Bilişim Sistemleri Denetimi Rehberi

NİSAN 2024

T.C. SAYIŞTAY BAŞKANLIĞI

BİLİŞİM SİSTEMLERİ DENETİMİ REHBERİ

Nisan 2024

ANKARA

BELGE ADI **:** SDR.4 Bilişim Sistemleri Denetimi Rehberi

VERSİYON NO **:** 2024/2

VERSİYON TARİHİ **:** Nisan/2024

24.06.2013 tarihinde yürürlüğe konulan 2013/1 sayılı Bilişim Sistemleri Denetimi Rehberinde değişiklik yapma ihtiyacı üzerine, kurulan komisyon marifetiyle hazırlanan bu rehber, Denetim Planlama ve Koordinasyon Kurulunun 26.04.2024 tarih ve 2024/4 sayılı toplantısında görüşülerek kabul edilmiş ve 26.04.2024 tarihinde Sayıştay Başkanı tarafından onaylanarak yürürlüğe girmiştir.

SUNUŞ

Kaynağını Türk İslam Devletlerinden ve Osmanlı Devleti'nden alan güçlü devlet geleneği birikimini günümüze dek taşıyan Sayıştay, Cumhuriyetimizin en köklü ve itibarlı kurumlarından biridir. Türkiye Büyük Millet Meclisi adına denetim yapan, yargı yetkisini haiz, anayasal ve bağımsız bir yüksek denetim kurumu olan Sayıştay, kamu yönetiminde iyi işleyişin sağlanmasında önemli bir role sahiptir.

Sayıştay denetimi; kamu mali yönetiminin hukuka uygun olarak yürütülmesi, kamu kaynaklarının korunması, hesap verebilirlik ve şeffaflığın yerleştirilmesi ve geliştirilmesi amaçlarıyla yerine getirilmektedir.

Sayıştay, denetim faaliyetlerini gerçekleştirirken denetim yaklaşımını, kullandığı denetim metot ve tekniklerini değişen eğilim ve teknolojilere uyumlu bir şekilde geliştirmektedir. Kurumsal iş süreçlerinin bilişim ortamında yürütüldüğü ve izlendiği günümüz dünyasında kurum ve kuruluşlarda yapılan denetimlerde, bilişim sistemleri kontrollerinin değerlendirilmesi büyük önem arz etmektedir.

Başkanlığımız, 2002 yılından itibaren bilişim sistemleri denetimi yapmaktadır. Bu denetimler ile hem denetlenen kurumların bilişim sistemlerinin güvenlik ve güvenilirliğine dair güvence elde edilmekte, hem de kurumların bilişim alanına ilişkin kontrollerine yönelik tespit ve öneriler raporlanarak kurumlara katkı sağlanmaktadır.

Sayıştay bilişim sistemleri denetimi rehberi ilk olarak 2013 yılında yayımlanmıştır. Bilgi teknolojilerindeki değişimin hızlı olması nedeniyle rehberin güncellenmesi ihtiyacı doğmuş ve BT alanındaki güncel metot ve teknolojiler rehbere yansıtılmıştır.

Güncelleme ile Uluslararası Yüksek Denetim Kurumları Teşkilatı (INTOSAI) tarafından oluşturulan Uluslararası Mesleki Bildirimler Çerçevesi (IFPP) bünyesinde INTOSAI Rehberliği (GUID) kısmı altında yer alan "GUID 5100 Bilgi Sistemlerinin Denetimine İlişkin Rehber" ile tanımlanan BT denetimi metodolojisine de uyum sağlanmıştır. Güncelleme çalışmalarında INTOSAI BT Denetimi Çalışma Grubu (WGITA) ile INTOSAI Geliştirme Girişimi (IDI) tarafından yayımlanan BT Denetimi El Kitabından da istifade edilmiş, denetim/kontrol alanları ve konular yeniden sınıflandırılmıştır.

Rehberin kurumumuz ve kullanıcılar için faydalı olmasını temenni eder, hazırlanmasında emeği geçen tüm mensuplarımıza teşekkür ederim.

Metin YENER

Sayıştay Başkanı

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

KISALTMALAR

BDDTA : Bilgisayar Destekli Denetim Teknik ve Araçları

BGYS : Bilgi Güvenliği Yönetim Sistemi

BS : Bilgi Sistemleri veya Bilişim Sistemleri

BT : Bilgi Teknolojileri

COBIT : Control Objectives for Information and Related Technology (Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri)

DDO : Dijital Dönüşüm Ofisi

EUROSAI : European Organization of Supreme Audit Institutions (Avrupa Yüksek Denetim Kurumları Teşkilatı)

HSA : Hizmet Seviyesi Anlaşması

IDI : INTOSAI Development Initiative (INTOSAI Gelişim İnisiyatifi)

IEC : International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)

IFPP : INTOSAI Framework of Professional Pronouncements (INTOSAI Mesleki Bildirimler Çerçevesi)

INTOSAI : International Organization of Supreme Audit Institutions (Uluslararası Yüksek Denetim Kurumları Teşkilatı)

ISACA : Information Systems Audit and Control Association (Bilgi Sistemleri Denetim ve Kontrol Birliği)

ISO : International Organization for Standardization (Uluslararası Standardizasyon Örgütü)

ISSAI : International Standards of Supreme Audit Institutions (Uluslararası Yüksek Denetim Kurumları Standartları)

ITAF : Information Technology Assurance Framework (Bilgi Teknolojileri Güvence Çerçevesi)

ITIL : Information Technologies Infrastructure Library (Bilgi Teknolojisi Altyapı Kütüphanesi)

PMBOK : Project Management Body of Knowledge (Proje Yönetimi Bilgi Birikimi Kılavuzu)

PMI : Project Management Institute (Proje Yönetimi Enstitüsü)

SGYD : Sistem Geliştirme Yaşam Döngüsü

SIEM : Security Information and Event Management (Güvenlik Bilgileri ve Olay Yönetimi)

SOME : Siber Olaylara Müdahale Ekibi

TÜBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

WGITA : Working Group on IT Audit (Bilgi Teknolojileri Denetimi Çalışma Grubu)

GİRİŞ

Kamuda bilgi teknolojilerinin (BT) yaygın kullanımı bu teknolojiye özgü riskleri de beraberinde getirmektedir. Söz konusu riskleri minimize edecek etkin kontrol mekanizmalarının oluşturulmaması durumunda sistemlerin ve dolayısıyla bu sistemler tarafından işlenen, tutulan ve raporlanan bilginin gizliliği, bütünlüğü, erişilebilirliği ve güvenilirliği zarar görebilmektedir. Bu nedenle, BT kullanımı olan kurum ve alanlarda yürütülecek denetimler sırasında bu risklerin etkilerini dikkate alan yaklaşım, metot ve tekniklerin benimsenmesi gerekmektedir.

Nitekim, Uluslararası Yüksek Denetim Kurumları Standartlarına (ISSAI) göre, muhasebe veya diğer bilgi sistemlerinin (BS) bilgisayarlaştırıldığı ortamlarda denetçi, denetlenen kurumun verilerinin doğruluk, tamlık ve güvenilirliğini sağlayan iç kontrollerin uygun çalışıp çalışmadığını belirlemelidir.

Bunun yanında, kamu hizmetlerinin dijital dönüşümü, iyileştirilmesi veya entegrasyonu nedeniyle BT yatırımlarında önemli bir artış görülmektedir. Ancak; proje gereksinimlerinin eksik tanımlanması, risklerin yönetilememesi, rol ve sorumlulukların iyi tanımlanmaması, karar alma süreçlerinin sağlıklı işletilememesi, dış tedarikçi seçiminin iyi yapılamaması, kamu kurum ve kuruluşları ile tedarikçiler arasındaki iletişim problemleri, vb. sebeplerden dolayı BT projelerinin başarı ile tamamlanma oranlarının düşüklüğü sorunu yaşanmaktadır. Bu soruna çözüm bulmak ve başarı oranlarını artırmak için BS denetimleri önem kazanmaktadır. BS denetimleri, BT projelerinin başarısına olumsuz etki eden faktörlerin giderilmesine veya bu faktörlerin kontrol altında tutularak projelerin başarıyla tamamlanmasına katkı sağlamaktadır. Ulusal e-Devlet Stratejisi gereği, Sayıştayın kamu idarelerinde BS denetimi yaparak projelerin başarıyla tamamlanmasına katkı sağlaması beklentisi artmıştır.

Sayıştay, kamu idarelerinde kullanılan dijitalleştirilmiş sistemlerinin güvenliğine ve verilerin güvenilirliğine ilişkin güvence elde etme ihtiyacının yanında, kamu idarelerinin BT ile ilgili mevzuata uyumunu incelemek, BT yönetiminin, yatırımlarının ve dijitalleşmiş kamu hizmetlerinin verimlilik ve etkililiğini değerlendirmek ve geliştirilmekte olan sistemlerin ve BT projelerinin başarı ile tamamlanmasına katkı sağlamak amacıyla da BS denetimleri yapmaktadır.

Bu rehber, Sayıştay tarafından yapılan BS denetim faaliyetlerinin uluslararası standartlarına uygun şekilde yürütülmesi için denetçiye yol göstermek amacıyla hazırlanmıştır.

Rehberin hazırlanmasında, başta INTOSAI, EUROSAI, ISACA, ISO, PMI, DDO ve TÜBİTAK olmak üzere ulusal ve uluslararası kurum ve kuruluşların standart, rehber, çerçeve belge ve diğer yayınlarından yararlanılmıştır.

Rehber, üç bölümden oluşmaktadır. Birinci bölümde BS denetimine ilişkin temel kavramsal ve yönetsel çerçevenin de yer aldığı "Denetim Çerçevesi", ikinci bölümde BS denetiminin adım adım nasıl gerçekleştirileceğinin gösterildiği "Denetim Süreci" ve üçüncü bölümde ise denetimin yürütüldüğü "Denetim/Kontrol Alanları" ele alınmıştır.

BİRİNCİ BÖLÜM
DENETİM ÇERÇEVESİ

1.1 Dayanak ve Uygulama Alanları

Genel anlamda Sayıştayların BS denetimi yapmasının uluslararası alandaki temel dayanağı INTOSAI Mesleki Bildirimler Çerçevesinin (IFPP) birinci düzeyi içinde yer alan ve INTOSAI'nin kurucu ilkelerini içeren "INTOSAI-P 1 Lima Deklarasyonu"dur.

1977 yılında yayımlanan Lima Deklarasyonunun "VII. Yüksek Denetim Kurumlarının Denetim Yetkisi" kısmı altında yer alan "Elektronik Veri İşleme Sistemlerinin Denetimi" başlıklı 22'nci bölümünde;

"*Elektronik veri işleme sistemlerine önemli miktarda kaynak harcanması, uygun denetimlerin yapılmasını gerekli* kılar. *Bu denetimler, sistem tabanlıdır ve gerekliliklere yönelik planlama, veri işleme donanımının ekonomik kullanımı, uygun uzmanlığa sahip (tercihen denetlenen kurumdaki) personelden istifade etme, istismarın engellenmesi ve üretilen bilginin kullanışlılığı gibi hususları içerir.*" denilmektedir.

Sayıştayın BS denetimi yapmasının temel dayanağını ise, kamu idarelerinin iç kontrol sistemlerinin incelenmesini öngören 6085 sayılı Sayıştay Kanunu'nun 35'inci maddesi oluşturmaktadır.

"Denetimin genel esasları" başlıklı 35'inci maddede;

"*(1) Denetimin* genel *esasları şunlardır:*

a) Denetim; kamu idarelerinin *hesap, mali işlem ve faaliyetleri ile* ***iç kontrol sistemlerinin incelenmesi*** *ve kaynakların etkili, ekonomik, verimli ve hukuka uygun olarak kullanılmasının değerlendirilmesidir.*

b) Denetim genel kabul *görmüş uluslararası denetim standartlarına uygun olarak yürütülür.*" ifadesi yer almaktadır.

Konu bazında BS denetiminin dayanağı ise, konu bazında denetimi düzenleyen 6085 sayılı Sayıştay Kanunu'nun 6'ncı maddesinin 4'üncü fıkradır.

"Sayıştayın yetkileri" başlıklı 6'ncı maddenin 4'üncü fıkrasına göre;

"*(4) Sayıştay, kamu idarelerinin hesap, işlem ve faaliyetleri ile mallarını, hesap veya faaliyet dönemine bağlı olmaksızın yılı içinde veya yıllar itibariyle denetleyebileceği gibi sektör, program, proje ve konu bazında da denetleyebilir.*"

BS denetimleri, Sayıştay Kanunu'nun yukarıda belirtilen maddelerine uygun şekilde aşağıda belirtilen kapsamlarda gerçekleştirilebilir:

- Konu bazlı denetim kapsamında,

- Düzenlilik denetimi kapsamında,
- Performans denetimi kapsamında.

Konu bazlı BS denetimi, bağımsız bir şekilde planlanır, yürütülür ve müstakil olarak raporlanır. Bu nedenle rehber, denetim süreçlerinin tümünü göstermeye daha uygun olduğu için konu bazlı denetim odağında hazırlanmıştır.

Düzenlilik ve performans denetimi kapsamında yapılan BS denetimlerinde, bilişim sistemlerinin değerlendirilmesine ilişkin faaliyetler, ilgili olduğu denetim türünün denetim süreçlerine uyumlu yürütülür.

1.2 Tanım

BT denetimi ile ilgilenen kişi ve organizasyonlar tarafından farklı BT denetimi tanımları yapılmıştır. Sayıştay kendi BS denetim yaklaşımına uygun olması sebebiyle ISACA tarafından da kabul gören aşağıdaki tanımı benimsemiştir:

"*BT Denetimi; bir bilgisayar sisteminin varlıkları güvence altına alacak, veri bütünlüğünü sağlayacak, kurumsal amaçlara etkin biçimde ulaşılmasını sağlayacak ve kaynakları verimli kullanacak şekilde tasarlanıp tasarlanmadığını belirlemek amacıyla yapılan kanıt toplama ve değerlendirme sürecidir.*"

Bilgi ve iletişim sektöründe, BT ve BS kavramları birbirinin yerine kullanılmakla birlikte aralarında fark vardır. ISACA tarafından BT ve BS kavramları aşağıda belirtildiği şekilde tanımlanmaktadır:

Bilgi Teknolojileri (BT): Verilerin girişi, saklanması, işlenmesi, iletilmesi ve çıktılarının alınması için kullanılan donanım, yazılım, iletişim ve diğer tesisat (ISACA-Terimler Sözlüğü).

Bilgi Sistemleri (BS): Bilgi ve ilgili teknolojileri toplama, işleme, depolama, dağıtma ve kullanımı ile ilgili stratejik, yönetsel ve operasyonel faaliyetlerin birleşimi (ISACA-Terimler Sözlüğü).

BT ve BS ilişkisi aşağıdaki şekilde gösterilmiştir:

Şekil 1: BT ve BS İlişkisi

Sayıştay, öncelikli olarak denetlediği kamu idarelerinde kullanılan sistemlerinin güvenliği ve güvenilirliği konusunda güvence elde etmeye çalıştığından, sistemleri yazılım, donanım, veri, iletişim, süreçler ve insan kaynakları itibariyle bütün yönleri ile inceleme ihtiyacı duymaktadır. Bu nedenle yaptığı denetime uygun şekilde BS kavramını kullanmayı tercih etmektedir.

Bu rehberde, diğer kurum ve organizasyonlar tarafından "BT" ve "BT Denetimi" kavramları kullanımının yerleştiği alanlarda, onlarla uyumlu olması için bu kavramlar aynen kullanılmıştır. Sayıştay denetim uygulamasına ilişkin durumlarda ise, "BS" ve "BS Denetimi" kavramları kullanılmıştır.

1.3 Amaç

BS denetiminin yapılma amacı;

- BS'nin ürettiği bilginin doğruluk, tamlık ve güvenilirliğine ilişkin güvence elde etmek,
- BS ile ilgili iç kontrol zafiyetlerinin tespit edilmesi ve öneriler sunulması suretiyle kamu kurum ve kuruluşlarına katkı sağlamak ve
- İlgililerine incelenen BS'ye ilişkin bilgi sunmaktır.

BS denetimlerinde, temel olarak, BS'nin güvenliğinin, performansının ve uygunluğunun değerlendirmesi amaçlanır.

1.4 Denetim Yaklaşımı

Bilişim sistemleri denetimi, temel olarak iç kontrollerin değerlendirilmesi suretiyle gerçekleştirilir.

İç kontrollerin değerlendirilmesinde risk tabanlı denetim yaklaşımı benimsenir. Buna göre;

- Riskler belirlenir,
- Riskleri minimize edecek kontrol mekanizmaları belirlenir,
- Kontrol mekanizmalarının kurum tarafından oluşturulup oluşturulmadığı, oluşturuldu ise etkin çalışıp çalışmadığı incelenir,
- İnceleme sonrası kontrol zafiyetleri değerlendirilir ve
- Önemli kontrol zafiyetleri raporlanır.

Denetimlerde iç kontroller incelenirken, varsa ürünler/çıktılar ve performans göstergeleri de değerlendirilir. Ürünlerin değerlendirilmesinde, üretilen ürünlerin/çıktıların belirlenen şartlara uygunluğu değerlendirilir. Performans göstergelerinin değerlendirilmesinde ise, gerçekleşen performansın hedeflenen performans göstergelerine uygunluğu değerlendirilir.

1.5 BT Riskleri ve BT Kontrolleri

BS denetimlerinin temel konusunu, risk tabanlı denetim yaklaşımına uygun şekilde, BT riskleri ve bu riskleri minimize edecek BT kontrollerinin incelenmesi oluşturur.

1.5.1 BT Riskleri

BT Riskleri: Bilgi varlıklarındaki bir ya da daha fazla zafiyetin bir tehdit tarafından istismar edilmesi sonucu bir kurumun zarar görme ihtimali olarak tanımlanabilir.

Bu tanıma göre, BT risklerinin temel unsurları şunlardır:

- **Zafiyet:** Bir tehdit tarafından bilgiye yetkisiz erişim ya da sistemleri aksatma/bozma amacıyla istismar edilebilen iç kontrol zayıflıkları.
- **Tehdit:** Bilgi varlıklarına yönelik olası tehlike (tabi afetler, çevresel tehditler, insan kaynaklı tehditler, virüsler, vb.).
- **Zarar:** Bir tehdidin bir zafiyeti istismar etmesi ile ortaya çıkan sonuç.

Örnekler:

Zafiyet	Tehdit	Zarar
Güncel olmayan işletim sistemi, etkin olmayan anti-virüs yazılımı kullanımı	Virüs	Uygulama ve verinin zarar görmesi, iş faaliyetlerinin kesintiye uğraması
Sisteme kimlik doğrulama olmaksızın yalnızca ortak bir kullanıcı hesabı üzerinden erişilmesi	Kullanıcılar	Veri ihlalleri, sorumluluğun tespit edilememesi
Kurum girişinde güvenlik personeli olmaması, kimlik kontrolü yapılmaması	Ziyaretçiler	Bilgi varlıklarının çalınması

BT ile ilgili riskler en temel haliyle aşağıdaki gibi sıralanabilir:

- BT kaynaklarının etkin kullanılamaması, kurumun iş ihtiyaçlarını karşılamaması,
- Yetkisiz kişiler tarafından verinin değiştirilmesi,
- Yetkisiz kişiler tarafından verinin silinmesi,
- Veri bütünlüğünün bozulması,
- Bilgi varlıklarının zarar görmesi,
- Bilgi varlıklarının çalınması,
- Bilginin ifşa olması,
- İşin/hizmetin kesintiye uğraması,
- Hizmet kalitesinin düşmesi,
- Bilginin kötüye kullanılması,
- Denetim izinin kaybolması, sorumluluğun tespit edilememesi,
- Mevzuata aykırı işlemlerin yapılması,
- Sistematik hataların yaşanması,
- BT projelerinin zamanında, bütçesinde ve uygun kalitede tamamlanamaması.

1.5.2 BT Kontrolleri

BT Kontrolleri: BT risklerini azaltmak için uygulamaya konulan politikalar, prosedürler, uygulamalar ve organizasyon yapılarını da içeren her türlü kontrol mekanizmalarıdır.

BT Kontrolleri, genel kontroller ve uygulama kontrolleri olarak sınıflandırılabilir.

Genel Kontroller: Kuruma ait tüm bilişim sistemleri faaliyetlerinin sürekli ve uygun biçimde yerine getirilmesini sağlamaya yönelik yapı, yöntem ve prosedürlere ilişkin kontrollerdir.

