim izlerinde, işlemi gerçekleştiren uygulama, işlemi gerçekleştiren ve varsa onaylayan yetkili kişiler veya yetkisiz erişim kayıtları, işlemin açıklaması, yapılan işlemin zaman bilgisi, işlemin olumlu veya olumsuz sonucu, etkilenen veri ve sistemlerin bilgisi yer alıyor mu?	
H5	Denetim izlerinde hassas bir veri kaydının geçmediği teyit edildi mi?	
H6	Veri tabanı katmanı, uygulama katmanı, ağ cihazları ile işletim sistemleri için denetim izlerinin nasıl oluştuğu ve saklandığı kayıt altına alınmış mı?	
H7	Denetim izlerinin bütünlüğünün korunması ve tahrifatı halinde bunun tespiti için yeterli tedbirler alınmış mı?	
H8	Denetim izlerinin en az 10 yıl süreyle güvenli biçimde saklanması için yeterli altyapı oluşturulmuş mu?	
H9	Özel entegratör, GİB ile arasında çalışan Veri Aktarım Protokolü ve mükellef ile arasında çalışan güvenli haberleşme protokolüne dair tüm işlem kayıtlarını, bütünlüğünü de koruyacak biçimde 10 yıl süreyle saklıyor mu?	
H10	Denetim izlerini aktif olarak analiz eden ve şüpheli olay halinde SMS, e-posta gibi otomatik uyarı veren mekanizmalar var mı?	
H11	Ayrıcalıklı yetkiye sahip olanlarca dahi denetim izlerinin değiştirilememesi veya değiştirilmesi halinde tespiti amacıyla 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun uyarınca gerekli tedbirler alınmış mı?	

İ. ÖEBSD_SIS.6: Dış Hizmet Sağlayıcılarının Yönetimi

Özel entegratörün "Dış Hizmet Sağlayıcılarının Yönetiminin" kurallara uygunluğu aşağıdaki tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SIS.6: Dış Hizmet Sağlayıcılarının Yönetimi		
Kontrol No	**Kontrol Maddesi**	**Sonuç**
I1	Özel entegratör dış hizmet alımı yapıyorsa bir sözleşmesi var mı?	
I2	Bu sözleşmede alınan hizmetin türü, konusu, kapsamı, işin süresi, tarafların açık unvan ve adresleri, hak ve sorumlulukları yer alıyor mu?	
I3	Mevcut ve yürürlükte olmayan tüm sözleşmeler 10 yıl süreyle saklanıyor mu?	
I4	Alınan hizmetin niteliğine bağlı olarak, nedeniyle, ÖEBSD_SER.1, SER. 2, SIS.5, ÖEBSD_SIS.1, ÖEBSD_SIS.2, ÖEBSD_SIS.3, ÖEBSD_SIS.4 kontrollerinin bir bölümü veya tamamı için dış hizmet sağlayıcısının yerinde denetimi yapıldı mı?	
I5	Bir dış hizmet sağlayıcısında yerinde yapılan denetim kayıt altına alınarak denetim raporuna eklendi mi?	
I6	Dış hizmet sağlayıcısının merkezi yurt içinde mi?	
I7	Dış hizmet sağlayıcısının FKM'si bu kılavuz hükümlerine uygun nitelikte mi?	
I8	Dış hizmet sağlayıcının, özel entegratör için verdiği hizmetler için ayrıca bir taşeron kullanmadığı teyit edildi mi?	
I9	Özel entegratör, dış hizmet sağlayıcısını iç kontrol ve denetim prosedürleri uyarınca düzenli aralıklarla yerinde denetliyor mu?	
I10	Özel entegratör, dış hizmet sağlayıcısını tedarikçi performansı açısından düzenli aralıklarla değerlendiriyor mu?	
I11	Dış hizmet sağlayıcısı denetim ve değerlendirmeleri kayıt altına alınmış mı?	
I12	Dış hizmet sağlayıcısı denetim ve değerlendirmeleri sonucu karara bağlanan iyileştirme önerileri izlenmiş mi?	

