ICT Bulut Bilişim AŞ

23.06.2026 için ISAE 3402 Tip 1

Operasyonel Kontrollerin Test Edilmesi Hakkında Rapor

İÇİNDEKİLER

BÖLÜM 1

1. BAĞIMSIZ HİZMET DENETÇİSİ RAPORU

Deloitte.

Kontrollerin Tanımı ve Tasarımı Hakkında Bağımsız Hizmet Denetçi Güvence Raporu

ICT Bulut Bilişim AŞ Yönetim Kurulu'na

Kapsam

ICT Bulut Bilişim AŞ (bundan böyle Bulutistan olarak anılacaktır) ile "3. BULUTİSTAN SİSTEM TANIMI" bölümünde ifade edilen müşterilerine sunduğu Bulut ve Veri Merkezi Hizmetleri sistem tanımının ve tanımda ifade edilen kontrol hedefleri ile ilişkili kontrollerin tasarımının 23.06.2026 tarihi için raporlanması çalışmaları gerçekleştirilmiştir.

Bulutistan'ın Sorumlulukları

Bulutistan, "3. BULUTİSTAN SİSTEM TANIMI" bölümünde ifade edilen tanımın ve beraberindeki beyanın hazırlanmasından, tanımın ve beyanın eksiksizliğinden, uygunluğundan ve sunum yönteminden, tanımda kapsanan hizmetlerin sunulmasından, kontrol hedeflerinin belirlenmesinden, belirlenen kontrol hedeflerinin gerçekleşmesi için kontrollerin tasarlanmasından, uygulamaya alınmasından ve etkin bir şekilde işletilmesinden sorumludur.

Raporun 5. bölümündeki bilgiler, müşterileri için ilave bilgiler sağlamak için Bulutistan tarafından sunulmaktadır ve Bulutistan'ın operasyonunda yer alan kontrollerin tanımının bir parçası değildir. 5. Bölümdeki bilgiler, tanımın ve tanımda ifade edilen kontrol hedefleri ile ilişkili kontrollerin tasarımının denetlenmesinde uygulanan prosedürlere tabi tutulmamıştır.

Hizmet Denetçisi Sorumlulukları

Söz konusu çalışmada denetçi olarak sorumluluğumuz, prosedürlerimize dayanarak Bulutistan tanımı ve bu tanımda ifade edilen kontrol hedefleri ile ilişkili kontrollerin tasarımı hakkında görüş belirtmektir. Uluslararası Denetleme ve Güvence Standartları Kurulu (International Auditing and Assurance Standards Board) tarafından yayımlanan ISAE 3402 standardına (International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization") göre bir çalışma gerçekleştirilmiştir. Bu standart etik gereksinimlerle uyumlu olmamızı ve tanımın açık bir şekilde sunulması ve kontrollerin uygun şekilde tasarlanması hakkında tüm önemli açılardan kabul edilebilir bir güvence elde etmek amacıyla prosedürler planlamamızı ve gerçekleştirmemizi gerektirmektedir.

Bir hizmet organizasyonunun tanımını, kontrollerinin tasarımını raporlayan güvence çalışması hizmet organizasyonu sistem tanımı açıklamaları, kontrollerin tasarımı hakkında kanıt elde etmek amacıyla prosedürler gerçekleştirmeyi kapsamaktadır. Tanımın açık bir şekilde sunulmaması, kontrollerin uygun şekilde tasarlanmaması risklerinin değerlendirilmesini içeren prosedürler, hizmet denetçisi muhakemesine dayanarak seçilmiştir. Bu güvence çalışması aynı zamanda tanımın genel sunumunun, içinde ifade edilen hedeflerin uygunluğunun ve hizmet organizasyonu tarafından belirlenen ve Bölüm 3.4'de açıklanan kriterlerin de değerlendirilmesini kapsamaktadır.

Elde ettiğimiz kanıtların, görüşümüze dayanak oluşturmak için yeterli ve uygun olduğuna inanmaktayız.

Hizmet Organizasyonu Kontrollerindeki Sınırlamalar

Bulutistan'ın tanımı, müşterilerin ve onların denetçilerinin genel olarak ortak ihtiyaçlarını karşılamak amacıyla hazırlanmıştır ve bundan ötürü müşterilerin tek tek kendi özel ortamlarında önemli olduğunu değerlendirebildiği sistemin her bir parçasını içermeyebilir. Ayrıca doğası gereği, bir hizmet organizasyonundaki kontroller, işletim veya raporlama işlemlerinde oluşan tüm hataları veya eksiklikleri önleyemeyebilir veya tespit edemeyebilir. Gelecek dönemlerin etkinliğinin değerlendirilmesi öngörüsü de bir hizmet organizasyonundaki kontrollerin uygun olmayan veya hatalı hale gelebilmesi riskine bağlıdır.

Olumlu Görüş

Görüşümüz, bu raporda açıklanmış hususlara dayanarak oluşturulmuştur. Görüşümüzü oluştururken kullandığımız kriterler bölüm 3.4'de açıklanmıştır. Görüşümüze göre:

a) Sistem tanımı 23.06.2026 tarihinde tasarlandığı haliyle sistemi uygun bir biçimde sunmaktadır ve

b) Tanımda belirtilen kontrol amaçlarıyla ilgili kontroller 23.06.2026 tarihinde uygun bir şekilde tasarlanmıştır.

Kontrol Testlerinin Tanımı

Test edilen belirli kontroller ve bu testlerin yapısı, zamanlaması ve sonuçları Bölüm 4'de yer almaktadır.

Hedef Kullanıcılar ve Amaç

Bu rapor ve Bölüm 4'de yer alan kontrollerin testlerinin tanımı, müşterilerin finansal tablolarına ilişkin riskleri müşteriler tarafından işletilen kontrollere ait bilgiler gibi ilave bilgilerle değerlendirmek için yeterli fikre sahip Bulutistan sistemlerini kullanan müşterileri ve denetçilerini hedeflemektedir.

İstanbul, 23.06.2026

Barış Bağcı

Sorumlu Bilgi Sistemleri Başdenetçisi

DRT Bağımsız Denetim ve Serbest Muhasebeci Mali Müşavirlik AŞ

Member of **DELOITTE TOUCHE TOHMATSU LİMİTED**

BARIŞ BAĞCI
Digitally signed by BARIŞ BAĞCI
Date: 2026.06.23 16:43:16 +03'00'

BÖLÜM 2

2. BULUTİSTAN YÖNETİM BEYANI

2.1. YÖNETİM BEYANI

ICT BULUT BİLİŞİM AŞ

Tarih: 04.05.2026

DRT Bağımsız Denetim ve Serbest Muhasebeci Mali Müşavirlik AŞ'ye

Bu mektubu, tarafınızca gerçekleştirilen veri merkezi hizmetlerine ilişkin operasyonel kontrollerin ve işletim etkinliğinin test edilmesine yönelik denetim kapsamında iletiyoruz. Mektubumuzda, 04.05.2026 tarihi itibariyle sistem tanımımızda belirtilen kontrol hedefleri, bu kontrol hedeflerine ilişkin kontroller ve bu kontrollerin işletim etkinliklerine ilişkin bilgiler sunulmaktadır. Denetim çalışmalarınızın, "International Standards on Assurance Engagements" kapsamında gerçekleştirildiğini ve sadece verilen hizmetlere ilişkin kontrollerin tasarımı ile işletim etkinliklerine yönelik bir görüş oluşturulduğu tarafımıza iletilmiştir. Denetim boyunca, bu amaca ulaşmak için oluşturulan prosedürler uygulanmıştır.

Bu mektup ile aşağıdaki noktalarda sorumlu olduğumuzu bildirmekteyiz:

a. Yönetim mektubunu ve sistem tanımı dokümanını aşağıdaki hususlara uyarak hazırlamak:
   - Tasarlanan ve uygulanan kontrollerin durumunun sistem tanımı dokümanında etkilenen hizmet alanları seviyesinde iletilmesi,
   - Sistem tanımının, bütünlük ve doğruluk kontrollerinden geçirilerek iletilmesi.

b. Belirtilen hizmete özel kontrol hedeflerinin uygunluğu.

c. Kapsamdaki tüm hizmetlere ilişkin kontrollere sistem tanımı dokümanında yer verilmesi.

d. Sistem Tanımına göre belirlenmiş kontrol ortamının uygunluğunu tehdit edecek risk unsurlarının belirlenmesi.

e. Etkin ve sürekli bir iç kontrol mekanizması kurarak, ICT Bulut Bilişim AŞ yönetimi tarafından seçilen kriterler doğrultusunda ICT Bulut Bilişim AŞ iç kontrol sisteminin kurgulanmasının sağlanması.

Aşağıda bahsi geçen konuların denetiminiz sırasında size iletildiğini onaylıyoruz:

1. "3. BULUTİSTAN SİSTEM TANIMI" bölümünde belirtilen Sistem Tanımı'na göre mutabık kaldığımızı tekrar onaylıyoruz.
2. Sistem tanımında yer alan kontrollere ilişkin tüm dokümanlar ve kayıtlar, gerekli tüm hizmet anlaşmaları ile bilgiler tarafınıza iletilmiştir. Sistem tanımı ayrıca müşteriler tarafından işletildiği kabul edilen kontroller hakkında bilgileri de içermektedir.
3. Denetim süresince gelecek tüm sorularınızı cevaplandırmayı kabul ediyoruz.
4. Bilgimiz dâhilinde müşterilerimize bir etkisi olabilecek, kendi yönetimimiz ya da çalışanlarımıza isnat edilen ve sistem tanımındaki kontrollerimizi etkileyecek, bu dokümanda belirtilecek kontrol hedeflerine ulaşmayı etkileyecek düzeltilmemiş hatalar, dolandırıcılık ya da yasadışı hiçbir eylem bulunmamaktadır.
5. Belirtilen kontrol hedeflerine ulaşmak için aşağıdaki hususlar haricinde herhangi bir kontrolde tasarım seviyesinde eksiklik bulunmamaktadır:

1

a. Gerçekleştirilen iş etki analizi kapsamında belirlenenen kabul edilebilir kesinti süreleri ve veri kaybı limitleri doğrultusunda, bilgi sistemleri servislerinin tekrar erişime açılabilmesini sağlayacak kurtarma prosedürlerinin tüm hizmetleri kapsayacak şekilde oluşturulmaması

b. Uygulama ve sistemler üzerinde kullanıcıların görev ve sorumluluklarına uygun olarak atanması gereken rollerin dokümante edilmemesi

6. Denetim süresi boyunca, kullanıcı aktivitelerini ya da finansal raporlamaları etkileyecek, sistem tanımında belirtilen kontrollerin etkinliği ve yönetim mektubunu etkileyecek bir kontrol değişikliği ve beklemedik olay olmamıştır.

7. Denetim süresi boyunca, hizmet verilen firmaları etkileyebilecek, kendi yönetimimiz veya çalışanlarımız tarafından yürürlükteki kanunlara uyumsuzluk yaratacak bir hata gerçekleşmemiştir.

8. Rapor içerisinde "5. BULUTİSTAN İLAVE BİLGİLERİ" bölümünün oluşturulması için sizin denetiminiz sırasında kapsanmayan ek bilgilerin sağlanmasından ve bu bilgilerin doğruluğundan sorumluyuz.

9. Sistem tanımında belirtilen kontrollerin tamamında denetim dönemi boyunca en az bir örnek oluşmuştur.

10. Bu denetim raporunun basılı kopyalarının oluşturulması gerektiğinde, dağıtımının bu anlaşmanın hükümleri altında yönetim ile hizmet alan kuruluşlar ve onların dış denetçileri ile sınırlı olacağını kabul ediyoruz.

11. Ict Bulut Bilişim AŞ olarak tarafınıza sunduğumuz ekteki sistem tanımı müşteri hizmetlerine yönelik süreçleri içermektedir. Bu tanımın hazırlanmasında izlenilen kriterler müşterilerin kendi çalışma ortamları dikkate alındığında sistem ile ilgili önemli olarak kabul edilen her bilgiyi içermektedir. Denetim raporu veya belirli bölümleri gerektiğinde potansiyel müşteriler ile sözlü olarak paylaşılabilecektir.

Saygılarımızla,

ICT BULUT BİLİŞİM AŞ adına,

YÖNETİM BEYANI

ICT Bulut Bilişim AŞ

Tarih: 04.05.2026

Sistem tanımı, ICT Bulut Bilişim A.Ş. (Bulutistan) tarafından veri merkezi hizmetleri alan müşterilerimiz ve sistem tanımını değerlendirebilecek yeterli bir anlayışa sahip denetçileri için hazırlanmıştır. Sistem tanımı ayrıca müşteriler tarafından işletildiği kabul edilen kontroller hakkında bilgileri de içermektedir. Aşağıda bahsi geçen konuların denetiminiz sırasında size iletildiğini onaylıyoruz:

1. Sistem tanımlarının, müşterilere sunulan hizmetleri ve uygulanmakta olan kontrol çerçevesini, 04.05.2026 tarihi itibariyle yansıttığını beyan ederiz. Bu beyanın dayandırıldığı ve değerlendirmeye konu olan öğeler:
   a) Müşterilere sunulan hizmetlerin nasıl tasarlandığı ve iletildiğine dair kapsama alınan aşağıdaki süreç adımlarını kapsamaktadır. Sistemin aşağıdaki noktalarda, ilgili kontrollerin tasarlanması ve operasyonel etkinliklerinde nasıl yer aldığını belirtmektedir:
      i. Şirketimizin sunduğu hizmetleri destekleyen bilgi sistemleri süreçleri ve organizasyon yapısının yönetimi,
      ii. Sunulan hizmetlere ilişkin bilgi güvenliği prensiplerinin tanımlanması, yönetilmesi ve izlenmesi,
      iii. Sunulan hizmetlere konu olan bileşenlerde oluşan problemlere müşteriler ve Şirketimiz tarafından yapılan müdahale ve çözüm süreçlerinin yönetimi,
      iv. Hem otomatik hem manuel sistemlerdeki süreçlere göre başlatılan, yetki verilen, kaydedilen, işlenen, gerektiği gibi düzeltilen prosedürler,
      v. Sistemin, iz kayıtları ve işlemlere ilişkin önemli olaylara ilişkin kontrol süreci,
      vi. Belirlenmiş kontrol hedefleri ve hedeflerin gerçekleştirilmesi için tasarlanmış kontroller,
      vii. Kontrol ortamının tüm aşamaları, risk değerlendirme süreci, bilgi ve iletişim teknolojileri kontrol aktiviteleri ile sistemin işlemleri işlemesi ile ilgili kontroller,
      viii. Sistemin, işlemler dışındaki önemli olayları ve durumları ne şekilde ele aldığı,
      ix. Müşteri hizmetlerinin yürütülmesi ve raporlanmasıyla ilgili olan kontrol çevresinin, risk değerlendirme sürecinin, bilgi sistemi ve iletişiminin, kontrol faaliyetlerinin ve izleme kontrollerinin diğer yönleri,
   b) Açıklanan sistemin hizmet alan taraflar ve bu tarafların bağımsız denetçilerinin ihtiyaçlarını geniş bir yelpazede karşılamak için hazırlanmış olduğunu beyan etmekteyiz. Bununla beraber ilgili taraflar sisteme ilişkin kontrollerini kendi aldığı hizmetlere yönelik olarak değerlendirmelidir. Sistem tanımının çok sayıda müşterinin ve onların denetçilerinin ortak ihtiyaçlarını karşılamak üzere hazırlandığı ve dolayısıyla her bir müşterinin kendi özel çevresi açısından önemli olabileceğini düşündüğü sistemin her yönünü kapsamayabileceği kabul edilmekle birlikte; tanımlanan sistemin kapsamıyla ilgili bilgileri içermektedir -eksiksiz göstermektedir- veya bu bilgileri çarpıtmamaktadır.

1

2. Beyan bir dönemi kapsamakta ve kapsanan dönem boyunca Şirketimizin sistem ile ilgili değişim detaylarını da kapsamaktadır.
3. Kontrol tanımlarının, Şirketimizin sunduğu hizmetlerdeki değişiklikleri bu beyanla kapsanan zaman aralığı süresince doğru ve tam olarak yansıttığını beyan ederiz.
4. Kontroller, sistem tanımındaki kontrol hedeflerine uygun olacak şekilde tasarlanmıştır. Bu kontroller için belirlenmiş kriterler aşağıdaki gibidir:
   a) Kontrol hedeflerinin başarılı olmasını engelleyebilecek riskler tarafımızca belirlenmiştir.
   b) Belirlenen kontroller, tanımlandığı şekilde işletildiği takdirde, bu risklerin kontrol hedeflerinin başarılı olmasını engelleyememesine yönelik kabul edilebilir bir güvence vermektedir.
   c) Otomatik kontroller tasarıma tutarlı şekilde uygulanmıştır, manuel kontroller, uygun yetkinlik ve yetkiye sahip kişiler tarafından uygulanmaktadır.

Unvan: Ekrem Şekman

İmza:

ICT BULUT BİLİŞİM A.Ş.
Kısıklı Çamlıca Mah. Alaaddin Cad. No: 55 Üsküdar/İST.
Tel: 0850 222 65 98 Mersis No: 0465 0459 9710 0011
Üsküdar V.D: 468 045 9971 Tic.Sic.No: 983551-0

B.Ö

2.2. BEYANIN GEREKÇELERİ (KRİTERLER)

Bu beyanın hazırlanmasında izlenen kriterler aşağıdaki gibidir:

- İşlemlerin sınıflandırılması,
- Hem otomatik hem manuel sistemlerdeki süreçlere göre başlatılan, yetki verilen, kaydedilen, işlenen, gerektiği gibi düzeltilen prosedürler,
- Sistemin, iz kayıtları ve işlemlere ilişkin önemli olaylara ilişkin kontrol süreci,
- Belirlenmiş kontrol hedefleri ve hedeflerin gerçekleştirilmesi için tasarlanmış kontroller,
- Kontrol ortamının tüm aşamaları, risk değerlendirme süreci, bilgi ve iletişim teknolojileri (ilgili iş süreçleri de dâhil olmak üzere) kontrol aktiviteleri ile sistemin işlemleri işlemek ile ilgili kontroller,
- Bilgi sistemleri genel kontrolleri, önemlilik kriteri esas alınarak belirlenen kapsam dâhilinde uyumluluk, etkinlik ve yeterlilik açısından incelemeye tâbi tutulmuştur.
- Genel kontroller, tesis edilmelerinde esas alınan çerçeve, standart ya da metodolojiden bağımsız olarak; mevzuat hükümleri de gözetilerek, COBIT başta olmak üzere genel kabul görmüş disiplin ve çerçevelere ve iş süreçlerine göre belirlenmiştir.
- Kontrol hedeflerinin başarılı olmasını engelleyebilecek riskler tarafımızca belirlenmiştir.
- Belirlenen kontroller, tanımlandığı şekilde işletildiği takdirde, bu risklerin kontrol hedeflerinin başarılı olmasını engelleyememesine yönelik kabul edilebilir bir güvence vermektedir.
- Otomatik kontroller tasarıma tutarlı şekilde uygulanmıştır, manuel kontroller, uygun yetkinlik ve yetkiye sahip kişiler tarafından uygulanmaktadır.
- Şirket bünyesinde oluşturulan kontroller 23.06.2026 tarihi için tasarlandığı şekilde uygulanmaktadır.

BÖLÜM 3

3. BULUTİSTAN SİSTEM TANIMI

3.1. GİRİŞ

Bu rapor ICT Bulut Bilişim AŞ'nin (Bulutistan) müşterileri ve ilgili müşterilerin denetçileri için ve ISAE 3402 (International Standard on Assurance Engagements 3402) standardının gereksinimlerini yerine getirmek üzere hazırlanmıştır. Hizmet Organizasyonunda bulunan kontrollere ilişkin güvence raporudur. Bu rapor Bulut ve Veri Merkezi hizmetlerine ilişkin kontrollerin tanımlanmasına yönelik, bu hizmetleri kullanan müşteriler için hazırlanmıştır.

3.2. RAPORUN KAPSAMI

Bu rapor Bulut ve Veri Merkezi hizmetlerine ilişkin geçerli kontrollerin tanımlanmasına yönelik olarak oluşturulmuştur. Bulut ve Veri Merkezi hizmetlerine yönelik Bulutistan iç kontrolleri ile ilişkili kontrol hedeflerine odaklanmaktadır.

Raporun kapsamı, Bulutistan'ın müşterileri için finansal raporlama bakış açısından ve destekleyen genel bilgisayar kontrolleri için önemli olan kritik iş süreçlerini içermektedir. Kapsam, Bulutistan ve müşterileri tarafından seçilen Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik (Yönetmelik) süreçleri dikkate alınarak belirlenmiştir. Bulutistan, bu süreçlere ilişkin Yönetmelik kontrol hedeflerinin ve bu kontrol hedeflerini gerçekleştirmek için oluşturulan ve işletilen manuel ve otomatik kontrollerin belirlenmesinden sorumludur.

Bu rapor Bulut ve Veri Merkezi hizmetleri alan Bulutistan müşterileri için hazırlandığından, bahsi geçen hizmetler dışında oluşabilecek farklı müşteri ihtiyaçları bu raporun kapsamı dışındadır.

3.3. BULUTİSTAN HAKINDA GENEL BİLGİ

Bulutistan, 2015 yılından bu yana bulut hizmet sağlayıcısı olarak faaliyet göstermekte olup, Türkiye'nin önde gelen yerel bulut sağlayıcıları arasında yer almaktadır. 1000'i aşkın müşterisi ve 350'den fazla iş ortağı ile hizmet ağını sürekli genişletmektedir. Merkezi İstanbul'da bulunan şirket; Türkiye'de 3 ilde, 8 farklı veri merkezinde ve yurt dışında Bakü, Frankfurt, Londra ve Özbekistan'daki altyapıları ile 60'tan fazla ülkeye hizmet sunmaktadır. 107 kişilik uzman kadrosu ve çözüm ortaklarıyla toplamda 500 kişilik bir ekip tarafından yönetilen Bulutistan, 2024 yılında Turcorn programına seçilen ilk ve tek bulut hizmet sağlayıcısı olmuştur. Aynı yıl, Sabancı Holding'in dijital teknoloji şirketi DxBV tarafından yapılan yatırım kapsamında şirketin %65'i yaklaşık 39 milyon ABD doları bedelle satın alınmış, Sabancı Topluluğu'nun etkin ortaklık oranı %75,5 seviyesine ulaşmıştır. Bulutistan; siber güvenlik, veri ve ağ güvenliği, olay müdahalesi, sistem çözümleri ve danışmanlık hizmetlerinin yanı sıra hibrit ve çoklu bulut yönetimi, DevOps, veri tabanı yönetimi, izleme ve konteyner yönetimi (Kubernetes, Docker, Rancher) gibi alanlarda uçtan uca çözümler sunarak kurumların dijital dönüşüm süreçlerini desteklemektedir.

3.4. KRİTER

Aşağıdaki genel bilgi ve kontrol kriterleri sistemin bütününün ve süreç tanımlarının hazırlanmasında, kontrollerin uygun şekilde tasarlanmış olup olmadığının değerlendirilmesinde kullanılmıştır. Bu kriterler, bankacılık mevzuatı gibi Bulutistan müşterilerinin yasal ve iş gereksinimlerinden alınmıştır.

- Gizlilik - Bilgi varlığının sadece, Yönetim tarafından iş gereklerine uygun olarak erişim hakkı tanınmış kişiler tarafından izlenebilir olması
- Bütünlük - Bilgi varlığının saklandığı veya iletildiği medyalarda sadece düzenlenmiş uygun yöntemler ile değişime uğratılması ve/veya orijinal halinin korunması
- Erişilebilirlik - Bilgi sistemleri hizmetlerinin Şirket amaçlarına hizmet edecek yönde zamanında kullanılabilmesi
- Etkinlik - Bilginin, müşteri iş süreçleri ihtiyaçları ile ilgili ve bu ihtiyaçlara cevap verir nitelikte olması
- Verimlilik - Bilginin, kaynakların en etkin kullanımı ile elde edilmesi
- Uyumluluk - Kanun, düzenleme ve sözleşmelere uyumun sağlanması
- Güvenilirlik - Yönetimin finansal ve diğer raporlamalar için güvenilir veriye ulaşabilmesi

3.5. KONTROL ORTAMI, RİSK DEĞERLENDİRME VE İZLEME

Bulutistan'ın kontrol ortamı, üst yönetimin değerlerini ve kurumsal risk yaklaşımını yansıtmaktadır. Sunulan hizmetlerin sürekliliği, güvenliği ve kalitesi için oluşturulan kontrol ortamının temel unsurları aşağıdaki gibidir:

- **Yönetim Kurulu ve Genel Müdür Tarafından Gözetim:** Stratejik yönetişim ve iç kontrol süreçleri, Yönetim Kurulu ve Genel Müdür düzeyinde izlenmekte ve denetlenmektedir.
- **Organizasyonel Yapı**: Fonksiyonel ayrışma ve rol bazlı sorumluluklar ile iş süreçleri yapılandırılmış; görev tanımları ve yetkilendirme süreçleri net olarak belirlenmiştir.
- **İnsan Kaynakları Politikaları ve Prosedürleri:** İşe alım, oryantasyon, performans yönetimi ve sürekli eğitim süreçleri, bilgi güvenliği ve iş sürekliliği gerekliliklerini destekleyecek şekilde düzenlenmiştir.
- **Risk Yönetimi ve İzleme:** Tüm iç kontrol mekanizmaları düzenli olarak izlenmekte, bulgular üst yönetime raporlanmakta ve gerekli iyileştirmeler uygulanmaktadır.