Bir başka tanıma göre; "Bilgisayar uygulamaları ve sistemlerinin geliştirildiği, bakımının yapıldığı ve işletildiği ortam ile ilgili olan ve bu nedenle tüm uygulamalarda genel olarak kullanılabilen manuel ya da programlanmış kontrollerdir. Temel amacı; sistem ve uygulamaların düzgün şekilde geliştirilmesini güvence altına almak ve programlar, veri dosyaları ve bilgisayar işlemlerinin bütünlüğünü sağlamaktır." (ISACA - Terimler Sözlüğü)

Örnekler:

- Bir BT Stratejisinin ve bir BT Güvenlik Politikasının geliştirilmesi ve uygulanması
- Bir BT Yönlendirme Kurulunun kurulması
- BT personeli görev tanımlarının görevlerin ayrılığı ilkesine uygun yapılması
- Felaket kurtarma planlaması

Genel kontroller, uygulama yazılımlarının düzgün ve öngörüldüğü şekilde çalışması için güvenli ve uygun bir ortam oluşturur.

Uygulama yazılımları, muhasebe, vergi, alacak takip işlemleri gibi bir iş fonksiyonuna destek veren yazılımlardır. Bu yazılımlar, kurumun iş süreçlerinin bir kısmının veya tamamının bilgisayar ortamında yapılmasını sağlar.

Uygulama Kontrolleri: Her bir uygulamaya ilişkin spesifik kontrollerdir. "Belirli bir uygulama ile ilgili hedeflerin gerçekleştirildiğine dair makul güvence sağlamak üzere tasarlanan politikalar, prosedürler ve aktivitelerdir." (ISACA - Terimler Sözlüğü)

Örnekler:

- Veri girişi doğrulaması
- İletilecek verilerin şifrelenmesi

BT kontrolleri, önleyici, tespit edici ve düzeltici kontroller olarak da sınıflandırabilir. Bu kontroller yönetsel, teknik veya fiziksel olabilir.

Önleyici Kontroller: Sorunların ortaya çıkmadan önce tespit edilmesi/öngörülmesi ve gerekli düzenlemelerin yapılmasını amaçlayan kontrollerdir.

Örnekler:

- Görevler ayrılığı, yazılı prosedürler >> Yönetsel
- Şifreleme, güvenlik duvarı >> Teknik

- Kilitli kapılar, güvenlik personeli >> Fiziksel

Tespit Edici Kontroller: Hata, ihmal ya da zararlı faaliyetin ortaya çıktığında tespit edilmesini ve raporlanmasını amaçlayan kontrollerdir.

Örnekler:

- Olay kayıtlarının incelenmesi >> Yönetsel
- Saldırı tespit sistemleri, ağ taramaları >> Teknik
- Duman ve yangın detektörleri, fiziksel sayım >> Fiziksel

Düzeltici Kontroller: Tehdidin etkisinin en aza indirilmesini, sorunların nedenlerinin anlaşılmasını amaçlayan kontrollerdir.

Örnekler:

- İş sürekliliği ve felaket kurtarma planları >> Yönetsel
- Yedeklerden geri dönülmesi >> Teknik
- Felaket kurtarma merkezi, yangın söndürme cihazları >> Fiziksel

1.6 Standartlar ve Çerçeve Belgeler

Yararlanılan standartlar ve çerçeve belgelerin bir kısmı denetimin yürütülmesinde kullanılmakta iken, bir kısmı da denetim esnasında BT kontrollerinin değerlendirilmesinde referans alınmaktadır.

1.6.1 Denetimin Yürütülmesinde Kullanılanlar

INTOSAI Mesleki Bildirimler Çerçevesi (IFPP)

IFPP bünyesinde INTOSAI Rehberliği (GUID) kısmı altında yer alan GUID 5100 Bilgi Sistemlerinin Denetimine İlişkin Rehber, gerek tekil olarak gerekse diğer denetimlerin bir parçası olarak yürütülen BT denetimlerine ilişkin genel ilkeleri, yaklaşımı ve metodolojiyi ele alarak denetimin planlama, yürütme, raporlama ve izleme süreçlerini tanımlamaktadır.

Bunun yanında, mali denetime, performans denetimine ve uygunluk denetimine ilişkin Uluslararası Yüksek Denetim Kurumları Standartları da (ISSAI), ilgili oldukları denetim türü ve süreçleri çerçevesinde BT riskleri ve kontrollerine ve bunların incelenmesine ve değerlendirilmesine ilişkin hükümler içermektedir.

Bilgi Teknolojileri Güvence Çerçevesi (ITAF)

ISACA tarafından yayımlanan ve BS denetimine ilişkin mesleki rol ve sorumluluklara, bilgi ve becerilere, gayret, davranış ve raporlama gereksinimlerine ilişkin standartları belirleyen; BS denetimine özgü terim ve kavramları tanımlayan; BS denetiminin planlanması,

tasarımı, yürütülmesi ve raporlanması ile ilgili rehberlik, araçlar ve teknikler sağlayan kapsamlı ve iyi uygulama odaklı bir referans modelidir.

1.6.2 Kontrollerin Değerlendirilmesinde Referans Alınanlar

Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri (COBIT)

ISACA tarafından yayımlanan ve BT'ye ilişkin genel kabul görmüş standartlar ve düzenlemeler ışığında BS'nin maruz kaldığı riskleri, bu risklerin değerlendirilmesi, yönetilmesi ve ortadan kaldırılmasına yönelik kontrolleri ve bu kontrollerin denetlenme yöntemlerini ele alan temel bir çerçevedir. İlk başta bir denetim aracı olarak tasarlanmış olan COBIT, zaman içerisinde kontrol ve yönetim boyutlarını da içerir hale gelmiş, günümüzde ise BT'nin yönetimi ve yönetişimi odaklı bir çerçeveye dönüşmüştür. Bu bağlamda, temel amacı iş hedefleriyle BT hedeflerini bağdaştırmak ve BT yönetişimi için temel hedefleri ve bileşenleri sunmaktır.

Bilgi Güvenliği Standartları (ISO/IEC 27K)

Uluslararası Standardizasyon Örgütü (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC) tarafından ortaklaşa yayımlanan ve bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korumaya yönelik olan standart serisidir. Bilgi güvenliği yönetimi, riskler ve kontroller hakkında iyi uygulama önerileri sunan serinin ana standardı olan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) için gereklilikleri ortaya koyarken, ISO/IEC 27002 ise bilgi güvenliği kontrolleri için uygulama kurallarını tanımlamaktadır.

Bilgi Teknolojisi Altyapı Kütüphanesi (ITIL)

BT hizmet yönetimini strateji, tasarım, geçiş, operasyon ve sürekli iyileştirme aşamalarından oluşan bir yaşam döngüsü olarak ele alan, hizmet yönetimini ve süreçlerini ayrıntılı olarak anlatan ve en iyi şekilde sürdürmek için yol gösteren bir yöntemler dizisidir.

Proje Yönetimi Bilgi Birikimi (PMBOK) Kılavuzu

Proje Yönetim Enstitüsü (PMI) tarafından yayımlanan ve uluslararası kabul görmüş proje yönetim yöntemlerine yer veren kılavuz, bütün proje türleri için kullanılabilecek standart bir terminoloji ve yönergeler seti sunmaktadır.

COSO İç Kontrol Bütünleşik Çerçevesi

Amacı, iç kontrol kavramının anlaşılmasını sağlamak ve kurumlarda uygulanabilmesi için yol gösterici önerilerde bulunmak olan COSO (The Committee of Sponsoring Organizations of the Treadway Commission) tarafından geliştirilen iç kontrol modelidir. Buna göre, iç kontrolün bileşenleri "kontrol ortamı", "risklerin değerlendirilmesi", "kontrol faaliyetleri", "bilgi paylaşımı ve iletişim" ve "izleme"dir. İçeriğinin kapsayıcılığı, kurumlara uygulama rehberi sunması ve yaşayan bir model olması gibi nedenlerle dünya çapında en yaygın kabul görmüş iç kontrol modelidir.

1.7 Önemlilik

BS denetimleri yürütülürken önemlilik unsuru dikkate alınır. Denetçi, önemliliği mesleki yargısını kullanarak niteliksel olarak belirler.

Önemlilik, incelenecek kontrollerin/konuların belirlenmesinde ve denetim sonuçlarının raporlamasında bir seçim kriteri olarak kullanılır.

Kontrollerin/Konuların Belirlenmesinde Önemlilik

Denetim planlanırken, denetim kapsamında incelenecek kontrollerin/konuların belirlenmesi gerekir.

İncelenecek kontroller/konular belirlenirken, kontrollerin önemliliği göz önüne alınır. Kontrol mekanizmalarının hepsi aynı etkiye sahip değildir. Denetimlerde, kontrol hedefini sağlama/ riski düşürme etkisi yüksek olan kontrollerin incelenmesine öncelik ve ağırlık verilir.

Raporlamada Önemlilik

Denetim raporuna önemli bulgular alınır. Raporlama açısından temel önemlilik kriteri, belirlenen kontrol zafiyetinin ilgili kontrolü etkileme derecesi ve neden olabileceği sonuçlardır.

Bununla birlikte, tek başına düşük bir öneme sahip olan hata ve eksikliklerinin kümülatif bir etkiyle önemli bir kontrol zafiyetine dönüşme ihtimali de denetçi tarafından bu aşamada değerlendirilmelidir.

1.8 Belgeleme ve Kalite Kontrolü

Denetim esnasında, yapılan inceleme ve denetim sonuçlarına temel oluşturacak belgeler zamanında ve uygun şekilde hazırlanır.

Belgeleme çalışmaları denetimin planlanması, uygulanması, raporlanması ve gözden geçirilmesine yardım edecek şekilde yapılır. Denetim sürecinde denetim planı, çalışma programı, yapılan denetim çalışmaları, toplanan denetim kanıtları ve denetim sonuçları belgelenir.

Denetim faaliyetleri çalışma kağıtları hazırlanmak suretiyle belgelendirilir. Çalışma kağıtlarında hazırlanma ve gözden geçirme tarihleri belirtilir.

Çalışma kağıtları ve denetim esnasında edinilen belgeler güvenli ortamlarda arşivlenir ve muhafaza edilir.

Yapılan denetim çalışmaları mevzuat, rehber ve uluslararası denetim standartlarına uygunluk açısından değerlendirilir.

Denetim esnasında yapılan çalışmaların kalite kontrolü, Ekip Başkanı ve Grup Başkanı tarafından yapılan gözden geçirme faaliyetleri ile sağlanır.

Gözden geçirme yapılırken, çalışma kağıtları,

- gerekli prosedürlerin gerçekleştirilmesi,
- uygun ve yeterli denetim kanıtlarının toplanması,
- bulguların denetim görüşünü veya genel değerlendirmeyi desteklemesi

açılarından değerlendirilir.

Raporlama aşamasında yapılan çalışmaların kalite kontrolü için ise aşağıdaki süreç takip edilir:

- Taslak rapor, ilgili kamu idaresine görüş alınmak üzere gönderilmeden önce, raporu hazırlayan ekibin dışında görevlendirilen başka bir ekip (Değerlendirme Komisyonu) tarafından değerlendirilir. Değerlendirme sonuçları ilgili denetim ekibine önerileri ile birlikte sunulur. Denetim ekibi, Değerlendirme Komisyonu görüşlerini dikkate alarak taslak rapora son halini verir.
- Kamu idaresi görüşü alındıktan sonra denetim ekibi tarafından son şekli verilen denetim raporu, Daire ve Rapor Değerlendirme Kurulunda görüşülür. Rapor, kalite kontrol süreçleri tamamlandıktan sonra son şekli verilerek ilgililerine sunulur/gönderilir.

1.9 Denetçi Yetkinliği ve Eğitim

BS denetimi yürütecek denetçilerin aşağıda yer alan konularda bilgi sahibi olması gerekir:

- Temel BS bilgisi (donanım, yazılım, iletişim ve ağ, insan kaynağı, vb.),
- Bilgi güvenliği (temel kavramlar, ağ güvenliği, işletim sistemleri güvenliği, veri tabanı güvenliği, uygulama güvenliği, vb.),
- BT yönetişimi ve yönetimi (BT stratejisi, BT risk yönetimi, vb.),
- BT proje yönetimi,
- BT işletimi (olay ve problem yönetimi, değişiklik yönetimi, vb.),
- İş sürekliliği yönetimi,
- BS denetim metodolojisi,
- BS denetim standartları,
- BS denetimlerinde kontrollerin değerlendirilmesinde yararlanılan standartlar.

Denetçilerin yukarda belirtilen konulardaki bilgi eksikliği veya bilgi güncelleme ihtiyacı belirlenir. İhtiyaca göre, hizmet içi eğitim verilerek veya uzman kişi veya kurumlardan teorik ve uygulama eğitim desteği alınarak denetçilerin BS denetim kapasitesi geliştirilir.

Bunun yanında, denetçilerin BS denetimi ile ilgili sertifika programlarına katılımı ve edinimi teşvik edilir.

1.10 Stratejik Planlama ve Kurum/Sistem Seçimi

BS denetimleri için uzun vadeli stratejik planlama yapılır. Bu planlama "Sayıştay Stratejik Planı" veya "Denetim Stratejik Planı" kapsamında yapılabileceği gibi bağımsız "BS Denetimi Stratejik Planı" olarak da yapılabilir.

Sorumlu Grup Başkanlığınca, BS denetimi ile ilgili stratejik planlama gereklerine uygun şekilde Gruptaki insan kaynağı da dikkate alınarak yıllık planlama yapılır. Bunun için yeterli sayıda sistemde ön inceleme yapılır.

Denetime alınacak kurum ve sistemlere ilişkin seçim yapılabilmesi için ön incelemeye alınan sistemler değerlendirilir. Bunun için "EK-2: Sistem Risk Değerlendirme Formu" kullanılabilir.

Grup Başkanlığı tarafından denetlenebilecek sistemler ve ilgili kamu idarelerinin yer aldığı bir öneri listesi hazırlanarak Başkanlığa sunulur.

Denetlenecek bilişim sistemleri Başkanlık tarafından belirlenir.

İKİNCİ BÖLÜM
DENETİM SÜRECİ

Denetimler, genel hatları ile aşağıda belirtilen sürece uygun şekilde yürütülür:

- Denetimin planlanması
- Denetimin yürütülmesi
- Denetim sonuçlarının raporlanması ve izlenmesi

2.1 Denetimin Planlanması

BS denetimleri, yıllık denetim planına uygun şekilde Başkanlıkça görevlendirilen denetim ekipleri tarafından gerçekleştirilir.

BS denetim faaliyetleri, planlamayla başlar. Planlama, denetim süresince takip edilecek yol gösterici bir süreç olup, denetlenen sisteme ilişkin kontrolleri değerlendirmek için denetim kanıtı toplamanın etkili ve verimli metotlarının belirlenmesine imkân verir.

Planlama süreci, kurumun ve bilişim sistemlerinin tanınması, risklerin değerlendirilmesi, uzman ihtiyacının belirlenmesi, denetim amaçları ve kapsamının belirlenmesi, denetim planının hazırlanması ve denetim programlarının hazırlanmasından oluşur.

2.1.1 Kurum ve Bilişim Sistemlerinin Tanınması

Denetçi, denetlediği sistemleri ve bu sistemleri kullanan veya geliştiren kurum hakkında yeterli düzeyde bilgi sahibi olmalıdır.

Kurum ve BS'ye ilişkin bilgi toplanması amacıyla "EK-1: Genel Bilgi Edinme Formu" kullanılabilir. Genel bilgi edinme formunda istenen bilgilerin tek elde toplanmasının kurum açısından güvenlik zafiyeti oluşturabileceği değerlendiriliyorsa, formda yer alan bilgiler ilgili birimlerden ayrı ayrı istenebilir.

Kurum ve sistemleri anlamaya yönelik olarak aşağıdaki faaliyetler yürütülür:

Kuruma İlişkin Temel Düzenlemelerin Belirlenmesi

Kurumun görevleri, ana faaliyetleri ve uyması gereken ve kurum sistemlerini etkileyebilecek olan her türlü düzenleme incelenmelidir. Bunlar arasında kurumla ilgili mevzuat, stratejik planlar, yıllık programlar, faaliyet raporları ve bütçeler sayılabilir.

Bilişim Sistemlerini Oluşturan Unsurların Anlaşılması

Kurumu ve sistemleri anlamak için öncelikle kurum iş süreçlerinin anlaşılması gerekir. Bunun için iş akış şemaları incelenmelidir.

Kurum iş süreçleri belirlendikten sonra kurum tarafından yürütülen işlerden hangilerinin bilişim ortamında gerçekleştirildiği, kullanılan uygulamalar ve bu uygulamaların birbiri ile etkileşimi belirlenmelidir.

Kurum bilişim sistemlerinin yazılım, donanım, ağ ve iletişim yapısı ile insan kaynakları incelenmelidir. Sistemi işleten ve kullanan personel ile sisteme veri giriş yöntemleri konusunda bilgi edinilmelidir.

Düzenlilik denetimi kapsamında yürütülen bilişim sistemleri denetimlerinde, özellikle mali nitelikte bilgi üreten uygulamalar ve bunların hangi hesap alanlarını etkilediği belirlenmelidir.

Önceki Dönem Raporlarından Bilgi Toplanması

Önceki dönemlerde yazılmış BS'yi ilgilendiren uzman raporları, bağımsız BS denetim raporları, diğer denetim raporları ve iç denetim raporları incelenerek hem kurum sistemleri hem de BS'ye ilişkin kontrol faaliyetleri hakkında bilgi toplanmalıdır.

Kurumda daha önce Sayıştay tarafından BS denetimi yapılmış ise bu denetim sonucunda hazırlanmış olan "İzleme Tabloları" değerlendirilmelidir.

Üçüncü Taraflarla İlişkilerin Anlaşılması

Kurumun üçüncü taraflarla, özellikle kamu kurumları ile ilişkisi belirlenmelidir. Bu ilişkinin iş süreçleriyle bağlantısı incelenmeli ve BS bazındaki ilişki üzerinde yoğunlaşılmalıdır.

Üçüncü taraflarla, hizmet, bakım ve destek ilişkileri genel hatlarıyla ortaya konmalı, ilgili belgeler temin edilmelidir.

Dış kaynak kullanımı varsa, tedarikçilere ilişkin bilgi toplanmalıdır.

Sistem Geliştirme Faaliyetlerine İlişkin Bilgi Toplanması

Kurum tarafından sistem geliştirme faaliyetleri gerçekleştirilip gerçekleştirilmediği belirlenmelidir. Eğer varsa, sistem geliştirmeye ilişkin belgeler temin edilmelidir.

Denetimin konusu bir BT projesi ise, denetlenecek projeye ilişkin her türlü hazırlık dokümanı, proje yönetimi ve görevlendirme belgeleri, incelemenin yapıldığı zamana kadar yapılan işlere ilişkin üretilen belgeler, projeye ilişkin varsa ihale dosyaları incelenmelidir.

Projeye ilişkin elde edilen bilgiler değerlendirilerek, projenin türü ve alt bileşenleri tespit edilmelidir. Bir proje içerdiği faaliyetlere göre birden fazla iş paketinden oluşabileceği gibi tek iş paketinden de oluşabilir. BT projesinin içeriği ve öngörülen faaliyetler incelenerek baskın özelliği açısından ne tür bir proje olduğu ve alt bileşenlerinin ne olduğu belirlenmelidir.

Proje dokümanlarının incelenmesi, fiili inceleme ve görüşmeler yapılması suretiyle proje ve alt bileşenlerinin bulundukları aşama da belirlenmelidir.

Bir proje kapsamında olması gereken fakat parçalara bölünmek suretiyle yürütülen işler proje kapsamında değerlendirilmelidir.

2.1.2 Risklerin Değerlendirilmesi

Kurum ve BS ile ilgili toplanan bilgiler kullanılarak risk değerlendirmesi yapılmalıdır.

Risk değerlendirmesi yapılırken denetlenen kamu idaresinin kurumsal ve BT risk yönetimi süreci de incelenmelidir.

Risk değerlendirmesi yapılma amacı, denetim riskini düşürmek ve denetim kapsamı belirlenirken hangi denetim/kontrol alanları ile hangi kontrol konularının seçileceğini ve hangi uygulamalara daha fazla odaklanılacağını tespit etmektir.

Denetim Riski: Denetçinin, yürüttüğü denetim faaliyetleri ve elde ettiği bulgulara dayanarak hatalı bir değerlendirmeye ya da sonuca ulaşması riskidir. Denetim riski, yapısal risk, kontrol riski ve tespit riskinin birleşiminden oluşur. Bu nedenle, risk değerlendirmesi yaparken denetçi bu riskleri birlikte değerlendirir.