J. ÖEBSD_SIS.7: Hizmet Yazılımlarına İlişkin Kontroller

Özel entegratörün "Hizmet Yazılımlarına İlişkin Kontroller" kurallara uygunluğu aşağıdaki tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SIS.7: Hizmet Yazılımlarına İlişkin Kontroller		
e-Fatura		
Kontrol No	**Kontrol Maddesi**	**Sonuç**
	1.Güvenlik	
J1	Her kullanıcı sadece kendi firması adına fatura gönderebilmekte mi?	
J2	Her kullanıcı sadece kendi firmasının alıcısı veya satıcısı olduğu faturaları görebilmekte mi?	
J3	Her kullanıcı sadece kendi firması adına uygulama yanıtı gönderebilmekte mi?	
J4	Her kullanıcı sadece kendi firmasının alıcısı veya satıcısı olduğu faturalara verilen uygulama yanıtlarını görebilmekte mi?	
	2.İşlem Kayıtlarının Saklanması	
J5	Kullanıcıların yaptığı tüm işlemlerin kayıtları saklanmakta mı?	
J6	Kullanıcıların yaptığı tüm işlemleri içeren kayıtların değişmezliği sağlanmakta mı?	
J7	Sistemlerin yazılım ve donanım alt yapısının Türkiye Cumhuriyeti sınırları içerisinde ve Türkiye Cumhuriyeti Kanunlarının geçerli olduğu yerlerde mi bulunuyor?	
J8	Saklama hizmeti kapsamında GİB ile entegrasyon sağlandı mı?	
	3. Standartlara Uyum	
J9	Web ara yüzünde veya web servis, SFTP vb. gibi çeşitli kanallarla müşterilerden alınan bilgilerle oluşturulan UBL faturalar son halinde saklanmadan ve gönderilmeden önce GİB tarafından yayınlanan güncel şematron (schematron) kontrolünden geçirilmekte mi?	
J10	Özel entegratör tarafından imzalanmayıp farklı kanallardan imzalı olarak alınan faturalar son halinde saklanmadan ve gönderilmeden önce imza kontrolünden geçirilmekte mi?	
J11	Özel entegratör tarafından imzalanan faturalar imzalanırken GİB'in belirlediği standartlara uyarak imzalanmakta mı?	
J12	Özel entegratör tarafından imzalanan faturalar imzalanırken imza sertifikasının geçerlilik süreleri kontrol edilmekte mi?	

J13	Özel entegratör tarafından imzalanan faturalar imzalanırken imza sertifikasının geçerlilik süreleriyle CRL ve OCSP sonuçları kontrol edilmekte mi?	
J14	Fatura ve uygulama yanıtlarının gönderimi için oluşturulan zarflar GİB'e gönderilemezse müşterilerin müdahalesine gerek kalmadan bir süre sonra yeniden denenmekte mi?	
J15	Gönderilen fatura veya uygulama yanıtlarının zarf durum sorguları gönderim anından itibaren hemen ve sık sık yapılmamakta, sadece gönderim tarihinden itibaren 24 saat içinde GİB'den ve alıcıdan sistem yanıtı gelmeyen zarfların durumları GİB'den kontrol edilmekte ve en sık 5 saatte bir sorgulanmakta mı?	
J16	GİB tarafından iletilen zarflar hemen kontrol edilip işlenmemekte, kaydedilip hemen dönülmekte, kontrol ve işleme daha sonra yapılmakta mı?	
J17	GİB tarafından iletilen zarflar kontrol edilip işlendikten sonra hatalı veya hatasız olarak sistem yanıtı dönülmekte mi?	
J18	Oluşturulan sistem yanıtlarının gönderilip gönderilemedikleri veya gönderildikten sonra başarıyla işlenip işlenemedikleri belirli aralıklarla sorgulanarak yeniden gönderilmekte mi?	
J19	Alınan zarflar kontrol edilirken GİB tarafından yayınlanan güncel şema kontrolleri yapılmakta ve geçersiz olanlar kabul edilmeyip hatayı gösteren sistem yanıtı dönülmekte mi?	
J20	Alınan zarflar kontrol edilirken GİB tarafından yayınlanan güncel şematron (schematron) kontrolleri yapılmakta ve geçersiz olanlar kabul edilmeyip hatayı gösteren sistem yanıtı dönülmekte mi?	
J21	Alınan zarflar kontrol edilirken fatura ve uygulama yanıtları için imza olup olmadığı, varsa geçerli olup olmadığı kontrol edilmekte ve geçerli imzalar için geçerli, geçersiz imzalar için geçersiz şeklinde sistem yanıtı dönülmekte mi?	
J22	Alınan fatura veya uygulama yanıtları için oluşturulan sistem yanıtları sadece sistem tarafından otomatik olarak oluşturabilmekte, kullanıcıların web servis gibi yöntemlerle sistem yanıtı zarfları göndermesine izin verilmemekte mi?	
J23	Gelen temel faturalara uygulama yanıtı oluşturulmasına izin verilmemekte mi?	
J24	Gelen ticari faturalara zarfın alınma zamanından itibaren 8 gün içinde uygulama yanıtı oluşturulabilmekte daha sonra uygulama yanıtı oluşturulamamakta mı?	
J25	Gelen ticari faturalara zarfın alınma zamanından itibaren 8 gün içinde uygulama yanıtı gönderilebilmekte daha sonra uygulama yanıtı gönderilmekte mi?	
J26	Gelen faturalara uygulama yanıtı oluşturulup oluşturulamayacağı kontrol edilirken faturanın alındığı saat kontrol edilmemekte uygulama yanıtının 8. günde 23:59'a kadar oluşturulmasına izin verilmekte mi?	
J27	Gelen ticari faturalara bir defa uygulama yanıtı verildiğinde bir daha uygulama yanıtı oluşturulmasına izin verilmemekte mi?	