Bulutistan, organizasyonel ve operasyonel olarak müşterilerinden bağımsız hareket etmekte olup, bilgi güvenliği, gizlilik ve tarafsızlık ilkeleri doğrultusunda yapılandırılmıştır. Sorumluluklar, süreçlere göre farklı birimler arasında açık şekilde paylaşılmıştır.

3.5.1. Yönetim Kurulu ve Genel Müdür Tarafından Gözetim

Bulutistan'da Yönetim Kurulu ve Genel Müdür, şirketin stratejik yönetişiminden nihai olarak sorumlu olup, kurum politikalarının belirlenmesi, uygulanmasının gözetimi ve genel işleyişin denetimi görevlerini üstlenmektedir. Yönetim Kurulu ve Genel Müdür, yılda en az bir kez olmak üzere periyodik olarak toplanarak şirketin operasyonel performansını, finansal sürdürülebilirliğini ve müşteri memnuniyetini kapsamlı biçimde değerlendirir. Bu kapsamda üst yönetimin sorumluluk alanları şunları içermektedir:

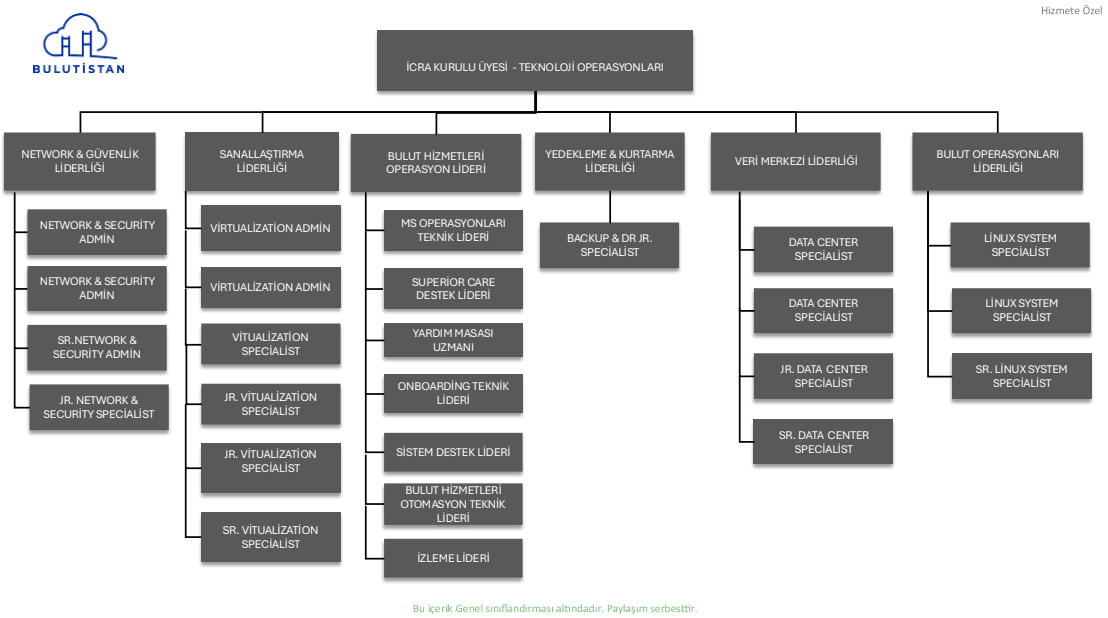
- **Finansal Durumun Yönetimi:** Şirketin mali yapısının sürdürülebilirliği, büyüme hedefleriyle uyumlu bütçe ve yatırım kararlarının alınması,
- **Müşteri İlişkileri Yönetimi:** Müşteri memnuniyeti, hizmet kalitesi ve sözleşmeye dayalı yükümlülüklerin etkin şekilde yerine getirilmesinin gözetimi,
- **Operasyonel Hizmet Sürekliliği:** Bulut altyapılarının kesintisiz hizmet verebilmesi için iş sürekliliği ve felaket kurtarma planlarının geliştirilmesi ve uygulanmasının sağlanması.

Bu yönetim yapısı, Bulutistan'ın stratejik hedeflerine ulaşmasını, paydaşlarına değer yaratmasını ve yüksek müşteri memnuniyetinin korunmasını sağlamaktadır.

3.5.2. Organizasyon Şeması

Bulutistan 107 kişilik uzman kadrosu ve stratejik iş ortaklarıyla birlikte toplamda 500 kişilik bir ekip ile hizmet vermektedir. Bulutistan Operasyon Departmanı, Operasyondan Sorumlu İcra Kurulu Üyesine bağlı olarak Bulut Operasyon Müdürü'nün yönetiminde Linux Sistem Yönetimi, Bulut Operasyonları Yönetimi, Ağ ve Güvenlik Yönetimi, Sanallaştırma Yönetimi, Veri Merkezi Yönetimi, Yedekleme & Felaket Kurtarma Yönetimi birimlerinden oluşmaktadır. Bulutistan organizasyon şeması aşağıdaki gibidir:

Bulutistan organizasyon yapısı, fonksiyonel uzmanlık ilkesi doğrultusunda kurgulanmış olup, müşteri memnuniyetine, hizmet kalitesine ve sürdürülebilir operasyonel başarıya öncelik vermektedir.



Şekil 1: Bulutistan Operasyon Departmanı Organizasyon Şeması

3.5.3. İnsan Kaynakları Politika ve Prosedürleri

Bulutistan'da insan kaynakları süreçleri standart, belgelenmiş uygulamalar çerçevesinde yürütülmektedir. İşe alım uygulamaları, kurumun stratejik hedeflerine ve büyüme planlarına uygun şekilde planlanır. Üst yönetim, yıllık hedef ve iş gücü ihtiyaçlarını İnsan Kaynakları birimiyle birlikte değerlendirerek insan kaynağı planlamasını oluşturur. Kadro planlamasında aşağıdaki unsurlar dikkate alınmaktadır.

- Kurumsal vizyon ve büyüme stratejileri
- Yıllık iş planı ve operasyonel hedefler
- Mevcut çalışan profili ve yetkinlikler
- Teknolojik dönüşüm ve yeni ürün ihtiyaçları
- Organizasyonel gelişim ve yeniden yapılandırma gereksinimleri

İnsan Kaynakları Departmanı, Genel Müdür'ün onayı doğrultusunda yıllık işe alım bütçesini oluşturur ve tüm işe alım süreçleri sistematik olarak yönetilir.

Bulutistan'da İnsan Kaynakları yönetmelikleri kapsamında aşağıdaki başlıca alanlarda politikalar mevcuttur.

- **Etik ve Uyum:** Tüm çalışanlar için etik ilkelere ve davranış kurallarına uyum zorunludur.
- **Eğitim ve Gelişim**: Çalışanların mesleki ve kişisel gelişimlerini desteklemek amacıyla eğitim planları hazırlanır.
- **Gizlilik ve Veri Güvenliği**: Çalışanların kurum içi verileri güvenle kullanmasına yönelik bilinçlendirme yapılır.

Bulutistan, çalışanlarının yetkinliklerini artırmak ve kurumsal vizyonu yaygınlaştırmak amacıyla aşağıdaki alanlarda eğitimler düzenlemektedirç

- Teknik eğitimler (bulut altyapısı, güvenlik, yazılım vb.)
- Kurum kültürü ve vizyon eğitimleri
- Liderlik, iletişim ve kişisel gelişim eğitimleri

- Çalışan farkındalığının artırılması, süreçlerin standardize edilmesi ve uluslararası uyumluluğun sağlanması için ISO Farkındalık eğitimleri

3.6. RİSK DEĞERLENDİRME VE İZLEME

3.6.1. Risk Değerlendirme

Bulutistan, operasyonel, finansal, bilgi güvenliği ve hizmet sürekliliği alanlarında karşılaşabileceği riskleri önceden tanımlamak, analiz etmek ve gerekli kontrol mekanizmalarını oluşturmak amacıyla düzenli olarak risk değerlendirme faaliyetleri yürütmektedir. Risk yönetimi süreci, ISO standartları çerçevesinde yapılandırılmıştır.

Risk değerlendirme çalışmaları, birim yöneticileri ve üst yönetim katkısıyla yıllık olarak güncellenmekte, yeni projeler ve hizmetler öncesinde proaktif olarak gözden geçirilmektedir. Tespit edilen riskler; olasılık, etki ve kontrol yeterliliğine göre derecelendirilmekte ve risk iştahı çerçevesinde aksiyon planları oluşturulmaktadır.

Ayrıca, Bulutistan Bilgi Güvenliği Yönetim Sistemi (BGYS), İş Sürekliliği Yönetim Sistemi (ISYS) ve Hizmet Yönetim Sistemi (HYS) kapsamında risklerin entegre şekilde izlenmesi ve yönetilmesi sağlanmaktadır. Kritik süreçler için düzenli olarak risk değerlendirme ve etki analizleri (BIA) gerçekleştirilmekte, bu sayede önleyici ve düzeltici faaliyetler planlı şekilde hayata geçirilmektedir.

Üst Yönetim, ticari, mali ve teknolojik riskleri tartışmak üzere düzenli olarak bir araya gelmektedir. Üst yönetim ayrıca birim müdürleri ile birlikte proje ve operasyonel risklerini değerlendirmek üzere gerekli görüldüğü takdirde toplantılar düzenlemektedir.

3.6.2. İzleme

Bulutistan'da izleme faaliyetleri; hizmet performansı, bilgi güvenliği, iş sürekliliği ve operasyonel risklerin kontrol altında tutulması amacıyla yapılandırılmıştır. İzleme süreçleri, ISO/IEC 20000-1, ISO/IEC 27001, ISO 22301 ve ISO 9001 standartlarına uyumlu şekilde sürdürülmekte olup, hem manuel hem de otomasyon destekli sistemlerle gerçekleştirilmektedir.

Operasyonel izleme faaliyetleri, aşağıdaki başlıca alanları kapsamaktadır.

- **Hizmet Performansı İzleme:** Hizmet Seviyesi Anlaşmaları bazlı anahtar performans göstergeleri, erişilebilirlik süreleri, kaynak kullanımı gibi performans göstergeleri sürekli olarak izlenir. Kritik metrikler, merkezi izleme araçları üzerinden görselleştirilir ve alarmlar tanımlanır.
- **Bilgi Güvenliği İzleme:** Güvenlik duvarı, saldırı tespit ve önleme sistemleri, veri sızıntısı önleme çözümleri, antivirüs yazılımları ve güvenlik bilgisi ve olay yönetim sistemi platformları aracılığıyla anormal aktiviteler, yetkisiz erişim girişimleri ve tehdit göstergeleri izlenir. Elde edilen bulgular düzenli olarak Bilgi Güvenliği Ekibi tarafından analiz edilir.
- **Değişiklik ve Olay İzleme:** Değişiklik yönetimi ve olay yönetimi sistemleri (ITSM platformu üzerinden) ile açılan her bir kayıt izlenir. Olayların çözüm süreleri, tekrarlanma sıklığı ve kök neden analizlerine göre iyileştirme aksiyonları belirlenir.
- **Risk ve Uyum İzleme:** Risk yönetimi süreciyle ilişkilendirilmiş kontrollerin uygulanma düzeyi, denetim bulguları ve düzeltici faaliyetlerin kapanma oranları sürekli olarak gözlemlenir. Regülasyonlara ve şirket politikalarına uyum; iç tetkikler, denetimler ve otomasyon tabanlı kontrol listeleriyle izlenir.
- **İş Sürekliliği İzleme:** Kritik sistemler için iş sürekliliği senaryoları kapsamında failover testleri, yedekleme senaryoları, kabul edilebilir kesinti süresi ve kabul edilebilir veri kaybı süresi değerlerinin takibi yapılır. Felaket kurtarma planlarının uygulanabilirliği düzenli tatbikatlarla test edilir.

Tüm izleme faaliyetleri kayıt altına alınmaktadır ve belirli periyotlarla Üst Yönetim'e, Kalite ve Bilgi Güvenliği ekiplerine raporlanmaktadır. Bulgular, Yönetim Gözden Geçirme Toplantıları'nda değerlendirilerek stratejik karar süreçlerine veri sağlamaktadır. Bu sayede, Bulutistan'da proaktif hizmet yönetimi ve sürekli iyileştirme kültürü desteklenmektedir.

3.7. BİLGİ & İLETİŞİM

3.7.1. Genel Bilgisayar Kontrolleri

Uygulama sistemlerinin geliştirildiği ve bakımının yapıldığı genel bilgisayar kontrolleri kontrol ortamını oluşturmaktadır. Bundan ötürü, genel bilgisayar kontrolleri Bulutistan hizmetleri kapsamında müşterileri tarafından kullanılmakta olan uygulama sistemlerindeki kontrollerin etkinliğini etkilemektedir. Aşağıdakiler Bulutistan ve hizmetleri ile ilişkili genel bilgisayar kontrollerini açıklamaktadır:

- Bilgi sistemleri politika, prosedür ve süreç dokümanları
- Bilgi güvenliği organizasyonu, roller ve sorumluluklar
- Kimlik ve erişim yönetimi
- İz kayıtlarının oluşturulması ve takibi
- Ağ Güvenliği
- Güvenlik konfigürasyonu yönetimi
- Güvenlik açıkları ve yama yönetimi
- Fiziksel güvenlik kontrolleri
- Siber olay yönetimi, sızma testi ve siber istihbarat paylaşımı
- Değişiklik yönetimi
- Erişilebilirlik yönetimi ve yedekleme
- Bilgi sistemleri sürekliliğinin sağlanması

3.7.2. Çalışanlarla İletişim

Bulutistan, çalışanlarıyla etkin, şeffaf ve sürekli iletişim kurmayı kurumsal kültürünün temel unsurlarından biri olarak görmektedir. Kurum içi iletişim, çalışanların beklentilerinin anlaşılması, katılımının artırılması ve stratejik hedeflerin kurum geneline yayılması açısından önemli bir rol oynamaktadır. Bu kapsamda aşağıda kullanılan başlıca iletişim araçları ve yöntemler belirtilmiştir.

- **Yönetimin Bilgilendirme Toplantıları:** Üst yönetim tarafından tüm çalışanlara yönelik olarak düzenlenen toplantılarda; şirketin güncel durumu, hedefleri ve gelişmeler paylaşılır.
- **İK Bültenleri ve Kurum İçi Duyurular:** İnsan Kaynakları birimi ve Kurumsal İletişim birimi tarafından yayınlanan dijital bültenlerle personel gelişimleri, yeni projeler ve etkinlikler hakkında bilgilendirme yapılır.
- **Yönetici ile Birebir Görüşmeler:** Departman yöneticileri, ekip üyeleriyle düzenli birebir görüşmeler yaparak kariyer planlaması, geri bildirim ve motivasyon konularını ele alır.
- **Kurumsal İletişim Platformları**: Microsoft Teams, e-posta grupları üzerinden tüm çalışanlar arasında bilgi paylaşımı ve hızlı iletişim sağlanır.
- **Anket ve Geri Bildirim Mekanizmaları:** Çalışan memnuniyeti anketleri, öneri kutuları ve açık kapı politikaları ile çalışanların görüş ve önerileri toplanır, değerlendirilir.
- **Sosyal ve Kültürel Etkinlikler:** Takım ruhunu ve kurum içi iletişimi güçlendirmek amacıyla düzenlenen çeşitli etkinlikler ile sosyal bağlar pekiştirilir.

Bulutistan, iletişim kanallarını sürekli olarak güncelleyip geliştirerek çalışan bağlılığını ve motivasyonunu artırmayı hedeflemektedir.

3.7.3. Hizmet Verilen Kurumlar

Bulutistan, müşterileriyle olan iletişimini güçlendirmek ve hizmet kalitesini artırmak amacıyla çeşitli iletişim kanalları kullanmaktadır. Müşteri İlişkileri Yönetimi ekibi, müşterileriyle doğrudan iletişime geçerek (telefon, e-posta, web portalı, çağrı merkezi vb.) projelerin ve hizmetlerin sürekliliği hakkında düzenli olarak bilgilendirmeler yapmaktadır. Müşteriler, aldıkları hizmetle ilgili karşılaştıkları sorunları e-posta veya telefon aracılığıyla Bulutistan'a iletmekte, böylece hızlı ve etkin çözümler sağlanmaktadır. Ayrıca, son kullanıcılar, kendilerine sağlanan hizmetlere ilişkin sorunları ve talepleri izleyebilmek için çevrimiçi erişim sağlayabilecekleri uygulamalara sahiptir. Bu sayede, müşteri memnuniyetini artırmak ve hizmet süreçlerinin verimli bir şekilde yönetilmesi sağlanmaktadır.

3.8. SÜREÇLER & KONTROLLER

3.8.1. Bilgi sistemleri politika, prosedür ve süreç dokümanları

a. Kontrol Hedefleri

Şirket, bilgi sistemlerinin kullanımından kaynaklanan riskleri yönetmek ve bilgi varlıklarını korumak amacıyla uygulanması gereken usul ve esaslar ile tesis edilmesi gereken kontrolleri tarif eden BS politika, prosedür ve süreç dokümanlarını oluşturur. Dokümanların gizlilik derecesi ve Şirket çalışanlarının görev ve sorumluluklarının uygunluğu nispetinde dokümanlara erişim imkânı verilir. BS politika, prosedür ve süreç dokümanlarının gerekleri, Şirketin organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilir, bunların işlerliğine ilişkin gözetim ve takip gerçekleştirilir. Politika ve prosedürlerin işletilmesinden sorumlu birimler ve görev tanımları ile süreç dokümanlarının işletilmesinden sorumlu süreç sahipleri ilgili politika, prosedür ve süreç dokümanları içinde belirtilir. BS politika, prosedür ve süreç dokümanları yılda en az bir defa gözden geçirilir ve gerekli güncellemeler yapılır. Dokümanlarda meydana gelen değişiklikleri takip edebilmek adına, dokümanın önceki versiyonu ile asgari olarak dokümanı onaylayan, revizyon tarihi ve gözden geçirme tarihi bilgileri kayıt altına alınır.

b. Kontroller

Bilgi sistemlerinin kullanımından kaynaklanan riskleri yönetmek ve bilgi varlıklarını korumak amacıyla uygulanması gereken usul ve esaslar ile tesis edilmesi gereken kontrolleri tarif eden BS politika, prosedür ve süreç dokümanları oluşturulmuştur. Bütün dokümanların hazırlanma süreçleri için Doküman Yönetim Prosedürü bulunmaktadır. Dokümantasyonda asgari olarak doküman numarası, dokümanı hazırlayan, dokümanı onaylayan, revizyon tarihi, yayım tarihi, gözden geçirme tarihi ve değişiklik nedeni yer almaktadır. Dokümanlar Sharepoint platformu üzerinde çalışanlar ile paylaşılmaktadır. Bu dokümanların düzenlenme yetkisi İş Mükemmelliği Direktörü olan Burcu Öğütçü'de bulunmaktadır. Yönetim Kurulu kararı doğrultusunda BS Politikaları kullanıma alınarak onaylanmıştır. Yılda bir defa, iç dokümanların güncelliği kontrol edilmekte ve gözden geçirilmektedir. Gözden geçirme aşamasında işletilen süreçte herhangi bir değişiklik olduğu tespit edilirse dokümana yansıtılması için revizyon başlatılmaktadır. Değişiklik yok ise revizyon numarası atlatılmadan Bulutistan Süreç ve Doküman Ailesi adlı doküman listesine ilgili dokümanın gözden geçirme tarihi işlenmektedir.

3.8.2. Bilgi güvenliği organizasyonu, roller ve sorumluluklar

a. Kontrol Hedefleri

Bilgi güvenliğinin sağlanmasında nihai sorumluluk yönetim kuruluna aittir. Yönetim kurulu, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi hususunda gerekli kararlılığı göstermekle ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis etmekle yükümlüdür. Bu sorumluluk kapsamında yönetim kurulu, Şirket genelinde uygulanmasını gözetmekle yükümlü olduğu bir bilgi güvenliği yönetim sistemi tesis eder. Bilgi güvenliği yönetim sisteminin ulusal veya uluslararası standartları ya da en iyi uygulamaları referans alması ve ilgili faaliyetleri içermesi esastır. Bilgi güvenliği yönetim sisteminin nasıl uygulanacağı bilgi güvenliği politikası, prosedürleri ve süreç dokümanları ile düzenlenir. Bilgi güvenliği politikası yönetim kurulu tarafından onaylanır ve Şirket genelinde çalışanlara ulaştırılması sağlanır. Bu kapsamda bilgi sistemlerine ilişkin kabul edilebilir kullanım standartları belirlenir. Bilgi güvenliği politikasının oluşturulması ve uygulanması faaliyetleri yönetim kurulu adına Bilgi Güvenliği Komitesi tarafından gerçekleştirilir. Bilgi Güvenliği Komitesine, belirlenen bir yönetim kurulu üyesi veya genel müdür başkanlık eder ve komitenin koordinasyonunu bilgi güvenliği sorumlusu yerine getirir. Bilgi Güvenliği Komitesinin toplanması ve yılda en az bir defa yönetim kuruluna rapor sunması sağlanır. Bilgi güvenliği politikası, prosedürleri ve süreç dokümanları yılda en az bir defa gözden geçirilir. Önemli güvenlik olayları, yeni güvenlik açıkları ya da teknik altyapıdaki önemli değişikliklerden sonra da bunların ayrıca gözden geçirilmesi sağlanır. Şirket bünyesinde, BS güvenlik fonksiyonu oluşturulur. BS güvenlik fonksiyonunun doğrudan yönetim

kuruluna veya genel müdüre bağlı olması esastır. BS güvenlik fonksiyonu, bilgi güvenliği sorumlusu tarafından yönetilir.

b. Kontroller

Şirket bünyesinde bilgi güvenliğinin sağlanmasında nihai sorumluluk üst yönetime adreslenmiştir. Üst Yönetim, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi faaliyetlerine yönelik olarak yeterli kaynağı tahsis etmektedir. Bilgi güvenliği ihlaline ilişkin olaylar izlenmekte ve raporlanmaktadır. Şirket genelinde ve verilen hizmetlerde, görevler ayrılığı prensibi ile etkin bir kimlik doğrulama ve erişim yönetimi tesis edilmiştir. Üst yönetim de dâhil olmak üzere çalışanlar, dış hizmet sağlayıcılar ve müşteriler gibi bilgi güvenliğini ilgilendiren paydaşlara yönelik, bilgi güvenliği farkındalığını artıracak çalışmalar yapılmaktadır. İş sürekliliği yönetimi kapsamında bilgi güvenliğini ilgilendiren hususların da yer alması sağlanmıştır. Bilgi Güvenliği ve Veri Gizlilik Politikası Yönetim Kurulu tarafından onaylanmış ve Şirket genelinde çalışanlara ulaştırılması sağlanmıştır. Bilgi sistemlerine ilişkin kabul edilebilir kullanım standartları belirlenmiş ve bilgi güvenliği politikası içerisinde dokümante edilmiştir. Bilgi Güvenliği ve Veri Gizlilik Politikası, prosedürleri ve süreç dokümanları önemli güvenlik olayları, yeni güvenlik açıkları ya da teknik altyapıdaki önemli değişikliklerden sonra gözden geçirilmektedir. Şirket bünyesinde bir Bilgi Sistemleri güvenlik fonksiyonu oluşturulmuştur. Bilgi Güvenliği Sorumlusu Genel Müdüre bağlı olarak atanmış ve BT operasyonundan bağımsızlığı sağlanmıştır. Bilgi güvenliği sorumlusu bilgi güvenliği politika, prosedürleri ve süreç dokümanlarının oluşturulması, bunların güncellenmesi ve onaya sunulması faaliyetini yerine getirmektedir. Bilgi güvenliği sorumlusu BS risk yönetimi çalışmalarında, bilgi güvenliği bakış açısıyla, ilişkili bilgi varlıklarına yönelik olarak gizlilik, bütünlük, erişilebilirlik kriterleri bakımından BS risk yönetimi çalışmalarına aktif katkı sunulması ve yardımcı olunması faaliyetlerini yerine getirmektedir. Bilgi güvenliği sorumlusu ilgili birimlerle uyum içinde, iş gereksinimleri ve iş hedefleriyle uyumlu bilgi güvenliğinin tesis edilmesi, bilgi güvenliği ile ilgili mevzuat hükümleri, standartlar, politika, prosedür ve süreç dokümanlarına uyumun takip edilmesi, bilgi güvenliği faaliyetlerinin ve testlerinin yürütülmesinin sağlanması ve bunların takip edilmesi faaliyetlerini yerine getirmektedir. Bilgi güvenliği sorumlusu önemli projeler ve değişiklikler için bilgi güvenliği gereksinimlerinin belirlenmesi çalışmalarına katkıda bulunulmaktadır. Bilgi güvenliği sorumlusu bilgi güvenliğini ilgilendiren paydaşlara yönelik bilgi güvenliği farkındalık programını yürütmektedir.