Yapısal Riskler: Denetlenen kamu idaresinin ve BS'nin sahip olduğu özelliklerden kaynaklanan ve kontrol mekanizmalarından bağımsız olarak var olan risklerdir. Örneğin; denetlenen kamu idaresinin faaliyet gösterdiği alana ilişkin düzenlemelerin karmaşıklığı ve sıklıkla değişikliklere konu olması sistem geliştirme ve değişiklik yönetimi açısından, kullanılan bilişim sistemlerinin kritikliği iş sürekliliği yönetimi açısından, sahip olunan teknolojik altyapının karmaşıklığı BT işletimi açısından, internet üzerinden dışa açık hizmetler sunulması ise bilgi güvenliği açısından birer yapısal risk faktörü olarak değerlendirilebilir.

Kontrol Riski: Kontrollerin hataları/zararları önleyememe, tespit edememe ya da düzeltememe ihtimalidir. Bu bağlamda denetçi kurum tarafından tesis edilen kontrollerin güvenilirliğini/riski minimize etmeye uygun tasarlanmama ihtimalini bazı temel göstergeleri inceleyerek değerlendirir. Örneğin; yeterli belgeleme olgunluğuna sahip olunup olunmadığı, BT'ye ilişkin politikaların ve düzenlemelerin yeterli olup olmadığı, BT'ye ilişkin sorumlulukların uygun belirlenip belirlenmediği, uygun organizasyon yapılarının kurulup kurulmadığı, vb.

Tespit Riski ise, uygulanan denetim prosedürlerinin önemli hata ya da zararları tespit edememesidir. Örneğin; bir uygulama sistemindeki güvenlik ihlallerine ilişkin tespit riski yüksek olarak değerlendirilebilir çünkü denetim yürütüldüğü esnada denetlenen dönemin tamamına ilişkin işlem kayıtları denetçi tarafından elde edilip incelenemeyebilir. Öte yandan, denetlenen kurumun bir felaket kurtarma planının olup olmadığını belirlemeye ilişkin tespit riski ise, bir dokümanın var olup olmadığı kolaylıkla doğrulanabileceğinden, görece daha düşüktür. Denetçi, yapısal riskler ve kontrol risklerine ilişkin yaptığı değerlendirmeye dayanarak, denetim riskini en aza indirmek amacıyla denetim kaynaklarını ne şekilde planlayacağına ve hangi inceleme ve kanıt toplama yöntem ve tekniklerini kullanacağına bu çerçevede karar verir.

Denetim/Kontrol Alanları Bazında Risk Değerlendirmesi

Kurum ve BS'ye ilişkin yapısal riskler ve kontrol riskleri değerlendirilerek hangi denetim/kontrol alanlarında hangi kontrol konularının riskli olduğu belirlenir. Bunun için "EK-3: Denetim/Kontrol Alanları Bazında Risk Değerlendirme Formu" kullanılabilir. Formdaki "Alt Alan" ve "Konu" sütunlarının doldurulması için "EK-8: Önerilen Kontrol Değerlendirme Matrisleri"nden yararlanılır.

"Risk" sütununda, denetim/kontrol alanları bazında her bir kontrol konusu için bir risk düzeyi belirlenir. Risk düzeyi belirlenirken, ilgili konuda, sorumluluğun uygun şekilde belirlenip belirlenmediği, yeterli ve uygun organizasyonel yapıların oluşturulup oluşturulmadığı, gerekli düzenlemelerin yapılıp yapılmadığı ve yeterli ve uygun belgelemenin olup olmadığı gibi hususlar değerlendirilir.

"Denetlenebilirlik" sütununda, ilgili konunun denetim kapsamında incelenip incelenmeyeceği belirtilir. Konunun denetim kapsamına alınıp alınmayacağı kararı verilirken, risk düzeyinin yanında ilgili kontrolün, kontrol hedefini sağlama/riski düşürme etkisi açısından önemliliği de dikkate alınır. Önemli kontroller, riski düşük olarak belirlense bile denetim kapsamına alınabilir.

"Açıklama" sütununda ise, tespit edilen riskler yanında, denetçinin konuya ilişkin görüş ve notlarına da yer verilir. Örneğin, denetçi ilgili konunun incelenmesi sırasında uzman desteğine ihtiyaç duyup duymayacağını not alabilir.

Uygulamaların Seçiminde Risk Değerlendirmesi

Denetlenen kurum ve sistemde birden fazla uygulama varsa, hangi uygulamaların ayrıntılı inceleneceğinin belirlenmesi açısından da risk değerlendirmesi yapılır. Uygulamalar arasında risk derecelendirmesi yapılırken, denetlenen kurum ve sisteme ilişkin olarak "EK-2: Sistem Risk Değerlendirme Formu"ndan da yararlanılabilir. Bu durumda, uygulamaların kurum faaliyetleri açısından önemi, karmaşıklığı ve kritikliği seçim kriteri olarak kullanılabilir.

Düzenlilik denetimleri kapsamında yürütülen bilişim sistemleri denetimlerinde, denetimin odağında mali nitelikte bilgi üreten uygulamalar bulunduğundan, risk değerlendirmesi yapılırken, uygulamanın kurumun mali tablolarına olan etkisi temel seçim kriteri olarak kullanılır.

2.1.3 Uzman İhtiyacının Belirlenmesi

Risk değerlendirme sonuçlarına göre denetlenecek konular belirlenirken, ilgili konunun incelenmesi için teknik destek ve uzman çalıştırılmasına ihtiyaç olup olmadığı da değerlendirilir.

Denetimlerde, aşağıda belirtilen sebeplerle uzman çalıştırılmasına ihtiyaç duyulabilir:

- Bilişim sistemlerinin teknik ve karmaşık unsurlarının değerlendirilmesinde destek alma,

- Özel uzmanlık gerektiren alanlarda kurum dışı uzmanlık ve tecrübelerden yararlanma,
- Yeni yaklaşım ve farklı bakış açılarından yararlanma,
- Kurum dışında geliştirilmiş iyi uygulamaları denetimde kullanma,
- Denetim kanıtlarının, bulguların ve geliştirilen önerilerin kalitesini arttırma,
- Denetim süresinin sınırlı olması durumunda denetimi zamanında tamamlama.

Uzman desteği alınmasına karar verilmesi halinde, uzman çalıştırma şartları yazılı hale getirilerek aşağıdaki hususlara yer verilir:

- Çalışmanın amacı, kapsamı ve süresi,
- Özel çalışma yapılacak alanlar,
- Uzmanın hangi sistemlerde hangi bilgilere erişebileceği,
- Denetim ekibi ile uzmanın birlikte çalışma esasları ve iletişimin nasıl sağlanacağı,
- Denetlenen kurum ile uzman arasındaki ilişkilerin nasıl sağlanacağı,
- Denetlenen kurum bilgilerinin gizliliği ve uyulması gereken kurallar,
- Uzman tarafından kullanılacak metotlar,
- Uzman çalışmalarının sonuçlarının nasıl raporlanacağı.

Uzman çalıştırılırken, uzmanın çalışacağı alandaki yeterliliği değerlendirilmelidir. Uzmanın konusunda yetkin ve tecrübeli olmasına özen gösterilmelidir. Uzmanın çalıştırılacağı alanla ilgili uzmanlık sertifikalarının bulunup bulunmadığı ve daha önceki çalışmalarına ilişkin referansları incelenmelidir. Ayrıca uzmanın tarafsız olmasına ve denetlenen kurumla ve bu kurumla bağlantısı olan kuruluşlarla denetim açısından çıkar çatışmasına yol açabilecek herhangi bir ilişkisinin bulunmamasına dikkat edilmelidir.

Uzmanların yapacağı testler ve diğer çalışmalar denetçi refakatinde yerine getirilir.

Denetçi, uzman tarafından yapılan çalışmaları inceleyerek çalışma sonuçlarını değerlendirmelidir. Değerlendirme yapılırken aşağıdaki hususlar göz önünde bulundurulmalıdır:

- Çalışmanın uzman çalıştırmaya ilişkin şartnameye uygunluğu,
- Uzman tarafından kullanılan kaynak verilerin yeterliliği,
- Kullanılan metotların ve denetim kanıtlarının uygunluğu,
- Çalışma zamanlarının ve sürelerinin uygunluğu,

- Çalışma sonuçlarının ve bulguların diğer çalışmalara uygunluğu.

2.1.4 Denetim Amaçları ve Kapsamın Belirlenmesi

Kurum ve BS'nin tanınması ve risk değerlendirmesi sonrası denetim amaçlarında değişiklik olabilir. Bu durumda, tespit edilen risklere göre denetimin amaçları yeniden değerlendirilerek netleştirilmelidir.

Denetimlerde aşağıda belirtilenlerden biri veya birkaçı birden amaçlanabilir:

- Verilerin güvenilirliğine ilişkin güvence elde etmek için sistem kontrollerini değerlendirmek,
- BT yönetişimi ve yönetiminin veya belirli bir BT sisteminin/hizmetinin performansını değerlendirmek,
- Bilgi güvenliğini değerlendirmek,
- Bilişim mevzuatına uyumu değerlendirmek,
- Sistem geliştirme süreçlerini ve prosedürlerini değerlendirmek.

Denetim, kapsamında yürütülen denetim türüne göre farklı amaçlarla yapılabilir. Örnek olarak, düzenlilik denetimleri kapsamında yürütülen BS denetimlerinde temel amaç, BS'ye ilişkin iç kontrollerin güvenlik (gizlilik, bütünlük, erişilebilirlik), güvenilirlik ve mevzuata uygunluk açısından değerlendirilmesidir.

Risk değerlendirmesi ile birlikte, netleştirilen denetim amaçları, denetimde görevlendirilen denetçi sayısı ve inceleme yapılabilecek zaman gibi unsurlar da göz önüne alınarak denetimin kapsamı belirlenir.

Kapsam belirlenirken, denetlenen kuruma ve sistemlere özgü olarak, hangi denetim/kontrol alanlarında ve hangi kontrol konularında inceleme yapılacağı belirlenmelidir.

Bu rehberde denetim/kontrol alanları aşağıdaki şekilde sınıflandırılmıştır:

- BT Yönetişimi ve Yönetimi,
- Sistem Geliştirme ve Edinim,
- BT İşletimi,
- Dış Kaynak Kullanımı,
- İş Sürekliliği Yönetimi,
- Bilgi Güvenliği,
- Uygulama Kontrolleri.

Denetim/Kontrol alanlarının yukarıda belirtildiği şekilde sınıflandırılması zorunlu olmayıp denetimin yürütülmesini ve raporlanmasını kolaylaştırmak için önerilmiştir. Denetlenen kurumun ve BS'nin özelliğine ve risk değerlendirmesine göre bu alanlara yenileri eklenebilir, riskli görülmeyen alanlar denetim dışında bırakılabilir veya önemli görülen bir alt alan temel denetim/kontrol alanı olarak belirlenebilir. Bu aşamada denetim/kontrol alanları bazında risk değerlendirme sonuçlarına göre hangi kontrol konularında inceleme yapılacağı da belirlenir.

Denetlenmesine karar verilen sistemin birden fazla alt uygulamasının olması durumunda, denetimde görevlendirilen denetçi sayısı ve denetim için belirlenen süre de dikkate alınarak yapılan risk değerlendirmesine göre riski yüksek uygulamadan başlamak üzere hangi uygulamaların ayrıntılı inceleneceği belirlenir.

Ayrıca, denetlenen kurumun farklı mekânlarda kurulu olan ve işletilen bilişim altyapısı ve/veya sistemleri bulunuyorsa, hangi mekânlarda inceleme yapılacağı da belirlenmelidir.

2.1.5 Denetim Planının Hazırlanması

Kurumun ve BS'inin tanınması, risk değerlendirmesinin yapılması, kapsam ve uzman ihtiyacının belirlenmesi sonrasında denetimin nasıl yürütüleceğini gösteren denetim planı hazırlanır.

Denetim planı aşağıda belirtilen başlıkları içerecek şekilde oluşturulur:

- Kurum ve bilişim sistemleri hakkında bilgi,
- Denetimin amacı,
- Denetim metodolojisi,
- Risk değerlendirmesi,
- Kapsam,
- Denetim takvimi,
- Denetim ekibi ve çalıştırılacak uzmanlar.

Kurumu bilgilendirmek ve yapılacak denetimin sağlıklı yürütülmesi için gerekli hazırlıkların kurumca yapılmasını sağlamak amacıyla denetim planının kurumu ilgilendiren yönleri aşağıdaki bilgileri içerecek şekilde kurum yönetimi ile paylaşılır:

- Denetim sürecini gösteren tarihler,
- Denetimin amacı ve metodolojisi,
- İncelenecek kontrol alanları,
- İncelemeleri yapacak denetçiler ve uzmanlar,

- İnceleme yapılacak yerler,
- Erişim yetkileri,
- Yerinde yapılacak testlerin ve denetim çalışmalarının kurum faaliyetlerine olası etkileri.

2.1.6 Denetim Programlarının Hazırlanması

Denetçi, denetimin yürütülmesine geçmeden önce, yapılan risk değerlendirme sonuçlarına göre incelenmesine karar verilen denetim/kontrol alanları ve kontrol konularını nasıl inceleyeceğini belirlemelidir. Bunun için "EK-4: Denetim Programı Formu" kullanılarak kuruma özgü denetim programları hazırlanır.

Denetim programları, denetim/kontrol alanları bazında hazırlanır. Risk değerlendirme sonuçlarına göre, denetim/kontrol alanları bazında incelenmesine karar verilen kontrol konularının hangi sorular sorularak inceleneceği ve inceleme yöntemlerinin ne olacağının belirlenmesi için rehberin ekinde bulunan "EK-8: Önerilen Kontrol Değerlendirme Matrisleri"nde yer alan kontrol soruları ile inceleme yöntemlerinden yararlanılabilir. Önerilen inceleme yöntemleri denetçiyi sınırlayıcı olmayıp kontrollerinin değerlendirilmesi için asgari bir çerçeve sunmaktadır. Denetçi, kullanacağı inceleme ve kanıt toplama yöntem ve tekniklerini belirlerken tespit riskini dikkate almalıdır.

2.2 Denetimin Yürütülmesi

Planlama tamamlandıktan sonra denetim, hazırlanan denetim programlarına uygun şekilde kontrollerin ve bulguların değerlendirilmesi suretiyle yürütülür.

2.2.1 Kontrollerin Değerlendirilmesi

Kontrollerin değerlendirilmesi için denetim/kontrol alanları itibariyle oluşturulmuş olan denetim programlarına göre BT kontrolleri incelenir. Kontrollerinin değerlendirilmesi esnasında iç kontrol eksikliklerine veya zayıflıklarına ilişkin kanıt toplanır.

İnceleme esnasında kurumdan yazılı toplu bilgi alınması ihtiyacı olursa, her bir denetim/kontrol alanına ilişkin denetim programlarında yer alan kontrol sorularından kuruma sorulması uygun görülen soruları içeren "Kontrol Setleri" hazırlanarak ilgililerine verilebilir. Bu kontrol setleri, incelenecek konuları, kontrol sorularını ve kurum cevabını içerecek şekilde düzenlenir. Bu amaçla "EK-5: Kontrol Seti Formu" kullanılır.

Kurumdan alınan cevaplar ve kanıtlayıcı belgelerin incelenmesi sonrasında ilgili kontrollerin var olup olmadığına ilişkin denetçi değerlendirmesi, denetim esnasında elde edilen diğer bilgiler ile karşılaştırılmak -ve gerekli görülürse maddi doğrulama testleri yapılmak- suretiyle "EK-4: Denetim Programı Formu"nun "Denetçi Değerlendirmesi" sütununa yazılır.

Kontrol eksikliği olması durumunda, konu denetim bulgusu yapılmak üzere not edilir. Kontrolün var olduğu düşünülen durumlarda ise, ilgili kontrol etkinlik açısından değerlendirilir. Bunun için "Denetim Programı Formu"nda belirlenmiş olan "İnceleme Yöntemleri"

kullanılarak kontrolün tasarım ve işleyiş etkinliği incelenir. Kontrolün tasarım ve işleyiş etkinliğine ilişkin tespit edilen zayıflıklar da formun "Denetçi Değerlendirmesi" sütununa not edilir.

Kontrol eksiklik ve zayıflıkları belirlenirken kurum tarafından telafi edici kontrol mekanizmaları oluşturulup oluşturulmadığı dikkate alınmalıdır.

Denetim ekibi kontrolleri incelerken ihtiyaç duyduğunda bilgisayar destekli denetim tekniklerinden ve araçlarından (BDDTA) yararlanabilir.

BDDTA; en genel tanımıyla, denetim kanıtı toplamada bilgisayarların gücü ve hızından yararlanarak denetimin etkinliğini ve verimliliğini artırmaya olanak tanıyan bilgisayar tabanlı araç ve tekniklerdir.

Diğer denetim türlerinde olduğu gibi, BS denetiminde de, denetim ekibi BDDTA kullanmak konusunda planlama yaparken,

- Araç ve tekniklerin kullanılmasının fayda ve maliyetini analiz etmeli,
- Hangi araç ve tekniklerin kullanımında yetkinlik sahibi olduğunu göz önüne almalı,
- Hangi araç ve tekniklerin hangi amaçla ve ne zaman kullanılabileceğini belirlemeli,
- Kullanılmasına karar verilen araç ve tekniklerin güvenilir sonuçlar ürettiğine ve denetlenen kurumun sistemlerine zarar vermeyeceğine dair makul güvenceye sahip olmalıdır.

2.2.2 Bulguların Değerlendirilmesi

İncelemeler sonunda elde edilen bulgular, denetçi tarafından, yeterli kanıt toplanıp toplanmadığı açısından değerlendirilerek ek incelemeye ihtiyaç olup olmadığı belirlenmeli ve gerekli ek incelemeler yapılarak inceleme süreci tamamlanmalıdır.

Tespit edilen bulgular kriterlerine/referanslarına ve olası etkilerine ilişkin bilgileri de içerecek şekilde düzenlenir. Bunun için "EK-6: Bulgu Formatı" kullanılır.

Bulgunun;

Bulgu başlığı kısmında, tespit edilen kontrol zafiyeti öz bir şekilde tanımlanır.

Kriter/Referans kısmında, olması gereken kontrol tanımlanır ve/veya ilgili mevzuat, standart, çerçeve belge ya da iyi uygulama örneğine (adı ve gerek görülürse ilgili kısmın metni alınarak) atıf yapılır.

Açıklama kısmında, kontrol zafiyetine ilişkin tespitler belirtilir.

Etki kısmında, kontrol zafiyetinin olası etkileri belirtilir.

Raporda önemli görülen bulgulara yer verilir.

Kontrollerin değerlendirilmesi sırasında, riskin gerçekleştiği ve zararın oluştuğunun tespit edilmesi durumunda bu zararlar değerlendirilir. Kamu zararı tespiti varsa, yargılamaya esas raporlama süreci işletilir. Kamu zararı söz konusu olmayan diğer zarar tespitlerine ise, ilgili olduğu kontrol zafiyeti için düzenlenen bulgu içinde yer verilir. Örneğin, gerçekleşmiş yetkisiz veri değişikliği, veri kaybı, vb.

2.3 Denetim Sonuçlarının Raporlanması ve İzlenmesi

Denetim sonuçlarının raporlanma şekli, denetimin kapsamında yürütüldüğü denetim türüne göre farklılık gösterebilir. Denetim, düzenlilik veya performans denetimi kapsamında yürütülüyorsa, denetim sonuçlarına ilgili olduğu denetim türünde belirlenmiş süreç izlenerek ilgili olduğu denetim raporunun içinde yer verilebilir.

Denetim, konu bazlı denetim kapsamında yürütülüyorsa bağımsız denetim raporu hazırlanır.

Denetim raporu tam, güvenilir, objektif, yeterli kanıta dayalı, açık, öz ve anlaşılır olmalıdır.

Raporun tam olması, denetimden beklenen amaçların tamamının raporda yer alması, raporda yer verilmeyen hususlara ilişkin olarak objektif kriterlere dayalı açıklamaların yapılmasıdır.

Raporun güvenilir olması, raporda yer alan bulguların yeterli ve ispat edilebilir kanıtlara dayalı olmasını ve raporun tam olmasını gerektirir.

Raporun objektif olması, denetim sonucu elde edilen bulguların tarafsız bir şekilde rapora yansıtılmasıdır. Raporda denetimin tarafsızlığını zedeleyebilecek savunucu ve/veya suçlayıcı ifadelerden kaçınılmalıdır.

Raporun yeterli kanıta dayalı olması, denetim sonunda elde edilen bulgu ve sonuçların yeterli sayıda ve ikna edici nitelikte olmasıdır.