J28	Gelen faturaların içindeki XSLT fatura şablonlarındaki hatalar nedeniyle görüntülenemeyen faturalar için GİB'in e-Fatura paketlerinde önerdiği gibi bir varsayılan XSLT fatura şablonu kullanılabilmekte, en azından fatura numarası, fatura tutarı, fatura tarihi, notlar gibi temel bilgilerin görüntülenmesi sağlanabilmekte mi?	
J29	Gönderilen ticari faturalara gelen uygulama yanıtları alıcının gönderilen zarfa gönderdiği sistem yanıtının özel entegratör tarafından alınma zamanından 8 gün sonrasına kadar kabul edilmekte, daha sonra gelen uygulama yanıtları kabul edilmemekte mi?	
J30	Gönderilen ticari faturaya daha önce uygulama yanıtı geldiyse gelen uygulama yanıtı kabul edilmemekte mi?	
J31	Gönderilen faturalara ve uygulama yanıtlarına GİB veya alıcı tarafından hatalı sistem yanıtı dönülmesi durumunda yeni fatura ve uygulama yanıtı oluşturulması gerekmeyen durumlarda yeni fatura ve uygulama yanıtı oluşturulması zorlanmadan mevcut fatura ve uygulama yanıtı farklı bir zarfa konarak gönderilebilmekte mi?	
J32	Gönderilen fatura ve uygulama yanıtlarının gönderim sonucu belirlenene kadar veya başarılı olduktan sonra yeniden başka bir zarfla gönderilmesine izin verilmemekte mi?	
J33	Özel entegratör, müşteri firmanın istemesi durumunda faturalarını kendi mali mührüyle imzalamasına imkân sağlamakta mı?	
	4. Hizmetin Kapatılması	
	Hizmeti kapatmak isteyen müşteri için GİB'e kapatma isteği gönderilmekte mi?	
J35	Hizmeti kapatmak isteyen müşterilere fatura ve uygulama yanıtları UBL ya da zarf olarak XML formatında teslim edilmekte mi?	