3.8.3. Kimlik ve erişim yönetimi

a. Kontrol Hedefleri

Şirket, bilgi varlıklarına olan erişimlerin, görevler ayrılığı prensibine göre belirlenmiş ve kullanıcıların sorumluluğu gereği kendileri için tanımlanan erişim kontrolleri uyarınca, ilişkili bilgi varlığının güvenlik sınıfına uygun bir kimlik doğrulama yöntemiyle gerçekleştirilmesini sağlar. Şirket, süreçler ve sistemler üzerinde kullanıcılarına sağlayacağı yetkilerin, kullanıcılara görev ve sorumluluklarına uygun roller ve/veya profiller aracılığı ile temin edilmesini sağlar ve kullanıcıların görev tanımlarına uygun uygulama ve sistemler üzerindeki rolleri dokümante eder. Bilgi sistemleri üzerindeki kullanıcılara uygulanacak kimlik doğrulama mekanizması, kullanıcıların bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek süreci kapsayacak şekilde tesis edilir ve kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek önlemler alınır.

Şirket, bilgi sistemleri üzerindeki kullanıcılara ait kimlik doğrulama bilgilerinin güvenliğine yönelik; kimlik doğrulama bilgilerinin veritabanlarında şifreli olarak veya matematiksel olarak geriye dönüştürülmesi mümkün olmayan yöntemlerle muhafaza edilmesi, kimlik doğrulama amacıyla aktarılırken şifrelenmesi, yetkisiz erişimlere veya görevler ayrılığı prensibine aykırı olarak kontrolsüz bir şekilde gerçekleştirilecek değişikliklere karşı korunması, bu veritabanları üzerinde gerçekleştirilen işlemlere ilişkin yeterli iz kayıtlarının tutulması ve bu iz kayıtlarının güvenliğinin sağlanması gibi önlemler alır. Kullanıcılara uygulanacak kimlik doğrulama mekanizmasının şu fonksiyonları yerine getirmesi sağlanır; Başarısız kimlik doğrulama teşebbüslerinin belirli bir sayıyı aşması halinde ilgili kullanıcının erişimini engellemesi, Başarısız kimlik doğrulama teşebbüsleri sonrasında, bu teşebbüsü gerçekleştiren kişiye, hatalı girilen kullanıcı adı bilgisi veya parola ile ilgili, böyle bir kullanıcı adının sistemde olmadığı veya parolanın hatalı girildiği bilgisini vermemesi, Hiçbir işlem yapılmayan hareketsiz oturumlar için oturumu belirli bir süre sonra sonlandırması veya kilitlemesi, Birden fazla kullanıcının aynı kullanıcı hesabını kullanabilmesi ya da bir kullanıcının aynı anda farklı oturumlar açabilmesi konusunda bilgi güvenliği sorumlusunun onay verdiği durumlar hariç olmak üzere, aynı kullanıcı için aynı anda birden fazla oturum açılmaya çalışılması durumunda buna izin vermemesi ve kullanıcıya uyarı vermesi.

Kullanıcılara uygulanacak erişim kontrolleri ve atanacak yetkilerin belirlenmesinde görevler ayrılığı prensibi esas alınır. Süreçler ve sistemler, kritik bir işlemin tek bir kişi tarafından başlatılması, onaylanması ve tamamlanmasına imkân vermeyecek şekilde tasarlanır ve işletilir. Şirket, görevler ayrılığı prensibinin uygulanmasına yönelik BS süreçlerinde uygulanacak erişim kontrollerini ve atanacak yetkileri net olarak belirler ve dokümante eder. Erişim yetkilerinin talep edilmesi, yetkilendirilmesi ve yönetilmesi görevlerinin birbirinden ayrılması sağlanır. Görevlerin tam manasıyla ve uygun şekilde ayrıştırılmasının mümkün olmadığı durumlarda, bu durumdan kaynaklanabilecek hata ve suistimalleri önlemeye yönelik risk azaltıcı veya telafi edici ilave kontroller tesis edilir. Kullanıcılar, geçerli bir iş ihtiyacının mevcut olduğu ve erişimin gerekli olduğu süre zarfında, bilgi varlıklarına erişebilmeleri için yetkilendirilir. Bilgi varlıklarına erişim yetkisi olan kullanıcılar, ilgili bilgi varlığı sahibi tarafından yılda en az bir defa gözden geçirilir. Kullanıcıların görev ve sorumlulukları göz önünde bulundurularak sadece bu görevleri yerine getirmelerine yetecek ve sadece bilmeleri gereken verilere erişmelerini sağlayacak kadar yetkiye sahip olmaları sağlanır.

Ayrıcalıklı yetkilere sahip kullanıcı ve uygulama hesapları ile ilgili asgari tedbirlerin alınması sağlanır. Personelin işten ayrılması ve görev değişikliği gibi insan kaynaklarında yaşanan değişiklikler sonrasında, gecikmeksizin ilgili kullanıcı hesaplarının silinmesi, askıya alınması, kullanıcıya atanmış yetkilerin geri alınması ya da değiştirilmesi gibi işlemler yerine getirilir. İnsan kaynakları değişikliklerine dayanan yetkilendirme işlemleri otomatik olarak gerçekleştirilmiyorsa, manuel değişiklik gerçekleştirme sürecinde görevler ayrılığı prensibi uygulanır ve değişikliği gerçekleştirmeye yetkili personelin faaliyetlerine ilişkin iz kayıtları ile insan kaynaklarındaki değişikliklerin uyumlu olup olmadığı düzenli olarak gözden geçirilir. Bilgi sistemleri üzerindeki kullanıcılar için benzersiz kullanıcı tanımlama kodları belirlenir ve zorunlu olmadığı müddetçe ortak veya ön tanımlı kullanıcı hesapları kullanılmaz. Ortak veya ön tanımlı kullanıcı hesaplarının kullanımının zorunlu olduğu durumlarda ise bu kullanıcı hesapları ile işlemi yapan kişiye sorumluluk atamaya yönelik ilave kontroller tesis edilir.

Kullanıcı parolalarının yönetiminde asgari olarak şu tedbirlerin alınması sağlanır; sistem tarafından geçici olarak verilen parolaların kullanıcı tarafından sisteme ilk girişte değiştirilmesinin sağlanması, Kullanıcıların, parolalarını belirlerken tahmin edilmesi zor, günün teknolojisine uygun uzunlukta ve zorlukta parola seçimine zorlanması, Kullanıcıların, düzenli aralıklarla ve sistem güvenliği ile ilgili bir kuşku oluşması halinde parolalarını değiştirmeye zorlanması, Kullanıcıların eski parolalarının hatırlanması suretiyle geriye dönük olarak belirli sayıda eski parolanın kullanılmasının engellenmesi.

b. Kontroller

Bilgi varlıklarına erişimlerin, görevler ayrılığı prensibine uygun şekilde belirlenmesi, kullanıcıların sorumlulukları kapsamında kendileri için tanımlanan erişim kontrollerine uyması ve erişimin ilgili bilgi varlığının güvenlik sınıfına uygun bir kimlik doğrulama yöntemiyle gerçekleştirilmesi Erişim Kontrol Politikası kapsamında tanımlanmaktadır. Bilgi sistemleri üzerindeki kullanıcılara uygulanacak kimlik doğrulama mekanizması, kullanıcıların bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek süreci kapsayacak şekilde tesis edilmekte ve kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek önlemler alınmaktadır. Bilgi sistemleri üzerindeki kullanıcılara ait kimlik doğrulama bilgileri kimlik doğrulama amacıyla aktarılırken zafiyet içermediği bilinen güvenli protokoller (LDAPs, https, vb.) kullanılmaktadır.

3.8.4. İz kayıtlarının oluşturulması ve takibi

a. Kontrol Hedefleri

Şirket, bilgi sistemlerinin ve faaliyetlerinin boyutu ve karmaşıklığıyla orantılı olacak şekilde bilgi sistemleri dâhilinde gerçekleşen işlem ve olaylara ilişkin etkin bir iz kayıt mekanizması tesis eder. İz kayıtları, işlemin doğasına uygun detay ve içerikte bilgileri barındırır. Tesis edilecek iz kayıt mekanizmasının, yaşanan bilgi güvenliği olaylarının sonradan incelenmesine ve bunlar hakkında güvenilir delillerin elde edilmesine imkân tanıyacak nitelikte olması sağlanır. Bilgi sistemleri dâhilinde gerçekleşen kayıtlarda değişikliğe sebep olan işlemler ve kritik bilgi varlıklarına yönelik erişim yetkilerinin verilmesine, değiştirilmesine ve geri alınmasına yönelik aktiviteler ile bu varlıklara yönelik yetkisiz erişim teşebbüslerine ilişkin iz kayıtları asgari beş yıl boyunca Şirket nezdinde saklanır.

İz kayıtları güvenilir ortamlarda yedeklenir ve ihtiyaç duyulması halinde makul bir sürede bu yedeklerden geri dönüş sağlanarak inceleme yapılmasına imkân verecek şekilde Şirket nezdinde saklanır. İz kayıtlarının bütünlüğünün bozulmasının önlenmesine ve herhangi bir bozulma durumunda bunun tespit edilebilmesine ilişkin teknikler kullanılır. İz kayıtlarına, bilmesi gerektiği kadar prensibine uygun olarak sadece erişim yetkisi verilen kişilerin ulaşabilmesi ve kayıt sisteminin her türlü yetkisiz değişiklik ve müdahalelere karşı korunması sağlanır. Kullanıcıların

kendi faaliyetlerine ilişkin iz kayıtlarına müdahalesi engellenir ve iz kayıt sisteminin durdurulmasını önlemeye veya durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılır.

b. Kontroller

Şirket, bilgi sistemlerinin ve faaliyetlerinin boyutu ve karmaşıklığıyla orantılı olacak şekilde bilgi sistemleri dâhilinde gerçekleşen işlem ve olayların iz kayıt mekanizması oluşturulmasına ilişkin süreç Log Yönetimi Prosedürü içerisinde tasarlanmıştır. İşletim sistemine ilişkin iz kayıtları Qradar; veri tabanı seviyesine ilişkin iz kayıtları DataScope uygulamaları üzerinde tutulmaktadır. İz kayıtlarına erişimler bilmesi gerektiği kadar prensibi doğrultusunda sınırlandırılarak yalnızca yetkilendirilmiş kişilerle kısıtlanmaktadır. Bu çerçevede iz kayıt sistemlerinin yetkisiz erişim, değişiklik veya müdahalelere karşı korunması ve kayıtların güvenilirliğinin sağlanmasına yönelik temel kontroller süreçlerde tanımlı olarak uygulanmaktadır. Kullanıcıların kendi faaliyetlerine ilişkin iz kayıtlarına müdahalesi engellenmesine ve iz kayıt sisteminin durdurulmasını önlemeye veya durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılmasına ilişkin süreç tasarlanmıştır.

3.8.5. Ağ güvenliği

a. Kontrol Hedefleri

Şirket, gerek kendi kurumsal ağı gerek dış ağlardan gelebilecek tehditler için gerekli ağ güvenlik kontrol sistemlerini tesis eder. Şirket, dış ağı ve iç ağı arasındaki trafiği kontrol altında tutmak için gerektiği şekilde konfigürasyonu yapılmış ve sürekli gözetim altında tutulan güvenlik duvarı çözümleri ile saldırıları tespit edebilecek ve önleyebilecek günün teknolojisine uygun sistemler kullanır. Hassas veya sır kapsamındaki verilere sahip sistemlerin özel iç ağda bulunması ve hiçbir şekilde doğrudan internetten erişilemiyor olması sağlanır. Özel iç ağdaki sistemlerle yalnızca güvenlik duvarı cihazları üzerinden iletişim kurulmalıdır. Bilgi güvenliği sorumlusu tarafından onaylanmadıkça Şirket personeli ya da dış hizmet sağlayıcıları tarafından Şirket içi uygulama ve sistemlere, Şirket dışından uzaktan erişim gerçekleştirilmez. Uzaktan erişimin gerçekleştiği hallerde ise erişimlere ilişkin iz kayıtları tutulur, bağlantının süresi ve bağlantının yapılabileceği cihazlar kısıtlanır ve kullanıcı belli aralıklarla kimliğini tekrar doğrulamaya zorlanır.

b. Kontroller

Şirket, kurumsal ağındaki ve dış ağlardan gelen trafiği güvence altına almaktadır. Katmanlı bir güvenlik mimarisi yaklaşımını benimseyerek, güvenlik kontrol sistemlerini etkin ve sürekli bir şekilde işletmektedir. Dış ağ ve iç ağ arasındaki trafiği kontrol altında tutmak için gerektiği şekilde konfigürasyonu yapılmış ve sürekli gözetim altında tutulan güvenlik duvarı çözümleri kullanılmaktadır. Dış ağdan gelen ve dış ağa giden trafiğin kontrolü için Fortigate güvenlik duvarı, iç ağ segmentleri arasındaki trafiğin izlenmesi ve filtrelenmesi için ise Check Point güvenlik duvarı çözümü kullanılmaktadır. Güvenlik duvarları üzerinde, ağ trafiğini analiz ederek olası saldırıları tespit edip önleyebilen Saldırı Tespit ve Önleme Sistemleri (IPS) aktif olarak konumlandırılmıştır. Şirket, iç ağdaki tehditleri minimize etmek için ağ segmentasyonunu uygulamakta ve farklı güvenlik hassasiyetine sahip alt bölgeler arasında trafiği kontrollü bir şekilde yönetmektedir. Hassas veya sır niteliğindeki verilere sahip sistemler özel iç ağda izole edilerek, doğrudan internet erişimine kapatılmaktadır. İnternete çıkış kontrolleri DMZ katmanında gerçekleştirilmekte olup, dış ağ iç ağdan firewall çözümü ile ayrıştırılmaktadır. Şirket bünyesinde kurulu olan etki alanı yönetimi sunucuları, yalnızca şirketin ihtiyaçlarına göre özel olarak tasarlanmış ve yapılandırılmıştır.

3.8.6. Güvenlik konfigürasyonu yönetimi

a. Kontrol Hedefleri

Masaüstü, dizüstü, mobil cihazlar ve sunucuları üzerindeki işletim sistemi, veritabanları ve uygulamalar ile güvenlik duvarları, yönlendirici ve anahtarlama cihazları gibi ağ cihazları için sıkılaştırılmış ve test edilmiş güvenli standart konfigürasyon bilgilerini oluşturulur. Bu standart konfigürasyon bilgileri, standart konfigürasyondan sapmalar veya standart konfigürasyondaki güncellemeler değişiklik yönetiminin bir parçası olarak kayıt altına alınır ve onay mekanizmasına tabi tutulur. Güvenli standart konfigürasyon dışında kalacak her türlü değişiklik isteği için bu değişikliği gerektiren iş gereksinimi ve bu iş gereksinimine ihtiyaç duyan iş sorumlusunun kim olduğu ve gereksinim süresi gibi bilgiler de kayıt altına alınır. Masaüstü, dizüstü, mobil cihazlar ve sunucular üzerindeki işletim sistemleri için bu işletim sistemlerinin tipi, versiyon numarası, yama seviyesi ve üzerinde yüklü olan veritabanları ve uygulamaların listesini gösterecek şekilde bir yazılım envanteri tutulur. Kullanılacak yazılım envanterinin aynı zamanda donanım envanteri ile de entegre olması ve tek bir noktadan hangi donanım üzerinde hangi yazılımların olduğu bilgisinin takip edilebilir olması sağlanır. Masaüstü ve dizüstü makineleri ile sunucuları, bu makinelere taşınabilir bir medya veya harici cihaz takıldığında otomatik olarak içeriği oynatmayacak şekilde yapılandırılır ve zararlı yazılım engelleme araçları bu tür cihazlar takıldığında otomatik olarak bu cihazları tarayacak şekilde ayarlanır. Bunun yanında bu tür harici cihazların makinelere bağlanacağı bağlantı arayüzlerinin ön tanımlı olarak

kullanıma kapatılarak bu tür cihazların kullanımının yalnızca iş gereksinimi olan kullanıcılarla sınırlı tutulması ve harici cihazları kullanma denemesi yapılan durumların da takip edilmesi sağlanır. Ağa bağlı her bir sistem üzerindeki portların, protokol ve servislerin sadece gerekliliği onaylanmış iş ihtiyaçlarına istinaden açık ve çalışıyor olması sağlanır. Bu doğrultuda, güvenli bir baz konfigürasyonu temel alınarak önemli sunucu ve sistemler için düzenli olarak port taraması gerçekleştirilir ve güvenli baz konfigürasyonda bulunmadığı halde açık durumda olan portların kapatılması sağlanır.

b. Kontroller

Masaüstü, dizüstü, mobil cihazlar ve sunucular üzerindeki işletim sistemleri, veritabanları ve uygulamalar ile güvenlik duvarları, yönlendiriciler ve anahtarlama cihazları gibi ağ cihazları için güvenli standart yapılandırma bilgileri oluşturulmuş olup söz konusu bilgiler CMDB çözümü üzerinden merkezi olarak izlenmekte ve güncel tutulmaktadır. Güvenlik baz konfigürasyonları değişiklikleri, değişiklik sürecinin bir parçası olarak gerçekleştirilerek kayıt altına alınmakta ve talep onay dâhilinde ilerletilmektedir. Windows işletim sistemine sahip cihazlar, Endpoint Central ürünü aracılığıyla izlenmekte olup bu ürün üzerinden donanım envanteri ile entegre şekilde çalışan yazılım envanteri takip edilmektedir. Şirket, uç nokta güvenliğini sağlamak amacıyla Trend Micro XDR ürünü kullanmaktadır. Bu kapsamda, taşınabilir medya veya harici cihazlar sisteme takıldığında otomatik tarama işlemi başlatılmakta ve zararlı yazılım tespiti halinde alarm üretilmektedir. Ayrıca, yetkisiz kullanıcılar için USB portları varsayılan olarak devre dışı bırakılmış olup yalnızca iş gereksinimi bulunan kullanıcıların harici cihaz kullanımına izin verilmektedir.

3.8.7. Güvenlik açıkları ve yama yönetimi

a. Kontrol Hedefleri

İş faaliyetlerini kesintiye uğratacak veya önemli ölçüde olumsuz etkileyecek durumların ortaya çıkma olasılığını azaltmak için sistem, yazılım ve cihazlardaki güvenlik açıklarını hızlı ve etkin bir şekilde ele alacak bir güvenlik açıkları ve yama yönetimi süreci tesis edilir. Sağlayıcı veya üretici desteği biten sistem, yazılım ve cihazlar artık güncellenemediğinde, bunlar için yüklenebilen en son güncellemelerin günün şartlarına göre artık güvenli olmaması ve telafi edici kontroller ile de makul seviyede bir güvenlik sağlanamaması halinde sistem, yazılım ve cihazlar kullanımdan kaldırılır. Şirket, masaüstü ve dizüstü makineleri ile sunucularını, sürekli bir şekilde izleyerek üzerindeki zararlı yazılımları tespit edecek etkin araçlar kullanır. Şirket, e-posta sunucusuna gelen ve giden e-postaları tarayarak zararlı yazılım barındıran ya da iş ihtiyaçları doğrultusunda gereksiz olan eklentiler içeren e-postaları engelleyecek çözümler kullanır.

b. Kontroller

İş faaliyetlerini kesintiye uğratacak veya önemli ölçüde olumsuz etkileyecek durumların ortaya çıkma olasılığını azaltmak amacıyla, sistem, yazılım ve cihazlardaki güvenlik açıklarının hızlı ve etkin bir şekilde ele alınmasına yönelik bir güvenlik açıkları ve yama yönetimi süreci, Yama Yönetimi Prosedürü kapsamında tesis edilmiştir. Bu kapsamda kullanılan ManageEngine Desktop Central Plus ürünü, üretici tarafından yayımlanan yamaları düzenli olarak tarayarak merkezi bir konsol üzerinden tespit edilmesini sağlar. Yamaların yalnızca üretici tarafından dijital olarak imzalanmış ve güvenilir kaynaklardan indirildiği doğrulanmakta, yetkili sistem yöneticisinin onayı sonrasında dağıtım gerçekleştirilmektedir. Yaygın dağıtımdan önce, tüm yamalar test sunucularında uygulanarak olası uyumsuzluklar değerlendirilmekte, ardından canlı sistemlere yaygınlaştırılmaktadır. Zararlı yazılımların tespit edilmesi ve önlenmesi amacıyla şirket genelinde tüm istemci ve sunucu sistemlerde Trend Micro Uç Nokta Güvenliği çözümü kullanılmaktadır.

3.8.8. Fiziksel güvenlik kontrolleri

a. Kontrol Hedefleri

Kritik bilgi sistemleri, uygun güvenlik engelleri ve giriş kontrollerine sahip veri merkezleri, sistem odaları, ağ ekipman odaları gibi güvenli alanlarda barındırılır. Bu alanlara erişim, sadece erişim yetkisine sahip olması gereken personelle sınırlandırılır, erişim yetkileri düzenli olarak gözden geçirilir ve güncellenir. Şirket, veri merkezlerinin yerlerini seçerken doğal riskleri ve çevresel tehditleri göz önünde bulundurur. Binaların, barındırdıkları bilgi işlem tesislerinin varlığını açık edecek işaretler ve bilgiler bulundurmaması sağlanır. Şirket, veri merkezlerinin çalışmasını olumsuz etkileyebilecek elektrik kesintisi, yangın, duman, sıcaklık, su, toz ve nem gibi çevresel koşulları izleyecek sistem ve sensörler kullanır, bunların bakımlarını düzenli olarak yapar. Yetkilendirilen personel dışında kalan herhangi bir Şirket personeli, ziyaretçi, dış hizmet sağlayıcı ya da yüklenici firma personelinin veri merkezlerine ve kritik bilgi sistemlerine erişimleri onay mekanizmasına tabi tutulur, veri merkezindeki çalışmaları boyunca

faaliyetleri yakından izlenir ve mutlaka kendilerine refakat edilir. Bu çerçevede, veri merkezlerine ve sistem odalarına yapılan erişim talepleri ve onayları ile bu erişimler kapsamında gerçekleştirilen işlemler ve giriş çıkışlar için iz kaydı tutulur. Bu alanlar için kör nokta barındırmayacak şekilde kamera kayıt sistemleri kullanılır.

b. Kontroller

Kritik bilgi sistemleri, uygun güvenlik engelleri ve giriş kontrollerine sahip alanlarda barındırılmaktadır. Şirket, veri merkezlerinin yerlerini seçerken doğal riskleri ve çevresel tehditleri göz önünde bulundurmaktadır. Veri merkezleri olası felaket ve risklere karşı güvenilirliği yüksek lokasyonlarda barındırılmaktadır. Binada barındırdıkları bilgi işlem tesisinin varlığını açık edecek işaretler ve bilgiler bulundurmaması sağlanmaktadır. Yetkilendirilen personel dışında kalan herhangi bir personel, ziyaretçi, dış hizmet sağlayıcı ya da yüklenici firma personelinin veri merkezine erişimleri onay mekanizmasına tabi tutulmakta, veri merkezindeki çalışmaları boyunca faaliyetleri yakından izlenmekte ve mutlaka kendilerine refakat edilmektedir. Veri merkezi ziyaretlerine ilişkin süreç Bilgi Güvenliği Politika'sında tasarlanmıştır.

3.8.9. Siber olay yönetimi, sızma testi ve siber istihbarat paylaşımı

a. Kontrol Hedefleri

Şirket, siber olaylardan sonra iş faaliyetlerini en az etkileyecek şekilde ve mümkün olan en kısa sürede BS hizmetlerini normal işleyişine döndürmek üzere gerçekleşen siber olayların ele alınmasına ve takibine yönelik siber olay yönetimi ve siber olaylara müdahale süreci oluşturur. Siber olayların önem derecelerine uygun olacak şekilde ele alınmasını sağlamak üzere, siber olayların önemlilik sınıflandırmasına yönelik kriterler yazılı hale getirilir ve gerçekleşen her bir siber olayın bu kriterlere göre belirlenen önem düzeyiyle orantılı olan bir zaman zarfında ele alınması ve çözüme kavuşturulmasına yönelik prosedürler ile müdahale planları oluşturulur. Oluşturulan müdahale planlarında öngörülen senaryolar için, faaliyetlerin güvenilir bir şekilde sürdürülmesini sağlayan hızlı, etkili ve düzenli bir tepki süreci tesis edilir.

b. Kontroller

Kurum, gerçekleşen siber olayların bilgi sistemleri hizmetlerini asgari düzeyde etkilemesini sağlamak ve faaliyetlerin mümkün olan en kısa sürede normale dönmesini temin etmek amacıyla siber olaylara müdahale ve yönetim sürecini tesis etmiştir. Bu kapsamda, "Siber Güvenlik Prosedürü" ile "Bilgi Güvenliği Vaka Yönetimi Prosedürü" dokümante edilmiştir. Siber güvenlik süreçlerinden Bulutistan Üst Yönetimi sorumlu olup, üst yönetim tarafından bir Siber Güvenlik Sorumlusu atanmıştır. Bu sorumlu kişi; kurumun siber güvenlik stratejilerini belirlemek, stratejilerin uygulanmasını sağlamak, güvenlik olaylarını izlemek ve yönetmekle yükümlüdür. Kurum bünyesinde siber güvenlik yönetimi beş ana başlık çerçevesinde yürütülmektedir: Siber Tehditlerin Tanımlanması ve Değerlendirilmesi, Güvenlik Kontrollerinin Uygulanması, Olay İzleme ve Müdahale Süreçleri, Farkındalık ve Eğitim Faaliyetleri, Acil Durum Hazırlığı ve Kurtarma Planlaması. Süreç, olası tehditlere karşı proaktif koruma sağlamakla birlikte, gerçekleşen olaylara hızlı müdahale edilmesini ve iyileştirme faaliyetlerinin etkili şekilde yürütülmesini hedeflemektedir.