Raporunun açık, öz ve anlaşılır olması, yazılacak ifadelerin sade ve kısa olmasını, gereksiz detay ve tekrarlardan, teknik terim ve kısaltmalardan kaçınılmasını gerektirir. Teknik terimlerin veya kısaltmaların kullanılmasının gerekli olduğu durumlarda bu terimler ayrıca açıklanır ve kullanılan kısaltmalara ilişkin bilgilere raporda ayrı bir bölümde yer verilir.

Denetim sonuçlarının raporlanması, taslak raporun hazırlanması, kurum görüşünün alınması, nihai raporun yazılması ve ilgililere sunulması süreçlerinden oluşur.

2.3.1 Taslak Raporun Hazırlanması

Denetim sonuçlarının değerlendirileceği taslak rapor, aşağıda belirtilen bölümlerden oluşacak şekilde hazırlanır:

- Kurum ve bilişim sistemleri hakkında bilgi,
- Denetimin dayanağı, amacı, kapsamı ve metodu,

- Denetim bulguları,
- Ekler.

Taslak raporun kapağında Sayıştay Başkanlığı ibaresi, denetlenen kurumun ve/veya sistemin adı, raporun bilişim sistemleri denetim raporu olduğuna ilişkin ibare ve rapor tarihi yer alır.

Kurum ve bilişim sistemleri hakkında bilgi verilirken, kurumun görevleri, ana faaliyetleri ve birimlerine ilişkin açıklamalardan sonra, bilişim sistemlerinin amacı, diğer sistemlerle etkileşimi ve dış kaynak kullanımı söz konusu ise buna ilişkin kısa açıklamalar yapılabilir.

Denetimin dayanağı, amacı, kapsamı ve metodu başlığı altında; yapılan denetimin dayanağı, amacı, denetimin hangi kontrol alanlarında, uygulamalarda ve lokasyonlarda yürütüldüğü, temel denetim yaklaşımının ne olduğu, denetim süreci ve denetimin yürütülmesinde kullanılan metotlar konusunda bilgi verilebilir.

Denetim bulguları bölümünde, her bir kontrol alanı bir başlık oluşturacak şekilde belirlenen önemli bulgulara yer verilir.

Ekler bölümünde ise, varsa gerekli görülen tablolara ve bulguların nasıl elde edildiğine ilişkin detay bilgilere yer verilir.

Taslak rapor, yazımı tamamlanınca, denetim ekibi dışında görevlendirilen başka bir ekip (Değerlendirme Komisyonu) tarafından değerlendirilir.

Denetim ekibi, Değerlendirme Komisyonu görüşlerini dikkate alarak taslak rapora son halini verir.

2.3.2 Kurum Görüşünün Alınması

Hazırlanan taslak rapor, denetlenen kurum yönetimine gönderilerek belirli bir süre içinde görüşlerini yazılı bir şekilde sunmaları istenir. Kurum görüşü alınırken, raporda yer alan bulgulara ilişkin olarak kurum tarafından yapılan veya gelecekte yapılması planlanan çözüm çalışmalarının da muhtemel tarihleri ile birlikte bildirilmesi istenir.

Gerekli görülmesi durumunda, kurum üst yönetimi ile değerlendirme toplantısı düzenlenebilir.

2.3.3 Nihai Raporun Yazılması

Kurumun yazılı görüşleri dikkate alınarak rapora son şekli verilir.

Denetçi, denetlenen kurumun görüşlerini haklı bulması halinde, raporda gerekli düzeltmeleri yapar.

Denetlenen kurum herhangi bir nedenle taslak raporla ilgili görüş bildirmediği takdirde, bu durum nihai raporda belirtilir.

Nihai rapor, aşağıda belirtilen bölümlerden oluşacak şekilde yeniden düzenlenir:

- Kurum ve bilişim sistemleri hakkında bilgi,
- Denetimin dayanağı, amacı, kapsamı ve metodu,
- Genel değerlendirme,
- Denetim bulguları,
- Ekler.

Nihai raporda, raporun başına, "sunuş" ve "özet" bölümleri eklenebilir.

Özet bölümünde, raporun tümünü okuyamayacak ilgililere, rapor içeriği ve denetim sonuçları kısa ve öz bir şekilde açıklanır.

Nihai rapora, taslak raporda yer almayan "genel değerlendirme" bölümü eklenir.

Genel değerlendirme bölümünde, tespit edilen kontrol zafiyetlerine ilişkin genel değerlendirmeler yapılır.

Denetim bulguları bölümünde, her bir bulguya, o bulguya ilişkin "çözüm çalışmaları" ve "öneri" kısımları eklenebilir.

Çözüm çalışmaları kısmında, bulgu konusu edilen kontrol zafiyetlerinin çözümü ile ilgili olarak, kurum tarafından taslak rapora verilen görüşte belirtilen ve yapıldığı ya da yapılacağı ifade edilen çalışmalara yer verilir.

Öneri kısmında, taslak rapora ilişkin kurum görüşleri içinde bulgulara ilişkin kurum itirazı varsa ve haklı bulunmuyorsa, itirazı karşılayacak şekilde gerekli açıklamalar yapılarak ihtiyaç görülürse öneri sunulur.

2.3.4 Raporun İlgililere Sunulması / Gönderilmesi

Nihai rapor, yazımı tamamlanınca gereği yapılmak üzere Başkanlığa sunulur.

Rapor, Başkanlık tarafından kalite kontrol süreçlerinden geçtikten sonra ilgililerine sunulur/gönderilir.

Rapor, gizlilik gerektiren bilgi içeriyorsa, yazışma ve raporlama süreçlerinde gizlilik esaslarına dikkat edilir. Denetlenen kurum dışındaki ilgililere gizliliği ihlal etmeyecek şekilde sunulabilir/gönderilebilir.

2.3.5 İzleme

Denetim raporunda tespit edilen hususlar ve getirilen öneriler konusunda kurum tarafından yapılan çalışmalar izlenir.

Çözüm için kurum tarafından verilmiş bir tarih varsa bunu da gösterecek şekilde bir izleme tablosu hazırlanır.

Bunun için “EK-7: İzleme Tablosu Formu” kullanılır.

İzleme çalışmasının zamanı ve yöntemi (izleme anketi veya izleme denetimi) ayrıca planlanır.

İzleme yapılırken, denetim bulgularına ilişkin kurum tarafından yapılan çalışmalar değerlendirilir.

İzleme faaliyeti sonrası ileri bir tarihte yeni bir izleme yapılması veya denetim yapılması konusunda karar verilir.

ÜÇÜNCÜ BÖLÜM
DENETİM/KONTROL ALANLARI

3.1. BT Yönetişimi ve Yönetimi

3.1.1. Kavramlar

BT Yönetişimi: Kurumsal yönetişimin bütünleyici bir parçası olmakla birlikte BT hedeflerinin, stratejik iş hedefleriyle uyumlu bir şekilde belirlenerek BT faaliyetlerinin kurum amaçları doğrultusunda ve kurumun ihtiyaçlarını karşılayacak, değer yaratacak şekilde yürütülmesini ifade eder. Bu yaklaşım çerçevesinde bütün paydaşların karar alma sürecine katkısı öngörülmekte, risk optimizasyonu gözetilerek kaynakların etkin ve etkili kullanımı ile kurumun belirlenen amaçlarına ulaşması, aynı zamanda değişen çevre ve teknoloji koşullarına göre geleceğe ilişkin ihtiyaçların belirlenerek büyüme planlaması yapılması hedeflenmektedir.

BT yönetişimini sağlamak kurum üst yönetiminin sorumluluğudur. Üst yönetim bu sorumluluğu yerine getirirken BT yönlendirme kurulu ya da eşdeğeri yapılardan faydalanır.

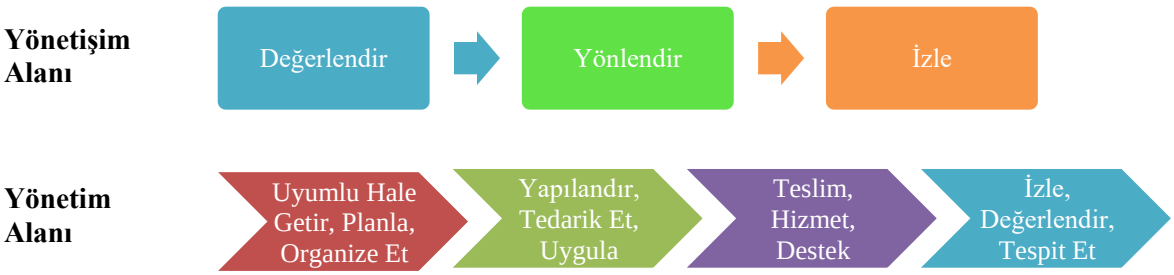
Yönetişim ve yönetim, birbirinden farklı etki alanlarına sahip süreçlerdir.

BT Yönetişimi;

- Kurumun mevcut ve gelecekteki BT kullanımına yön vermek maksadıyla paydaş ihtiyaçlarının, koşulların ve seçeneklerin değerlendirilmesini,
- Bu değerlendirmeler sonucunda amaç ve hedeflerin, belirli kriterlere göre önceliklendirilmesini; iş hedeflerini karşılayan bir BT kullanımını sağlamak için gerekli plan ve politikaların hazırlanarak hayata geçirilmesinin yönetilmesini,
- Gerçekleştirilen performansın, önceden belirlenen amaç ve hedeflerle karşılaştırılarak izlenmesini

sağlar.

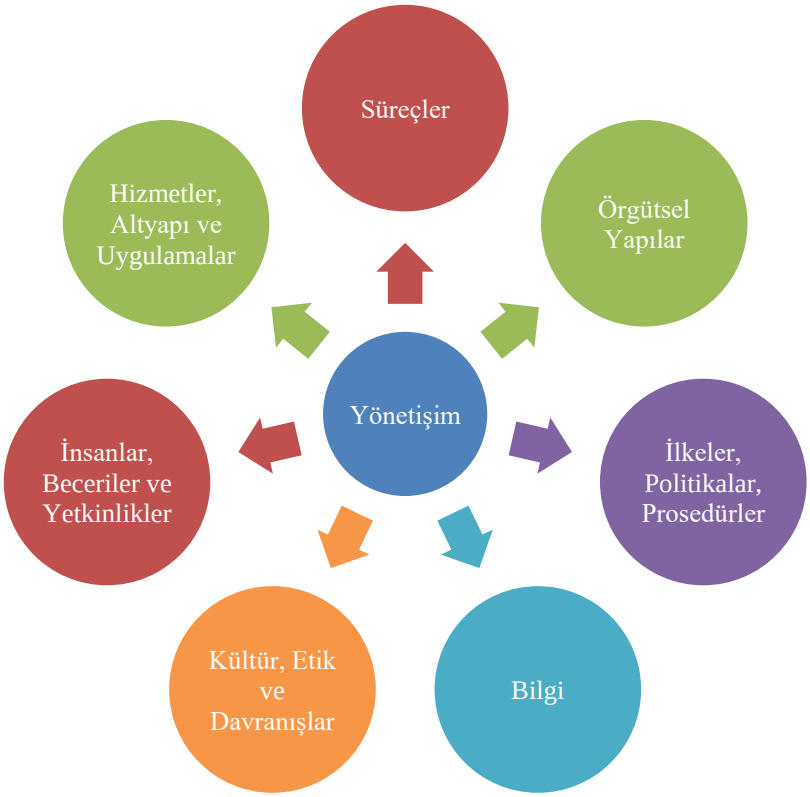
BT Yönetimi ise kurumsal hedeflere ulaşmak için yönetişim organının belirlediği doğrultuda planlama yapar, faaliyetler geliştirir, bu faaliyetleri yürütür ve izler.



Şekil 2: BT Yönetişimi ve Yönetimi Etki Alanı
Kaynak: COBIT 2019 Çerçevesi: Yönetişim ve Yönetim Hedefleri

BT Yönetişimi Bileşenleri

İyi ve düzgün işleyen bir yönetişim sistemi kurmak ve sürdürmek için gerekli bileşenler şunlardır:



Şekil 3: BT Yönetişimi Bileşenleri
Kaynak: COBIT 2019 Çerçevesi: Yönetişim ve Yönetim Hedefleri

- **Süreçler:** Belirli hedeflere ulaşmak için organize edilen uygulama ve faaliyetler dizisini tanımlar ve BT'ye ilişkin amaçların gerçekleştirilmesini destekleyen bir dizi çıktı üretirler.
- **Örgütsel Yapılar:** Bir kurumdaki kilit karar alma yapılarıdır. Kaynak dağılımı, yatırım kararları veya BT projelerinin önceliklendirilmesine ilişkin kararlar üst yönetim ve BT Yönlendirme Kurulu gibi örgütsel yapılar aracılığıyla alınır. BT, İç Denetim, Risk Yönetimi gibi birimler/yapılar ise nihai karar alıcılara, karar alma sürecinde kullanacakları bilginin aktarımını gerçekleştirir. Bu bağlamda her birim/yapının görev, yetki ve sorumluluklarının tanımının yapılması; yetki devrine ilişkin şartların belirlenmesi önemlidir.
- **İlkeler, Politikalar ve Prosedürler:** Günlük yönetim faaliyetlerine rehberlik etmesi için oluşturulan araçlardır.
- **Bilgi:** Kurum tarafından üretilen ve kullanılan tüm bilgileri içerir. Bilgi; insanları, iş süreçlerini, örgütsel yapıları, kurum içinde ve dışında yer almakla birlikte değer yaratma sürecinde rol oynayan her şeyi birbirine bağlayan anahtar bir unsurdur.

Dolayısıyla iyi bir yönetişim sistemi, kurum içinde düzgün bir bilgi akışının sağlanması ile mümkündür.

- **Kültür, Etik ve Davranışlar:** Bir kurumdaki BT yönetişimi ve yönetimi faaliyetlerinin yürütülmesinde dikkate alınması gereken bireysel ve kolektif davranışlar bütünüdür.

- **İnsan, Beceriler ve Yetkinlikler:** İnsan kaynağı bir kurumun sahip olduğu en önemli varlıktır. İyi kurumsal kararlar alınması, düzeltici faaliyetlerin yürütülmesi ve tüm faaliyetlerin başarılı bir şekilde tamamlanmasını, gerek teknik gerekse davranışsal anlamda yeterli donanıma sahip insan kaynağı mümkün kılmaktadır.

- **Hizmetler, Altyapı ve Uygulamalar:** Kuruma, faaliyetlerini yürütmede ihtiyaç duyduğu bilgiyi işleme imkânı sağlayan teknolojilerdir. Yetersiz BT, kurumu istenmeyen risklere maruz bırakabildiği gibi iş performansı üzerinde negatif bir etki de yaratabilir. İyi altyapı, hizmet ve uygulamalar ise kuruma iş yetkinliğini geliştirme imkânı sağlar.

3.1.2. Riskler

Kurumda etkin bir BT yönetişimi ve yönetimi sağlanmaması halinde karşılaşılabilecek başlıca riskler aşağıda yer almaktadır:

- Üst yönetimin, kurumun bilişim sistemlerine ilişkin alınacak önemli kararlarda etkin bir rol alamaması,

- Sorumluluklarda karmaşa, aşırı yetki verme veya hiç yetki vermeme durumlarının oluşması,

- Görevler ayrılığı ilkesine aykırı durumların ortaya çıkması,

- Kurum tarafından belirlenen politikaların ve prosedürlerin anlaşılmaması veya kabul görmemesi,

- Bilişim sistemlerinin kurumun iş gereklerini karşılamaması,

- İş önceliklerinin doğru tanımlanamaması ve kaynakların yanlış tahsis edilmesi,

- Kurum hedefleri ve ihtiyaçları göz önünde bulundurulmadan üstlenilen BT projelerinin başarısızlığa uğraması,

- Hesap verilebilirlik ve şeffaflık ilkelerinin ihlali,

- Mevzuat ve düzenlemelere uyum sorunu,

- Mevzuata uymama sonucu kurumun karşılaşacağı maddi yaptırımlar ve cezalar,

- Suç teşkil eden fiillerin ortaya çıkması,

- Tehditlerin zamanında belirlenememesi, etkilerinin ölçülememesi ve riskin yönetilememesi,
- BT'ye ilişkin mevcut ve geleceğe dair insan kaynakları ve diğer ihtiyaçların uygun şekilde belirlenememesi.

3.1.3. Kontroller

BT yönetişimi ve yönetimi ile ilgili riskleri minimize etmek için olması gereken kontrollerin (kriterlerin) başlıcaları şunlardır:

BT İhtiyaçlarının Belirlenmesi, Yönlendirilmesi ve İzlenmesi

- Kurumun gelişen iş ve BT ihtiyaçlarını belirlemeye yönelik tanımlı bir süreci bulunmalı ve üst yönetim bu ihtiyaçları onaylarken yeterli bilgiye sahip olmalıdır.
- İş ve BT hedefleri için performans ölçütleri oluşturularak BT Yönlendirme Kurulu veya eşdeğer yapıların periyodik olarak gözden geçirme toplantıları yoluyla gerekli önlemleri alması sağlanmalı; üst yönetime anahtar performans ölçütlerinin mevcut durumu hakkında bilgi verecek bir raporlama sistemi oluşturulmalıdır.
- Kurum BT yatırım yönetimine ilişkin süreç ve prosedürlere sahip olmalı; projeler analizler çerçevesinde değerlendirilerek periyodik gözden geçirmeler neticesinde yatırım yönetiminin etkinliği değerlendirilmelidir.

BT Stratejisi ve Planlama

- Kurumun, iş hedefleri doğrultusunda BT amaç ve ihtiyaçlarına yer veren ve iş ihtiyaçlarına cevap verecek BT kaynaklarının tanımlandığı, periyodik olarak gözden geçirilen ve güncellenen bir BT stratejik planı olmalıdır.
- Kurumun risk yönetimine ilişkin bir politika ve planı olmalı, risklerin belirlenmesi ve yönetilmesi için gerekli kaynaklar tahsis edilmelidir. BT risklerinin yönetimi için genel risk değerlendirmesi ve stratejik planlarla uyumlu yönetişim süreçleri mevcut olmalıdır.

Organizasyon, Standart, Politika ve Prosedürler

- Kurumdaki BT yapılanması, organizasyon içinde mümkün olduğunca üst düzeyde olmalı, roller ve sorumluluklar açıkça tanımlanmalıdır.
- Kurum, iş ve BT faaliyetlerine rehberlik etmesi için uygun politika ve prosedürleri yazılı olarak belirlemeli ve ilgililerini bu konuda bilgilendirmelidir.

İnsan Kaynakları ve Eğitim

- Kurum, iş ihtiyaçları doğrultusunda, mevcut ve gelecekteki insan kaynakları ihtiyaçlarını karşılamak için bir plana sahip olmalıdır.

Uygunluk

- Kurum, belirlenmiş bütün politika ve prosedürlerin izlenmesini sağlayacak iç denetim, kalite kontrol gibi mekanizmalara sahip olmalıdır.

Bu alana ilişkin kontrollerin değerlendirilmesi için önerilen, alt alanlara ilişkin denetim hedefleri ile referansların yer aldığı, kontrol konuları bazında ilgili kriterleri, kontrol sorularını ve inceleme yöntemlerini de içeren matris (EK-8.1: BT Yönetişimi ve Yönetimi Önerilen Kontrol Değerlendirme Matrisi) ekte yer almaktadır.

3.2. Sistem Geliştirme ve Edinim

3.2.1. Kavramlar

Sistem Geliştirme: Bir kurumun, stratejik ve operasyonel hedeflerine yönelik ihtiyaçlarını karşılaması düşünülen bilgi sistemlerini ortaya çıkarmak için gerçekleştirdiği faaliyetler bütünü şeklinde tanımlanabilir. Geniş anlamıyla ele alındığında, yeni bir sistemin geliştirilmesi ya da edinimi yanında, mevcut sistemler üzerinde gerçekleştirilen ekleme ve iyileştirme faaliyetleri de sistem geliştirme kapsamında değerlendirilir.

Sistem Geliştirme Yaşam Döngüsü (SGYD): En genel haliyle, bir bilgi sisteminin geliştirilmesi veya ediniminde gerçekleştirilen aşamalardır. Daha geniş bir tanıma göre ise SGYD; bir bilgi sistemini planlamak, tasarlamak, geliştirmek, test etmek ve devreye almak veya mevcut bir bilgi sistemine ekleme ve değişiklikler yapmak için takip edilen safhalardır.