ÖEBSD_SIS.7: Hizmet Yazılımlarına İlişkin Kontroller		
e-Arşiv		
Kontrol No	**Kontrol Maddesi**	**Sonuç**
	1. Güvenlik	
K1	Her kullanıcı sadece yetkisi olduğu firma adına fatura gönderebilmekte mi?	
K2	Her kullanıcı sadece kendi firması tarafından oluşturulan faturaları görebilmekte mi?	
K3	Her kullanıcı sadece kendi firması adına e-Arşiv raporu oluşturabilmekte mi?	
K4	Her kullanıcı sadece kendi firmasına ait e-Arşiv raporlarını görebilmekte mi?	
	2. İşlem Kayıtlarının Saklanması	
K5	Kullanıcıların yaptığı tüm işlemlerin kayıtları saklanmakta mı?	
K6	Kullanıcıların yaptığı tüm işlemleri içeren kayıtların değişmezliği sağlanmakta mı?	
	3. Standartlara Uyum	
K7	Web ara yüzünde veya web servis, SFTP vb. gibi çeşitli kanallarla müşterilerden alınan bilgilerle oluşturulan UBL faturalar son halinde saklanmadan önce GİB tarafından yayınlanan güncel şematron (schematron) kontrolünden geçirilmekte mi?	
K8	Web ara yüzünde veya web servis, SFTP vb. gibi çeşitli kanallarla müşterilerden alınan bilgilerle oluşturulan UBL faturalar son halinde saklanmadan önce GİB tarafından yayınlanan güncel şema ve şematron (schematron) kontrollerine ilave olarak, e-Arşiv Raporunun gereksinimlerine göre ek kontrollerden geçirilmekte mi?	
K9	Özel izinle PDF formatında fatura gönderen mükelleflerin PDF faturaları fatura bilgilerini içeren bir UBL PDF'e eklenmiş olarak GİB'in yayınladığı standartlara uygun olarak (PADES yöntemi ile) imzalanmakta mı?	
K10	e-Arşiv Raporu oluşturulduktan sonra GİB'e gönderilmeden önce GİB tarafından yayınlanan güncel şema kontrolünden geçirilmekte mi?	
K11	e-Arşiv Raporu oluşturulduktan sonra GİB'e gönderilmeden önce GİB tarafından yayınlanan güncel şematron (schematron) kontrolünden geçirilmekte mi?	
K12	Özel entegratör tarafından imzalanmayıp farklı kanallardan imzalı olarak alınan faturalar son halinde saklanmadan ve gönderilmeden önce imza kontrolünden geçirilmekte mi?	
K13	Özel entegratör tarafından imzalanan faturalar imzalanırken GİB'in belirlediği standartlara uyarak imzalanmakta mı?	
K14	Özel entegratör tarafından imzalanan faturalar imzalanırken imza sertifikasının geçerlilik süreleri kontrol edilmekte mi?	
K15	Özel entegratör tarafından imzalanan faturalar imzalanırken imza sertifikasının geçerlilik süreleriyle CRL ve OCSP sonuçları kontrol edilmekte mi?	
K16	e-Arşiv Raporları imzalanırken GİB'in belirlediği standartlara uyarak imzalanmakta mı?	
K17	Sistemde birden çok faturanın aynı ETTN ile kaydedilmesine izin verilmemekte	

	mi?	
K18	Sistemde aynı mükellefe ait aynı fatura numarası ile birden fazla fatura kaydedilmesine izin verilmemekte mi?	
K19	Özel entegratör, müşteri firmanın istemesi durumunda faturalarını kendi mali mührüyle imzalamasına imkân sağlamakta mı?	
K20	e-Arşiv Fatura özel entegratör üzerinden faturanın alıcısına e-posta ile gönderilirken imzalı UBL ek olarak veya imzalı UBL'in özel entegratörün sistemlerinden indirilebileceği bir URL eposta ile birlikte gönderilmekte mi?	
K21	e-Arşiv Raporlarının gönderimleri özel entegratör üzerinden belirlenen terminlerde mi yapılmış?	
K22	Özel entegratör, müşteri firmanın düzenlenen her e-Arşiv Faturasının özel entegratör bilgi işlem sistemleri aracılığı ile oluşturup ve düzenlenen her e-Arşiv Faturasının GİB'e e-Arşiv Raporu ile raporlanmasını garanti edecek tedbirleri almış mı?	
	4. Hizmetin Kapatılması	
K24	Hizmeti kapatmak isteyen müşteri için GİB'e kapatma isteği gönderilmekte mi?	
K25	Hizmeti kapatmak isteyen müşterilere e-Arşiv fatura / e-Arşiv Raporları UBL / GİB Rapor XML'i formatında teslim edilmekte mi?	