3.8.10. Değişiklik yönetimi

a. Kontrol Hedefleri

Şirket, meydana gelen değişiklikler sebebiyle gerçekleşebilecek hata ve sorunların sayısını ve etkisini en aza indirecek, değişikliklerin etkili, hızlı ve kontrollü bir şekilde gerçekleştirilmesini ve değişiklikler sırasında yapılan işlemlerin değişiklik sonrasında da denetlenebilir olmasını sağlayacak etkin bir değişiklik yönetimi süreci tesis eder. Bu süreç kapsamında, ağ altyapısı, donanım, işletim sistemleri, yazılım gibi bilgi sistemleri öğeleri ile sistem, servis, uygulama konfigürasyonu ve parametrelerinde yapılacak her türlü değişikliğin bir değişiklik talep yönetimi süreci çerçevesinde başlatılması, değişiklik talebinin geçerli bir iş ihtiyacına dayalı olması ve görevler ayrılığı prensibine uygun olarak yetkilendirilmesi, test edilmesi, gerçekleştirilmesi, kaydedilmesi ve dokümantasyonu sağlanır.

Şirket, bilgi sistemi yazılım bileşenlerinin ana versiyonunun kaydını tutar ve bilgi sistemi bileşenlerinde meydana gelen değişiklikleri, meydana geldiği sırayla ve değişimin gerçekleştiği tarihle birlikte kaydederek belgelendirir. Değişiklik yönetimi süreci, asgari olarak talep yönetimi, risk değerlendirmesi, yetkili merci onayı, yapılan değişikliğin uygulanması, test edilmesi ve doğrulanması adımlarını içerir. Acil durum değişiklikleri kapsamında değişiklik yönetim süreci içerisinde tanımlanan istisnaların değişiklik sonrasında mümkün olan en kısa sürede tamamlanması sağlanır.

b. Kontroller

Şirket bünyesinde bilgi sistemleri üzerinde gerçekleştirilecek değişikliklerin kontrollü bir şekilde yönetilebilmesi amacıyla değişiklik yönetimi süreci yapılandırılmıştır. Süreç; değişiklik taleplerinin iletilmesi ve kayda alınması, analiz edilerek kategorize edilmesi, önceliklendirilmesi, yetkilendirilmesi, test edilmesi, uygulanması, başarısız durumlar için geri dönüş planlarının hazırlanması, son değerlendirme ve kapanış adımlarını kapsamaktadır. Tüm değişiklik talepleri ITSM platformu üzerinden oluşturulmakta, elektronik ortamda kayıt altına alınarak takip edilmektedir. Talep oluşturulurken değişikliğin türü (majör, minör, standart veya acil) belirtilmekte; ayrıca değişikliğin gerekçesi, potansiyel etkileri, uygulama planı, başarısızlık durumunda uygulanacak kurtarma planı ve test planı gibi bilgiler girilmektedir. Majör ve minör değişiklikler, her hafta belirli bir gün toplanan Değişiklik Değerlendirme Kurulu (Change Advisory Board - CAB) gündemine alınmakta ve kurul onayı ile hayata geçirilmektedir. CAB toplantılarında ayrıca, önceki hafta uygulanan değişikliklerin geriye dönük gözden geçirme faaliyetleri de yürütülmektedir. Acil değişiklikler için ayrı bir süreç tanımlanmış olup, bu tür değişikliklerin ancak belirli bir olay ile ilişkilendirilmesi halinde acil olarak sınıflandırılmasına izin verilmektedir. Acil değişiklikler, hızlı onay mekanizmaları aracılığıyla kontrol altına alınarak uygulanmaktadır.

3.8.11. Erişilebilirlik yönetimi ve yedekleme

a. Kontrol Hedefleri

Herhangi bir donanım veya yazılım bileşeninin beklendiği gibi çalışmadığı durumlarda, sistemin veya hizmetlerin önemli bir bölümünün çalışamaz hale gelmesini önlemek adına kritik donanım ve sistemler için yedekli çalışma ya da hazırda bekleme düzenleri kurulur. Hangi donanım ve sistemlerin kritik olduğu belirlenirken, hizmetler ve bunların bağlı olduğu hizmet seviyeleri ile bilgi varlıklarının erişilebilirlik gereksinimleri dikkate alınır. Verilerin erişilebilirliğini sağlamak adına her bir verinin erişilebilirlik gereksinimlerine uygun yedekleme düzeni tesis edilir. Sistemin alınan yedeğinden geri yüklenebilmesi için, işletim sistemi, uygulama yazılımı ve veriler gibi sistemin çalışmasını sağlayan bileşenler yedekleme prosedürüne dâhil edilir. Yedeklemenin düzgün bir şekilde çalıştığından emin olmak için, geri yükleme işlemleri gerçekleştirilerek yedekleme ortamındaki veriler düzenli olarak test edilir. Yedeklerin taşınırken, uygun şifreleme teknikleri ve fiziksel güvenlik kontrolleri yoluyla korunması sağlanır. Ağ ve iletişim altyapısından kaynaklanabilecek kesintilere karşı uygun alternatif iletişim kanalları oluşturulur. Hangi sistem, sunucu ve veri yedeklerinin, hangi sıklıkta ve hangi yöntemlerle alındığını ve bu yedeklerin hangi ortam ve konumlarda tutulduğunu, güncel durumu yansıtacak şekilde kayıt altına alınır.

b. Kontroller

Şirket, bilgi sistemleri üzerinde çalışan yazılımların ve depolanan verilerin, sistemlerde herhangi bir arıza veya hata ortaya çıkması durumunda geri dönülemez biçimde kaybolmasını engellemek üzere geri yüklenebilmesi ve operasyonel amaçlar için eski tarihli verilere erişim sağlanması ihtiyacı duyulduğunda bu verilerin geri yüklenebilmesi amacıyla yedekleme süreci oluşturmuştur. Yedeklemede üç farklı araç kullanılmaktadır. Sunucu yedekleri Nutanix Prism uygulaması, veri tabanı yedekleri Veritas Netbackup uygulaması ve müşteri sunucularının yedekleri Veeam Backup and Replication uygulamasıyla alınmaktadır. Yedeklemeler sanal sunucular üzerinden uygulama yazılımları ile ilgili uygulama disklerine yazılmaktadır. Yedeklenen veriler fiziksel olarak kartuşlarda, dijital olarak disklerde tutulmaktadır.

3.8.12. Bilgi sistemleri sürekliliğinin sağlanması

a. Kontrol Hedefleri

İş faaliyetlerini yürütmede kullanılan BS servislerinin sürekliliğini sağlamak üzere iş sürekliliği yönetimi ve planının bir parçası olan bilgi sistemleri süreklilik yönetimi süreci ve Yönetim Kurulu onaylı bir bilgi sistemleri süreklilik planı hazırlanır, süreç sorumlusu atanır. Bu süreç kapsamında Şirket bilgi sistemleri süreklilik planıyla ilgili olarak şu faaliyetleri yerine getirir; iş etki analizi, risk değerlendirmesi, risk yönetimi, izleme ve test faaliyetlerini içeren bir bilgi sistemleri süreklilik yönetim süreci tesis etmek, iş birimlerinin de katılımıyla gerçekleştirilen iş etki analizi ve önceliklendirilen iş hedefleri çerçevesinde planı geliştirmek ve kurtarma için gerekli olan işlemleri belirlemek, planın uygulanabilir olmasını ve bakımını sağlamak, yılda en az bir defa, denetimler ve risk analiz çalışmaları sonucu tespit edilen bulgular ve testlerden öğrenilen derslere göre veya iş süreçlerini ya da bilgi sistemleri sürekliliğini etkileyen değişikliklerden sonra planın gözden geçirilerek güncellenmesini sağlamak, yaşanan acil durum ve felaketlerden kaynaklanan yasal konuları ele almak ve halkla ilişkiler ve basın ile olan iletişimi yürütmek, ilgili ekiplere ve çalışanlara plan kapsamında eğitim verilmesini ve farkındalığın artırılmasını sağlamak.

Planın hazırlanması sürecinde, bilgi varlıklarının ve tutulan verilerin önem düzeyi değerlendirilerek iş etki analizi çerçevesinde her bir BS servisi için kabul edilebilir kesinti süreleri ile kabul edilebilir veri kayıpları belirlenir ve

belirlenen bu limitler doğrultusunda servisin tekrar erişime açılabilmesine imkân tanıyacak kurtarma prosedürleri geliştirilir. Şirket, felaket durumunun sona ermesi sonrası ikincil merkezden birincil merkeze geri dönüşün sağlanmasına yönelik prosedürleri de hazırlar. Plan kapsamında ikincil merkez tesis edilir. Veri ve sistem yedeklerinin ikincil merkezde kullanıma hazır bulundurulması sağlanır. Planın yürütülmesinden sorumlu kritik kişiler ile plan kapsamında sorumluluğu bulunan personel, her yıl sorumlulukları ile orantılı bir detay ve içerikte BS sürekliliği eğitimine tabi tutulur ve plan kapsamındaki görev ve sorumlulukları hakkında bilgilendirilir. Birincil sistemlerin tamamen devre dışı kaldığı felaket senaryolarında dahi Şirketin faaliyetlerini yeniden sürdürebiliyor olması esastır. Bu çerçevede planın etkinliğini ve güncelliğini temin etmek üzere yılda en az bir defa gerçek bir felaket senaryosunun simülasyonunu sağlamaya ve ikincil merkez üzerinden faaliyetleri sürdürmeye yönelik testler yapılır. Testlere varsa dış hizmet sağlayıcılar da dâhil edilir, test sonuçları üst yönetime raporlanır ve bu sonuçlara göre plan güncellenir.

b. Kontroller

Hizmetleri yürütmede kullanılan BS servislerinin sürekliliğini sağlamak üzere iş sürekliliği yönetimi ve planının bir parçası olan bilgi sistemleri süreklilik yönetimi süreci ve Genel Müdür onaylı bir bilgi sistemleri süreklilik planı hazırlanmış, süreç sorumlusu atanmıştır. İş etki analizi, risk değerlendirmesi, risk yönetimi, izleme ve test faaliyetlerini içeren bir bilgi sistemleri süreklilik yönetim süreci tesis edilmiştir. Planının bakımı sağlanmaktadır. Yılda en az bir defa, denetimler ve risk analiz çalışmaları sonucu tespit edilen bulgular ve testlerden öğrenilen derslere göre veya iş süreçlerini ya da bilgi sistemleri sürekliliğini etkileyen değişikliklerden sonra plan gözden geçirilerek güncellenmesini sağlanmaktadır. Şirket, felaket durumunun sona ermesi sonrası ikincil merkezden birincil merkeze geri dönüşün sağlanmasına yönelik prosedürleri hazırlamıştır. Plan kapsamında ikincil merkez tesis edilmiştir. Planın etkinliğini ve güncelliğini temin etmek üzere 2026 yılında ikincil merkez üzerinden faaliyetleri sürdürmeye yönelik testler yapılmıştır.

3.9 MÜŞTERİLER TARAFINDAN UYGULANMASI GEREKEN KULLANICI KONTROLLERİ

Bulutistan kontrolleri bazı iç kontrollerin müşteriler tarafından uygulandığı varsayılarak tasarlanmıştır. Bulutistan tarafından belirlenen kontrol hedeflerinin başarılı olması için bahsi geçen iç kontrollerin müşteriler tarafından uygulanması önemlidir. Bu raporda belirtilen kontroller dışında da, Bulutistan tarafından belirlenen kontrol hedeflerinin başarılı olması için müşteriler tarafından oluşturulmuş ek kontroller olabilir.

Bu alan Bulutistan tarafından belirlenen kontrol hedeflerinin başarılı olması müşteri tarafından uygulandığı varsayılan kontrol hedeflerini açıklamaktadır. Aşağıda bahsi geçen kontrollerin müşteriler tarafından gerçekleştirilen kontrollerin tümünü içerdiği düşünülmemelidir.

- **Kimlik ve erişim yönetimi (MD11):** Her kullanıcının normal günlük kullanım ve erişim süresi belirlenerek tipik hesap kullanım profili oluşturulur.
- **Kimlik ve erişim yönetimi (MD11):** Kullanım profilleri, olağandışı saatlerde giriş yapmış, normal giriş sürelerini aşmış ya da genel olarak çalıştığı bilgisayar dışındaki bir bilgisayardan işlem gerçekleştirmiş olan kullanıcıların raporlanarak olağandışı durumların tespit edilmesinde kullanılır.
- **Kimlik ve erişim yönetimi (MD11):** Kullanım profilleri, uzun süredir hiç bir aktivite göstermeyen pasif hesapların tespit edilip bu tür hesaplar için gerekli bir iş ihtiyacı kalmamış ise bunların kullanımının engellenmesinde kullanılır.
- **İz kayıtlarının oluşturulması ve takibi (MD13):** Bilgi sistemleri dâhilinde gerçekleşen ve hassas ya da sır kapsamındaki verilere erişilmesine veya bunların sorgulanmasına, görüntülenmesine, kopyalanmasına, değiştirilmesine yönelik işlemlere ilişkin iz kayıtları asgari beş yıl boyunca saklanır.
- **İz kayıtlarının oluşturulması ve takibi (MD13):** Web servisleri, API ya da benzeri metotlarla diğer kurum veya kuruluşlar nezdinde tutulan verilere ilişkin yaptığı sorgulamalar ve bu sorgulamaları hangi amaçla yaptığına ilişkin iz kayıtları beş yıl boyunca saklanır ve bu tür sorgulamalara ilişkin iz kayıtları en geç aylık periyotlarla raporlanarak yetkisiz ya da amaç dışı sorgulama yapılıp yapılmadığına dair inceleme yapılır ve bu incelemeden elde edilen sonuçların gerekleri yerine getirilmesine ilişkin süreç tasarlanır.
- **İz kayıtlarının oluşturulması ve takibi (MD13):** İz kayıt sisteminin önceden belirlenmiş ve belirli periyotlarla güncellenen senaryolar çerçevesinde düzenli olarak gözden geçirilmesine, takip edilmesine

ve olağandışı durumlar ile riskli işlemlerin raporlanmasına ilişkin süreçleri tesis edilir. Olağandışı durumlar ile riskli işlemlere yönelik rapor sonuçlarının denetim birimlerince takip edilmesi sağlanır.

- **Ağ Güvenliği (MD14):** Kritik ağ segmentlerine yapılan bağlantılar düzenli tespit edilerek bağlantıların gereksinim değerlendirmesi yapılır. Gereksiz bağlantılar sonlandırılır.
- **Ağ Güvenliği (MD14):** Banka iç ağına yalnızca Banka'nın onayladığı ve izin verdiği cihazların bağlanabilmesi amacıyla uygun kontroller bulunur.
- **Ağ Güvenliği (MD14):** Personeli veya dış hizmet sağlayıcılarının banka içi uygulama ve sistemlere uzaktan erişimleri için Bilgi Güvenliği onayı bulunur.
- **Ağ Güvenliği (MD14):** Uzaktan erişimin gerçekleştiği durumlarda (banka personeli veya dış hizmet sağlayıcıları) çok bileşenli kimlik doğrulama yöntemlerinin olduğu güvenli bağlantı uygulanır. Uzaktan erişimlerin iz kayıtları tutulur. Uzaktan erişim bağlantı süresi ve bağlanan cihazlar kısıtlanır. Uzaktan erişimi sağlayan kullanıcının belli aralıklarla kimliğini tekrar doğrulaması gerekir.
- **Ağ Güvenliği (MD14):** İnternet üzerinden veya banka dış ağından görünen sunucu ve sistemler, görünür olmalarını gerektirecek geçerli iş ihtiyacı olup olmadığının tespiti amacıyla düzenli olarak kontrol edilir. Dış ağdan görünür olması gerekli olmayan sunucu ve sistemlerin banka iç ağına taşınması ve iç ağ IP adreslerine sahip olması sağlanır. İç ağdan dış ağa akan trafik içeriği kontrol edilir. Yapılacak içerik kontrolünün, zararlı IP adreslerine olan trafik akışını ve hassas veriler ile sır kapsamındaki verilerin sızdırılmasını engelleyecek nitelikte olması ve oturum bilgilerini kayıt altına alarak olağan dışı uzun süreli oturumları tespit edecek ve bunlar için uyarı üretebilecek yetenekte olması sağlanır. Bankadan gönderilen e-postalar için e-posta sunucularında gönderici kimliği doğrulayıcı teknikler kullanılır.
- **Güvenlik Konfigürasyonu Yönetimi (MD15):** Güvenli standart konfigürasyon dışında kalacak her türlü değişiklik isteği için bu değişikliği gerektiren iş gereksinimi ve bu iş gereksinimine ihtiyaç duyan iş sorumlusunun kim olduğu ve gereksinim süresi gibi bilgilerinin de kayıt altına alınmasına ilişkin süreç tasarlanır.
- **Güvenlik Konfigürasyonu Yönetimi (MD15):** Kullanılmakta olduğu veya ihtiyaç duyabilecek uygulamalar için bir beyaz liste uygulanır. Böylelikle yalnızca ihtiyaç duyulan uygulamaların sistemlerde yüklü olması ve bu beyaz liste dışındaki herhangi bir uygulamanın sistemlere yüklenmesi veya çalıştırılmasının engellenmesi sağlanır. Aynı zamanda, sistemler üzerinde beyaz listede yer almayan herhangi bir uygulamanın yüklü olup olmadığına yönelik düzenli olarak tarama gerçekleştirilir. Beyaz listedeki uygulamaların çalıştırılabilir dosyalarının veya bunların kullandığı kütüphane dosyalarının zararlı yazılımlar yoluyla değiştirilip değiştirilmediği, dosya bütünlük kontrol araçları kullanılarak kontrol edilir.
- **Güvenlik Konfigürasyonu Yönetimi (MD15):** Ağa bağlı her bir sistem üzerindeki portların, protokol ve servislerin sadece gerekliliği onaylanmış iş ihtiyaçlarına istinaden açık ve çalışıyor olması sağlanır. Bu doğrultuda, güvenli bir baz konfigürasyonu temel alınarak güvenli baz konfigürasyonda bulunmadığı halde açık durumda olan portların kapatılması sağlanır.
- **Güvenlik açıkları ve yama yönetimi (MD16):** Uygulanamayan yamaların gidermeye çalıştığı güvenlik açıklarına ilişkin riskleri azaltmaya yönelik telafi edici kontroller tesis edilir.
- **Değişiklik Yönetimi (MD24):** Bilgi sistemi yazılım bileşenlerinin ana versiyonunun kaydı tutulur ve bilgi sistemi bileşenlerinde meydana gelen değişiklikler, meydana geldiği sırayla ve değişimin gerçekleştiği tarihle birlikte kaydedilerek belgelendirilir.
- **Erişilebilirlik Yönetimi ve Yedekleme (MD27):** Soruşturma veya kovuşturma yürüten adli merciler ile Kurumdan gelen veri taleplerini alınır alınmaz bu verilerin bir kopyası alınarak yedeklenir ya da aslı talep yerine getirilene kadar idame ettirilir. Aynı zamanda veriler, talepte bulunan mercilerin kolaylıkla inceleyebileceği bilinen formatlara dönüştürülerek tevdi edilir veya talepte bulunan mercilere bu verilerle birlikte verilerin incelenmesini mümkün kılan uygulama ve araçlar temin edilir. Talep edilen verilere ilişkin alınmış olan kopyalar veya ilave yedekleri en az iki yıl süreyle saklanır.

- **Bilgi Sistemleri Sürekliliğinin Sağlanması (MD28):** İletişim bilgileri ile süreklilik planın ve ilgili kurtarma veya geri dönüş prosedürlerinin güncel kopyaları, yalnızca bilmesi gereken kişilerin erişebileceği şekilde sürekli olarak erişime açık tutulur ve gereken konumlarda kopyalarının bulundurulması sağlanır.
- **Bilgi Sistemleri Sürekliliğinin Sağlanması (MD28):** Birincil merkezdeki sistem, sunucu, ağ cihazı ve diğer BT bileşenlerinde yapılan güncellemelerin, yama yüklemelerinin ve konfigürasyon değişikliklerinin ikincil merkezdeki yedeklerinde aynı şekilde uygulanması sağlanır, ikincil merkeze kopyalanan veri ve sistem yedeklerinin birincil merkez ile aynı olduğunu garanti edecek bütünlük kontrollerini gerçekleştirilir.
- **Bilgi Sistemleri Sürekliliğinin Sağlanması (MD28):** İkincil merkez kapsamına alınan BS servisleri, sunucu, sistem, uygulama ve verilerin listesi ile ikincil merkez kapsamına alınmayan BS servisleri, sunucu, sistem, uygulama ve verilerin listesi güncel durumu yansıtacak şekilde belgelendirilir.
- **Bilgi Sistemleri Sürekliliğinin Sağlanması (MD28):** Birincil veya ikincil merkez için dış hizmet alınması ya da başka kuruluşlarla paylaşılan bir veri merkezinde barındırılması halinde, veri merkezlerinin bulunduğu konumda veya bölgesel olarak yaşanacak gerçek bir felaket anında birincil ve ikincil merkezdeki çalışma ortamının ve dış hizmet sağlayıcıların ayıracağı kaynağın, bankanın iş sürekliliğini sağlamayı garanti edecek nitelikte olması esastır.

BÖLÜM 4

4. DENETİM SONUÇLARI

4.1. DENETİMİN AMACI

Bu rapor, müşteri işlemlerinin gerçekleştirilmesini etkileyebilecek Bulutistan'daki kontroller hakkındaki bilgilerle Bulutistan müşterilerine sunulmaya yöneliktir.

Bu rapor, müşterilerdeki kontrollerin anlaşılması ve değerlendirmesi ile birleştirildiğinde, (1) müşteri finansal tablolarının denetiminin planlanmasında (2) müşteri finansal tabloları hakkındaki beyanı için Bulutistan'daki kontrollerle etkilenebilecek kontrol riskinin değerlendirilmesinde müşterilerin denetçilerine yardımcı olmaya yöneliktir.

Bulutistan kontrolleri testlerimiz, raporun bu bölümündeki matrislerde listelenen kontrol hedefleri ve ilişkili kontroller ile sınırlıdır ve sistem tanımında açıklanan ancak söz konusu matrislere dâhil edilmemiş kontrollerle ve müşterilerdeki kontrollerle genişletilmemiştir. Her bir müşterideki kontrollerle ilişkisinin değerlendirilmesi müşterilerin denetçilerinin ayrı ayrı kendi sorumluluğudur. Eğer müşterilerde belli tamamlayıcı kontroller bulunmazsa, Bulutistan'ı kontrolleri zayıflıkları karşılamaya yeterli gelmeyebilecektir.

4.2. DENETİM METODOLOJİSİ

Denetim çalışması kapsamına alınan süreçler tanımlanmış olup, süreç sahipleri belirlenmiştir. Süreç sahipleri ile gerçekleştirilecek görüşme planları oluşturulmuş, Bulutistan ile paylaşılmıştır. Her bir süreç için kontrol alanları belirlenmiş ve denetim planı oluşturulmuştur. Denetim çalışmalarımız sırasında uluslararası kabul görmüş denetim standartlarına bağlı olarak, süreç sahipleri ile yapılan görüşmelere ek olarak aşağıdaki yöntem ve analiz tekniklerinden en az biri ve gerekli görüldüğü yerlerde birden fazlası kullanılmıştır:

a) Gözlem: Özellikleri itibarıyla uygulama aşamasında gözleme dayalı tespit yapılmasını gerektiren kontrollerin (Ör. Güvenliğe yönelik fiziksel kontroller) incelenmesi,

b) Belge İncelemesi: Örnekleme yöntemi ile süreçlerdeki kontrollere ilişkin belgelerin içerik olarak incelenmesi ve bu belgelerin Şirket genel standartları ve diğer kayıtlar ile uygunluğunun belirlenmesi,

c) Yeniden Gerçekleştirme: Mevcut kontrollerin yeniden gerçekleştirilerek sonuçların karşılaştırılması,

d) Doğrulama: Gerekli görülen noktalarda, alınan görüş ve belgelerin üçüncü kaynaklar tarafından doğrulanması,

e) Çapraz Mülakat: Süreç sahipleri ile ilgili kontroller üzerinde yapılan görüşmelerin doğrulanması amacıyla, üçüncü kişilerle görüşmeler yapılması.