Farklı sistem geliştirme yaklaşımları olmakla birlikte, SGYD'nin bütün yaklaşımlarda yer alan ortak aşamaları -aşağıdaki şekilde de yer aldığı üzere- gereksinimlerin geliştirilmesi, tasarım-kodlama, edinim-yapılandırma, test, kurulum ve kurulum sonrası çalışmalardır.

Şekil 4: Sistem Geliştirme ve Edinim Aşamaları

- **Gereksinimlerin Geliştirilmesi:** Geliştirilecek/edinilecek sisteme ilişkin taleplerin belirlendiği, değerlendirildiği ve önceliklendirildiği aşamadır. Gereksinimlerin geliştirilmesinde kullanıcıların sürece etkin katılımı önemli bir gerekliliktir.

  Toplanan gereksinimler çerçevesinde takip eden aşamalara temel oluşturacak değerlendirmeler gerçekleştirilir. Bu kapsamda; talep edilen sistemin sahip olması gereken özellikler ve sağlayacağı (parasal veya operasyonel) kazanımlar ortaya konur, maliyet ve süre tahmini yapılır, riskler öngörülür ve sistemin ortaya çıkarılmasına uygun yöntemler belirlenir.

- **Tasarım:** Yüksek derecede özelleştirme veya ekstra otomasyon ihtiyacı nedeniyle kuruma özel bir sistem geliştirilmesine karar verildiğinde, sistemin iç tasarımının ayrıntılı özelliklerinin oluşturulduğu aşamadır. Toplanmış ve değerlendirilmiş olan gereksinimler çerçevesinde program ara yüzleri tanımlanır, veri tabanı özellikleri oluşturulur, iş akış şemaları üzerinden sistemin takip edeceği iş mantığı hazırlanır.

- **Kodlama:** Bu aşamasında programcılar, geliştirilmekte olan bilgisayar programının kodunu yazarlar. Sistem tasarımı fazında oluşturulan dokümanlar (tasarım özellikleri, akış şemaları, vs.) kodlamanın yapıldığı geliştirme aşaması için temel oluşturur.

- **Edinim:** Gereksinimlerin değerlendirilmesi sonucunda kuruma özel bir sistem geliştirilmesi yerine ticari bir ürünün satın alınmasına karar verildiğinde, ihtiyaca yanıt verecek çözümün en uygun koşullarda temin edilmesine yönelik satın alma sürecinin işletildiği aşamadır. Bu kapsamda genellikle birkaç prototip kurulur ve ürünlerin beklendiği gibi birlikte çalışıp çalışmadığı satın almadan önce test edilir.

- **Yapılandırma:** Bu aşamasında piyasadan temin edilen ticari ürün kurum ihtiyaçlarına en iyi yanıtı verecek şekilde konfigüre edilir.

- **Test ve Kurulum:** Bu aşamasında, geliştirme veya edinim yoluyla meydana getirilen sistemin unsurları (donanım, işletim sistemi, aygıt sürücüleri, yardımcı programlar, uygulama yazılımı, vb.) yüklenir ve işlerliği test edilir. Son kullanıcı kabul testi bu aşamada gerçekleştirilir.

- **Kurulum Sonrası Çalışmalar:** geliştirilen sistemin, kullanılmaya başlandıktan sonra, başlangıçtaki amaçları yerine getirmedeki etkinliği yönünden gözden geçirildiği ve eksikliklerin tespit edildiği aşamadır. Kullanıcı memnuniyetinin ölçülmesine yönelik çalışmalar bu aşamada gerçekleştirilir.

Sistem geliştirme ve edinim faaliyetlerinin planlanması ve ilgili risklerin yönetilmesi temel bir gerekliliktir. Bu bağlamda, anılan faaliyetlerin proje yönetimi yaklaşımıyla etkin ve kontrollü bir çerçevede planlanması ve gerçekleştirilmesi gerekir.

Proje: Genel kabul görmüş tanıma göre; özgün bir ürün, hizmet ya da sonuç yaratmak için yürütülen geçici girişimdir (PMI-PMBOK Kılavuzu Beşinci Baskı). Bir başka tanıma göre ise; bir ekibin, başlangıcı ve bitişi belirli bir süre ve sınırlı bir bütçe dâhilinde, birtakım

kaynaklar kullanarak, kullanıcı memnuniyetini ve kaliteyi göz önünde bulundururken, olası riskleri yönetmek şartıyla, tanımlanmış bir kapsama uygun amaç ve hedefler doğrultusunda özgün bir planı başlatma, yürütme, kontrol etme ve sonuca bağlama sürecidir.

Proje "özgün" ve "geçici" olma yönüyle operasyondan ayrılır. Örneğin "denetim yönetimi" sürekliliği olan operasyonel bir faaliyet iken; "yeni bir denetim yönetimi sistemini devreye almak" bir projedir. Denetim yönetimi yazılımı faaliyete geçtikten sonraki (rutin) süreç operasyon olarak adlandırılır.

Proje Yönetimi: Bilgilerin, becerilerin, araçların ve tekniklerin projenin gereksinimlerini yerine getirmek amacıyla proje aktivitelerine uygulanmasıdır (PMI-PMBOK Kılavuzu Beşinci Baskı). Başka bir ifadeyle proje yönetimi; proje hedeflerinin başarıyla gerçekleştirilmesi için projenin kapsam, zaman, maliyet, kalite, insan kaynağı, iletişim, risk, satın alma süreçleri ve paydaşlarının uygun yöntem ve teknikler kullanılarak yönetilmesidir.

3.2.2. Riskler

Kurumda sistem geliştirme ve edinim süreçlerinin etkin şekilde yürütülememesi durumunda karşılaşılabilecek temel riskler şunlardır:

- Sistem geliştirme ve edinim faaliyetlerinin öngörülen kapsamda, planlanan takvimde ve belirlenen bütçede tamamlanamaması
- Geliştirilen/edinilen sistemin iş ihtiyaçlarını ve kullanıcı beklentilerini karşılayamaması
- Eksiklikleri/hataları olan sistemlerin devreye alınması
- Geliştirilen/edinilen sistemin kurumun BT ortamı ile uyumsuzluk göstermesi
- Geliştirilen/edinilen sistemin işletiminin/kullanılabilirliğinin kurum tarafından sürdürülememesi
- Geliştirilen/edinilen sistemin güvenlik zafiyetleri taşıması
- Geliştirilen/edinilen sisteme aktarılan verinin bütünlüğünün bozulması

3.2.3. Kontroller

Sistem geliştirme ve edinim ile ilgili riskleri minimize etmek için olması gereken kontrollerin (kriterlerin) başlıcaları şunlardır:

Gereksinimlerin Geliştirilmesi ve Yönetimi

- Kurumun yeni BT sistemlerine ya da ek işlevlere yönelik gereksinimleri toplama, inceleme ve gruplandırma süreçleri tanımlı olmalıdır.

- İş ve kullanıcı ihtiyaçlarının en doğru ve maliyet etkin şekilde karşılanması amacıyla geliştirilecek/edinilecek sisteme ilişkin gereksinimler belgelendirilmeli, analiz edilmeli ve izlenmelidir.

Proje Yönetimi ve Kontrolü

- Onaylanmış her sistem geliştirme ve edinim projesinin yürütülmesine rehberlik edecek bir proje yönetim planı (veya dengi bir düzenleme) bulunmalıdır.
- Projeler maliyet, zaman ve performans gerekliliklerine uygunluk açısından izlenmeli ve kontrol edilmelidir.

Uygulama Geliştirme

- Tasarım dokümanları geliştirilerek sistemin tüm boyutlarıyla ele alınması sağlanmalı, bilgi güvenliği ve birlikte çalışabilirlik hususları göz önüne alınmalıdır.
- Kodlama işlemleri belirli prosedürler çerçevesinde güvenli yazılım geliştirme kurallarına uygun şekilde gerçekleştirilmelidir.

Uygulama Edinim (Tedarik)

- Tedarik faaliyetleri (ihtiyaç/talep dokümanlarının ve şartnamelerin hazırlanması, tekliflerin alınması ve değerlendirilmesi, yüklenicinin seçimi, sözleşmenin imzalanması, vb.) yürürlükteki mevzuata ve Kurumun bu alandaki düzenlemelerine uygun şekilde gerçekleştirilmelidir.
- Yüklenicilerin seçiminde tarafsız olunmalı ve önceden belirlenmiş olan kriterler kullanılmalıdır.

Kalite Güvence ve Test

- Sistem geliştirme ve edinime ilişkin kalite güvence faaliyetleri rolleri ve sorumlulukları belirlenmiş bir birim/ekip tarafından ve tanımlanmış olan süreç ve prosedürlere göre yürütülmelidir.
- Geliştirilen ve edinilen sistemler üzerinde gerçekleştirilecek testler planlanmalı, planlandığı şekilde uygulanmalı ve sistem, test sonuçlarına göre kabul veya reddedilmelidir.

Kurulum ve Değişiklikler

- Geliştirilen/edinilen sistemler belgelendirilmeli, kurulumuna ve yapılandırılmasına yönelik gereklilikler tanımlanarak uygulanmalıdır.
- Geliştirilen/edinilen sistem uygulamaya alındıktan sonra izlenmeli ve değerlendirilmelidir.

- Geliştirilen/edinilen sistemlerde/uygulamalarda yalnızca yetkilendirilmiş ve onaylanan değişikliklerin gerçekleştirilmesi sağlanmalı ve gerçekleştirilen değişikliklerin kaydı tutulmalıdır.

Bu alana ilişkin kontrollerin değerlendirilmesi için önerilen, alt alanlara ilişkin denetim hedefleri ile referansların yer aldığı, kontrol konuları bazında ilgili kriterleri, kontrol sorularını ve inceleme yöntemlerini de içeren matris (EK-8.2: Sistem Geliştirme ve Edinim Önerilen Kontrol Değerlendirme Matrisi) ekte yer almaktadır.

3.3. BT İşletimi

3.3.1. Kavramlar

BT İşletimi: Kurumun sahip olduğu BT varlıklarının ve sunduğu BT hizmetlerinin sağlıklı bir şekilde çalışmasını teminen gerçekleştirdiği faaliyetler bütünüdür.

Bu kapsamda BT hizmetlerinin planlanması, değişikliği öngörülen hizmetlerin önceden belirlenen çerçevede ve kontrollü bir biçimde devreye alınması, hizmet kalitesinin sürekli iyileştirilmesi, BT hizmetlerinin yönetimi faaliyetleri gerçekleştirilir.

Hizmet seviyesi yönetimi, kapasite yönetimi, olay ve problem yönetimi ile değişiklik yönetimi BT işletiminin temel unsurlarını oluşturmaktadırlar.

Hizmet Seviyesi Yönetimi: BT hizmetlerinin ihtiyaçlar doğrultusunda ve üzerinde uzlaşılan şartlar çerçevesinde temin edilmesini sağlamak üzere Hizmet Seviyesi Anlaşmaları (HSA) düzenlenmektedir. Hizmet Seviyesi Yönetimi ise BT hizmetlerini sunan birim ile hizmetlerden faydalanan birimler arasında koordinasyonun sağlanarak hizmetin HSA'larda belirlenen koşullar ve hedefler doğrultusunda yürütülmesini sağlayan bir süreçtir.

Şekil 5: Hizmet Seviyesi Yönetimi Akışı
Kaynak: TÜBİTAK İşletim ve Bakım Rehberi

- **Hizmet Seviyesi Anlaşmalarının Oluşturulması:** BT hizmetlerini sunan birim ile hizmetlerden faydalanan birimler arasında kullanım ihtiyaçlarının, bu ihtiyaçlara uygun hedeflerin ve karşılıklı sorumlulukların belirlenebilmesi için görüşmeler

yapılır. Bu görüşmeler sonucunda, üzerinde uzlaşma sağlanan şartlar ve hedefler HSA'lar düzenlenerek yazılı hale getirilir.

- **Hizmetlerin İzlenmesi ve Raporlanması:** BT hizmetlerinin HSA'lar çerçevesinde yürütülüp yürütülmediği izlenerek belirli aralıklarla, o zamana kadar sergilenen hizmetin ve mevcut durumun analizini, geleceğe yönelik karar almayı kolaylaştıracak bilgileri içeren raporlar düzenlenir.

- **Hizmetlerin Gözden Geçirilmesi ve Değerlendirilmesi:** Söz konusu raporlar değerlendirilerek BT hizmetlerinin istenilen seviyede sürdürülmesi, sapmaların olduğu hallerde ise yapılması gereken faaliyetlerin planlanması amacıyla BT hizmetini sunan birim ile ihtiyaç duyulan sıklıkta gözden geçirme toplantıları düzenlenir.

- **Hizmet Seviyesi Anlaşmalarının Gözden Geçirilmesi:** Zaman içerisinde koşulların ve hizmete ilişkin beklentilerin değişiklik gösterebilmesi nedeniyle, belirli dönemlerde BT hizmetini sunan birim ile bu değişen koşulların, beklentilerin değerlendirmesinin yapıldığı, HSA'ların gözden geçirildiği toplantılar düzenlenir. Bu toplantılar neticesinde hedef güncellemesi yapılabilir; geçerliliği kalmamış hedefler kaldırılabilir veya yeni hedef eklenebilir.

Kapasite Yönetimi: Mevcut kapasite ve performans verilerinin analiz edilmesi, işin gereklilikleri ve kullanıcıların talepleri göz önünde bulundurulmak suretiyle BT hizmetleri için gerekli kaynak kapasitesinin tahmin edilmesi, planlanması, sonuçların izlenmesi ve raporlanması faaliyetlerini içerir. Kapasite planı, BT hizmetleri ve bu hizmetlerin sunumunda kullanılan donanım, yazılım gibi tüm BT kaynaklarını kapsar.

Şekil 6: Kapasite Yönetimi Akış Şeması
Kaynak: TÜBİTAK İşletim ve Bakım Rehberi

Kapasite planlaması için toplanan verilerin analizi neticesinde, kaynak kullanım ve performansa ilişkin değerlendirmeler yapmak, altyapıda bulunan dar boğazlar, etkin noktalar, iş yükü dağılımlarındaki dengesizlikler, uygulama tasarımında yer alan verimsizlikler gibi hususları tespit etmek mümkündür. Bu sayede kaynak artırımı, iş yükü dağılımını düzenleme, görevleri önceliklendirme gibi düzeltici faaliyetler tanımlanabilir.

Olay ve Problem Yönetimi: Olay yönetimi, meydana gelen sorunların, hataların kayıt altına alınıp analiz edilmesi ve zamanında müdahale edilerek çözülmesi sürecini ifade eder. BT

hizmet yönetiminin kritik süreçlerinden biri olan olay yönetiminde karşılaşılan sorunun, BT hizmetleri üzerindeki olumsuz etkisinin ortadan kaldırılması veya en aza indirilmesi, bu sayede hizmetin devamlılığının sağlanmasına odaklanılır. Dolayısıyla sorunların aciliyet, önem gibi kriterler belirlenerek önceliklendirilmesi önemlidir. Örneğin aynı anda yazıcıda meydana gelen bir sorun ile sunuculardaki meydana gelen bir sorunun aciliyeti ve önemi aynı olmayacaktır.

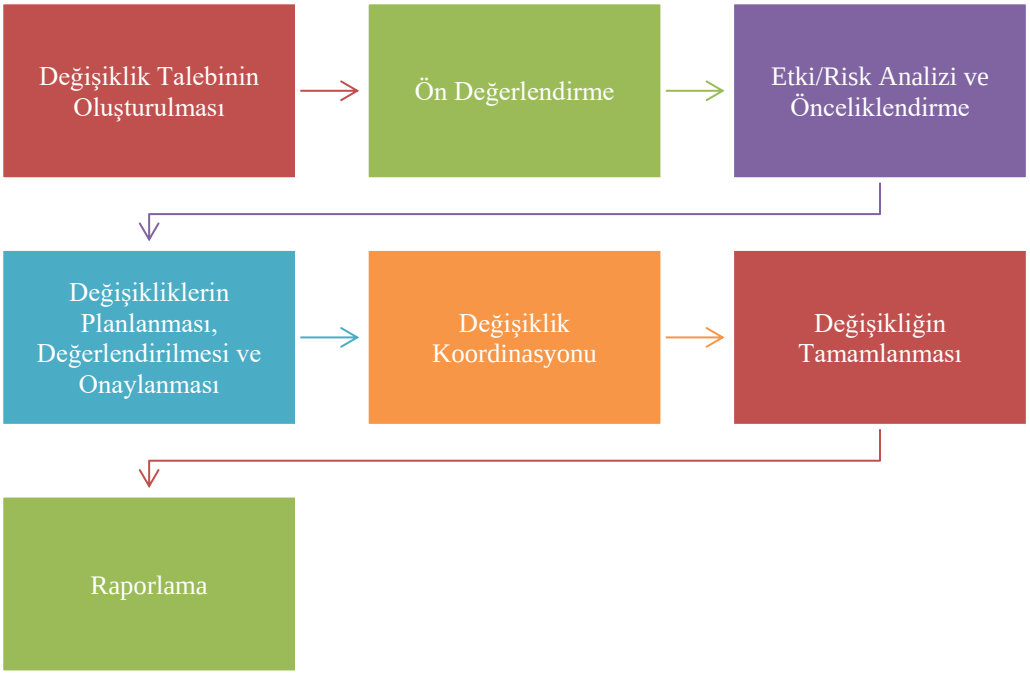
Şekil 7: Olay Yönetimi Akışı

Problem Yönetimi ise tekrarlanan veya büyük çapta ortaya çıkan olayların derin bir analiz ile ana sebeplerinin araştırılması sürecidir. Problem tanımlandıktan ve kaynağına yani kök nedenine ilişkin analiz yapıldıktan sonra kurum için bu "bilinen bir hata" haline gelir ve problemin ortadan kaldırılması, gelecekte tekrarlanmasını önlemek amacıyla çözüm geliştirilir. Bu sebeple olayların ve normal olmayan durumların daha hızlı tespit edilip çözüme kavuşturulması için birtakım prosedürler geliştirilerek problemlerin analizi sonucunda elde edilen bilgilerin, bu probleme neden olan kök nedenlerin ve geliştirilen çözümlerin kayıt altına alınması bir başka ifadeyle 'bilinen hata veri tabanı' oluşturulması sağlanmalıdır.

Şekil 8: Problem Yönetimi Akışı
Kaynak: TÜBİTAK İşletim ve Bakım Rehberi

Problem Yönetimi ile Olay Yönetimi birbirleriyle ilişkili olsa da kullandıkları yöntemler ve hedefleri açısından farklılık göstermektedirler. Problem yönetiminin amacı Balık Kılçığı Tekniği, 5 Neden Analizi gibi derin analiz yöntemleri aracılığıyla kök nedene ulaşarak ortaya çıkan olayların etkisini azaltıp tekrarını önlemek iken, olay yönetiminin amacı olaydan etkilenen iş sürecini mümkün olduğunca hızlı bir şekilde eski haline getirmeye çalışmak ve iş üzerindeki olumsuz etkiyi minimize etmektir.

Değişiklik Yönetimi: BT hizmetleri ile bu hizmetleri oluşturan tüm bileşenler üzerinde gerçekleştirilecek bütün değişikliklerin planlı ve kontrollü bir biçimde yönetilmesi sürecidir.



Şekil 9: Değişiklik Yönetimi Akış Şeması
Kaynak: TÜBİTAK İşletim ve Bakım Rehberi

- **Değişiklik Talebinin Oluşturulması:** Kurum içerisinde talep edilen ve gerçekleştirilen değişikliklerin izlenip değerlendirilebilmesi; nihayetinde raporlanabilmesi için değişiklik talebinde bulunanlarca doldurulacak ve "değişiklik açıklaması", "değişiklik gerekçesi", "değişiklik talep eden kişinin iletişim bilgileri" gibi bilgileri içeren standart bir form aracılığıyla değişiklik talebinin kayıt altına alınması gerekmektedir.

- **Ön Değerlendirme:** Toplanan değişiklik talepleri, zaman ve kaynak kısıtları nedeniyle sadece gerekli değişiklikler üzerinde çalışılabilmesi için bir ön değerlendirmeye tabi tutulur; bu sayede tekrar niteliğindeki, gerçekçi olmayan veya yeterli açıklama içermeyen taleplerin ayıklanması sağlanır.

- **Etki/Risk Analizi ve Önceliklendirme:** Ön değerlendirme aşamasından sonra gerçekleştirilmesi düşünülen değişikliklerin BT hizmetleri ve bileşenleri üzerinde yaratabileceği muhtemel etkiler, oluşturabileceği riskler değerlendirilir. Bu etki ve risk analizi sonucunda ise talep edilen değişiklikler önceliklendirilir.