ÖEBSD_SIS.7: Hizmet Yazılımlarına İlişkin Kontroller		
e-İrsaliye		
Kontrol No	**Kontrol Maddesi**	**Sonuç**
	1. Güvenlik	
L1	Her kullanıcı sadece kendi firması adına irsaliye gönderebilmekte mi?	
L2	Her kullanıcı sadece yetkisi olduğu firmanın alıcısı veya satıcısı olduğu irsaliyeleri görebilmekte mi?	
L3	Her kullanıcı sadece kendi firması adına irsaliye yanıtı gönderebilmekte mi?	
L4	Her kullanıcı sadece kendi firmasının alıcısı veya satıcısı olduğu irsaliyelere verilen irsaliye yanıtlarını görebilmekte mi?	
	2. İşlem Kayıtlarının Saklanması	
L5	Kullanıcıların yaptığı tüm işlemlerin kayıtları saklanmakta mı?	
L6	Kullanıcıların yaptığı tüm işlemleri içeren kayıtların değişmezliği sağlanmakta mı?	
	3. Standartlara Uyum	
L7	Web ara yüzünde veya web servis, SFTP vb. gibi çeşitli kanallarla müşterilerden alınan bilgilerle oluşturulan UBL irsaliyeler son halinde saklanmadan ve gönderilmeden önce GİB tarafından yayınlanan güncel şematron (schematron) kontrolünden geçirilmekte mi?	
L8	Özel entegratör tarafından imzalanmayıp farklı kanallardan imzalı olarak alınan irsaliyeler son halinde saklanmadan ve gönderilmeden önce imza kontrolünden geçirilmekte mi?	

L9	Özel entegratör tarafından imzalanan irsaliyeler imzalanırken GİB'in belirlediği standartlara uyarak imzalanmakta mı?	
L10	Özel entegratör tarafından imzalanan irsaliyeler imzalanırken imza sertifikasının geçerlilik süreleri kontrol edilmekte mi?	
L11	Özel entegratör tarafından imzalanan irsaliyeler imzalanırken imza sertifikasının geçerlilik süreleriyle CRL ve OCSP sonuçları kontrol edilmekte mi?	
L12	İrsaliye ve irsaliye yanıtlarının gönderimi için oluşturulan zarflar GİB'e gönderilemezse müşterilerin müdahalesine gerek kalmadan bir süre sonra yeniden denenmekte mi?	
L13	Gönderilen irsaliye veya irsaliye yanıtlarının zarf durum sorguları gönderim anından itibaren hemen ve sık sık yapılmamakta, sadece gönderim tarihinden itibaren 24 saat içinde GİB'den ve alıcıdan sistem yanıtı gelmeyen zarfların durumları GİB'den kontrol edilmekte ve en sık 5 saatte bir sorgulanmakta mı?	
L14	GİB tarafından iletilen zarflar hemen kontrol edilip işlenmemekte kaydedilip hemen dönülmekte, kontrol ve işleme daha sonra yapılmakta mı?	
L15	GİB tarafından iletilen zarflar kontrol edilip işlendikten sonra hatalı veya hatasız olarak sistem yanıtı dönülmekte mi?	
L16	Oluşturulan sistem yanıtlarının gönderilip gönderilemedikleri veya gönderildikten sonra başarıyla işlenip işlenemedikleri belirli aralıklarla sorgulanarak yeniden gönderilmekte mi?	
L17	Alınan zarflar kontrol edilirken GİB tarafından yayınlanan güncel şema kontrolleri yapılmakta ve geçersiz olanlar kabul edilmeyip hatayı gösteren sistem yanıtı dönülmekte mi?	
L18	Alınan zarflar kontrol edilirken GİB tarafından yayınlanan güncel şematron (schematron) kontrolleri yapılmakta ve geçersiz olanlar kabul edilmeyip hatayı gösteren sistem yanıtı dönülmekte mi?	
L19	Alınan zarflar kontrol edilirken irsaliye ve irsaliye yanıtları için imza olup olmadığı, varsa geçerli olup olmadığı kontrol edilmekte ve geçerli imzalar için geçerli, geçersiz imzalar için geçersiz şeklinde sistem yanıtı dönülmekte mi?	
L20	Alınan irsaliye ve irsaliye yanıtları için oluşturulan sistem yanıtları sadece sistem tarafından otomatik olarak oluşturabilmekte, kullanıcıların web servis gibi yöntemlerle sistem yanıtı zarfları göndermesine izin verilmemekte mi?	
L21	Gelen irsaliyelere zarfın alınma zamanından itibaren 7 gün içinde irsaliye yanıtı oluşturulabilmekte daha sonra irsaliye yanıtı oluşturulamamakta mı?	
L22	Gelen irsaliyeler zarfın alınma zamanından itibaren 7 gün içinde irsaliye yanıtı gönderilebilmekte daha sonra irsaliye yanıtı gönderilmekte mi?	
L23	Gelen irsaliyelere irsaliye yanıtı oluşturulup oluşturulamayacağı kontrol edilirken irsaliyenin alındığı saat kontrol edilmemekte irsaliye yanıtının 7. günde 23:59'a kadar oluşturulmasına izin verilmekte mi?	
L24	Gelen irsaliyelere bir defa irsaliye yanıtı verildiğinde bir daha irsaliye yanıtı oluşturulmasına izin verilmemekte mi?	
L25	Gelen irsaliyelerin içindeki XSLT şablonlarındaki hatalar nedeniyle görüntülenemeyen irsaliyeler için GİB'in e-İrsaliye paketlerinde önerdiği gibi	