4.3. DENETİMİN ÇALIŞMASINDA DİKKATE ALINAN VARSAYIMLAR

Genel kontrollerin doğasında bulunan kısıtlamalar nedeni ile hata ya da suistimaller, sahtecilik, kanun dışı uygulamalar, sözleşme ihlali, oluşabilir ve tespit edilemeyebilir. Denetim sırasında talep edilen her türlü bilgi ve belgenin Bulutistan tarafından doğru, eksiksiz ve güncel olarak temin edildiği kabul edilmektedir. Denetim sonuçları test edilen dönemle sınırlıdır ve sonuçlar gelecek dönemleri kapsayacak şekilde değerlendirilmemelidir. Kontroller değerlendirilirken aynı süreçteki kontrollerin Bulutistan'ın ilgili tüm bölüm ve birimlerinde aynı şekilde uygulandığı kabul edilmiştir.

4.4. DENETİM EKİBİ VE SÜRESİ

Bulutistan'da gerçekleştirilen denetimde aşağıdaki denetçiler görev almıştır:

- Barış Bağcı
- Ece Sanem Orak
- Tuba Bakaç
- Duru Metcan

Denetim çalışmalarına 07.04.2026 tarihinde başlanmış ve çalışmalar 23.06.2026 tarihinde tamamlanmıştır.

4.5. KONTROL ORTAMI VE ELEMANLARI

Raporun bu bölümündeki kontrol matrislerinde yer alan kontrollerin tasarımının test edilmesinin yanı sıra, prosedürlerimiz, Bulutistan kontrol ortamındaki aşağıdaki elemanların da test edilmesini içermektedir:

- Yönetim Kurulu
- İnsan Kaynakları Politikaları ve Uygulamaları
- Risk Yönetimi
- İzleme

Kontrol ortamı testlerimiz, uygun yönetimin, gözetimin ve personelin sorgulanmasını ve Bulutistan dokümanlarının ve kayıtlarının incelenmesini içermektedir. Kontrol ortamı kontrollerin tasarım testlerinin yapısının, zamanlamasının ve kapsamının belirlenmesi açısından değerlendirilmiştir.

4.6. YÖNETİM BEYANININ DEĞERLENDİRİLMESİ

Bulutistan tarafından hazırlanan ve denetim ekibi tarafından okunan ve değerlendirilen yönetim yazısı ekte yönetim beyanı içermektedir.

Yönetim ekibinin yönetim yazısının dışında, yönetimden Bulutistan'ın organizasyon sistemini ve risk taşıyan süreçleri ve kontrollere ilişkin bilgileri açıklayan herhangi bir belge alınmamış ve değerlendirilmemiştir.

4.7. KONTROL HEDEFLERİ VE KONTROL AKTİVİTELERİ

4.7.1. Bilgi sistemleri politika, prosedür ve süreç dokümanları

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD05.01	Bilgi sistemlerinin kullanımından kaynaklanan riskleri yönetmek ve bilgi varlıklarını korumak amacıyla uygulanması gereken usul ve esaslar ile tesis edilmesi gereken kontrolleri tarif eden politika, prosedür ve süreç dokümanları oluşturulur.	Politikalar, Prosedürler ve Doküman Yönetim Prosedürü talep edilir ve bilgi sistemlerinin kullanımından kaynaklanan riskleri yönetmek ve bilgi varlıklarını korumak amacıyla uygulanması gereken usul ve esaslar ile tesis edilmesi gereken kontrolleri tarif eden politika, prosedür ve süreç dokümanları oluşturulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD05.02	Dokümanların gizlilik derecesi ve çalışanların görev ve sorumluluklarının uygunluğu nispetinde dokümanlara erişim imkânı verilmesine ve dokümantasyonda asgari olarak doküman kodu ve dokümanın gizlilik derecesi bulunmasına ilişkin süreç oluşturulur.	Politikalar, Prosedürler ve Doküman Yönetim Prosedürü talep edilir ve dokümanların gizlilik derecesi ve çalışanların görev ve sorumluluklarının uygunluğu nispetinde dokümanlara erişim imkânı verilmesine ve dokümantasyonda asgari olarak doküman kodu ve dokümanın gizlilik derecesi bulunmasına ilişkin süreç oluşturulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD05.03	Dokümantasyonda asgari olarak doküman kodu ve dokümanın gizlilik derecesine yer verilir.	Politikalar, Prosedürler ve Doküman Yönetim Prosedürü talep edilir ve dokümantasyonda asgari olarak doküman kodu ve dokümanın gizlilik derecesine yer verildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD05.04	BS politikaları yönetim kurulu tarafından, BS prosedürleri ve süreç dokümanları ise yönetim kurulu ya da yönetim kurulunun bu yönde yetkisini devrettiği yöneticilerce onaylanır.	Politikalar, Prosedürler ve Doküman Yönetim Prosedürü talep edilir ve BS politikalarının yönetim kurulu tarafından, BS prosedürlerinin ve süreç dokümanlarının ise yönetim kurulu ya da yönetim kurulunun bu yönde yetkisini devrettiği yöneticilerce onaylandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD05.05	BS politika, prosedür ve süreç dokümanlarının gerekleri, organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilmiş ve bunların işlerliğine ilişkin gözetim ve takip gerçekleştirilir.	Politikalar, Prosedürler ve Doküman Yönetim Prosedürü talep edilir ve BS politika, prosedür ve süreç dokümanlarının gereklerinin, organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilmiş ve bunların işlerliğine ilişkin gözetim ve takip gerçekleştirildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD05.06	Politika, prosedür ve süreç dokümanlarının yılda en az bir defa gözden geçirilerek ve gerekli güncellemelerin yapılmasına ve dokümanlarda meydana gelen değişiklikleri takip edebilmek adına, dokümanın önceki versiyonu ile asgari olarak dokümanı onaylayan, revizyon tarihi ve gözden geçirme tarihi bilgileri kayıt altına alınmasına ilişkin süreç bulunulur.	Politikalar, Prosedürler ve Doküman Yönetim Prosedürü talep edilir ve politika, prosedür ve süreç dokümanlarının yılda en az bir defa gözden geçirilerek ve gerekli güncellemelerin yapılmasına ve dokümanlarda meydana gelen değişiklikleri takip edebilmek adına, dokümanın önceki versiyonu ile asgari olarak dokümanı onaylayan, revizyon tarihi ve gözden geçirme tarihi bilgileri kayıt altına alınmasına ilişkin süreç bulunduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

4.7.2. Bilgi güvenliği organizasyonu, roller ve sorumluluklar

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD08.01	Bilgi güvenliği yönetim sistemi oluşturulurken, ulusal veya uluslararası standartlar ya da en iyi uygulamalar referans alınır.	Bilgi güvenliği dokümanları talep edilir ve bilgi güvenliği yönetim sistemi oluşturulurken, ulusal veya uluslararası standartlar ya da en iyi uygulamalar referans alındığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.02	İlgili politika ile Şirket bünyesinde bilgi güvenliğinin sağlanmasında nihai sorumluluk yönetim kuruluna tayin edilir ve bilgi güvenliği politikası yönetim kurulu tarafından onaylanır.	Bilgi güvenliği dokümanları talep edilir ve ilgili politika ile Şirket bünyesinde bilgi güvenliğinin sağlanmasında nihai sorumluluk yönetim kuruluna tayin edildiği ve bilgi güvenliği politikasının yönetim kurulu tarafından onaylandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.03	Bilgi güvenliği yönetim sisteminin Şirket genelinde nasıl uygulanacağı ile ilgili bilgi güvenliği politikası, prosedürleri ve süreç dokümanları ile düzenlenir.	Bilgi güvenliği dokümanları talep edilir ve bilgi güvenliği yönetim sisteminin Şirket genelinde nasıl uygulanacağı ile ilgili bilgi güvenliği politikası, prosedürleri ve süreç dokümanları ile düzenlendiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.04	Bilgi Güvenliği Politikası tüm çalışanların ulaşabileceği şekilde bir ortamda tutulur ve değişiklik ve güncellemelerin ardından personele bildirimi yapılır.	Bilgi güvenliği dokümanları ve portal ekranları talep edilir ve Bilgi Güvenliği Politikası tüm çalışanların ulaşabileceği şekilde bir ortamda tutulduğu ve değişiklik ve güncellemelerin ardından personele bildirimi yapıldığı belge inceleme ve gözlem yöntemleri ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.05	Bilgi güvenliği politikası, prosedürleri ve süreç dokümanlarının yılda en az bir defa gözden geçirilmesini sağlayan bir prosedür oluşturulur.	Bilgi güvenliği dokümanları talep edilir ve bilgi güvenliği politikası, prosedürleri ve süreç dokümanlarının yılda en az bir defa gözden geçirilmesini sağlayan bir prosedür oluşturulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.06	Bilgi güvenliği politikasının oluşturulması ve uygulanması faaliyetleri için yönetim kurulu adına Bilgi Güvenliği Komitesi oluşturulur.	Bilgi güvenliği dokümanları talep edilir ve Bilgi güvenliği politikasının oluşturulması ve uygulanması faaliyetleri için yönetim kurulu adına Bilgi Güvenliği Komitesinin oluşturulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.07	Bilgi Güvenliği Komitesine, belirlenen bir yönetim kurulu üyesi veya genel müdür başkanlık eder ve komitenin koordinasyonunu bilgi güvenliği sorumlusu yerine getirir.	Bilgi güvenliği komitesi dokümanları talep edilir ve komiteye, belirlenen bir yönetim kurulu üyesi veya genel müdürün başkanlık ettiği ve komitenin koordinasyonunu bilgi güvenliği sorumlusunun yerine getirdiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.08	Bilgi Güvenliği Komitesi toplantılarına bilgi sistemlerinden sorumlu üst düzey yöneticinin, ilgili iş birimlerinden üst düzey yöneticilerin, insan kaynakları birimlerinden ve organizasyonda bulunması durumunda uyum ve hukuk ile ilgili birim ya da pozisyonlardan temsilcilerin de katılması sağlanır.	Bilgi güvenliği komitesi dokümanları talep edilir ve komite toplantılarına bilgi sistemlerinden sorumlu üst düzey yöneticinin, ilgili iş birimlerinden üst düzey yöneticilerin, insan kaynakları birimlerinden ve organizasyonda bulunması durumunda uyum ve hukuk ile ilgili birim ya da pozisyonlardan temsilcilerin de katılmasının sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.09	Bilgi Güvenliği Komitesinin görev tanımları ve çalışma esaslarının, yönetim kurulu tarafından onaylı olacak şekilde yazılı hale	Bilgi güvenliği komitesi dokümanları talep edilir ve komitenin görev tanımları ve çalışma esaslarının, yönetim kurulu	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
	getirilip, yılda en az iki defa toplanması ve yılda en az bir defa yönetim kuruluna rapor sunması sağlanır.	tarafından onaylı olacak şekilde yazılı hale getirilip, yılda en az iki defa toplanması ve yılda en az bir defa yönetim kuruluna rapor sunmasının sağlandığı belge inceleme yöntemi ile test edilir.	
MD08.10	BS Güvenlik Fonksiyonunu yönetmesi için bir Bilgi Güvenliği Sorumlusu atanır ve aşağıdaki detayları içeren görev tanımı oluşturulur. a) Bilgi güvenliği politikası, prosedürleri ve süreç dokümanlarının oluşturulması, bunların güncellenmesi ve onaya sunulması, b) Bilgi güvenliği bakış açısıyla, bilgi varlıklarının sınıflandırılması ve bilgi varlıklarına yönelik gizlilik, bütünlük, erişilebilirlik kriterleri bakımından BS risk yönetimi çalışmalarına aktif katkı sunulması ve yardımcı olunması, c) İlgili birimlerle uyum içinde, iş gereksinimleri ve iş hedefleriyle uyumlu bilgi güvenliğinin tesis edilmesi, ç) Bilgi güvenliği ile ilgili mevzuat hükümlerine, standartlara, politika, prosedür ve süreç dokümanlarına uyumun takip edilmesi, d) Bilgi güvenliği faaliyetlerinin ve testlerinin yürütülmesinin sağlanması ve bunların takip edilmesi, e) Önemli projeler ve değişiklikler için bilgi güvenliği gereksinimlerinin belirlenmesi çalışmalarına katkıda bulunulması, f) Bilgi güvenliğini ilgilendiren paydaşlara yönelik bilgi güvenliği farkındalık programının yürütülmesi.	Bilgi güvenliği dokümanları talep edilir ve BS güvenlik fonksiyonunu yönetmesi için bir Bilgi Güvenliği Sorumlusu atandığı ve ilgili detayları içeren görev tanımı oluşturulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.11	Bilgi güvenliği sorumlusu, bilgi güvenliği politikası, prosedürleri ve süreç dokümanlarının oluşturulması, bunların güncellenmesi ve onaya sunulması ile görevlendirilir.	Bilgi güvenliği dokümanları talep edilir ve bilgi güvenliği sorumlusunun, bilgi güvenliği politikası, prosedürleri ve süreç dokümanlarının oluşturulması, bunların güncellenmesi ve onaya sunulması ile görevlendirildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.12	Bilgi güvenliği sorumlusu, bilgi güvenliği bakış açısıyla, bilgi varlıklarının sınıflandırılması ve bilgi varlıklarına yönelik gizlilik, bütünlük, erişilebilirlik kriterleri bakımından BS risk yönetimi çalışmalarına aktif katkı sağlar.	Bilgi güvenliği dokümanları talep edilir ve bilgi güvenliği sorumlusunun, bilgi güvenliği bakış açısıyla, bilgi varlıklarının sınıflandırılması ve bilgi varlıklarına yönelik gizlilik, bütünlük, erişilebilirlik kriterleri bakımından BS risk yönetimi çalışmalarına aktif katkı sağladığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.13	Bilgi güvenliği sorumlusu, İlgili birimlerle uyum içinde, bilgi güvenliği fonksiyonunun iş gereksinimleri ve iş hedefleriyle uyumlu olması hususunu gözetir.	Bilgi güvenliği dokümanları talep edilir ve bilgi güvenliği sorumlusunun, ilgili birimlerle uyum içinde, bilgi güvenliği fonksiyonunun iş gereksinimleri ve iş hedefleriyle uyumlu olması hususunu gözettiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.14	Bilgi güvenliği sorumlusu, Bilgi güvenliği ile ilgili mevzuat hükümlerine, standartlara, politika, prosedür ve süreç dokümanlarına uyuma dair değerlendirme çalışmaları gerçekleştirir.	Bilgi güvenliği dokümanları talep edilir ve bilgi güvenliği sorumlusunun, bilgi güvenliği ile ilgili mevzuat hükümlerine, standartlara, politika, prosedür ve süreç dokümanlarına uyuma dair değerlendirme çalışmaları gerçekleştirdiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD08.15	Bilgi güvenliği sorumlusu, önemli projeler ve değişiklikler için bilgi güvenliği gereksinimlerinin belirlenmesi çalışmalarına katkıda bulunur.	Bilgi güvenliği dokümanları talep edilir ve bilgi güvenliği sorumlusunun, önemli projeler ve değişiklikler için bilgi güvenliği gereksinimlerinin belirlenmesi çalışmalarına katkıda bulunduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.16	Bilgi güvenliği sorumlusu, bilgi güvenliğini ilgilendiren paydaşlara yönelik bilgi güvenliği farkındalık programını oluşturur.	Bilgi güvenliği dokümanları talep edilir ve bilgi güvenliği sorumlusunun, bilgi güvenliğini ilgilendiren paydaşlara yönelik bilgi güvenliği farkındalık programını oluşturduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.17	Bilgi Güvenliği Fonksiyonunun gözetiminde bilgi varlıkları sınıflandırılır ve varlık sahipleri belirlenir.	Bilgi güvenliği ve bilgi varlıkları dokümanları talep edilir ve bilgi güvenliği fonksiyonunun gözetiminde bilgi varlıklarının sınıflandırıldığı ve varlık sahiplerinin belirlendiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.18	Bilgi varlıklarının güvenlik sınıflandırmalarına göre uygun güvenlik kontrolleri uygulanır.	Bilgi güvenliği ve bilgi varlıkları dokümanları talep edilir ve bilgi varlıklarının güvenlik sınıflandırmalarına göre uygun güvenlik kontrolleri uygulandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.19	Bilgi varlıklarına yönelik olarak düzenli bir şekilde tehdit ve risk değerlendirme çalışmaları yapılır.	Bilgi güvenliği ve bilgi varlıkları dokümanları talep edilir ve bilgi varlıklarına yönelik olarak düzenli bir şekilde tehdit ve risk değerlendirme çalışmaları yapıldığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.20	Bilgi güvenliği ihlaline ilişkin olayların izlenmesi ve raporlanmasına dair kontroller bulunur.	Bilgi güvenliği dokümanları talep edilir ve bilgi güvenliği ihlaline ilişkin olayların izlenmesi ve raporlanmasına dair kontrollerin bulunduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.21	Görevler ayrılığı prensibine uygun şekilde kimlik doğrulama ve erişim yönetiminin tesis edilmesi sürecinde Bilgi Güvenliği Fonksiyonu etkin bir şekilde bulunur.	Bilgi güvenliği dokümanları talep edilir ve görevler ayrılığı prensibine uygun şekilde kimlik doğrulama ve erişim yönetiminin tesis edilmesi sürecinde Bilgi Güvenliği Fonksiyonunun etkin bir şekilde bulunduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.22	Bilgi güvenliğinin sağlanmasına ilişkin kontrollerin ve tesis edilen yapılar test edilir.	Bilgi güvenliği dokümanları talep edilir ve bilgi güvenliğinin sağlanmasına ilişkin kontrollerin ve tesis edilen yapıların test edildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.23	Bilgi güvenliğinin sağlanmasına ilişkin kontrollerin ve tesis edilen yapıların test sonuçları takip edilir ve raporlanır.	Bilgi güvenliği dokümanları talep edilir ve bilgi güvenliğinin sağlanmasına ilişkin kontrollerin ve tesis edilen yapıların test sonuçlarının takip edildiği ve raporlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.24	Bilgi varlıklarına yönelik güncel güvenlik açıkları takip edilir ve gerekli aksiyonlar alınır.	Bilgi güvenliği dokümanları talep edilir ve bilgi varlıklarına yönelik güncel güvenlik açıklarının takip edildiği ve gerekli aksiyonların alındığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.25	Üst yönetim de dâhil olmak üzere çalışanlar, dış hizmet sağlayıcılar ve müşteriler gibi bilgi güvenliğini ilgilendiren paydaşlara yönelik, bilgi güvenliği farkındalığını artıracak çalışmalar yapılır.	Bilgi güvenliği dokümanları talep edilir ve üst yönetim de dâhil olmak üzere çalışanlar, dış hizmet sağlayıcılar ve müşteriler gibi bilgi güvenliğini ilgilendiren paydaşlara yönelik, bilgi güvenliği farkındalığını artıracak çalışmalar yapıldığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD08.26	İş sürekliliği yönetimi kapsamında bilgi güvenliğini ilgilendiren hususlarda Bilgi Güvenliği Fonksiyonunun katılımı sağlanır.	Bilgi güvenliği ve iş sürekliliği dokümanları talep edilir ve İş sürekliliği yönetimi kapsamında bilgi güvenliğini ilgilendiren hususlarda Bilgi Güvenliği Fonksiyonunun katılımının sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD08.27	Dış hizmet alımlarının yönetimi kapsamında bilgi güvenliğini ilgilendiren hususlarda Bilgi Güvenliği Fonksiyonunun katılımı sağlanır.	Bilgi güvenliği ve dış hizmet alım dokümanları talep edilir ve dış hizmet alımlarının yönetimi kapsamında bilgi güvenliğini ilgilendiren hususlarda Bilgi Güvenliği Fonksiyonunun katılımının sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