- **Değişikliklerin Planlanması, Değerlendirilmesi ve Onaylanması:** Yapılacak değişikliklere ilişkin bir planlama gerçekleştirilir. Planlama kapsamında, değişikliğin başarısızlıkla sonuçlanması halinde yapılacak faaliyetleri içeren geri dönüş planları da hazırlanır. Daha önce belirlenen etki-risk analizi çerçevesinde yetkili mercilerin de süreçten haberdar olması sağlanarak, onayları dâhilinde değişiklik süreci başlatılır.

- **Değişiklik Koordinasyonu:** Değişiklik kapsamında farklı ekiplerce gerçekleştirilebilecek faaliyetlerin koordinasyonu sağlanarak değişikliğin canlı

ortama aktarılmadan önce test edilmesi, sonrasında canlı ortama aktarılması değişikliğin sorunsuzca hayata geçirilmesi açısından önemlidir.

- **Değişikliğin Tamamlanması:** Devreye alınan değişikliğin planlanan şekilde çalışıp çalışmadığının gözlemlenmesi sonucunda eğer değişiklik beklenen etkiyi yarattıysa süreç tamamlanmış sayılır. Ancak beklenen etki oluşmadıysa yetkili mercilerce, değişikliğin mevcut haliyle kabulüne, değişikliğin geri alınmasına veyahut eksikliklerin tespit edilerek sürecin yeniden başlatılmasına karar verilebilir.

- **Raporlama:** Son olarak belirli aralıklarla sürecin kendisine ilişkin (değişiklik başarı oranları, tamamlanma süreleri, önceliklendirmeye göre değişiklik dağılımı, vb.) raporlama yapmak değişiklik yönetiminin işleyişini değerlendirmek, sürecin istenilen şekilde ilerleyip ilerlemediğini kontrol etmek için önemlidir.

Kritik iş süreçlerinde yaşanan bazı sorunların ise normal değişim prosedürleri dışında **Acil Değişiklik Yönetimi** çerçevesinde değerlendirilmesi gerekebilir. Bu tür değişikliklerin zaman kaybetmeden devreye sokulması için daha hızlı bir onay ve test mekanizması geliştirilir. Hatta bazı durumlarda test edilmeksizin değişiklikler yapılabilir. Ancak Acil Değişiklik Yönetimi kapsamında yapılan değişiklikler, içerdiği riskler nedeniyle mümkün olduğunca az sayıda tutulmalı, zaman kıstı nedeniyle değişiklik öncesi oluşturulamayan dokümantasyon sonrasında tamamlanmalıdır.

3.3.2. Riskler

Kurumların etkin bir BT işletim faaliyeti yürütmemeleri halinde karşı karşıya kalabileceği riskler şunlardır:

- İş birimlerinin beklentileri ile BT'nin yapabilecekleri arasında farklılık olması sebebiyle anlaşmazlıkların ortaya çıkması, iş birimlerinin hedefledikleri başarıya ulaşamaması,

- Hizmet seviyelerinin doğru belirlenmemesi neticesinde verimsiz ve yüksek maliyetli hizmetlerin sağlanması,

- BT hizmetlerine ilişkin kullanıcı memnuniyetinin sağlanamaması,

- BT hizmetlerinin kalitesinde ve sürekliliğinde sıkıntılar meydana gelmesi,

- Gelecekte oluşabilecek kapasite sorunlarının çözümünün planlanamaması,

- Hizmetler ile ilgili kritik olayların ve problemlerin zamanında çözülememesi,

- Çözülemeyen ya da saptanamayan olaylar sebebiyle BT hizmetlerinde ve iş süreçlerinde kesintilerin oluşması,

- Hizmetlerin değişen iş ihtiyaçlarına cevap verememesi,

- Değişikliklerin öncelik derecesine göre sıralanmaması sonucu önemli değişikliklerin gözden kaçırılması ya da kurum için önem/öncelik arz etmeyen taleplere gereğinden fazla kaynak ayrılması,
- Değişikliklerin işlemleri kesintiye uğratması ve bozulmalara neden olması,
- Geri dönüş planı olmayan değişikliklerin sisteme alınması ve değişikliğin başarısızlıkla sonuçlanması halinde sistematik sorunların ortaya çıkması,
- Acil değişikliklerin kontrolsüz olarak ve kayıt altına alınmadan gerçekleştirilmesi sonucu bilgi güvenliği ihlallerinin yaşanması.

3.3.3. Kontroller

BT İşletimi ile ilgili riskleri minimize etmek için olması gereken kontrollerin (kriterlerin) başlıcaları şunlardır:

Hizmet Seviyesi Yönetimi

- HSA'lar iyi uygulama örneklerinde yer verilen (iş süreç sahipleri ile BT destek ekibi arasındaki sorumluluk dağılımı, iş hedefleri, hizmet teklif ve ölçütleri, problem türleri tanımı, yardım masası sorumlulukları gibi) hususları içermelidir.
- HSA'lar uygulanmalı, izlenmeli ve gerektiğinde değiştirilmelidir.
- BT hizmetlerinde, iş ihtiyaç ve hedefleri doğrultusunda belirlenen performans ölçütlerine ulaşılmalı ve kullanıcıların memnuniyeti sağlanmalıdır.

Kapasite Yönetimi

- Kurumun BT altyapısı performans ve kapasitesi, ölçülebilir kriterler belirlenerek planlanmalı ve düzenli aralıklarla güncellenmelidir.
- Performans verileri, kapasite ve performansın etkin yönetimi için izlenmeli, değerlendirilmeli ve raporlanmalıdır.
- Toplanan performans verileri periyodik olarak analiz edilerek, değişen ihtiyaç ve koşullar çerçevesinde kapasite sorunlarının çözümü planlanmalı ve gerekli iyileştirmeler gerçekleştirilmelidir.

Olay ve Problem Yönetimi

- Kurumda, olay ve problem yönetimine ilişkin etkin politikalar ve prosedürler olmalı; kullanıcılar bunlardan haberdar edilmelidir.
- Olay ve problemlere müdahale için yeterli bilgi ve beceriye sahip üyelerden oluşan ekipler oluşturulmalı, uygun araçlar kullanılmalı, gerekli kaynaklar tahsis edilmelidir.

- Kurum, olay ve problemlere belirlediği politika ve prosedürlere uyarak uygun ekip ve araçlarla etkili bir şekilde müdahalede bulunmalıdır.

Değişiklik Yönetimi

- Kurum, BT varlıkları ve süreçlerini etkileyebilecek değişikliklerin kontrollü ve etkin bir şekilde gerçekleştirilmesini sağlayacak politika ve prosedürlere sahip olmalıdır.
- Değişiklikler sonucunda istenmeyen bir etki görülmesi halinde etkilenen alanların iyileştirilmesine, önceki versiyona dönmeye yönelik prosedürler tanımlanmalıdır.
- Acil durum değişiklikleri için ayrı prosedürler belirlenmeli, uygulanmalı ve değişikliklerin kontrollü bir şekilde gerçekleşmesi sağlanmalıdır.
- Değişiklikler gerçekleştirildikten sonra, yeni sistem izlenmeli, analiz edilerek raporlanmalı ve yeni duruma uygun olarak varlık envanteri, kullanıcı kılavuzları, eğitim materyalleri gibi değişikliğin etkilediği tüm belgeler güncellenmelidir.

Bu alana ilişkin kontrollerin değerlendirilmesi için önerilen, alt alanlara ilişkin denetim hedefleri ile referansların yer aldığı, kontrol konuları bazında ilgili kriterleri, kontrol sorularını ve inceleme yöntemlerini de içeren matris (EK-8.3: BT İşletimi Önerilen Kontrol Değerlendirme Matrisi) ekte yer almaktadır.

3.4. Dış Kaynak Kullanımı

3.4.1. Kavramlar

Dış Kaynak Kullanımı: Bir kurumun, daha önce kurum içinde ve kendi imkânları ile gerçekleştirdiği mevcut bir iş sürecini veya yeni bir hizmeti dışarıdan bir kuruluşa yaptırma sürecidir. Sözleşme yapılan yüklenici kuruluş (tedarikçi) sözleşmeye bağlı olarak belirlenen hizmetleri, kararlaştırılan bir ücret karşılığında sağlamaktan sorumludur.

Kurumlar, BT ile ilgili hizmetlerin tamamını ya da bir kısmını aşağıdaki faydaları sağlamak için dış kaynak kullanımı yöntemi ile almaya karar verebilir:

- **Esneklik:** Dış kaynak kullanımı değişken BT gereksinimlerine sahip kurumlar için avantajlı bir yöntemdir. Dönemsel olarak ortaya çıkan ihtiyaçlarda, kuruma, ihtiyacı olan operasyona ilişkin hizmet alımı yoluyla dışardan iş gücü temin etme ve dönemsel operasyonlar bittiğinde bu hizmeti sonlandırma imkânı verir.
- **Personel Kapasitesinin Geliştirilmesi:** Bir proje, kurumun insan kaynağının hali hazırda sahip olmadığı becerileri gerektiriyorsa, kurum, zaman ve maliyet tasarrufunda bulunmak için kendi personelini eğitmek yerine projeyi dışarıdan hizmet alarak yaptırabilir. Kurumlar, dış kaynak kullanımı yoluyla temin ettiği nitelikli insan kaynağı ile kendi personelinin birlikte çalışmasını sağlayarak personelinin kapasitesini artırabilir.

- **Maliyet Azaltma:** Kurum içinde tamamlanması daha maliyetli olacak işler, dış kaynak kullanımı yöntemi ile daha uygun maliyetlerle temin edilebilir. Örnek olarak; nitelikli personel istihdamı gerektiren yazılım faaliyetleri için uygun personele sahip olmayan bir kurum, dış kaynak kullanımı yöntemi ile satın aldığı uzman işgücü sayesinde mali açıdan avantaj sağlayabilir. Küçük ölçekli kurumlar veri merkezi hizmeti alarak yüksek donanım maliyetlerini azaltabilir.

- **Ana İşe Odaklanma:** Kurumun ana görevi olmayan operasyonlarına ilişkin hizmetleri dış kaynak kullanımı yöntemi ile alması, kaynaklarını ana görev alanlarına aktarmasına ve bunlara daha etkin şekilde odaklanmasına yardımcı olur.

ISACA'ya göre, kurumlar işe ve BT altyapısına ilişkin çeşitli alanlarda dış kaynak kullanımına başvurabilir. Örneğin;

- Veri merkezi ve ilgili süreçlerin işletimi,
- Kurum içi uygulamaların işletilmesi,
- Sistem geliştirme veya uygulamaların bakımı,
- Bilgi işlem ağlarının kurulumu, bakımı ve yönetimi.

Bulut Bilişim: İşlemci gücü ve depolama alanı gibi bilişim kaynaklarının ihtiyaç duyulan anda, ihtiyaç duyulduğu kadar kullanılması esasına dayanan, uygulamalar ile altyapının birbirinden bağımsız olduğu ve veriye izin verilen her yerden kontrollü erişimin mümkün olduğu, gerektiğinde kapasitenin hızlı bir şekilde arttırılıp azaltılabildiği, kaynakların kullanımının kolaylıkla kontrol altında tutulabildiği ve raporlanabildiği bir bilişim türüdür.

Bulut bilişim hizmetleri dâhil, bilişim sistemlerine ilişkin uygulama geliştirme, altyapı, işletim, bakım ve yedekleme gibi hizmetlerin dış kaynak kullanımı yoluyla karşılanmasında; kurumun genel strateji ve planlarıyla uyumlu bir dış kaynak kullanımı planına sahip olması, yaptırılacak işin iyi tanımlanması, uygun niteliklere sahip yüklenicilerin seçilmesi, sözleşmenin tüm unsurları taşıması, yüklenici ile iletişim mekanizmalarının iyi kurulması ve idarenin gözetim-kontrol faaliyetlerinin sağlıklı şekilde gerçekleştirilmesi önem taşımaktadır. Buna ilave olarak, kurum verisinin korunması ve bilgi güvenliği gereklerinin gözetilmesi ile iş bilgisinin ve iş sahipliğinin kurum tarafından muhafaza edilmesi de gerekir.

3.4.2. Riskler

Kurumların dış kaynak kullanmaları durumunda karşı karşıya kalabileceği başlıca riskler şunlardır:

- İş, ürün ve hizmetin istenilen nitelikte ve zamanında tedarik edilememesi,
- Sözleşme, şartname ve eki belgelerin eksik ya da hatalı düzenlenmesi sonucu kurumun maddi zarara uğraması,
- Bilgi güvenliği ihlallerinin oluşması,

- Kurumun gözetim/izleme faaliyetlerini gereği gibi yerine getirmemesi nedeniyle veri kaybı ya da bilgi ifşası meydana gelmesi,
- İş bilgisinin ve iş süreçlerinin sahipliğinin kaybı,
- Tedarikçiye bağımlılık oluşması,
- İş sürekliliğinin sağlanamaması.

3.4.3. Kontroller

Dış kaynak kullanımı ile ilgili riskleri minimize etmek için olması gereken kontrollerin (kriterlerin) başlıcaları şunlardır:

Dış Kaynak Kullanımı Politikası

- Dış kaynak kullanımına ilişkin kurum politikası (dış kaynak kullanımına konu olacak hizmetler, kısıtlamalar, tedarik, güvenlik, iş sürekliliği, denetim ve izleme gibi temel unsurları kapsayacak şekilde) belirlenmiş olmalıdır.

Tedarik

- Kurum, hizmet gereksinimlerinin tanımlanarak doğru ve eksiksiz biçimde aktarılmasını ve uygun yüklenici seçimini sağlayacak süreçlere sahip olmalıdır.

Tedarikçi Yönetimi ve İzleme

- Tedarikçiden alınacak hizmete ilişkin koşullar, hedefler, roller ve sorumluluklar netleştirilerek karşılıklı anlaşmaya varılması ve uyumlu olarak hayata geçirilmesi sağlanmalıdır.

Veri Hakları

- Kurumun veri koruma ve erişim hakları tanımlanmış olmalı ve ilgili gerekliliklere yüklenicinin uyması sağlanmalıdır.

Yurtdışı Hizmet Sağlayıcı

- Dış kaynak kullanımı politikasının yurtdışı kuruluşlarından sağlanan dış kaynak kullanımıyla ilgili hükümleri açıkça belirlenmiş ve mevzuata uyum sağlanmış olmalıdır.

İş Bilgisinin ve İş Sahipliğinin Korunması

- Kurum iş bilgisini ve iş süreçlerinin sahipliğini korumalı ve yüklenicinin hizmeti aksatması ya da sağlayamaması durumunda önemli faaliyetlerine kendi kaynakları ile devam edebilmelidir.

Maliyet Kontrolü ve Yönetimi

- Dış kaynak kullanımında fayda maliyet analizi gerçekçi bir şekilde yapılmalı ve hizmetin uygun maliyet ile karşılanması sağlanmalıdır.

Hizmet Seviyesi Anlaşması

- Hizmet seviyesi anlaşması, tedarikçiyi teknik ve diğer gereksinimlere göre izleme ve kontrol etme hususunda bir temel oluşturmalıdır.

Güvenlik

- Kurum, tedarikçilere bilgi güvenliği gereksinimlerini aktarmalı ve uygulamasını izlemelidir.

Yedekleme ve Felaket Kurtarma Planlarına Uyum

- Tedarikçi, iş sürekliliği ve felaket kurtarma planlarına ilişkin yükümlülüklerini yerine getirmelidir.

Bu alana ilişkin kontrollerin değerlendirilmesi için önerilen, alt alanlara ilişkin denetim hedefleri ile referansların yer aldığı, kontrol konuları bazında ilgili kriterleri, kontrol sorularını ve inceleme yöntemlerini de içeren matris (EK-8.4: Dış Kaynak Kullanımı Önerilen Kontrol Değerlendirme Matrisi) ekte yer almaktadır.

3.5. İş Sürekliliği Yönetimi

3.5.1. Kavramlar

Kamu kurumları, günümüzde, yürüttükleri faaliyetlerin ve sundukları hizmetlerin neredeyse tamamını bilgisayar sistemleri aracılığıyla yerine getirmektedir. Bu nedenle; deprem, yangın, sel, sabotaj, donanım veya yazılım hatası, siber saldırılar, elektrik ve iletişim kesintisi gibi iç veya dış faktörler sonucu kullandıkları sistemlerin erişilebilirliğinin sağlanamaması, bütün kurumlar için dikkate alınması gereken önemli bir risk haline gelmiştir. Kurumlarda, olası bir felaket anında kurum faaliyetlerinin ve sunulan hizmetlerin hızla geri kazanılmasını sağlayacak kontrollerin kurum iç kontrol sisteminde oluşturulmuş olması gerekmektedir.

İş Sürekliliği Yönetimi: Felaket, kriz veya kesinti durumlarında, belirlenmiş olan faaliyet ve hizmetlerin sürekliliğinin temin edilmesi veya hedeflenen zaman diliminde geri kazanılarak kriz öncesi duruma dönülmesi amacıyla; potansiyel riskleri, alınacak önlemleri ve gerçekleştirilecek öncelikli eylemleri belirlemeye yönelik; politika, standart ve prosedürleri de içeren bütünsel yönetim sürecidir.

İş Sürekliliği Planı: İş sürekliliği yönetiminin bir parçası olan ve bir kesinti durumunda kurumun öncelikleriyle uyumlu olarak faaliyetlerin sürdürülmesine ve mevzuata uyum sağlanmasına yönelik yazılı plan veya planlar bütünüdür.

Felaket Kurtarma Planı (Bilgi Sistemleri Süreklilik Planı): Faaliyetlerin sürdürülmesini sağlayan bilgi sistemlerinin, bir kesinti durumunda sürekliliğinin sağlanmasına yönelik olarak hazırlanan ve iş sürekliliği planının bir parçası olan plandır.

İş Sürekliliği Planı ve Felaket Kurtarma Planı terimleri zaman zaman birbirleri yerine kullanılsa da aslında iki farklı ancak birbirini tamamlayan terimdir. İş sürekliliği planlaması organizasyonel iş fonksiyonları ile ilgili iken, felaket kurtarma planlaması kurum faaliyetlerini destekleyen BT kaynaklarına yöneliktir.

Kurumların, yürütmüş olduğu hizmetlere ve teşkilat yapılarına göre farklı planlamalara sahip olmaları kaçınılmazdır. Bununla birlikte; tüm kurumlar için ortak olan iş sürekliliği planlaması aşamaları aşağıdaki şekilde sayılabilir:

- İş sürekliliği politikasının oluşturulması,
- İş sürekliliği sürecini yürütecek uygun organizasyon yapısının kurulması,
- İş etki değerlendirmesinin ve risk yönetimi faaliyetlerinin gerçekleştirilmesi,
- İş sürekliliği ve felaket kurtarma planlarının hazırlanması,
- İş sürekliliği ve felaket kurtarma planlarının test edilmesi,
- İş sürekliliği ve felaket kurtarma planlarının gözden geçirilmesi.

3.5.2. Riskler

İş sürekliliği yönetiminin yetersiz olması, kurumu aşağıdaki risklerle karşı karşıya getirebilir:

- Hizmetin uzun süre kesintiye uğraması veya geri döndürülememesi,
- Veri kaybı yaşanması,
- Felaketten kaynaklanan kaybın veya zararın ağırlaşması,
- Yasal veya üçüncü kişilere karşı olan sorumlulukların zamanında yerine getirilememesi,
- Kurumsal itibarın zedelenmesi,
- Maddi zararlarla karşılaşılması,
- Dış kaynak kullanımında kurum planlarına uyumun sağlanamaması nedeniyle ortaya çıkabilecek güvenlik ihlali, veri kaybı, yetkisiz kullanım ve veri sızıntısı.

3.5.3. Kontroller

İş sürekliliği yönetimi ile ilgili riskleri minimize etmek için olması gereken kontrollerin (kriterlerin) başlıcaları şunlardır:

İş Sürekliliği Politikası

- Kurumun onaylanmış, yayınlanmış ve benimsenmiş bir acil durum planı ve acil durum operasyonlarının tüm alanlarını kapsamlı bir şekilde tanımlayan ve eğitim gereksinimlerini ve test programlarını belirleyen bir politikası olmalıdır.

İş Sürekliliği Organizasyonu

- İş sürekliliği sürecini yürüten bir iş sürekliliği ekibi mevcut olmalı ve ekibin görev ve sorumluluk alanları açıkça belirlenmiş olmalıdır.

Risk ve İş Etki Değerlendirmesi

- Risk değerlendirmesi ve iş etki analizi yapılmış, kritik veriler, uygulama yazılımları, işlemler ve kaynaklar tanımlanmış ve önceliklendirilmiş olmalıdır.
- Riski azaltma ve izleme süreçleri de dâhil olmak üzere bir risk yönetim süreci oluşturulmuş ve acil durum kurtarma öncelikleri belirlenmiş olmalıdır.