	bir varsayılan XSLT irsaliye şablonu kullanılabilmekte, en azından irsaliye numarası, irsaliye tarihi, notlar gibi temel bilgilerin görüntülenmesi sağlanabilmekte mi?	
L26	Gönderilen irsaliyelere gelen irsaliye yanıtları alıcının gönderilen zarfa gönderdiği sistem yanıtının özel entegratör tarafından alınma zamanından 8 gün sonrasına kadar kabul edilmekte, daha sonra gelen irsaliye yanıtları kabul edilmemekte mi?	
L27	Gönderilen irsaliyeye daha önce irsaliye yanıtı geldiyse gelen irsaliye yanıtı kabul edilmemekte mi?	
L28	Gönderilen irsaliye ve irsaliye yanıtlarına GİB veya alıcı tarafından hatalı sistem yanıtı dönülmesi durumunda yeni irsaliye ve irsaliye yanıtı oluşturulması gerekmeyen durumlarda yeni irsaliye ve irsaliye yanıtı oluşturulması zorlanmadan mevcut irsaliye ve irsaliye yanıtı farklı bir zarfa konarak gönderilebilmekte mi?	
L29	Gönderilen irsaliye ve irsaliye yanıtlarının gönderim sonucu belirlenene kadar veya başarılı olduktan sonra yeniden başka bir zarfla gönderilmesine izin verilmemekte mi?	
L30	Özel entegratör, müşteri firmanın istemesi durumunda irsaliyelerini kendi mali mührüyle imzalamasına imkân sağlamakta mı?	
	4. Hizmetin Kapatılması	
L31	Hizmeti kapatmak isteyen müşteri için GİB'e kapatma isteği gönderilmekte mi?	
L32	Hizmeti kapatmak isteyen müşterilere irsaliye ve irsaliye yanıtları UBL ya da zarf olarak XML formatında teslim edilmekte mi?	

EK 2. Denetçinin Görüşünü Oluşturması İçin Kılavuz

Denetçi, EK 1'de verilen 12 kontrol tablosunda yer alan toplam 208 kontrol maddesine göre denetim görüşünü oluşturacaktır. Görüşün oluşturulmasında, denetçinin uygulayacağı ilkeler aşağıda açıklanmıştır:

1. "Olumlu görüş" için, 208 kontrol maddesinin en az 166 maddesinin yanıtı "E" olmalı,

2. 1. Maddede belirtilen koşul sağlanmış olsa dahi, herhangi bir değerlendirme sınıfından "E" yanıtlarının sayısı %70'in altında kalıyorsa "olumlu görüş" verilemez. %70 için hesaplanacak madde sayısı, o değerlendirme sınıfındaki toplam kontrol maddesinin %70'i tam sayıya karşılık gelmiyorsa, bulunan sayıdan küçük en büyük tamsayıdır.