4.7.3. Kimlik ve erişim yönetimi

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD11.01	Bilgi varlıklarına olan erişimlerin, görevler ayrılığı prensibine göre belirlenmiş ve kullanıcıların sorumluluğu gereği kendileri için tanımlanan erişim kontrolleri uyarınca, ilişkili bilgi varlığının güvenlik sınıfına uygun bir kimlik doğrulama yöntemiyle gerçekleştirilmesini sağlanır.	Erişim Kontrol Politikası ve kimlik ve erişim bilgileri talep edilir ve bilgi varlıklarına olan erişimlerin, görevler ayrılığı prensibine göre belirlenmiş ve kullanıcıların sorumluluğu gereği kendileri için tanımlanan erişim kontrolleri uyarınca, ilişkili bilgi varlığının güvenlik sınıfına uygun bir kimlik doğrulama yöntemiyle gerçekleştirildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.02	Süreçler ve sistemler üzerinde kullanıcılara sağlanan yetkilerin, kullanıcılara görev ve sorumluluklarına uygun roller ve/veya profiller aracılığı ile temin edilmesini sağlanır ve kullanıcıların görev tanımlarına uygun uygulama ve sistemler üzerindeki rolleri dokümante edilir.	Erişim Kontrol Politikası ve kimlik ve erişim bilgileri talep edilir ve süreçler ve sistemler üzerinde kullanıcılara sağlanan yetkilerin, kullanıcılara görev ve sorumluluklarına uygun roller ve/veya profiller aracılığı ile temin edilmesinin sağlandığı ve kullanıcıların görev tanımlarına uygun uygulama ve sistemler üzerindeki rolleri dokümante edildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.03	Süreçler ve sistemler üzerinde kullanıcılara sağlanan yetkilerin, kullanıcılara görev ve sorumluluklarına uygun roller ve/veya profiller aracılığı ile temin edilmesi sağlanır.	Erişim Kontrol Politikası ve kimlik ve erişim bilgileri talep edilir ve süreçler ve sistemler üzerinde kullanıcılara sağlanan yetkilerin, kullanıcılara görev ve sorumluluklarına uygun roller ve/veya profiller aracılığı ile temin edilmesi sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.04	Süreçler ve sistemler üzerinde kullanıcıların görev tanımlarına uygun uygulama ve sistemler üzerindeki rolleri dokümante edilir.	Aktif Dizin kullanıcı listeleri talep edilir ve süreçler ve sistemler üzerinde kullanıcıların görev tanımlarına uygun uygulama ve sistemler üzerindeki rollerin dokümante edildiği belge inceleme yöntemi ile test edilir.	Uygulama ve sistemler üzerinde kullanıcıların görev ve sorumluluklarına uygun olarak atanması gereken rollerin dokümante edilmediği tespit edilmiştir. (Bulgu denetim esnasında düzeltilmiştir.)
MD11.05	Bilgi sistemleri üzerindeki kullanıcılara uygulanacak kimlik doğrulama mekanizması, kullanıcıların bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek süreci kapsayacak şekilde tesis edilir ve kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek önlemler alınır.	Erişim Kontrol Politikası, kimlik ve erişim bilgileri, Aktif Dizin parola parametreleri talep edilir ve bilgi sistemleri üzerindeki kullanıcılara uygulanacak kimlik doğrulama mekanizması, kullanıcıların bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek süreci kapsayacak şekilde tesis edildiği ve kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek önlemler alındığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.06	Bilgi sistemleri üzerindeki kullanıcılara ait kimlik doğrulama bilgilerinin güvenliğine yönelik; kimlik doğrulama bilgilerinin veritabanlarında şifreli olarak veya matematiksel olarak geriye dönüştürülmesi mümkün olmayan yöntemlerle muhafaza edilmesi, kimlik doğrulama amacıyla aktarılırken	Erişim Kontrol Politikası, kimlik ve erişim bilgileri, kimlik doğrulama bilgilerinin yer aldığı veri tabanı bilgileri, veri tabanı kullanıcı listeleri ve veri tabanları için tutulan iz kayıtları talep edilir ve bilgi sistemleri üzerindeki kullanıcılara ait kimlik doğrulama bilgilerinin güvenliğine yönelik; kimlik doğrulama bilgilerinin	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
	şifrelenmesi, yetkisiz erişimlere veya görevler ayrılığı prensibine aykırı olarak kontrolsüz bir şekilde gerçekleştirilecek değişikliklere karşı korunması, bu veritabanları üzerinde gerçekleştirilen işlemlere ilişkin yeterli iz kayıtlarının tutulması ve bu iz kayıtlarının güvenliğinin sağlanması gibi önlemler alınır.	veritabanlarında şifreli olarak veya matematiksel olarak geriye dönüştürülmesi mümkün olmayan yöntemlerle muhafaza edilmesi, kimlik doğrulama amacıyla aktarılırken şifrelenmesi, yetkisiz erişimlere veya görevler ayrılığı prensibine aykırı olarak kontrolsüz bir şekilde gerçekleştirilecek değişikliklere karşı korunması, bu veritabanları üzerinde gerçekleştirilen işlemlere ilişkin yeterli iz kayıtlarının tutulması ve bu iz kayıtlarının güvenliğinin sağlanması gibi önlemler alındığı belge inceleme yöntemi ile test edilir.	
MD11.07	Bilgi sistemleri üzerindeki kimlik doğrulama bilgilerinin veritabanlarında şifreli olarak veya matematiksel olarak geriye dönüştürülmesi mümkün olmayan yöntemlerle muhafaza edilmesi sağlanır.	Erişim Kontrol Politikası, kimlik ve erişim bilgileri, kimlik doğrulama bilgilerinin yer aldığı veri tabanı bilgileri, veri tabanı kullanıcı listeleri ve veri tabanları için tutulan iz kayıtları talep edilir ve bilgi sistemleri üzerindeki kimlik doğrulama bilgilerinin veritabanlarında şifreli olarak veya matematiksel olarak geriye dönüştürülmesi mümkün olmayan yöntemlerle muhafaza edilmesi sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.08	Bilgi sistemleri üzerindeki kimlik doğrulama bilgilerinin kimlik doğrulama amacıyla aktarılırken şifrelenmesi sağlanır.	Erişim Kontrol Politikası, kimlik ve erişim bilgileri, kimlik doğrulama bilgilerinin yer aldığı veri tabanı bilgileri, veri tabanı kullanıcı listeleri ve veri tabanları için tutulan iz kayıtları talep edilir ve bilgi sistemleri üzerindeki kimlik doğrulama bilgilerinin kimlik doğrulama amacıyla aktarılırken şifrelenmesi sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.09	Bilgi sistemleri üzerindeki kimlik doğrulama bilgilerinin yetkisiz erişimlere veya görevler ayrılığı prensibine aykırı olarak kontrolsüz bir şekilde gerçekleştirilecek değişikliklere karşı korunur.	Erişim Kontrol Politikası, kimlik ve erişim bilgileri, kimlik doğrulama bilgilerinin yer aldığı veri tabanı bilgileri, veri tabanı kullanıcı listeleri ve veri tabanları için tutulan iz kayıtları talep edilir ve bilgi sistemleri üzerindeki kimlik doğrulama bilgilerinin yetkisiz erişimlere veya görevler ayrılığı prensibine aykırı olarak kontrolsüz bir şekilde gerçekleştirilecek değişikliklere karşı korunduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.10	Bilgi sistemleri üzerindeki kimlik doğrulama bilgilerinin bu veritabanları üzerinde gerçekleştirilen işlemlere ilişkin yeterli iz kayıtları tutulur.	Erişim Kontrol Politikası, kimlik ve erişim bilgileri, kimlik doğrulama bilgilerinin yer aldığı veri tabanı bilgileri, veri tabanı kullanıcı listeleri ve veri tabanları için tutulan iz kayıtları talep edilir ve bilgi sistemleri üzerindeki kimlik doğrulama bilgilerinin bu veritabanları üzerinde gerçekleştirilen işlemlere ilişkin yeterli iz kayıtları tutulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.11	Bilgi sistemleri üzerindeki kimlik doğrulama bilgilerinin veritabanları üzerinde gerçekleştirilen işlemlere ilişkin tutulan iz kayıtlarının güvenliği sağlanır.	Erişim Kontrol Politikası, kimlik ve erişim bilgileri, kimlik doğrulama bilgilerinin yer aldığı veri tabanı bilgileri, veri tabanı kullanıcı listeleri ve veri tabanları için	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
		tutulan iz kayıtları talep edilir ve bilgi sistemleri üzerindeki kimlik doğrulama bilgilerinin veritabanları üzerinde gerçekleştirilen işlemlere ilişkin tutulan iz kayıtlarının güvenliği sağlandığı belge inceleme yöntemi ile test edilir.	
MD11.12	Bilgi sistemleri üzerindeki Kimlik doğrulama mekanizması (a) Başarısız kimlik doğrulama teşebbüsleri hakkında başarısız teşebbüslerin belirli bir sayıyı aşması halinde ilgili kullanıcının erişimini engeller (b) Başarısız kimlik doğrulama teşebbüsleri sonrasında, bu teşebbüsü gerçekleştiren kişiye, hatalı girilen kullanıcı adı bilgisi veya parola ile ilgili, böyle bir kullanıcı adının sistemde olmadığı veya parolanın hatalı girildiği bilgisini verilmez. (c) Hiçbir işlem yapılmayan hareketsiz oturumlar için oturumu belirli bir süre sonra sonlandırması veya kilitlemesi sağlanır. (ç) Birden fazla kullanıcının aynı kullanıcı hesabını kullanmaları ya da aynı anda farklı oturumlar açabilmeleri konusunda yetkilendirildiği durumlar hariç olmak üzere, aynı kullanıcı için aynı anda birden fazla oturum açılmaya çalışılması durumunda buna izin vermemesi ve kullanıcıya uyarı vermesi sağlanır.	Erişim Kontrol Politikası ve kimlik ve erişim bilgileri talep edilir ve bilgi sistemleri üzerindeki Kimlik doğrulama mekanizmasının a) Başarısız kimlik doğrulama teşebbüsleri hakkında başarısız teşebbüslerin belirli bir sayıyı aşması halinde ilgili kullanıcının erişimini engellediği (b) Başarısız kimlik doğrulama teşebbüsleri sonrasında, bu teşebbüsü gerçekleştiren kişiye, hatalı girilen kullanıcı adı bilgisi veya parola ile ilgili, böyle bir kullanıcı adının sistemde olmadığı veya parolanın hatalı girildiği bilgisini vermediği (c) Hiçbir işlem yapılmayan hareketsiz oturumlar için oturumu belirli bir süre sonra sonlandırması veya kilitlemesini sağladığı (ç) Birden fazla kullanıcının aynı kullanıcı hesabını kullanmaları ya da aynı anda farklı oturumlar açabilmeleri konusunda yetkilendirildiği durumlar hariç olmak üzere, aynı kullanıcı için aynı anda birden fazla oturum açılmaya çalışılması durumunda buna izin vermemesi ve kullanıcıya uyarı vermesini sağladığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.13	Kullanıcılara uygulanacak erişim kontrol kuralları ve atanacak yetkilerin belirlenmesinde görevler ayrılığı prensibi esas alınıp süreçler ve sistemler, kritik bir işlemin tek bir kişi tarafından başlatılması, onaylanması ve tamamlanmasına imkân vermeyecek şekilde tasarlanır.	Erişim Kontrol Politikası ve kimlik ve erişim bilgileri talep edilir ve kullanıcılara uygulanacak erişim kontrol kuralları ve atanacak yetkilerin belirlenmesinde görevler ayrılığı prensibi esas alınıp süreçler ve sistemler, kritik bir işlemin tek bir kişi tarafından başlatılması, onaylanması ve tamamlanmasına imkân vermeyecek şekilde tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.14	Süreçler ve sistemler, kritik bir işlemin tek bir kişi tarafından başlatılması, onaylanması ve tamamlanmasına imkân vermeyecek şekilde işletilir.	Erişim Kontrol Politikası ve kimlik ve erişim bilgileri talep edilir ve süreçler ve sistemlerin, kritik bir işlemin tek bir kişi tarafından başlatılması, onaylanması ve tamamlanmasına imkân vermeyecek şekilde işletildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.15	Süreçler ve sistemlerde erişim yetkilerinin talep edilmesi, yetkilendirilmesi ve yönetilmesi görevlerinin birbirinden ayrılması sağlanır.	Erişim Kontrol Politikası ve kimlik ve erişim bilgileri talep edilir ve süreçler ve sistemlerde erişim yetkilerinin talep edilmesi, yetkilendirilmesi ve yönetilmesi görevlerinin birbirinden ayrılmasının sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.16	Görevlerin tam manasıyla ve uygun şekilde ayrıştırılmasının mümkün olmadığı durumlarda, bu durumdan	Erişim Kontrol Politikası ve kimlik ve erişim bilgileri talep edilir ve görevlerin tam manasıyla ve uygun şekilde	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
	kaynaklanabilecek hata ve suistimalleri önlemeye yönelik risk azaltıcı veya telafi edici ilave kontroller tesis edilir.	ayrıştırılmasının mümkün olmadığı durumlarda, bu durumdan kaynaklanabilecek hata ve suistimalleri önlemeye yönelik risk azaltıcı veya telafi edici ilave kontroller tesis edildiği belge inceleme yöntemi ile test edilir.	
MD11.17	Kullanıcıların, geçerli bir iş ihtiyacının mevcut olduğu ve erişimin gerekli olduğu süre zarfında, bilgi varlıklarına erişebilmeleri için yetkilendirilmesi, Bilgi varlıklarına erişim yetkisi olan kullanıcılar, ilgili bilgi varlığı sahibi tarafından yılda en az bir defa gözden geçirilmesi, Kullanıcıların görev ve sorumlulukları göz önünde bulundurularak sadece bu görevleri yerine getirmelerine yetecek ve sadece bilmeleri gereken verilere erişmelerini sağlayacak kadar yetkiye sahip olmaları sağlanmasına ilişkin süreç tasarlanır.	Erişim Kontrol Politikası ve kimlik ve erişim bilgileri talep edilir ve kullanıcıların, geçerli bir iş ihtiyacının mevcut olduğu ve erişimin gerekli olduğu süre zarfında, bilgi varlıklarına erişebilmeleri için yetkilendirilmesi, bilgi varlıklarına erişim yetkisi olan kullanıcılar, ilgili bilgi varlığı sahibi tarafından yılda en az bir defa gözden geçirilmesi, Kullanıcıların görev ve sorumlulukları göz önünde bulundurularak sadece bu görevleri yerine getirmelerine yetecek ve sadece bilmeleri gereken verilere erişmelerini sağlayacak kadar yetkiye sahip olmaları sağlanmasına ilişkin sürecin tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.18	Yetkili kullanıcılar için geçerli bir iş ihtiyacının mevcut olduğu ve erişimin gerekli olduğu süre zarfında yetkilendirildikleri kontrol edilir.	Kullanıcı yetki gözden geçirme dokümantasyonu talep edilir ve yetkili kullanıcılar için geçerli bir iş ihtiyacının mevcut olduğu ve erişimin gerekli olduğu süre zarfında yetkilendirildiklerinin kontrol edildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.19	Bilgi varlıklarına erişim yetkisi olan kullanıcılar, ilgili bilgi varlığı sahibi tarafından yılda en az bir defa gözden geçirilir.	Kullanıcı yetki gözden geçirme dokümantasyonu talep edilir ve bilgi varlıklarına erişim yetkisi olan kullanıcıların, ilgili bilgi varlığı sahibi tarafından yılda en az bir defa gözden geçirildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.20	Ayrıcalıklı yetkilere sahip kullanıcı ve uygulama hesapları ile ilgili olarak belli tedbirlerin alınmasına ilişkin süreç tasarlanır.	Erişim Kontrol Politikası, Ayrıcalıklı Erişim Yönetimi Prosedürü ve kimlik ve erişim bilgileri talep edilir ve ayrıcalıklı yetkilere sahip kullanıcı ve uygulama hesapları ile ilgili olarak belli tedbirlerin alınmasına ilişkin süreç tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.21	Ayrıcalıklı yetkilere sahip kullanıcı ve uygulama hesapları ile ilgili olarak kimlik doğrulamayla birlikte ek güvenlik kontrolleri uygulanır.	Erişim Kontrol Politikası, Ayrıcalıklı Erişim Yönetimi Prosedürü ve kimlik ve erişim bilgileri talep edilir ve ayrıcalıklı yetkilere sahip kullanıcı ve uygulama hesapları ile ilgili olarak kimlik doğrulamayla birlikte ek güvenlik kontrolleri uygulandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.22	Ayrıcalıklı yetkilerin yalnızca gerekli olan kullanıcılara atanması ve sadece gerekli olan durumlarda bu tür hesapların kullanılması sağlanır.	Erişim Kontrol Politikası, Ayrıcalıklı Erişim Yönetimi Prosedürü, kullanıcı listeleri ve kimlik ve erişim bilgileri talep edilir ve ayrıcalıklı yetkilerin yalnızca gerekli olan kullanıcılara atanması ve sadece gerekli olan durumlarda bu tür hesapların kullanılmasının sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD11.23	Bu tür hesaplar ile gerçekleştirilen işlemleri takip edecek şekilde iz kayıtları tutulur ve bunlar düzenli olarak gözden geçirilir.	Erişim Kontrol Politikası, Ayrıcalıklı Erişim Yönetimi Prosedürü, ayrıcalıklı yetkilere sahip kullanıcı ve uygulama hesapları ile gerçekleştirilen işlemleri takip edecek şekilde tutulan iz kayıtları talep edilir ve bu tür hesaplar ile gerçekleştirilen işlemleri takip edecek şekilde iz kayıtları tutulduğu ve bunların düzenli olarak gözden geçirildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.24	Hesaplar oluşturulduğunda veya silindiğinde bu tür işlemler için iz kaydı tutulması ve uyarı üretilmesi sağlanır.	Erişim Kontrol Politikası, Ayrıcalıklı Erişim Yönetimi Prosedürü, ayrıcalıklı yetkilere sahip kullanıcı ve uygulama hesaplarının oluşturulması veya silinmesi gibi işlemler için iz kayıtları talep edilir ve hesaplar oluşturulduğunda veya silindiğinde bu tür işlemler için iz kaydı tutulması ve uyarı üretilmesinin sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.25	Yapılan başarısız giriş denemeleri için iz kaydı tutulur ve uyarı üretilir.	Erişim Kontrol Politikası, Ayrıcalıklı Erişim Yönetimi Prosedürü, ayrıcalıklı yetkilere sahip kullanıcı ve uygulama hesaplarına yapılan başarısız giriş denemeleri için iz kayıtları talep edilir ve yapılan başarısız giriş denemeleri için iz kaydı tutulduğu ve uyarı üretildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.26	Hesapların ortaklaşa kullanılması engellenir veya bu hesapları kullanan gerçek kişilere sorumluluk atayacak teknikler kullanılır.	Erişim Kontrol Politikası, Ayrıcalıklı Erişim Yönetimi Prosedürü, bilgi sistemleri üzerinde yer alan ayrıcalıklı kullanıcı hesapları ve ayrıcalıklı hesaplar için tutulan iz kayıtları talep edilir ve hesapların ortaklaşa kullanılmasının engellendiği veya bu hesapları kullanan gerçek kişilere sorumluluk atayacak teknikler kullanıldığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.27	Parolaların güvenli ortamlarda saklanması ve bu parolaların belirli periyotlarda değiştirilmesini sağlayacak konfigürasyonlar yapılır.	Parola dokümantasyonu talep edilir ve parolaların güvenli ortamlarda saklanması ve bu parolaların belirli periyotlarda değiştirilmesini sağlayacak konfigürasyonlar yapıldığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.28	Parolaların tahmin edilmesi zor ve günün teknolojisine uygun uzunluk ve zorlukta olacak şekilde sıklıkla değiştirilmesi sağlanır.	Parola dokümantasyonu talep edilir ve parolaların tahmin edilmesi zor ve günün teknolojisine uygun uzunluk ve zorlukta olacak şekilde sıklıkla değiştirilmesi sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.29	Sistemsel sebeplerle uygulama hesaplarına yönelik iz kayıtlarının oluşturulamaması veya takip edilememesi durumunda bu hesapların son kullanıcı tarafından kullanımı engellenir.	Erişim Kontrol Politikası, Ayrıcalıklı Erişim Yönetimi Prosedürü, bilgi sistemleri üzerinde yer alan ayrıcalıklı kullanıcı hesapları ve ayrıcalıklı hesaplar için tutulan iz kayıtları talep edilir ve sistemsel sebeplerle uygulama hesaplarına yönelik iz kayıtlarının oluşturulamaması veya takip edilememesi durumunda bu hesapların son kullanıcı tarafından kullanımı	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
		engellendiği belge inceleme yöntemi ile test edilir.	
MD11.30	Acil durumlara özgü yetkilendirmelerin geçici olarak yapılması ve bu yetkilendirme süresince gerçekleştirilecek işlemlerin takibine imkân verecek iz kayıtlarının tutulmasına ilişkin süreç tasarlanır.	Erişim Kontrol Politikası ve Ayrıcalıklı Erişim Yönetimi Prosedürü talep edilir ve acil durumlara özgü yetkilendirmelerin geçici olarak yapılması ve bu yetkilendirme süresince gerçekleştirilecek işlemlerin takibine imkân verecek iz kayıtlarının tutulmasına ilişkin süreç tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.31	Personelin işten ayrılması ve görev değişikliği gibi insan kaynaklarında yaşanan değişiklikler sonrasında, gecikmeksizin ilgili kullanıcı hesaplarının silinmesi, askıya alınması, kullanıcıya atanmış yetkilerin geri alınması ya da değiştirilmesi gibi işlemlerin yerine getirilmesine ilişkin süreç tasarlanır.	Erişim Kontrol Politikası ve kimlik ve erişim bilgileri talep edilir ve personelin işten ayrılması ve görev değişikliği gibi insan kaynaklarında yaşanan değişiklikler sonrasında, gecikmeksizin ilgili kullanıcı hesaplarının silinmesi, askıya alınması, kullanıcıya atanmış yetkilerin geri alınması ya da değiştirilmesi gibi işlemler yerine getirilmesine ilişkin sürecin tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.32	İnsan kaynakları değişikliklerine dayanan yetkilendirme işlemleri otomatik olarak gerçekleştirilmiyorsa, manuel değişiklik gerçekleştirme sürecinde görevler ayrılığı prensibi uygulanmasına ve değişikliği gerçekleştirmeye yetkili personelin faaliyetlerine ilişkin iz kayıtları ile insan kaynaklarındaki değişikliklerin uyumlu olup olmadığı düzenli olarak gözden geçirilmesine ilişkin süreç oluşturulur.	Erişim Kontrol Politikası ve kimlik ve erişim bilgileri talep edilir ve insan kaynakları değişikliklerine dayanan yetkilendirme işlemleri otomatik olarak gerçekleştirilmiyorsa, manuel değişiklik gerçekleştirme sürecinde görevler ayrılığı prensibi uygulanmasına ve değişikliği gerçekleştirmeye yetkili personelin faaliyetlerine ilişkin iz kayıtları ile insan kaynaklarındaki değişikliklerin uyumlu olup olmadığı düzenli olarak gözden geçirilmesine ilişkin süreç oluşturulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.33	İnsan kaynakları değişikliklerine dayanan yetkilendirme işlemleri otomatik olarak gerçekleştirilmiyorsa, manuel değişikliklerde görevler ayrılığı prensibi uygulanır.	Erişim Kontrol Politikası, Ayrıcalıklı Erişim Yönetimi Prosedürü ve kimlik ve erişim bilgileri talep edilir ve insan kaynakları değişikliklerine dayanan yetkilendirme işlemleri otomatik olarak gerçekleştirilmiyorsa, manuel değişikliklerde görevler ayrılığı prensibi uygulandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.34	Bilgi sistemleri üzerindeki kullanıcılar için benzersiz kullanıcı tanımlama kodları belirlenir ve zorunlu olmadığı müddetçe ortak veya ön tanımlı kullanıcı hesapları kullanılmaması; Ortak veya ön tanımlı kullanıcı hesaplarının kullanımının zorunlu olduğu durumlarda ise bu kullanıcı hesapları ile işlemi yapan kişiye sorumluluk atamaya yönelik ilave kontroller tesis edilmesine ilişkin süreç tasarlanır.	Erişim Kontrol Politikası, Ayrıcalıklı Erişim Yönetimi Prosedürü ve kimlik ve erişim bilgileri talep edilir ve bilgi sistemleri üzerindeki kullanıcılar için benzersiz kullanıcı tanımlama kodları belirlendiği ve zorunlu olmadığı müddetçe ortak veya ön tanımlı kullanıcı hesapları kullanılmaması; Ortak veya ön tanımlı kullanıcı hesaplarının kullanımının zorunlu olduğu durumlarda ise bu kullanıcı hesapları ile işlemi yapan kişiye sorumluluk atamaya yönelik ilave kontroller tesis edilmesine ilişkin süreç tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD11.35	Ortak veya ön tanımlı kullanıcı hesapları ile işlemi yapan kişiye sorumluluk atamaya yönelik ilave kontroller tesis edilir.	Erişim Kontrol Politikası, Ayrıcalıklı Erişim Yönetimi Prosedürü ve kimlik ve erişim bilgileri talep edilir ve ortak veya ön tanımlı kullanıcı hesapları ile işlemi yapan kişiye sorumluluk atamaya yönelik ilave kontroller tesis edildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.36	Kullanıcı parolalarının yönetiminde belirli tedbirlerin alınmasına ilişkin olarak süreç tasarlanır.	Erişim Kontrol Politikası, Ayrıcalıklı Erişim Yönetimi Prosedürü ve kimlik ve erişim bilgileri talep edilir ve kullanıcı parolalarının yönetiminde belirli tedbirlerin alınmasına ilişkin olarak süreç tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.37	Kullanıcı parolalarının yönetiminde sistem tarafından geçici olarak verilen parolaların kullanıcı tarafından sisteme ilk girişte değiştirilmesi sağlanır.	Parola dokümantasyonu talep edilir ve kullanıcı parolalarının yönetiminde sistem tarafından geçici olarak verilen parolaların kullanıcı tarafından sisteme ilk girişte değiştirilmesinin sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.38	Kullanıcıların, parolalarını belirlerken tahmin edilmesi zor, günün teknolojisine uygun uzunluk ve zorlukta parola seçimine zorlanması sağlanır.	Parola dokümantasyonu talep edilir ve kullanıcıların, parolalarını belirlerken tahmin edilmesi zor, günün teknolojisine uygun uzunluk ve zorlukta parola seçimine zorlanmasının sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.39	Kullanıcıların, sistem güvenliği ile ilgili bir kuşku oluşması halinde ve düzenli aralıklarla parolalarını değiştirmeye zorlanması sağlanır.	Parola dokümantasyonu talep edilir ve kullanıcıların, sistem güvenliği ile ilgili bir kuşku oluşması halinde ve düzenli aralıklarla parolalarını değiştirmeye zorlanmasının sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.40	Kullanıcıların eski parolalarının hatırlanması suretiyle geriye dönük olarak belirli sayıda eski parolanın kullanılmasının engellenmesi sağlanır.	Parola dokümantasyonu talep edilir ve kullanıcıların eski parolalarının hatırlanması suretiyle geriye dönük olarak belirli sayıda eski parolanın kullanılmasının engellenmesinin sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.41	Kullanıcı hesaplarına yönelik olarak kilitli hesaplar, devre dışı bırakılmış hesaplar, parola geçerlilik süresini aşan hesaplar ve parola son kullanma süresi hiçbir zaman dolmayacak şekilde ayarlanmış hesaplar için otomatik olarak rapor üreten yöntemler kullanılır ve bu raporları gerekli önlemleri alması için ilgili sistem yöneticisine iletilmesine ilişkin süreç tasarlanır.	Erişim Kontrol Politikası, Ayrıcalıklı Erişim Yönetimi Prosedürü ve kimlik ve erişim bilgileri talep edilir ve kullanıcı hesaplarına yönelik olarak kilitli hesaplar, devre dışı bırakılmış hesaplar, parola geçerlilik süresini aşan hesaplar ve parola son kullanma süresi hiçbir zaman dolmayacak şekilde ayarlanmış hesaplar için otomatik olarak rapor üreten yöntemler kullanıldığı ve bu raporları gerekli önlemleri alması için ilgili sistem yöneticisine iletilmesine ilişkin süreç tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD11.42	Uygulama, veritabanı, ağ güvenliği bileşenleri ve sistemlerde kullanıcı hesaplarına yönelik olarak İncelenen kilitli hesaplar, devre dışı bırakılmış hesaplar, parola geçerlilik süresini aşan hesaplar ve parola son kullanma süresi hiçbir zaman dolmayacak şekilde	Kullanıcı hesapları dokümantasyonu talep edilir ve uygulama, veritabanı, ağ güvenliği bileşenleri ve sistemlerde kullanıcı hesaplarına yönelik olarak İncelenen kilitli hesaplar, devre dışı bırakılmış hesaplar, parola geçerlilik süresini aşan hesaplar ve parola son kullanma süresi hiçbir zaman	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
	ayarlanmış hesaplar için otomatik olarak rapor üretilir.	dolmayacak şekilde ayarlanmış hesaplar için otomatik olarak rapor üretildiği belge inceleme yöntemi ile test edilir.	
MD11.43	Zorunlu bir iş gereksinimi olmadıkça ve bilgi güvenliği sorumlusu tarafından onaylanmadıkça personelin ya da dış hizmet sağlayıcıların yerel yönetici haklarına sahip olması engellenmesine ilişkin süreç tasarlanır.	Erişim Kontrol Politikası, Ayrıcalıklı Erişim Yönetimi Prosedürü, bilgi sistemleri üzerinde yer alan kullanıcı listeleri ve kimlik ve erişim bilgileri talep edilir ve zorunlu bir iş gereksinimi olmadıkça ve bilgi güvenliği sorumlusu tarafından onaylanmadıkça personelin ya da dış hizmet sağlayıcıların yerel yönetici haklarına sahip olması engellenmesine ilişkin sürecin tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