İş Sürekliliği ve Felaket Kurtarma Planı

- Kurumun bir iş kesintisinden sonra ya da iş yoğunluğunun arttığı dönemlerde işin sürdürülmesi ya da iş süreçlerinin yeniden kazanılması için gerekli eylem adımlarını içeren yazılı bir planı olmalıdır.

Yedekleme

- Bir felaket sonrası iş süreçlerinin yeniden kazanılması için gerekli olan sistem, veri ve uygulamaların yedekleri alınmış olmalıdır.

Çevresel Kontroller

- Yedekleme alanlarında elektrik, yangın, su, nem, sıcaklık kaynaklı çevresel tehditler için uygun kontrol mekanizmaları oluşturulmuş olmalıdır.

Test

- İş sürekliliği ve felaket kurtarma planları uygun şekilde ve düzenli olarak test faaliyetlerine tabi tutulmalıdır.

Güvenlik

- Yedekleme ve felaket kurtarma faaliyetleri sırasında veri, uygulama yazılımı, donanım ve veri merkezi güvenliği sağlanmalıdır.

Dış Kaynak Kullanımında Yedekleme ve Felaket Kurtarma

- Tedarikçi ile yapılan sözleşme veya hizmet seviyesi anlaşmalarında, kurumun iş sürekliliği ve felaket kurtarma planlarına uyumuna ilişkin hususlara yer verilmeli, dış

kaynak kullanım hizmetleri uygun şekilde yedeklenmeli ve bunlara felaket kurtarma çözümlerinin uygulanması sağlanmalıdır.

Bu alana ilişkin kontrollerin değerlendirilmesi için önerilen, alt alanlara ilişkin denetim hedefleri ile referansların yer aldığı, kontrol konuları bazında ilgili kriterleri, kontrol sorularını ve inceleme yöntemlerini de içeren matris (EK-8.5: İş Sürekliliği Yönetimi Önerilen Kontrol Değerlendirme Matrisi) ekte yer almaktadır.

3.6. Bilgi Güvenliği

3.6.1. Kavramlar

Bilgi Güvenliği: Bilginin, yetkisiz kullanıcılara ifşa edilmesine, uygun olmayan değişikliklerin yapılmasına ve gerektiği zamanlarda erişilememesine karşı korunmasıdır. (ISACA-Terimler Sözlüğü). Bu genel tanımdan da görüleceği üzere, bilgi güvenliğinin üç temel ayağı vardır:

- **Gizlilik:** Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olması,
- **Bütünlük:** Bilginin ve işleme yöntemlerinin doğruluğunun ve tamlığının sağlanması,
- **Erişilebilirlik:** Yetkili kullanıcıların, gerek duyduklarında bilgiye ve ilişkili kaynaklara erişebilmeleri.

Risk Değerlendirmesi: Bilgi varlıklarına yönelik iç ve dış tehditlerden kaynaklanan güvenlikle ilgili riskleri tanımlama, analiz etme ve irdeleme sürecidir. Bilgi güvenliğinin etkin şekilde sağlanabilmesinin ilk adımıdır. Bu yolla Kurum, bilgi güvenliği risklerini etkili bir şekilde azaltmak için uygun kontrolleri belirleme ve uygulama imkânına sahip olmaktadır.

Bilgi Güvenliği Politikası: Gerçekleştirmiş olan risk değerlendirmesi temelinde hazırlanan, Kurumun güvenlik felsefesini ve taahhüdünü gösteren, belirlemiş olduğu güvenlik hedeflerine ulaşmak için kaynaklarını nasıl yöneteceğini, koruyacağını ve dağıtacağını düzenleyen ve bu çerçevede ilgililerin rol ve sorumluluklarını tanımlayan kurallar ve uygulamalar dizisidir.

Bilgi Güvenliği Örgütlenmesi: Bilgi güvenliği politikasının Kurumda etkin bir şekilde ve eşgüdüm içerisinde uygulanmasını sağlar. Sorumlu birim ve/veya kişilerin rol ve yetkileri tanımlanarak görevlendirilmeleri ve bunlar tarafından gerçekleştirilen faaliyetleri ve işletilen süreçleri kapsar.

Varlık Yönetimi: Geniş anlamıyla, Kurum varlıklarının maliyet etkin bir şekilde işletilmesi, bakımı ve elden çıkarılmasına yönelik faaliyetlerden oluşur. Bilgi güvenliği açısından ele alındığında, BT ekipmanlarının envanterinin doğru şekilde tutulması, bakımının ve güvenliğinin sağlanması, güvenli şekilde elden çıkarılması yanında sahip olunan lisansların takibinin yapılmasını da içeren sistematik bir süreci ifade eder.

İnsan Kaynakları Güvenliği: Bilgi güvenliğinin temel bileşenlerinden biri insan unsurudur. İnsan kaynakları güvenliği; Kurum bilgi varlıklarına erişen iç ve dış kaynaklı çalışanların istihdam edilmeleri öncesinde, çalıştırıldıkları esnada ve istihdamlarının sona erdirilmesinde gerçekleştirilen faaliyetler vasıtasıyla, Kurum çapında bilgi güvenliği ile ilgili yeterli bir farkındalığa sahip olunması ve bilgi güvenliği hedefleri doğrultusunda gerekli önlemlerin alınması yoluyla sağlanır.

Fiziksel ve Çevresel Güvenlik: Kurum bilgi varlıklarının fiziksel olarak yeterli ve uygun bir korumaya sahip olması bilgi güvenliği açısından önemli bir gerekliliktir. Fiziksel ve çevresel güvenlik; Kurumun belirlenmiş olan güvenlik sınırları dâhilinde yer alan tesis ve binaları ile bilişim sistemlerinin konumlandırıldığı ve bilgi işlem faaliyetlerinin yürütüldüğü mekânların gizlilik ihlali, hasar ve hırsızlık ile sonuçlanabilecek yetkisiz fiziksel erişimlerden ve yangın, su, elektrik, iklimlendirme ve temizlik ile ilgili çevresel tehlikelerden korunmasıdır.

Mantıksal Erişim Kontrolleri: Kullanıcıların Kurumun BT altyapısına, bilişim sistemlerine ve ilgili bileşenlere erişimlerinin yetki dâhilinde ve güvenli şekilde gerçekleştirilmesini amaçlayan kontrollerdir. BT varlık ve kaynaklarına yetkisiz erişimin önlenmesine ve bu yolla bilginin gizlilik ve bütünlüğünün korunmasına yönelik kural ve uygulamalardan oluşur.

Ağ, İşletim Sistemi ve Veri Tabanlarının Yönetimi ve Güvenliği: Kurumda kullanılan ağ, işletim sistemi ve veri tabanlarının belirlenmiş olan bilgi güvenliği gerekleri doğrultusunda yapılandırılmaları, sıkılaştırılmaları ve tanımlı kural ve süreçlere göre yönetilmeleridir.

3.6.2. Riskler

Kurumların bilgi güvenliğini etkin şekilde sağlayamamaları halinde karşılaşılabileceği risklerden bazıları şunlardır:

- Yetersiz veya gereğinden fazla güvenlik önlemlerinin belirlenmesi ve uygulamaya konması,
- Bilgi güvenliği olaylarına zamanında ve uygun karşılık verilememesi,
- Varlıklar üzerindeki kontrolün kaybedilmesi, kayıp ve zararların meydana gelmesi,
- Çalışan kaynaklı bilgi güvenliği ihlalleri ve sistem hataları yaşanması,
- Bilgi işlem bileşenlerinin çalınması, bozulması, hasar görmesi, bilişim sistemlerinin kısmen veya tamamen çalışamaz duruma gelmesi,
- Gizli bilginin ifşası,
- Bilgilerin ve verilerin kaybolması, çalınması,
- Bilginin yetkisiz olarak değiştirilmesi veya silinmesi,

- Bilgiye ve bilgi sistemlerine erişimin kesintiye uğraması,
- İş süreçlerinde ve sunulan hizmetlerde aksamalar yaşanması,
- Bilgi güvenliği olaylarına ilişkin sorumlulukların tespit edilememesi, hesap verebilirliğin sağlanamaması,
- Mevzuattan kaynaklanan gerekliliklere uyumun sağlanamaması.

3.6.3. Kontroller

Bilgi güvenliği ile ilgili riskleri minimize etmek için olması gereken kontrollerin (kriterlerin) başlıcaları şunlardır:

Risk Değerlendirmesi

- Kurum iyi dokümante edilmiş ve etkin şekilde işletilen bir bilgi güvenliği risk değerlendirme mekanizmasına sahip olmalıdır.
- Bilgi güvenliğine ilişkin bütün önemli iç ve dış riskler uygun şekilde tanımlanmalı ve muhtemel etkileri ve sonuçları değerlendirilmelidir.
- Risklerin azaltılması için risk değerlendirme dokümanlarında belirlenmiş olan faaliyetler gerçekleştirilmelidir.

Bilgi Güvenliği Politikası

- Kurum, tüm operasyonel riskleri kapsayan ve Kurum faaliyetleri için önemli olan bütün bilgi varlıklarına kayıp, zarar ve kötüye kullanıma karşı makul bir koruma sağlayan bir bilgi güvenliği politikasına sahip olmalıdır.
- Kurumun bilgi güvenliği politikasında belirlenen ihtiyaçlarını uygun şekilde yansıtan ve iç paydaşlar ile üçüncü taraflar nezdinde gizli bilginin korunmasını sağlayan düzenlemeler bulunmalıdır. Kişisel verilerin korunmasına ilişkin yasal gereklilikler karşılanmalıdır.

Bilgi Güvenliği Örgütlenmesi

- Bilgi güvenliği politikası çerçevesinde ilgili roller ve sorumluluklar açık şekilde tanımlanarak dokümante edilmeli ve görevlendirmeler gerçekleştirilmelidir.
- Bilgi güvenliği faaliyetlerinde sorumluluk çatışması, uyumsuzluk ya da açıkta kalan alanlar olmamalıdır.

Varlık Yönetimi

- Kurumun bilgi varlıkları ilgili standartlar, çerçeve belgeler ve iç düzenlemelere uygun şekilde korunmalıdır.

İnsan Kaynakları Güvenliği

- Yüklenici firma personeli ve hassas bilgiyi kullanan bütün kullanıcılar da dâhil olmak üzere tüm çalışanların bilgi güvenliği gereklerine uyumunu sağlayacak etkin düzenleme ve mekanizmalar bulunmalıdır.
- Uygun kapsamda ve düzenli aralıklarla kurumsal bilgi güvenliği eğitimleri gerçekleştirilmelidir.

Fiziksel ve Çevresel Güvenlik

- Kurum, tesislerinin ve bilişim sistemlerinin fiziksel ve çevresel güvenliğine ilişkin yazılı güvenlik politikasına ve prosedürlerine sahip olmalıdır.
- Kurum tesislerine ve bilgisayar alanlarına (sistem odaları, veri depolama alanları, ağ teçhizatı, çalışma alanları, vb.) fiziksel erişimin yetki dâhilinde gerçekleştirilmesini sağlayacak önlemler alınmalıdır.
- Bilgisayar alanlarının yangın, su, elektrik, iklimlendirme ve temizlik ile ilgili çevresel tehlikelerden korunmasına ilişkin kontrol düzenlemeleri oluşturulmalı ve uygulanmalıdır.

Erişim

- Kurum, bilişim sistemlerine ve uygulamalara erişimi düzenleyen politika ve prosedürlere sahip olmalıdır.
- Kullanıcıların oluşturulmasına, kaldırılmasına, erişim haklarının ve ayrıcalıklarının verilmesine, yönetilmesine, izlenmesine ve geri alınmasına yönelik süreçler tanımlanmalı ve yetkisiz erişimi önleyecek mekanizmalar uygulanmalıdır.

Ağ Yönetimi ve Güvenliği

- Kurum, ağ yönetimi ve güvenliğine ilişkin yazılı politikalara ve alt düzenlemelere sahip olmalıdır.
- Ağın güvenli ve etkin bir şekilde yönetilmesi ve kullanılmasına ilişkin yapılandırmalar ve sıkılaştırma tedbirleri (dokümantasyon, yedeklilik, güncelleme, segmentasyon, yetkilendirme, erişim, kayıt alma, izleme, uzaktan erişim, e-posta, vb. konuları kapsayacak şekilde) gerçekleştirilmelidir.

İşletim Sistemleri Yönetimi ve Güvenliği

- Kurum, işletim sistemlerinin yönetimi ve güvenliğine ilişkin yazılı politikalara ve alt düzenlemelere sahip olmalıdır.
- İşletim sistemlerinin güvenli ve etkin bir şekilde yönetilmesi ve kullanılmasına ilişkin yapılandırmalar ve sıkılaştırma tedbirleri (güncelleme, yetkilendirme, erişim,

kayıt alma, zararlı yazılımlardan koruma, şifreleme, vb. konuları kapsayacak şekilde) gerçekleştirilmelidir.

Veri Tabanı Yönetimi ve Güvenliği

- Kurum, veri tabanlarının yönetimi ve güvenliğine ilişkin yazılı politikalara ve alt düzenlemelere sahip olmalıdır.
- Veri tabanlarının güvenli ve etkin bir şekilde yönetilmesi ve kullanılmasına ilişkin yapılandırmalar ve sıkılaştırma tedbirleri (güncelleme, yetkilendirme, kayıt alma, şifreleme, vb. konuları kapsayacak şekilde) gerçekleştirilmelidir.

Bu alana ilişkin kontrollerin değerlendirilmesi için önerilen, alt alanlara ilişkin denetim hedefleri ile referansların yer aldığı, kontrol konuları bazında ilgili kriterleri, kontrol sorularını ve inceleme yöntemlerini de içeren matris (EK-8.6: Bilgi Güvenliği Önerilen Kontrol Değerlendirme Matrisi) ekte yer almaktadır.

3.7. Uygulama Kontrolleri

3.7.1. Kavramlar

Uygulama: Belirli bir işlev için kayıtların işlenmesini gerçekleştiren bir bilgisayar programı veya program seti olup işletim sistemi veya ağ kontrol programı gibi sistem programları ile kopyalama veya sıralama gibi işlemler yapan yardımcı programlardan farklıdır. (ISACA Terimler Sözlüğü)

Uygulama Kontrolleri: Verilerin sistemlere yetki dâhilinde, tam olarak, zamanında ve mükerrerliği önleyecek şekilde girilmesini; bilgi-işlem ortamında tüm işlem ve süreçlerin istenilen sıra ve düzen içinde gerçekleşmesini; raporların tam ve güvenilir olarak üretilmesini, yetkili kişilere ulaştırılmasını ve uygun şekilde arşivlenmesini sağlayan kontrollerdir.

Genel kontroller bilgi sistemlerine yönelik kontrol ortamının genel çerçevesini çizerken, uygulama kontrolleri uygulama özelinde bilginin doğruluğu, bütünlüğü, güvenilirliği ve gizliliğini sağlamaya ve korumaya yöneliktir.

Uygulamaya veri girişinin yapılması, verinin işlenmesi, çıktının elde edilmesi ve tüm bu süreç boyunca güvenliğin sağlanması aşamaları göz önünde bulundurulduğunda uygulama kontrollerinin temel unsurlarını girdi, işlem, çıktı ve uygulama güvenliği olarak saymak mümkündür.

Şekil 10: Uygulama Kontrollerinin Temel Unsurları
Kaynak: WGITA-IDI Handbook on IT Audit for Supreme Audit Institutions

- **Girdi Kontrolleri:** Tam, doğru ve güvenilir verinin, sisteme yetkili kişilerce, zamanında ve mükerrerliği önleyecek şekilde girilmesini sağlayan kontrollerdir.
- **İşlem Kontrolleri:** Veri girişinin yapılmasından itibaren verinin işlenmesine, transferinin sağlanmasına ve çıktının elde edilmesine kadar olan süreç içerisinde verinin doğruluğu, bütünlüğü ve güvenilirliğini sağlamaya; mükerrerliğini önlemeye yönelik kontrollerdir.
- **Çıktı Kontrolleri:** Verinin işlenmesi sonucunda elde edilen çıktının, tam ve doğru olmasının, düzgün şekilde dağıtılmasının teminine; yetkisi olmayan kişiler tarafından elde edilmesinin veya değiştirilmesinin önlenmesine yönelik kontrollerdir.
- **Uygulama Güvenliği Kontrolleri:** Uygulama özelinde bilginin gizliliği, bütünlüğü ve erişilebilirliğini sağlamaya yönelik kontrollerdir.

Uygulama kontrollerinin etkinliğinin incelenmesi, her ne kadar aralarında katı bir hiyerarşik sıralama olmasa da iş süreçlerinin ve uygulamanın anlaşılması, risklerin belirlenmesi ve kontrollerin değerlendirilmesi aşamalarını kapsayan bir süreçtir.

- **İş Süreçlerinin Anlaşılması:** Uygulamanın teknik detaylarına girmeden önce uygulama tarafından otomatize edilen iş süreçleri, kurallar, roller hakkında bilgi sahibi olunmasıdır.
- **Uygulamanın Anlaşılması:** Organizasyon şemaları, bilgi akış şemaları, kullanıcı rehberleri gibi belgelerin incelenmesi veya ilgili personeller ile görüşülerek uygulamanın tasarımı, çalışma şekli ve fonksiyonlarının yanı sıra işletim sistemi, ağ ortamı, veri tabanı yönetim sistemi, uygulamanın diğer uygulamalar ile bağlantısı gibi teknik detaylar hakkında bilgi edinilmesidir.
- **Risklerin Belirlenmesi:** Uygulama tarafından yürütülen iş faaliyetlerinin içerdiği risklerin tanımlanması ve bu risklerin nasıl yönetildiğinin belirlenmesi sürecidir.

- **Kontrollerin Değerlendirilmesi:** Uygulamaya ilişkin gerek teknik detayların gerekse iş süreçlerinin anlaşılmasından sonra belirlenen risklerin yönetilmesine ilişkin olarak uygulama içerisinde oluşturulmuş olan kontroller değerlendirilir.

Şekil 11: Uygulama Kontrolleri İnceleme Döngüsü
Kaynak: WGITA-IDI Handbook on IT Audit for Supreme Audit Institutions

3.7.2. Riskler

Uygulamalara ilişkin olarak karşılaşılabilecek risklerden bazıları şunlardır:

- Yetkili olmayan kişilerce veri girilmesi,
- Eksik veya hatalı veri girilmesi,
- Mükerrer kayıtların sistem tarafından kabul edilmesi,
- Hatalı veri girişlerinin tespit edilememesi,
- İş süreçlerinin eksiksiz olarak, doğru sıra ve düzende gerçekleştirilememesi,
- Sistematik hatalar oluşması,
- İşlem hatalarının tespit edilip düzeltilememesi,
- Denetim izinin kaybolması ve işlem sahibine başvurulamaması,
- Çıktıların tam ve doğru üretilmemesi,
- Çıktıların uygun bir şekilde sınıflandırılıp dağıtılamaması,
- Çıktıların uygun şekilde muhafaza edilememesi,

- Çıktıların yetkisiz kişilerin eline geçmesi,
- Verilerin gizliliğinin ve bütünlüğünün korunamaması,
- Hizmet kesintileri ile karşılaşılması,
- Mevzuata uyum sorunlarının ortaya çıkması,
- Kurumsal itibar kaybı yaşanması.

3.7.3. Kontroller

Uygulamalar ile ilgili riskleri minimize etmek için olması gereken kontrollerin (kriterlerin) başlıcaları şunlardır:

Girdi

- Girdi doğrulama kuralları kapsamlı olarak belirlenmeli, belgelendirilmeli, uygulamanın veri giriş ara yüzlerine tanımlanmalı ve düzenli aralıklarla güncellenmelidir. Girdi doğrulama kontrolleri sadece yetkili kişiler tarafından devre dışı bırakılabilmeli ve bu işlemlerin kaydı tutulmalıdır.
- Veri hazırlama ve giriş prosedürleri yazılı olmalı ve kullanıcılara duyurulmalıdır. Kaynak belgeler imha edilene kadar kayıt altında tutulmalı, her işleme eşsiz ve sıralı bir numara atanmalıdır. Kaynak belgelerin asılları yasal gereklilikler veya politikalarda öngörülen süre boyunca saklanmalıdır.
- Uygulama, sorunları net ve öz bir şekilde tanımlayan bir hata mesajı mekanizmasına sahip olmalı, hata kayıtları düzenli olarak gözden geçirilmeli ve hatalı girişlere yönelik düzeltici önlemler, uygulamada işlem safhasına geçilmeden önce alınmalıdır.
- İşlemler için yetki seviyeleri oluşturulmalı ve düzgün yapılandırılmış kontroller aracılığıyla işlemlerin bunlara uygun şekilde yapılması sağlanmalıdır. Veri girişi için görevler ayrılığı ilkesi esas alınmalı, bu ilkenin uygulanamadığı durumlarda telafi edici kontroller kurulmalıdır.