3. "Olumlu görüş" verilememiş ise, verilecek görüş; "H", "K" veya "G" cevaplarından sayısı fazla olana göre, sırasıyla "olumsuz", "şartlı görüş" veya "görüşten kaçınma" kanaatine varılır.

Denetçi, kanaatinin oluşmasına dayanak bulgularını raporunda açıkça yazar. Bununla birlikte denetçi, bu Kılavuzda açıkça yazılmamış olsa dahi, her türlü görüş ve önerisine denetimin amacı ve kapsamına uygun olmak kaydıyla raporunda ayrıca yer verebilir.

EK 3. ÖEBSD Rapor Formatı

KAPAK

DİZİN

DENETİM GÖRÜŞ YAZISI

EK 4'de yer alan şablonlara uygun biçimde denetim görüş yazısı burada yer alır.

I- GENEL BİLGİ

Denetimin konusu ve kapsamı, denetim faaliyeti gerçekleştirilen özel entegratöre ilişkin tanımlayıcı bilgiler, denetim tarihleri, denetimin kapsadığı faaliyet dönemi ve denetim yapıldığı yer(ler) burada yazılır.

II- ÖEBSD DEĞERLENDİRMESİ

Denetim faaliyeti, kanıtları ve olguları içerecek biçimde burada açıklanır. EK 1'da yer alan tüm kontrollerin değerlendirmesi, ek belgeler, yorumlar ve açıklamalar ile EK 2'de yer alan kılavuza göre değerlendirme sonucuna nasıl ulaştığına bu bölümde yer verilir. Her değerlendirme sınıfı alt bileşeni ayrı bir başlık altında ele alınır. Bu Kılavuzda yer almayan veya yorumunda tereddüt duyulan bir hususla karşılaşılması halinde, uluslararası kabul görmüş bilgi teknolojileri kontrol hedefleri sunan COBIT dokümanlarında yer alan usul ve esaslara göre yapılan değerlendirme de ayrı bir başlık altında burada açıklanır.

EK 4. Olumlu, Şartlı, Görüşten Kaçınma ve Olumsuz Görüş Yazısı Şablonları

ÖZEL ENTEGRATÖRLER BİLGİ SİSTEMLERİ DENETİM RAPORU

Olumlu Görüş

.....Yönetim Kuruluna / Yönetimine:

..... A.S.'nin ...../...../..... tarihi itibarıyla ...../...../..... tarih ……. sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında bilgi sistemleri süreçlerini denetlemekle görevlendirilmiş bulunuyoruz.

[ÖE Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri süreçleri üzerindeki kontrollerin denetlenen nezdinde ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri süreçleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve ...../...../..... Tarih ve …….sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri süreçleri ile bu sistem ve süreçler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.

Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri süreçleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

[Bağımsız Denetçi Görüşü]

Görüşümüze göre, bütün önemli taraflarıyla, ...'nin ...../...../..... tarihi itibarıyla bilgi sistemleri süreçlerini üzerinde, .../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuzunda belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Raporun Düzenleme Yeri ve
Tarihi
Sorumlu Bilgi Sistemleri Baş Denetçisinin
Adı ve Soyadı, İmzası
Kuruluşun Ticari Unvanı
Sorumlu Ortak Baş Denetçinin
Adı ve Soyadı, İmzası
Kuruluşun Ticari Unvanı

ÖZEL ENTEGRATÖRLER BİLGİ SİSTEMLERİ DENETİM RAPORU

Şartlı Görüş

..... A.S. Yönetim Kuruluna:
..... A.S.'nin ...../...../..... tarihi itibarıyla ...../...../..... tarih …… sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında bilgi sistemleri süreçlerini denetlemekle görevlendirilmiş bulunuyoruz.
[ÖE Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri süreçleri üzerindeki kontrollerin denetlenen nezdinde ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.S. Yönetimi'nin sorumluluğundadır.
[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]
Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri süreçleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve ...../...../..... tarih ve …….sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri süreçleri ile bu sistem ve süreçler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.
Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.
[Doğal Kısıtlar]
Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri süreçleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.
(Bağımsız denetim faaliyetine getirilen sınırlandırma ve bu nedenle denetlenemeyen süreçler, uygulamalar, kontroller; denetlenenin bilgi sistemleri süreçleri üzerinde tespit edilen önemli kontrol eksiklikleri ve bu kontrol eksikliklerinin denetlenenin bilgi sistemleri süreçlerinin bütününü veya büyük bir kısmını etkilememesine ilişkin görüşüne esas neden ve gerekçeler)