4.7.4. İz kayıtlarının oluşturulması ve takibi

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD13.01	Bilgi sistemlerinin ve faaliyetlerinin boyutu ve karmaşıklığıyla orantılı olacak şekilde bilgi sistemleri dâhilinde gerçekleşen işlem ve olaylara ilişkin etkin bir iz kayıt mekanizması tesis edilir.	Log Yönetimi Prosedürü ve bilgi sistemlerine ait iz kayıtları talep edilir ve bilgi sistemlerinin ve faaliyetlerinin boyutu ve karmaşıklığıyla orantılı olacak şekilde bilgi sistemleri dâhilinde gerçekleşen işlem ve olaylara ilişkin etkin bir iz kayıt mekanizması tesis edildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD13.02	Tesis edilecek iz kayıt mekanizması, yaşanan bilgi güvenliği olaylarının sonradan incelenmesine ve bunlar hakkında güvenilir delillerin elde edilmesine imkân tanıyacak nitelikte tasarlanır.	Log Yönetimi Prosedürü ve bilgi sistemlerine ait iz kayıtları talep edilir ve tesis edilen iz kayıt mekanizmasının, yaşanan bilgi güvenliği olaylarının sonradan incelenmesine ve bunlar hakkında güvenilir delillerin elde edilmesine imkân tanıyacak nitelikte tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD13.03	Bilgi sistemleri dâhilinde gerçekleşen ve iş faaliyetlerine ait kayıtlarda değişikliğe sebep olan işlemler ile hassas ya da sır kapsamındaki verilere erişilmesine veya bunların sorgulanmasına, görüntülenmesine, kopyalanmasına, değiştirilmesine yönelik işlemler ve kritik bilgi varlıklarına yönelik erişim yetkilerinin verilmesine, değiştirilmesine ve geri alınmasına yönelik aktiviteler ile bu varlıklara yönelik yetkisiz erişim teşebbüslerine ilişkin iz kayıtları asgari beş yıl boyunca saklanmasına yönelik süreç oluşturulur.	Log Yönetimi Prosedürü ve bilgi sistemlerine ait iz kayıtları talep edilir ve bilgi sistemleri dâhilinde gerçekleşen ve iş faaliyetlerine ait kayıtlarda değişikliğe sebep olan işlemler ile hassas ya da sır kapsamındaki verilere erişilmesine veya bunların sorgulanmasına, görüntülenmesine, kopyalanmasına, değiştirilmesine yönelik işlemler ve kritik bilgi varlıklarına yönelik erişim yetkilerinin verilmesine, değiştirilmesine ve geri alınmasına yönelik aktiviteler ile bu varlıklara yönelik yetkisiz erişim teşebbüslerine ilişkin iz kayıtlarının asgari beş yıl boyunca saklanmasına yönelik süreç oluşturulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD13.04	İz kayıtları güvenilir ortamlarda yedeklenir ve ihtiyaç duyulması halinde makul bir sürede bu yedeklerden geri dönüş sağlanarak inceleme yapılmasına imkân verecek şekilde saklanmasına ilişkin süreç oluşturulur.	Log Yönetimi Prosedürü ve Backup Prosedürü talep edilir ve iz kayıtlarının güvenilir ortamlarda yedeklendiği ve ihtiyaç duyulması halinde makul bir sürede bu yedeklerden geri dönüş sağlanarak inceleme yapılmasına imkân verecek şekilde saklanmasına ilişkin süreç oluşturulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD13.05	İz kayıtlarının bütünlüğünün bozulmasının önlenmesine ve herhangi bir bozulma durumunda bunun tespit edilebilmesine ilişkin teknikler kullanılmasına ilişkin süreç tasarlanır.	Log Yönetimi Prosedürü talep edilir ve iz kayıtlarının bütünlüğünün bozulmasının önlenmesine ve herhangi bir bozulma durumunda bunun tespit edilebilmesine ilişkin teknikler kullanılmasına ilişkin süreç tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD13.06	İz kayıtlarına, bilmesi gerektiği kadar prensibine uygun olarak sadece erişim yetkisi verilen kişilerin ulaşabilmesi ve kayıt sisteminin her türlü yetkisiz değişiklik ve müdahalelere karşı korunmasına ilişkin süreç tasarlanır.	Log Yönetimi Prosedürü talep edilir ve iz kayıtlarına, bilmesi gerektiği kadar prensibine uygun olarak sadece erişim yetkisi verilen kişilerin ulaşabilmesi ve kayıt sisteminin her türlü yetkisiz değişiklik ve müdahalelere karşı korunmasına ilişkin süreç tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD13.07	Kullanıcıların kendi faaliyetlerine ilişkin iz kayıtlarına müdahalesi engellenmesine ve iz	Log Yönetimi Prosedürü talep edilir ve kullanıcıların kendi faaliyetlerine ilişkin iz	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
	kayıt sisteminin durdurulmasını önlemeye veya durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılmasına ilişkin süreç tasarlanır.	kayıtlarına müdahalesi engellenmesine ve iz kayıt sisteminin durdurulmasını önlemeye veya durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılmasına ilişkin süreç tasarlandığı belge inceleme yöntemi ile test edilir.	
MD13.08	İz kayıt sisteminin durdurulmasını önlemeye veya durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılmasına ilişkin süreç tasarlanır.	Log Yönetimi Prosedürü talep edilir ve iz kayıt sisteminin durdurulmasını önlemeye veya durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılmasına ilişkin süreç tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

4.7.5. Ağ güvenliği

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD14.01	Gerek kurumsal ağ gerek dış ağlardan gelebilecek tehditler için gerekli ağ kontrol güvenlik sistemlerinin ve güvenlik önlemlerinin tesis edilmesine güvenlik katmanlarının aşılması halinde diğer güvenlik katmanlarının devreye girmesine ilişkin süreç tasarlanır.	Şirket İçi Ağ Yönetimi Prosedürü, Bilgi Güvenliği ve Veri Gizliliği Politikası, Ağ Topolojileri talep edilir ve gerek kurumsal ağ gerek dış ağlardan gelebilecek tehditler için gerekli ağ kontrol güvenlik sistemlerinin ve güvenlik önlemlerinin tesis edilmesine güvenlik katmanlarının aşılması halinde diğer güvenlik katmanlarının devreye girmesine ilişkin süreç tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD14.02	Şirket ağ topolojisi katmanlı güvenlik mimarisi göz önünde bulundurularak dizayn edilir.	Şirket İçi Ağ Yönetimi Prosedürü, Bilgi Güvenliği ve Veri Gizliliği Politikası, Ağ Topolojileri talep edilir ve ağ dokümantasyonu talep edilir ve Şirket ağ topolojisinin katmanlı güvenlik mimarisi göz önünde bulundurularak dizayn edildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD14.03	Dış ağ ve iç ağ arasındaki trafiğin kontrolü için, gereken şekilde konfigürasyonu yapılmış, sürekli gözetim altında tutulan güvenlik duvarı çözümleri ile saldırıların tespiti ve önlenmesi için günün teknolojisine uygun sistemler kullanılır.	Şirket İçi Ağ Yönetimi Prosedürü, Bilgi Güvenliği ve Veri Gizliliği Politikası, Ağ Topolojileri talep edilir ve dış ağ ve iç ağ arasındaki trafiğin kontrolü için, gereken şekilde konfigürasyonu yapılmış, sürekli gözetim altında tutulan güvenlik duvarı çözümleri ile saldırıların tespiti ve önlenmesi için günün teknolojisine uygun sistemler kullanıldığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD14.04	Güvenlik duvarları üzerindeki konfigürasyonların uygun şekilde yapıldığı kontrol edilir.	Şirket İçi Ağ Yönetimi Prosedürü, Bilgi Güvenliği ve Veri Gizliliği Politikası, Ağ Topolojileri, Güvenlik duvarı üzerinde yer alan kurallar ve sistemler talep edilir ve güvenlik duvarları üzerindeki konfigürasyonların uygun şekilde yapıldığının kontrol edildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD14.05	Şirket iç ağındaki servislerin yalnızca kendilerine gereken ağ segmentlerine ulaşmasını sağlayacak şekilde Şirket iç ağı alt bölümlere ayrılır.	Şirket İçi Ağ Yönetimi Prosedürü, Bilgi Güvenliği ve Veri Gizliliği Politikası, Ağ Topolojileri, Güvenlik duvarı üzerinde yer alan kurallar talep edilir ve Şirket iç ağındaki servislerin yalnızca kendilerine gereken ağ segmentlerine ulaşmasını sağlayacak şekilde Şirket iç ağı alt bölümlere ayrıldığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD14.06	Farklı ağ segmentleri arasında veri trafiğinin güvenliği sağlanır.	Şirket İçi Ağ Yönetimi Prosedürü, Bilgi Güvenliği ve Veri Gizliliği Politikası, Ağ Topolojileri, Güvenlik duvarı üzerinde yer alan kurallar talep edilir ve farklı ağ segmentleri arasında veri trafiğinin güvenliğinin sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD14.07	Özel iç ağdaki sistemlerle yalnızca güvenlik duvarı cihazları üzerinden iletişim kurulur.	Şirket İçi Ağ Yönetimi Prosedürü, Bilgi Güvenliği ve Veri Gizliliği Politikası, Ağ Topolojileri, Güvenlik duvarı üzerinde yer alan kurallar ve sistemler talep edilir ve özel iç ağdaki sistemlerle yalnızca güvenlik duvarı cihazları üzerinden iletişim kurulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

4.7.6. Güvenlik Konfigürasyonu Yönetimi

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD15.01	Masaüstü, dizüstü, mobil cihazlar ve sunucular üzerindeki işletim sistemi, veritabanları ve uygulamalar ile güvenlik duvarları, yönlendirici ve anahtarlama cihazları gibi ağ cihazları için sıkılaştırılmış ve test edilmiş güvenli standart konfigürasyon bilgileri oluşturulur.	Konfigürasyon Yönetim Prosedürü talep edilir ve masaüstü, dizüstü, mobil cihazlar ve sunucular üzerindeki işletim sistemi, veritabanları ve uygulamalar ile güvenlik duvarları, yönlendirici ve anahtarlama cihazları gibi ağ cihazları için sıkılaştırılmış ve test edilmiş güvenli standart konfigürasyon bilgileri oluşturulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD15.02	Standart konfigürasyon bilgilerinin, standart konfigürasyondan sapmalar veya standart konfigürasyondaki güncellemeler değişiklik yönetiminin bir parçası olarak kayıt altına alınmasına ve onay mekanizmasına tabi tutulmasına ilişkin süreç tasarlanır.	Konfigürasyon Yönetim Prosedürü talep edilir ve standart konfigürasyon bilgilerinin, standart konfigürasyondan sapmalar veya standart konfigürasyondaki güncellemeler değişiklik yönetiminin bir parçası olarak kayıt altına alınmasına ve onay mekanizmasına tabi tutulmasına ilişkin süreç tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD15.03	Masaüstü, dizüstü, iş istasyonu ve sunucular üzerindeki işletim sistemleri için bu işletim sistemlerinin tipi, versiyon numarası, yama seviyesi ve üzerinde yüklü olan veritabanları ve uygulamaların listesini gösterecek şekilde bir yazılım envanteri oluşturulmasına ilişkin süreç tasarlanır.	Konfigürasyon Yönetim Prosedürü, Yazılım Envanteri ve Donanım Envanteri listeleri talep edilir ve masaüstü, dizüstü, iş istasyonu ve sunucular üzerindeki işletim sistemleri için bu işletim sistemlerinin tipi, versiyon numarası, yama seviyesi ve üzerinde yüklü olan veritabanları ve uygulamaların listesini gösterecek şekilde bir yazılım envanteri oluşturulmasına ilişkin süreç tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD15.04	Masaüstü, dizüstü ve iş istasyonu makineleri ile sunucular, bu makinelere taşınabilir bir medya veya harici cihaz takıldığında otomatik olarak içeriği oynatmayacak şekilde yapılandırılır ve zararlı yazılım engelleme araçları bu tür cihazlar takıldığında otomatik olarak bu cihazları tarayacak şekilde ayarlanır.	Konfigürasyon Yönetim Prosedürü talep edilir ve masaüstü, dizüstü ve iş istasyonu makineleri ile sunucuların, bu makinelere taşınabilir bir medya veya harici cihaz takıldığında otomatik olarak içeriği oynatmayacak şekilde yapılandırıldığı ve zararlı yazılım engelleme araçlarının bu tür cihazlar takıldığında otomatik olarak bu cihazları tarayacak şekilde ayarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD15.05	Ağa bağlı her bir sistem üzerindeki portların, protokol ve servislerin sadece gerekliliği onaylanmış iş ihtiyaçlarına istinaden açık ve çalışıyor olması sağlanır. Bu doğrultuda, güvenli bir baz konfigürasyonu temel alınarak önemli sunucu ve sistemler için düzenli olarak port taraması gerçekleştirilir ve güvenli baz konfigürasyonda bulunmadığı halde açık durumda olan portların kapatılması sağlanır.	Konfigürasyon Yönetim Prosedürü talep edilir ve güvenli bir baz konfigürasyonu temel alınarak önemli sunucu ve sistemler için düzenli olarak port taraması gerçekleştirildiği, güvenli baz konfigürasyonda bulunmadığı halde açık durumda olan portların kapatıldığı belge inceleme yöntemiyle test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

4.7.7. Güvenlik açıkları ve yama yönetimi

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD16.01	İş faaliyetlerini kesintiye uğratacak veya önemli ölçüde olumsuz etkileyecek durumların ortaya çıkma olasılığını azaltmak için sistem, yazılım ve cihazlardaki güvenlik açıklarını hızlı ve etkin bir şekilde ele alacak bir güvenlik açıkları ve yama yönetimi süreci tesis edilir.	Yama Yönetimi Prosedürü, Güvenlik İhlali Prosedürü ve yama dokümantasyonu talep edilir ve iş faaliyetlerini kesintiye uğratacak veya önemli ölçüde olumsuz etkileyecek durumların ortaya çıkma olasılığını azaltmak için sistem, yazılım ve cihazlardaki güvenlik açıklarını hızlı ve etkin bir şekilde ele alacak bir güvenlik açıkları ve yama yönetimi süreci tesis edildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD16.02	Uygulanacak yamaların güvenilir bir kaynaktan gelmesini sağlayacak ve bunu doğrulayacak teknikler kullanılır.	Yama Yönetimi Prosedürü, Güvenlik İhlali Prosedürü ve yama dokümantasyonu talep edilir ve uygulanacak yamaların güvenilir bir kaynaktan gelmesini sağlayacak ve bunu doğrulayacak teknikler kullanıldığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD16.03	Yamaların yanlış uygulanması ya da uygulanması sırasında sorun çıkması halinde sorunun ne şekilde çözüme kavuşturulacağına dair metotlar tanımlanır.	Yama Yönetimi Prosedürü, Güvenlik İhlali Prosedürü ve yama dokümantasyonu talep edilir ve yamaların yanlış uygulanması ya da uygulanması sırasında sorun çıkması halinde sorunun ne şekilde çözüme kavuşturulacağına dair metotlar tanımlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD16.04	Sağlayıcı veya üretici desteği biten sistem, yazılım ve cihazlar artık yamalanamadığında, bunlar için yüklenebilen en son güncellemelerin günün şartlarına göre artık güvenli olmamasının ve telafi edici kontroller ile de makul seviyede bir güvenlik sağlanamamasının tespit edilme süreci oluşturulur.	Yama Yönetimi Prosedürü, Güvenlik İhlali Prosedürü ve yama dokümantasyonu talep edilir ve tedarikçi veya üretici desteği biten sistem, yazılım ve cihazlar artık yamalanamadığında, bunlar için yüklenebilen en son güncellemelerin günün şartlarına göre artık güvenli olmamasının ve telafi edici kontroller ile de makul seviyede bir güvenlik sağlanamamasının tespit edilme süreci oluşturulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD16.05	Ağa bağlı olan sistem ve cihazlarına yönelik olarak otomatik güvenlik açığı tarama araçları kullanılır.	Yama Yönetimi Prosedürü, Güvenlik İhlali Prosedürü ve yama dokümantasyonu talep edilir ve ağa bağlı olan sistem ve cihazlarına yönelik olarak otomatik güvenlik açığı tarama araçları kullanıldığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD16.06	Güvenlik tarama araçları, ağa bağlı olan tüm sistem ve cihazlarda uygulanır. Gerçekleştirilen güvenlik taramaları sonuçları belirli periyotlarla kontrol edilir.	Yama Yönetimi Prosedürü, Güvenlik İhlali Prosedürü ve yama dokümantasyonu talep edilir ve güvenlik tarama araçları, ağa bağlı olan tüm sistem ve cihazlarda uygulanır. Gerçekleştirilen güvenlik taramaları sonuçları belirli periyotlarla kontrol edildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD16.07	Tespit edilen her bir güvenlik açığıyla ilgili olarak bilgi güvenliği sorumlusuna ve açığın tespit edildiği sistemden sorumlu sistem yöneticisine en kritik güvenlik açıklarını öncelikli olarak listeleyecek şekilde raporlama yapılma süreci tasarlanır.	Yama Yönetimi Prosedürü, Güvenlik İhlali Prosedürü ve yama dokümantasyonu talep edilir ve tespit edilen her bir güvenlik açığıyla ilgili olarak bilgi güvenliği sorumlusuna ve açığın tespit edildiği sistemden sorumlu sistem yöneticisine en kritik güvenlik açıklarını öncelikli olarak listeleyecek şekilde raporlama yapılma	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
		sürecinin tasarlandığı belge inceleme yöntemi ile test edilir.	
MD16.08	Masaüstü, dizüstü ile sunucuları, sürekli bir şekilde izlenerek üzerindeki zararlı yazılımları tespit edecek etkin araçlar kullanılır.	Antivirüs yönetimi dokümantasyonu talep edilir ve masaüstü, dizüstü ile sunucularını, sürekli bir şekilde izleyerek üzerindeki zararlı yazılımları tespit edecek etkin araçlar kullanıldığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

4.7.8. Fiziksel güvenlik kontrolleri

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD17.01	Kritik bilgi sistemleri, uygun güvenlik engelleri ve giriş kontrollerine sahip veri merkezleri, sistem odaları, ağ ekipman odaları gibi güvenli alanlarda barındırılır.	Sistem odası ziyaret edilir ve kritik bilgi sistemleri, uygun güvenlik engelleri ve giriş kontrollerine sahip veri merkezleri, sistem odaları, ağ ekipman odaları gibi güvenli alanlarda barındırıldığı gözlem yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD17.02	Veri merkezlerinin yerleri seçilirken doğal riskler ve çevresel tehditler göz önünde bulundurulur. Veri merkezleri olası felaket ve risklere karşı güvenilirliği yüksek lokasyonlarda barındırılır.	Sistem odası ziyaret edilir ve veri merkezlerinin yerleri seçilirken doğal riskler ve çevresel tehditler göz önünde bulundurulduğu, veri merkezlerinin olası felaket ve risklere karşı güvenilirliği yüksek lokasyonlarda barındırıldığı gözlem yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD17.03	Bina veya binaların, barındırdıkları bilgi işlem tesislerinin varlığını açık edecek işaretler ve bilgiler bulundurmaması sağlanır.	Sistem odası ziyaret edilir ve bina veya binaların, barındırdıkları bilgi işlem tesislerinin varlığını açık edecek işaretler ve bilgiler bulundurmamasının sağlandığı gözlem yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD17.04	Veri merkezlerinin çalışmasını olumsuz etkileyebilecek elektrik kesintisi, yangın, duman, sıcaklık, su, toz ve nem gibi çevresel koşulları izleyecek sistemlerin ve sensörlerin aktif olarak kullanılmasına ilişkin süreç tasarlanır.	Fiziksel Erişim Prosedürü talep edilir ve veri merkezlerinin çalışmasını olumsuz etkileyebilecek elektrik kesintisi, yangın, duman, sıcaklık, su, toz ve nem gibi çevresel koşulları izleyecek sistemlerin ve sensörlerin aktif olarak kullanılmasına ilişkin sürecin tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD17.05	İlgili sistem ve sensörler düzenli olarak gözden geçirilip, sistemlerin ve sensörlerin bakımları düzenli olarak yapılır.	Sistem odası bakım dokümantasyonu talep edilir ve ilgili sistem ve sensörlerin düzenli olarak gözden geçirilip, sistemlerin ve sensörlerin bakımlarının düzenli olarak yapıldığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD17.06	Yetkilendirilen personel dışında kalan herhangi bir personel, ziyaretçi, dış hizmet sağlayıcı ya da yüklenici firma personelinin veri merkezlerine ve kritik bilgi sistemlerine erişimleri onay mekanizmasına tabi tutulur, veri merkezindeki çalışmaları boyunca faaliyetleri yakından izlenir ve mutlaka kendilerine refakat edilir. Veri merkezi ziyaretlerine ilişkin süreç tasarlanır.	Fiziksel Erişim Prosedürü talep edilir ve yetkilendirilen personel dışında kalan herhangi bir personel, ziyaretçi, dış hizmet sağlayıcı ya da yüklenici firma personelinin veri merkezlerine ve kritik bilgi sistemlerine erişimlerinin onay mekanizmasına tabi tutulduğu, veri merkezindeki çalışmaları boyunca faaliyetlerinin yakından izlendiği ve mutlaka kendilerine refakat edildiği veri merkezi ziyaretlerine ilişkin sürecin tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD17.07	Veri merkezlerine ve sistem odalarına yapılan erişim talepleri ve onayları ile bu erişimler kapsamında gerçekleştirilen işlemler ve giriş çıkışlar için iz kaydı tutulur.	Sistem odası erişim yetki ve iz kayıt dokümantasyonu talep edilir ve veri merkezlerine ve sistem odalarına yapılan erişim talepleri ve onayları ile bu erişimler kapsamında gerçekleştirilen işlemler ve giriş çıkışlar için iz kaydı tutulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD17.08	Veri merkezi için kör nokta barındırmayacak ve en az bir yıl süreyle kayıt saklayacak şekilde kamera kayıt sistemleri kullanılır.	Sistem odası ziyaret edilir ve kör nokta barındırmayacak ve en az bir yıl süreyle kayıt saklayacak şekilde kamera kayıt	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
		sistemleri kullanıldığı gözlem yöntemi ile test edilir.	
MD17.9	Risk teşkil edebilecek durumların önüne geçilmek amacıyla kamera kayıtları düzenli olarak kontrol edilir.	Fiziksel Erişim Prosedürü talep edilir ve risk teşkil edebilecek durumların önüne geçilmek amacıyla kamera kayıtları düzenli olarak kontrol edildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD17.10	Kamera kayıt sistemleri tarafından kaydedilen görüntülerin farklı bir konumda yedeklenmesi sağlanır.	Fiziksel Erişim Prosedürü talep edilir ve kamera kayıt sistemleri tarafından kaydedilen görüntülerin farklı bir konumda yedeklenmesinin sağlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD17.11	Kamera kayıt sistemi tarafından kaydedilen görüntülerin yedekleri farklı bir konumda bulundurulur. Kamera kayıt yedeklerine ihtiyaç anında erişilebilir.	Fiziksel Erişim Prosedürü ve kamera kayıt sistemi tarafından kaydedilen görüntülerin yedeklerinin farklı bir konumda bulundurulduğu ve kamera kayıt yedeklerine ihtiyaç anında erişilebildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