[Bağımsız Denetçi Görüşü]
Görüşümüze göre, yukarıda *(....ncı paragrafta)* açıklanan *husus(lar) nedeniyle,* denetlenenin bilgi sistemleri üzerinde bu *hususun/hususların* muhtemel etkileri haricinde bütün önemli taraflarıyla, ... A.S.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri süreçleri üzerinde, .../...../.....tarih ve …… sayılı Resmi Gazete'de ÖEBSD Hakkında Kılavuzda belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Raporun Düzenleme Yeri ve
Tarihi
Sorumlu Bilgi Sistemleri Baş Denetçisinin
Adı ve Soyadı, İmzası
Kuruluşun Ticari Unvanı
Sorumlu Ortak Baş Denetçinin
Adı ve Soyadı, İmzası
Kuruluşun Ticari Unvanı

ÖZEL ENTEGRATÖRLER BİLGİ SİSTEMLERİ DENETİM RAPORU

Olumsuz Görüş

..... A.Ş. Yönetim Kuruluna:
..... A.Ş.'nin ...../...../..... tarihi itibarıyla ...../...../..... tarih ……. sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında bilgi sistemleri süreçlerini denetlemekle görevlendirilmiş bulunuyoruz.
[ÖE Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri süreçleri üzerindeki kontrollerin denetlenen nezdinde ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.
[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]
Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri süreçleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve ...../...../..... Tarih ve …….sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri süreçleri ile bu sistem ve süreçler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.
Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.
[Doğal Kısıtlar]
Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri süreçleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Denetlenenin bilgi sistemleri süreçleri üzerindeki kontrollerin etkin, yeterli ve uyumlu bulunmama Sebepleri)

[Bağımsız Denetçi Görüşü]

Görüşümüze göre, yukarıda *(....ncı paragrafta)* açıklanan *husus(lar) nedeniyle,*..... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri süreçleri üzerinde, .../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuzunda belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmemiştir.

Raporun Düzenleme Yeri ve
Tarihi
Sorumlu Bilgi Sistemleri Baş Denetçisinin
Adı ve Soyadı, İmzası
Kuruluşun Ticari Unvanı
Sorumlu Ortak Baş Denetçinin
Adı ve Soyadı, İmzası
Kuruluşun Ticari Unvanı

ÖZEL ENTEGRATÖRLER BİLGİ SİSTEMLERİ DENETİM RAPORU

Görüşten Kaçınma

..... A.S.'nin ...../...../..... tarihi itibarıyla ...../...../..... tarih ……. sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz bilgi sistemleri süreçlerini denetlemekle görevlendirilmiş bulunuyoruz.

[ÖE Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri süreçleri üzerindeki kontrollerin denetlenen nezdinde ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuzda belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması
……. A.S. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]
Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri süreçleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve ...../...../..... tarih ve ……sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuzda belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri süreçleri ile bu süreç ve sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.
Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.
(Denetçinin görüş bildirmemesinin nedenleri)
[Bağımsız Denetçi Görüşü]
Yukarıda (...ncı paragrafta) açıklanan husus(lar) nedeniyle ..... A.S.'nin ...../...../.....
tarihi itibarıyla bilgi sistemleri süreçleri üzerinde tesis edilen kontrollerin etkinliği, yeterliliği ve uyumluluğu hakkında görüş bildirmiyoruz.

Raporun Düzenleme
Yeri ve Tarihi
Sorumlu Bilgi Sistemleri Baş Denetçisinin
Adı ve Soyadı, İmzası
Kuruluşun Ticari Unvanı
Sorumlu Ortak Baş Denetçinin
Adı ve Soyadı, İmzası
Kuruluşun Ticari Unvanı