4.7.9. Siber olay yönetimi, sızma testi ve siber istihbarat paylaşımı

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD18.01	Siber olay yönetimi ve siber olaylara müdahale süreci oluşturulur.	Siber Güvenlik Prosedürü ve Bilgi Güvenliği Vaka Yönetimi Prosedürü talep edilir ve siber olay yönetimi ve siber olaylara müdahale sürecinin oluşturulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD18.02	Yeterli teknik ve operasyonel becerilere sahip bir Kurumsal SOME kurulur.	Siber Güvenlik Prosedürü ve Bilgi Güvenliği Vaka Yönetimi Prosedürü talep edilir ve yeterli teknik ve operasyonel becerilere sahip bir Kurumsal SOME kurulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD18.03	Siber olayların müşterilere ve ilgili yönetim birimlerine raporlanması tanımlanır.	Siber Güvenlik Prosedürü ve Bilgi Güvenliği Vaka Yönetimi Prosedürü talep edilir ve siber olayların müşterilere ve ilgili yönetim birimlerine raporlanmasının tanımlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD18.04	Kurumsal SOME'nin sorumlulukları siber olay öncesinde, bilgi işlem varlıkları üzerinde rutin sızma testi çalışması yapmayı veya yaptırmayı, kayıt yönetimi sistemi arayüzünden rutin olarak iz kayıtlarını takip etmeyi, iz kayıtları arasında anlamlı sonuçlar doğurabilecek korelasyonları kontrol etmeyi ve kurum içi bilgi güvenliği farkındalık çalışmalarını yürütmeyi; siber olay esnasında ise, BS fonksiyonunun yapacağı müdahaleyi yönetmeyi ve BS fonksiyonunda görevli ilgili personeli koordine etmeyi kapsar.	Siber Güvenlik Prosedürü ve Bilgi Güvenliği Vaka Yönetimi Prosedürü talep edilir ve kurumsal SOME'nin sorumluluklarının siber olay öncesinde, bilgi işlem varlıkları üzerinde rutin sızma testi çalışması yapmayı veya yaptırmayı, kayıt yönetimi sistemi arayüzünden rutin olarak iz kayıtlarını takip etmeyi, iz kayıtları arasında anlamlı sonuçlar doğurabilecek korelasyonları kontrol etmeyi ve kurum içi bilgi güvenliği farkındalık çalışmalarını yürütmeyi; siber olay esnasında ise, BS fonksiyonunun yapacağı müdahaleyi yönetmeyi ve BS fonksiyonunda görevli ilgili personeli koordine etmeyi kapsadığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD18.05	Siber olayların önem derecelerine uygun olacak şekilde ele alınmasını sağlamak üzere, siber olayların önemlilik sınıflandırmasına yönelik kriterler yazılı hale getirilir.	Siber Güvenlik Prosedürü ve Bilgi Güvenliği Vaka Yönetimi Prosedürü talep edilir ve siber olayların önem derecelerine uygun olacak şekilde ele alınmasını sağlamak üzere, siber olayların önemlilik sınıflandırmasına yönelik kriterler yazılı hale getirildiği belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD18.06	Gerçekleşen her bir siber olayın bu kriterlere göre belirlenen önem düzeyiyle orantılı olan bir zaman zarfında ele alınması ve çözüme kavuşturulmasına yönelik prosedürler ile müdahale planları oluşturulur.	Siber Güvenlik Prosedürü, Bilgi Güvenliği Vaka Yönetimi Prosedürü ve müdahale planları talep edilir ve gerçekleşen her bir siber olayın bu kriterlere göre belirlenen önem düzeyiyle orantılı olan bir zaman zarfında ele alınması ve çözüme kavuşturulmasına yönelik prosedürler ile müdahale planları oluşturulduğu belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD18.07	Oluşturulan müdahale planlarında öngörülen senaryolar için, faaliyetlerin güvenilir bir şekilde sürdürülmesini	Siber Güvenlik Prosedürü, Bilgi Güvenliği Vaka Yönetimi Prosedürü ve müdahale planları talep edilir ve oluşturulan müdahale planlarında öngörülen	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
	sağlayan hızlı, etkili ve düzenli bir tepki süreci tesis edilir.	senaryolar için, faaliyetlerin güvenilir bir şekilde sürdürülmesini sağlayan hızlı, etkili ve düzenli bir tepki süreci tesis edildiği belge inceleme yöntemi ile test edilir.	
MD18.08	Müdahale planları kapsamında, bilgi sistemlerine ilişkin olayın kaynağını hızlı bir şekilde bulmayı sağlama, yetkili birimlere ulaşmayı sağlama, olayın potansiyel boyutunu, etkisini, hasarı ve etkilenen müşterileri tespit etme ve olayı çözüme kavuşturma süreçleri ele alınır.	Siber Güvenlik Prosedürü, Bilgi Güvenliği Vaka Yönetimi Prosedürü ve müdahale planları talep edilir ve müdahale planları kapsamında, bilgi sistemlerine ilişkin olayın kaynağını hızlı bir şekilde bulmayı sağlama, yetkili birimlere ulaşmayı sağlama, olayın potansiyel boyutunu, etkisini, hasarı ve etkilenen müşterileri tespit etme ve olayı çözüme kavuşturma süreçlerinin ele alındığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD18.09	Yaşanan bir siber olayın büyüyerek bir krize dönüşmesi, hassas verilerin ya da kişisel verilerin sızması ya da ifşası ile sonuçlanması, Bilgi Sistemleri Süreklilik Planının ya da ikincil merkezin devreye alınması gibi hallerde derhal Sektörel SOME'yi bilgilendirme süreci tasarlanır.	Siber Güvenlik Prosedürü ve Bilgi Güvenliği Vaka Yönetimi Prosedürü talep edilir ve yaşanan bir siber olayın büyüyerek bir krize dönüşmesi, hassas verilerin ya da kişisel verilerin sızması ya da ifşası ile sonuçlanması, Bilgi Sistemleri Süreklilik Planının ya da ikincil merkezin devreye alınması gibi hallerde derhal Sektörel SOME'yi bilgilendirme süreci tasarlandığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD18.10	Sunulan hizmetlerin tasarımı, geliştirilmesi, uygulanması veya yürütülmesinde görevi bulunmayan bağımsız ekiplere yılda en az bir defa sızma testi yaptırılır.	Sızma testi raporu talep edilir ve sunulan hizmetlerin tasarımı, geliştirilmesi, uygulanması veya yürütülmesinde görevi bulunmayan bağımsız ekiplere yılda en az bir defa sızma testi yaptırıldığı belge inceleme yöntemi ile test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

4.7.10. Değişiklik yönetimi

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD24.01	Meydana gelen değişiklikler sebebiyle gerçekleşebilecek hata ve sorunların sayısını ve etkisini en aza indirecek, değişikliklerin etkili, hızlı ve kontrollü bir şekilde gerçekleştirilmesini ve değişiklikler sırasında yapılan işlemlerin değişiklik sonrasında da denetlenebilir olmasını sağlayacak etkin bir değişiklik yönetimi süreci oluşturulur.	Değişiklik Yönetimi Prosedürü talep edilir ve belge inceleme yöntemi ile meydana gelen değişiklikler sebebiyle gerçekleşebilecek hata ve sorunların sayısını ve etkisini en aza indirecek, değişikliklerin etkili, hızlı ve kontrollü bir şekilde gerçekleştirilmesini ve değişiklikler sırasında yapılan işlemlerin değişiklik sonrasında da denetlenebilir olmasını sağlayacak etkin bir değişiklik yönetimi süreci oluşturulduğu test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD24.02	Değişiklik yönetimi süreci kapsamında, ağ altyapısı, donanım, işletim sistemleri, yazılım gibi bilgi sistemleri öğeleri ile sistem, servis, uygulama konfigürasyonu ve parametrelerinde yapılacak her türlü değişiklik bir değişiklik talep yönetimi süreci çerçevesinde başlatılır.	Değişiklik Yönetimi Prosedürü talep edilir ve belge inceleme yöntemi ile değişiklik yönetimi süreci kapsamında, ağ altyapısı, donanım, işletim sistemleri, yazılım gibi bilgi sistemleri öğeleri ile sistem, servis, uygulama konfigürasyonu ve parametrelerinde yapılacak her türlü değişiklik bir değişiklik talep yönetimi süreci çerçevesinde başlatıldığı test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD24.03	Değişiklik talebinin geçerli bir iş ihtiyacına dayalı olması sağlanır.	Gerçekleşme sıklığına göre belirlenen örneklem sayısı kadar seçilen değişiklik dokümanları talep edilir ve belge inceleme yöntemi ile değişiklik talebinin geçerli bir iş ihtiyacına dayalı olduğu test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD24.04	Görevler ayrılığı prensibine uygun olarak yetkilendirilmesi, test edilmesi, gerçekleştirilmesi, kaydedilmesi ve dokümantasyonu sağlanmaktadır.	Değişiklik dokümanları talep edilir ve belge inceleme yöntemi ile görevler ayrılığı prensibine uygun olarak yetkilendirilmesi, test edilmesi, gerçekleştirilmesi, kaydedilmesi ve dokümantasyonu sağlandığı test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD24.05	Değişiklik yönetimi sürecine değişikliklerin kimlik doğrulaması uygun tekniklerle gerçekleştirilmiş yetkili kullanıcılar tarafından yapılması dâhil edilir.	Değişiklik Yönetimi Prosedürü talep edilir ve belge inceleme yöntemi ile değişiklik yönetimi sürecine değişikliklerin kimlik doğrulaması uygun tekniklerle gerçekleştirilmiş yetkili kullanıcılar tarafından yapılmasının dâhil edildiği test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD24.06	Değişiklik yönetimi süreci, asgari olarak talep yönetimi, risk değerlendirmesi, yetkili merci onayı, yapılan değişikliğin uygulanması, test edilmesi ve doğrulanması adımlarını içerir.	Değişiklik Yönetimi Prosedürü talep edilir ve belge inceleme yöntemi ile değişiklik yönetimi sürecinin, asgari olarak talep yönetimi, risk değerlendirmesi, yetkili merci onayı, yapılan değişikliğin uygulanması, test edilmesi ve doğrulanması adımlarını içerdiği test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD24.07	Değişikliklere ilişkin bir risk ve etki analizi yapılması, gelen taleplerin sınıflandırılması ve önceliklendirilmesi sağlanır.	Değişiklik dokümanları talep edilir ve belge inceleme yöntemi ile değişikliklere ilişkin bir risk ve etki analizi yapılması, gelen taleplerin sınıflandırılması ve önceliklendirilmesi sağlandığı test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD24.08	Değişiklikler uygun test planları doğrultusunda test edilir ve değiştirilen modüllerin üretim ortamına aktarılmasından önce kullanıcı ve ilgili birimlerin onayları alınır.	Değişiklik dokümanları talep edilir ve belge inceleme yöntemi ile değişikliklerin uygun test planları doğrultusunda test edildiği ve değiştirilen modüllerin üretim ortamına aktarılmasından önce kullanıcı ve ilgili birimlerin onaylarının alındığı test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD24.09	Acil durum değişiklikleri kapsamında değişiklik yönetim süreci içerisinde tanımlanan	Değişiklik Yönetimi Prosedürü talep edilir ve belge inceleme yöntemi ile acil durum değişiklikleri kapsamında değişiklik yönetim	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
	istisnaların değişiklik sonrasında mümkün olan en kısa sürede tamamlanması tanımlanır.	süreci içerisinde tanımlanan istisnaların değişiklik sonrasında mümkün olan en kısa sürede tamamlanması tanımlandığı test edilir.	

4.7.11. Erişilebilirlik Yönetimi ve Yedekleme

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD27.01	Herhangi bir donanım veya yazılım bileşeninin beklendiği gibi çalışmadığı durumlarda, sistemin veya faaliyetlerin önemli bir bölümünün çalışamaz hale gelmesini önlemek adına kritik donanım ve sistemler için yedekli çalışma ya da hazırda bekleme düzenleri kurulur.	Backup Prosedürü ve ilgili dokümantasyon talep edilir ve belge inceleme yöntemi ile herhangi bir donanım veya yazılım bileşeninin beklendiği gibi çalışmadığı durumlarda, sistemin veya faaliyetlerin önemli bir bölümünün çalışamaz hale gelmesini önlemek adına kritik donanım ve sistemler için yedekli çalışma ya da hazırda bekleme düzenleri kurulduğu test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD27.02	Verilerin erişilebilirliğini sağlamak adına her bir verinin erişilebilirlik gereksinimlerine uygun yedekleme düzeni tesis edilir.	Backup Prosedürü ve ilgili dokümantasyon talep edilir ve belge inceleme yöntemi ile verilerin erişilebilirliğini sağlamak adına her bir verinin erişilebilirlik gereksinimlerine uygun yedekleme düzeni tesis edildiği test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD27.03	Sistemin alınan yedeğinden geri yüklenebilmesi için, işletim sistemi, uygulama yazılımı ve veriler gibi sistemin çalışmasını sağlayan bileşenler yedekleme prosedürüne dâhil edilir.	Backup Prosedürü ve ilgili dokümantasyon talep edilir ve belge inceleme yöntemi ile sistemin alınan yedeğinden geri yüklenebilmesi için, işletim sistemi, uygulama yazılımı ve veriler gibi sistemin çalışmasını sağlayan bileşenler yedekleme prosedürüne dâhil edildiği test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD27.04	Sistem ve sistem bileşenlerinin yedekleri yedekleme planı dâhilinde alınır.	Backup Prosedürü ve ilgili dokümantasyon talep edilir ve belge inceleme yöntemi ile sistem ve sistem bileşenlerinin yedekleri yedekleme planı dâhilinde alındığı test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD27.05	Ağ ve iletişim altyapısından kaynaklanabilecek kesintilere karşı uygun alternatif iletişim kanalları oluşturulur.	Backup Prosedürü ve ilgili dokümantasyon talep edilir ve belge inceleme yöntemi ile ağ ve iletişim altyapısından kaynaklanabilecek kesintilere karşı uygun alternatif iletişim kanalları oluşturulduğu test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

4.7.12. Bilgi sistemleri sürekliliğinin sağlanması

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD28.01	Hizmetleri yürütmede kullanılan BS servislerinin sürekliliğini sağlamak üzere iş sürekliliği yönetimi ve planının bir parçası olan bilgi sistemleri süreklilik yönetimi süreci ve Yönetim Kurulu onaylı bir bilgi sistemleri süreklilik planı hazırlanır, süreç sorumlusu atanır.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı ve İletişim Planı talep edilir ve belge inceleme yöntemi ile hizmetleri yürütmede kullanılan BS servislerinin sürekliliğini sağlamak üzere iş sürekliliği yönetimi ve planının bir parçası olan bilgi sistemleri süreklilik yönetimi süreci ve Yönetim Kurulu onaylı bir bilgi sistemleri süreklilik planı hazırlandığı ve sorumlusu atandığı test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD28.02	BS Süreklilik Komitesi, insan kaynakları, iş birimleri, BS güvenlik fonksiyonu, ilgili BS birimlerinin temsilcileri ve organizasyonda bulunması durumunda hukuk birimi temsilcilerinden oluşur ve bilgi sistemleri süreklilik yönetimi süreci sorumlusu bu komiteye başkanlık eder.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı ve İletişim Planı talep edilir ve belge inceleme yöntemi ile BS Süreklilik Komitesinin, insan kaynakları, iş birimleri, BS güvenlik fonksiyonu, ilgili BS birimlerinin temsilcileri ve organizasyonda bulunması durumunda hukuk birimi temsilcilerinden oluştuğu ve bilgi sistemleri süreklilik yönetimi süreci sorumlusu bu komiteye başkanlık ettiği test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD28.03	BS Süreklilik Komitesi meydana gelen olaylarla ilgili bütün faktörleri göz önünde bulundurarak kriz durumu olduğunu ilan etmekle, bilgi sistemleri süreklilik planın devreye alınmasına karar vermekle ve diğer kurtarma, süreklilik ve müdahale ekipleriyle koordinasyonu sağlamakla yükümlüdür.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge inceleme yöntemi ile BS Süreklilik Komitesinin meydana gelen olaylarla ilgili bütün faktörleri göz önünde bulundurarak kriz durumu olduğunu ilan etmekle, bilgi sistemleri süreklilik planın devreye alınmasına karar vermekle ve diğer kurtarma, süreklilik ve müdahale ekipleriyle koordinasyonu sağlamakla yükümlü olduğu test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD28.04	Bilgi sistemleri süreklilik yönetimi sürecinin ulusal veya uluslararası bir standart ya da en iyi uygulamaları temel alır.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge inceleme yöntemi ile süreklilik yönetimi sürecinin ulusal veya uluslararası bir standart ya da en iyi uygulamaları temel aldığı test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD28.05	İş etki analizi, risk değerlendirmesi, risk yönetimi, izleme ve test faaliyetlerini içeren bir bilgi sistemleri süreklilik yönetim süreci tesis edilir.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge inceleme yöntemi ile iş etki analizi, risk değerlendirmesi, risk yönetimi, izleme ve test faaliyetlerini içeren bir bilgi sistemleri süreklilik yönetim süreci tesis edildiği test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD28.06	İş birimlerinin de katılımıyla gerçekleştirilen iş etki analizi ve önceliklendirilen iş hedefleri çerçevesinde planı geliştirilir ve kurtarma için gerekli olan işlemler belirlenir.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
		inceleme yöntemi ile iş birimlerinin de katılımıyla gerçekleştirilen iş etki analizi ve önceliklendirilen iş hedefleri çerçevesinde planı geliştirilir ve kurtarma için gerekli olan işlemler belirlendiği test edilir.	
MD28.07	Planın bakımı sağlanır.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge inceleme yöntemi ile planın bakımının sağlandığı test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD28.08	Yılda en az bir defa, denetimler ve risk analiz çalışmaları sonucu tespit edilen bulgular ve testlerden öğrenilen derslere göre veya iş süreçlerini ya da bilgi sistemleri sürekliliğini etkileyen değişikliklerden sonra plan gözden geçirilerek güncellenmesi sağlanır.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge inceleme yöntemi ile yılda en az bir defa, denetimler ve risk analiz çalışmaları sonucu tespit edilen bulgular ve testlerden öğrenilen derslere göre veya iş süreçlerini ya da bilgi sistemleri sürekliliğini etkileyen değişikliklerden sonra plan gözden geçirilerek güncellenmesi sağlandığı test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD28.09	Yaşanan acil durum ve felaketlerden kaynaklanan yasal konuları ele alınır ve halkla ilişkiler ve basın ile olan iletişim yürütülür.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge inceleme yöntemi ile yaşanan acil durum ve felaketlerden kaynaklanan yasal konuları ele alınır ve halkla ilişkiler ve basın ile olan iletişim yürütüldüğü test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD28.10	Planın hazırlanması sürecinde, bilgi varlıklarının ve tutulan verilerin önem düzeyi değerlendirilerek iş etki analizi çerçevesinde her bir BS servisi için kabul edilebilir kesinti süreleri ile kabul edilebilir veri kayıpları belirlenir ve belirlenen bu limitler doğrultusunda servisin tekrar erişime açılabilmesine imkân tanıyacak kurtarma prosedürleri geliştirilir.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge inceleme yöntemi ile planın hazırlanması sürecinde, bilgi varlıklarının ve tutulan verilerin önem düzeyi değerlendirilerek iş etki analizi çerçevesinde her bir BS servisi için kabul edilebilir kesinti süreleri ile kabul edilebilir veri kayıpları belirlendiği ve belirlenen bu limitler doğrultusunda servisin tekrar erişime açılabilmesine imkân tanıyacak kurtarma prosedürleri geliştirildiği test edilir.	ICT Bulut Bilişim tarafından gerçekleştirilen iş etki analizi kapsamında belirlenenen kabul edilebilir kesinti süreleri ve veri kaybı limitleri doğrultusunda, bilgi sistemleri servislerinin tekrar erişime açılabilmesini sağlayacak kurtarma prosedürlerinin tüm hizmetleri kapsayacak şekilde oluşturulmadığı tespit edilmiştir. (Bulgu denetim esnasında düzeltilmiştir.)
MD28.11	Felaket durumunun sona ermesi sonrası ikincil merkezden birincil merkeze geri dönüşün sağlanmasına yönelik prosedürleri hazırlanır.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge inceleme yöntemi ile felaket durumunun sona ermesi sonrası ikincil merkezden birincil merkeze geri dönüşün sağlanmasına yönelik prosedürlerin hazırlandığı test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD28.12	Plan kapsamında ikincil merkez tesis edilir. Veri ve sistem yedeklerinin ikincil merkezde kullanıma hazır bulundurulması sağlanır.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge inceleme ve gözlem yöntemleri ile plan kapsamında ikincil merkez tesis edildiği, veri ve sistem yedeklerinin ikincil merkezde kullanıma hazır bulundurulduğu test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

Kontrol Kodu	Kontrol Aktivitesi	Test Planı	Test Sonucu
MD28.13	İkincil merkez coğrafi olarak, deprem, yangın, patlama, sel, su baskını, heyelan, elektrik ve iletişim hattı kesintisi gibi sebeplerden kaynaklanacak zararlar açısından birincil merkez ile aynı risklere maruz olmaz.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge inceleme ve gözlem yöntemleri ile ikincil merkez coğrafi olarak, deprem, yangın, patlama, sel, su baskını, heyelan, elektrik ve iletişim hattı kesintisi gibi sebeplerden kaynaklanacak zararlar açısından birincil merkez ile aynı risklere maruz olmadığı test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD28.14	Planın yürütülmesinden sorumlu kritik kişiler ile plan kapsamında sorumluluğu bulunan personel, her yıl sorumlulukları ile orantılı bir detay ve içerikte BS sürekliliği eğitimine tabi tutulur ve plan kapsamındaki görev ve sorumlulukları hakkında bilgilendirilir.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge inceleme yöntemi ile planın yürütülmesinden sorumlu kritik kişiler ile plan kapsamında sorumluluğu bulunan personel, her yıl sorumlulukları ile orantılı bir detay ve içerikte BS sürekliliği eğitimine tabi tutulduğu ve plan kapsamındaki görev ve sorumlulukları hakkında bilgilendirildiği test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD28.15	Birincil sistemlerin tamamen devre dışı kaldığı felaket senaryolarında dahi en geç yirmi dört saat içerisinde faaliyetlerin yeniden sürdürülebiliyor olması sağlanır.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge inceleme yöntemi ile birincil sistemlerin tamamen devre dışı kaldığı felaket senaryolarında dahi en geç yirmi dört saat içerisinde faaliyetlerin yeniden sürdürülebiliyor olması sağlandığı test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD28.16	Planın etkinliğini ve güncelliğini temin etmek üzere yılda en az bir defa gerçek bir felaket senaryosunun simülasyonunu sağlamaya ve ikincil merkez üzerinden faaliyetleri sürdürmeye yönelik testler yapılır.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge inceleme yöntemi ile planın etkinliğini ve güncelliğini temin etmek üzere yılda en az bir defa gerçek bir felaket senaryosunun simülasyonunu sağlamaya ve ikincil merkez üzerinden faaliyetleri sürdürmeye yönelik testler yapıldığı test edilir.	Herhangi bir eksiklik tespit edilmemiştir.
MD28.17	Testlere varsa dış hizmet sağlayıcılar da dâhil edilir, test sonuçları üst yönetime raporlanır ve bu sonuçlara göre plan güncellenir.	İş Sürekliliği Prosedürü, İş Etki ve Risk Etki Analizi Prosedürü, İş Sürekliliği Planı, Normale Dönüş Planı, İletişim Planı ve süreklilik dokümantasyonu talep edilir ve belge inceleme yöntemi ile testlere varsa dış hizmet sağlayıcılar da dâhil edildiği, test sonuçlarının üst yönetime raporlandığı ve bu sonuçlara göre planın güncellendiği test edilir.	Herhangi bir eksiklik tespit edilmemiştir.

BÖLÜM 5

5. BULUTİSTAN İLAVE BİLGİLERİ

5.1 YAPILAN TESPİTLERE DENETLENENİN GÖRÜŞÜ

5.1.1. Giriş ve Yaklaşım

Bulutistan bünyesinde gerçekleştirilen denetim çalışmaları sırasında Bulutistan tarafındaki süreç sahipleri ve kontrol aktörleri ile denetim ekibinin iletişimi Sayın Seda Türkan Aydın tarafından sağlanmıştır. Denetimimiz sırasında bilgi sistemi dokümantasyonu ve bu dokümantasyonla ilgili her türlü kayıt, bilgi ve belge temini konusunda herhangi bir aksaklık yaşanmamıştır.

Denetim faaliyetleri ile ilgili olarak Bulutistan tarafından gerekli çaba gösterilmiş, Şirket içinde gerekli organizasyonlar yapılmış, gerekli girdilerin zamanında sağlanması için gerekli uyarılar yapılmış, süreçlere ilişkin politika ve prosedürler denetim ekibi üyelerine iletilmiştir. Denetim sırasında herhangi bir problem yaşanmamıştır. Denetim çalışmasının başlangıcında denetim kapsamına ilişkin olarak ilgili yöneticilerin katılımı ile açılış toplantısı yapılmış ve yönetmeliğin kapsamı ile yapılacak denetim çalışmasına ilişkin bilgi verilmiş ve denetçi olarak beklentilerimiz dile getirilmiştir.

Ayrıca, raporun 4. bölümünde sunulan Denetim Değerlendirmeleri, Deloitte Denetçilerinin ve Bulutistan paydaşlarının katılımı ile gerçekleşen Kapanış Toplantısı esnasında gözden geçirilmiş ve tartışılmıştır.

5.1.2. Önlem Alınacak Süreçler

Denetim esnasında tespitlerin yapıldığı kontrol alanları ile ilişkili Bulutistan yönetim cevaplarına aşağıda yer verilmektedir:

- MD11.04: Uygulama ve sistemler üzerinde kullanıcıların görev ve sorumluluklarına uygun olarak atanması gereken rollerin dokümante edilmediği tespit edilmiştir. (Bulgu denetim esnasında düzeltilmiştir.)

  Yönetim Cevabı: Mevcutta kullanılan Bulutistan Erişim Yetki Matrisi referans alınarak uygulama bazlı yetkilendirme ve sorumlulukları içeren Ek-A dokümanı oluşturulmuştur. Çalışma kapsamında yetki ve sorumlulukların daha net izlenebilmesi amacıyla RACI yaklaşımı kullanılarak mevcut yapı güncellenmiş, uygulamalara ilişkin rol, yetki ve sorumluluk ilişkileri dokümante edilmiştir. Yapılan güncelleme ile ilgili eksiklik giderilmiştir.

- MD28.10: ICT Bulut Bilişim tarafından gerçekleştirilen iş etki analizi kapsamında belirlenenen kabul edilebilir kesinti süreleri ve veri kaybı limitleri doğrultusunda, bilgi sistemleri servislerinin tekrar erişime açılabilmesini sağlayacak kurtarma prosedürlerinin tüm hizmetleri kapsayacak şekilde oluşturulmadığı tespit edilmiştir. (Bulgu denetim esnasında düzeltilmiştir.)(Bulgu denetim esnasında düzeltilmiştir.)

  Yönetim Cevabı: İş Etki Analizi çalışması gözden geçirilmiş ve denetim sırasında tespit edilen eksiklikler giderilmiştir. Bu kapsamda İş Etki Analizi envanterinde yer alan tüm sistem ve hizmetler için kurtarma stratejileri yeniden değerlendirilmiş, eksik bırakılan alanlar doldurulmuştur. Yapılan güncelleme ile her bir sistem ve hizmet için olası kesinti senaryolarında uygulanacak kurtarma yöntemi, yedeklilik yapısı, alternatif çalışma modeli ve operasyonel devamlılık yaklaşımı dokümante edilmiştir.