İşlem

- Uygulama, işlemleri iş süreçlerine ilişkin kurallara ve gerekliliklere uygun şekilde/ beklendiği gibi gerçekleştirmelidir.
- Uygulama işlem safhasındaki hataları doğru şekilde tespit etmeli ve tanımlamalıdır. İşlem esnasında yaşanan beklenmedik kesintilerde dahi verinin bütünlüğü korunmalıdır. İşleme hatalarının ele alınmasına, askı dosyalarının gözden geçirilmesine ve çözümüne ilişkin yeterli bir mekanizma bulunmalıdır.

Çıktı

- Çıktı kontrolleri; uygulama çıktısının, son kullanıcı işlemi dâhil olmak üzere müteakip işlemlerde kullanımından önce doğruluk ve bütünlüğünün onaylanmasını, düzgün şekilde izlenmesini, uygunluk ve doğruluk açısından gözden geçirilmesini ve bütünlük ve doğruluk kontrollerinin etkili olmasını sağlayacak şekilde tasarlanmış olmalıdır.

- Çıktılar, geçerli gizlilik sınıflandırması çerçevesinde yönetilmeli, doğru alıcılara dağıtılmalı ve mevzuatta öngörülen süre boyunca güvenli şekilde saklanmalıdır.

Uygulama Güvenliği

- Uygulamanın kullanıcıları tanımlı prosedürler dâhilinde oluşturulmalı ve kaldırılmalı, yetkileri görev tanımlarına uygun şekilde belirlenerek yönetilmeli ve mantıksal erişimlerinin güvenliği sağlanmalıdır.

- Kritik işlemlere ilişkin düzeltme, iptal ve yetkilendirmeler kayıt altına alınmalı, bu kayıtlar uygun şekilde tutulmalı ve muhafaza edilmeli, olağandışı (şüpheli) faaliyetlerin takibi amacıyla düzenli olarak gözden geçirilmelidir.

- Veri transferinden sorumlu personele rehberlik yapacak detaylı teknik bilgileri içeren prosedürler tanımlanmalı ve veri transferlerinin tam ve doğru olarak yapılmasını sağlayan manuel veya otomatik kontroller oluşturulmalıdır.

Bu alana ilişkin kontrollerin değerlendirilmesi için önerilen, alt alanlara ilişkin denetim hedefleri ile referansların yer aldığı, kontrol konuları bazında ilgili kriterleri, kontrol sorularını ve inceleme yöntemlerini de içeren matris (EK-8.7: Uygulama Kontrolleri Önerilen Kontrol Değerlendirme Matrisi) ekte yer almaktadır.

EKLER

Ek-1: Genel Bilgi Edinme Formu

1. Kurum Hakkında Genel Bilgiler

Kurumun Adı	
Ana Faaliyetleri	
Kurum Personel Sayısı	
İdari Hizmet Binaları (Sayısını ve adreslerini belirtiniz.)	

2. Mali Bilgiler

Yıllık Ödemeler / Harcamalar (TL)	
Toplam Varlıklar (TL)	
Bilişim Sistemleri Varlıklarının Toplam Değeri (TL)	

2.1. Son İki Yılın Bilişim Sistemleri Bütçe Tahminleri ile Gerçekleşen Harcama Miktarları

Bir tabloda gösteriniz.

2.2. Bilişim Sistemleriyle İlgili Olarak Son Bütçe Dönemi İçinde Yapılan Harcamaların Listesi

No	Harcamanın Niteliği	Tutar (TL)	Tarih
1			
2			
3			
4			

3. Stratejik Yönetim Belgeleri

Aşağıdaki tabloyu doldurunuz.

No	Belge Adı	Var*/ Yok	Açıklama**
1	Kurumsal stratejik plan		
2	BT strateji belgesi		
3.1	Bilgi güvenliği politika belgesi		
3.2	Bilgi güvenliği ile ilgili diğer politika, prosedür ve rehberler		
3.3	BGYS sertifikasyonu		
4.1	Kurumsal risk kütüğü		
4.2	BT risk değerlendirme metodolojisi		
4.3	BT risk kütüğü		
5.1	İş sürekliliği planı		
5.2	Felaket kurtarma planı		
5.3	İş sürekliliği ve felaket kurtarma planı test sonuçları		
6	Son 5 yıl içerisinde hazırlanmış BT denetim raporları veya diğer denetimlerde arasında BT'ye ilişkin bulgu içeren raporlar		
7	BT alanını ilgilendiren kurumsal mevzuat (yasa, yönetmelik, yönerge, genelge)		
8.1	BT Birimi ayrıntılı organizasyon şeması		
8.2	BT Birimi yazılı iş süreçleri		
8.3	BT Birimi yazılı görev tanımları		
9	Kurumunuzda uygulanan BT proje yönetimi metodolojisi veya rehberi		
10	Üçüncü taraflarla yapılan bilişim hizmet sözleşmeleri		

***** Var olan belgeleri ekleyiniz.

****** Gerekli olduğunda ilave bilgi vermek için kullanınız.

4. Bilgi İşlem Organizasyonu

4.1. Bilgi İşlem Biriminde Çalışan Personel

Aşağıdaki tabloyu doldurunuz.

Genel Yönetim: Bilgi İşlem Biriminin yönetiminden sorumlu kişi.

Yetkili Personel: Bilgi İşlem Biriminde yürütülen işlerden birim yönetimine karşı sorumlu olan kişi.

İrtibat Kişisi: Söz konusu alanla ilgili olarak denetim çalışmalarında muhatap olunacak kişi.

	Pozisyon		**İrtibat Kurulacak Personel**	
Faaliyet Alanı	**Yetkili Personel Sayısı**	**İşi Yürüten Personel Sayısı**	**Adı – Soyadı**	**Telefon Numarası**
Genel Yönetim				
BS Güvenliği				
Fiziksel Güvenlik				
Sistem Yönetimi				
İletişim/Ağ Yönetimi				
Veri Yönetimi				
Veritabanı Yönetimi				
Yazılım Geliştirme				
Web Tasarım				
Teknik Destek				
SOME				
Diğer				
Toplam Personel				

4.2. Kilit Nitelikteki Personel

Yukarıdaki tabloda yer alan personelden kilit nitelikte olanları belirtiniz.

4.3. Kilit Personel Değişiklikleri ve/veya Yeniden Yapılanma Sonucu Oluşan Değişiklikler

Son bir yıl içinde yapılan ve gelecekte yapılması öngörülen değişiklikleri belirtiniz.

Adı Soyadı	Eski Pozisyonu ve Çalışma Tarihleri	Yeni Pozisyonu ve Görevlendirme Tarihi

4.4. Bilgi İşlem Birimi Dışında Görevli Bilişim Personeli

Bilgi işlem birimi dışında çalışan kurum bilgi işlem personeli ya da bilgi işlem personeli olmamasına karşın ilgili birimdeki program ve sistemlerin yürütülmesinde görevli kişilere ait bilgileri belirtiniz.

Adı-Soyadı	Görevli Olduğu Birim	Görevi	İrtibat Bilgileri

5. Sistem Bilgileri

5.1. Ağ

Kurumda kullanılmakta olan ağ cihazlarının türlerini ve adedini belirtiniz. (Aynı yapılandırma ayarlarına sahip cihazları gruplayınız.)

Kurumda kullanılmakta olan ağ güvenlik cihazlarının türlerini ve adedini belirtiniz.

Kurumda kablosuz ağ kullanılıyor mu?

Kurum ağlarına bağlı akıllı cihazlar (televizyon, buzdolabı, vb.) var mı?

Kurum bilgi işlem altyapılarına kurum ağı dışından ya da internet üzerinden yönetimsel erişim yetkisi veriliyor mu?

5.2. Sunucular

Bilgi İşlem Birimi tarafından **yönetilen** sunucuların işletim sistemlerini ve adedini belirtiniz.

Bilgi İşlem Birimi tarafından **yönetilmeyen** sunucuların adedini belirtiniz.

5.3. Veri Tabanı Sistemleri

Kurumda bulunan veritabanı yönetim sistemlerinin işletim sistemlerini ve adedini belirtiniz.

5.4. Yedekleme Sistemi

Kurumda kullanılmakta olan yedekleme sistemini/yazılımını belirtiniz.

5.5. E-posta Sunucusu

Kurumda kullanılmakta olan e-posta sunucu yazılımını belirtiniz.

5.6. Virüs Koruma

Kurumda kullanılmakta olan virüs koruma (anti-virüs) yazılımını belirtiniz.

5.7. Windows Etki Alanı (Domain)

Windows Etki Alanı için aşağıdaki bilgileri veriniz.

Etki Alanı Adı:

Etki Alanı Üye Kullanıcı Sayısı:

Etki Alanı Üye Kullanıcı Bilgisayarı Sayısı:

Etki Alanı Üye Sunucu Sayısı:

Etki Alanı Kontrolcü (DC) Sayısı:

5.8. Web Sunucular

Sistemde bulunan web sunucuların yazılımını ve adedini belirtiniz.

5.9. Web Uygulamaları

Kuruma özel web uygulamalarının adlarını belirtiniz.

5.10. Genel Servisler

Kurum tarafından sunulan **internete açık ve herkes tarafından erişilebilen** servisler (örneğin; kurum web sitesi, uygulama yazılımları, e-posta, VPN, vb.) aşağıdaki tabloyu doldurunuz.

Servis Adı	Erişim Adresi

5.11. Dış Kurum Entegrasyonları

Veri değişimi yapılan dış kurum entegrasyonları için aşağıdaki tabloyu doldurunuz.

Veri Değişimi / Entegrasyon Yapılan Kurum Adı	Bağlantı Yöntemi (noktadan noktaya, VPN, internet, vb.)	Kullanım Amacı

5.12. Bulut Hizmetler

Kurum tarafından buluttan alınan hizmetler ve/veya bulut şeklinde sunulan hizmetler bulunmakta mıdır? Var ise lütfen belirtiniz.

5.13. Veri Merkezi

Kurumun veri merkezi kendi binasında mı bulunmaktadır?

Kurum tarafından veri merkezi için hizmet alımı gerçekleştirilmekte midir?

6. Kullanıcı Ortamı Bilgileri

6.1. Kullanıcı Bilgisayarları / İnce İstemci

Kullanıcı bilgisayarları için aşağıdaki tabloyu doldurunuz.

Platform / İşletim Sistemi	Yüklü Yazılımlar	Adet

6.2. Yazıcılar

Kurumda kullanılmakta olan yazıcıların adedini belirtiniz.

6.3. Diğer

Kurum sisteminde dizüstü bilgisayar kullanılmakta mıdır? Kullanılıyorsa adedini belirtiniz.

Kurum sisteminde mobil cihaz (tablet, telefon, vb.) kullanılmakta mıdır? Kullanılıyorsa adedini belirtiniz.

Kurum bilgisayarlarında USB disk (flash memory, vb.) kullanılmakta mıdır?

Kurum bilgisayarlarında CD/DVD yazıcı kullanılmakta mıdır?

7. Kurum Faaliyetlerinin Yürütülmesinde Kullanılan Programlar

Adı	Üreticisi	Kurulum Tarihi / Sürüm	Lisans Durumu	Kullanan Birim	Kullanım Amacı	Sorumlu Personel	Programlama Dili	Kullanıcı Sayısı	Veri Giriş Yöntemleri (Yığın-Online-Real Time)

Uygulama programlarının fonksiyonlarını, programın genel işleyişini tanımlayan bir bilgi notunu ve kullanıcı rehberlerini ve talimatlarını ekleyiniz.

8. Kurumda Yürütülen Projeler

Kurumda yürütülen BT projeleri için aşağıdaki tabloyu doldurunuz.

Adı	Amacı	Karakteristiği / Türü	Bütçesi	Başlangıç - Bitiş Tarihleri	Yüklenicisi

Formu Dolduran Personel

Hazırlayan:	
Görevi:	
Tarih:	
Telefon No:	
E-posta:	

Gözden Geçiren:	
Görevi:	
Tarih:	
Telefon No:	
E-posta:	

Ek-2: Sistem Risk Değerlendirme Formu

Kurum Adı:				
Sistem Adı:				
Kriter	**Parametreler**	**Puan**	**Ağırlık**	**Risk Puanı**
Önemlilik (%35)				
Sistemin ulusal güvenlik/ekonomik güvenlik açısından önemi	Yüksek	5	10	
	Orta	3		
	Düşük	1		
Sistemin Kurumun misyonu ve ana faaliyetleriyle ilişkisi (bunlar açısından taşıdığı önem, rol)	Yüksek	5	5	
	Orta	3		
	Düşük	1		
Sistemin ilgili olduğu faaliyetin etkisi	Tüm ülkeyi (tüm kurumları) ilgilendiriyor	5	7	
	Birden çok kurumu ilgilendiriyor	3		
	Kurumun tamamını ilgilendiriyor	2		
	Sadece birkaç birimi etkiliyor	1		
Sistemin kritiklik derecesi (hizmet kesintisi olduğunda tolere edilebilecek zaman)	4 saatten az	5	8	
	4-24 saat arası	3		
	1-3 gün	2		
	4 günden fazla	1		
e-Devlet hizmet sunumu	Var	5	5	
	Yok	1		
BT Yönetişimi (%15)				
BT ve ilgili politikalarının varlığı	Yok	5	5	
	Kısmen oluşturulmuş	3		
	Var	1		

BT hizmetlerinin yürütülmesi	Dış kaynak kullanımı yoluyla	5	5	
	Bazı BT fonksiyonları için dış kaynak kullanımı yoluyla	4		
	Kurum BT birimi tarafından	2		
BT faaliyetleri ile ilgili sorumluluk	Bir alt düzey personel sorumlu veya sorumluluk net değil	5	5	
	BT birim yöneticisi sorumlu	3		
	Bir üst düzey yönetici sorumlu	1		
Sistem Geliştirme ve Dış Tedarik (%10)				
Sistem geliştirme faaliyetleri	Kısmen kurum personeli tarafından, kısmen dış tedarik hizmeti alımı yoluyla	5	3	
	Dış tedarik hizmeti alımı yoluyla	3		
	Kurum personeli tarafından	2		
Sistemin belgelenmesi	%50'den az	5	3	
	%75-50	3		
	%90-75	2		
	%90'dan fazla	1		
Sistemde değişiklik yapılma sıklığı (yıllık)	5'ten çok	5	4	
	2-5 arası	3		
	1 veya yapılmayabiliyor	1		
İşletim ve Güvenlik (%30)				
Kurum içi kullanıcı sayısı	5.000'den çok	5	5	
	1.000-5.000 arası	3		
	100-1.000 arası	2		
	100'den az	1		
Ağ durumu	Web tabanlı	5	5	
	WAN	4		
	LAN	3		

	Ağ erişimi yok	1		
Lokasyon sayısı	3'ten fazla	5	4	
	1-3 arası	3		
	Yalnız bir yer	1		
Kurum dışına direkt bağlantı	Var	5	5	
	Yok	1		
Verinin ve uygulamanın muhafaza edildiği yer	Dış tedarik hizmeti alınan kurum tesislerinde	5	4	
	Kısmen Kurum içinde, kısmen dış tedarik hizmeti alınan kurum tesislerinde	3		
	Kurum içinde	1		
Sistemin hizmette bulunduğu süre	2 yıldan az	5	3	
	2-5 yıl arası	4		
	5-10 yıl arası	3		
	10 yıldan fazla	1		
Sistemdeki verinin hacmi	10 GB'den fazla	5	4	
	2-10 GB arası	3		
	2 GB'den az	1		
Denetim/İnceleme (%10)				
Sayıştay tarafından yapılmış bilişim sistemleri denetimi durumu	Daha önce hiç denetim yapılmamış	5	5	
	Son denetim yapıldığından beri 3 yıldan fazla zaman geçmiş	3		
	Son 3 yıl içinde denetlenmiş	1		
Sayıştay dışında, iç denetim birimi veya bir organizasyon tarafından yapılmış denetim/incelenme durumu	Daha önce hiç denetim/inceleme yapılmamış	5	2	
	Son denetim/inceleme yapıldığından beri 3 yıldan fazla zaman geçmiş	3		
	Son 3 yıl içinde denetlenmiş/incelenmiş	1		

Sistemle ilgili üçüncü kişiler tarafından verilmiş sertifika durumu	Yok	5	3	
	Var	1		
Toplam Risk Puanı:				
Risk Derecesi:				

Risk Derecesi:

- Toplam Risk puanı 250'den düşükse: **Düşük**
- Toplam Risk puanı 250 ile 325 arasında ise: **Orta**
- Toplam Risk puanı 325 ile 500 arasında ise: **Yüksek**

Ek-3: Denetim/Kontrol Alanları Bazında Risk Değerlendirme Formu

Kurum/Sistem Adı:	
Denetim/Kontrol Alanı:	

Risk belirlenirken, her bir konu için, sorumluluğun uygun şekilde belirlenip belirlenmediği, yeterli ve uygun organizasyonel yapıların oluşturulup oluşturulmadığı, gerekli düzenlemelerin yapılıp yapılmadığı, yeterli ve uygun belgelemenin olup olmadığı, vb. değerlendirilir.

Alt Alan	Konu	Risk (Yüksek/Orta/Düşük)	Denetlenebilirlik (E/H)	Açıklama

Ek-4: Denetim Programı Formu

Kurum/Sistem Adı:	
Denetim/Kontrol Alanı:	

Alt Alan	
Denetim Hedefi	
Referans	

Konu			
Kriter			
Kontrol Sorusu	**İnceleme Yöntemi**	**Kurum Cevabı (Varsa)**	**Denetçi Değerlendirmesi**

Ek-5: Kontrol Seti Formu

Kurum/Sistem Adı:	
Denetim/Kontrol Alanı:	

Konu	Kontrol Sorusu	Kurum Cevabı

Ek-6: Bulgu Formatı

BULGU (No): Bulgu Başlığı

Kriter/Referans

Açıklama

Etki

Çözüm Çalışmaları

(Taslak raporda yer almaz. Gerek görülürse nihai raporda yer verilir.)

Öneri

(Taslak raporda yer almaz. Gerek görülürse nihai raporda yer verilir.)

Ek-7: İzleme Tablosu Formu

Denetlenen Kurum/Sistem Adı:	
Denetim Tarihi:	
Denetim Ekibi:	

Denetim/Kontrol Alanı	**Bulgu**	**Öngörülen Çözüm Tarihi**	**Değerlendirme**	
			I. İzleme	**II. İzleme**

Ek-8: Önerilen Kontrol Değerlendirme Matrisleri

Ek-8.1:
BT Yönetişimi ve Yönetimi
Önerilen Kontrol Değerlendirme Matrisi

İhtiyaçların Belirlenmesi, Yönlendirilmesi ve İzlenmesi	
Denetim Hedefi	Kurumsal görevlerin yerine getirilmesinde BT'nin kullanımına ilişkin olarak Kurum üst yönetimi tarafından yürütülen yönlendirme, değerlendirme ve izleme faaliyetlerinin etkinliğini değerlendirmek
Referans	♦ COBIT 2019 / BAI02 Yönetilen Gereksinimlerin Tanımı ♦ COBIT 2019 / EDM01 Garanti Edilmiş Yönetişim Çerçevesi Kurulumu ve Sürdürülmesi
Konu	**BTY-1 BT İhtiyaçlarının Belirlenmesi** Kurum, iş ve BT ihtiyaçlarını belirlerken uygun bir yöntem ve onay mekanizması izliyor mu?
Kriter	Kurumun gelişen iş ve BT ihtiyaçlarını belirlemeye yönelik tanımlı bir süreci bulunmalı ve üst yönetim bu ihtiyaçları onaylarken yeterli bilgiye sahip olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. İş ve BT ihtiyaçlarının belirlenmesine, analizine ve onaylanmasına yönelik süreç ve mekanizmalar tanımlanmış mı?	• Yeni iş ve BT ihtiyaçlarının belirlenmesine ve değerlendirilmesine yönelik süreçlerin tanımlı olup olmadığının belge incelemesi yoluyla tespit edilmesi (örneğin, gereksinim yönetim süreçleri dokümanı gibi) • İhtiyaçların tanımlı süreçlere uygun şekilde belirlenerek analiz edilip edilmediğinin belge incelemesi ve mülakat yoluyla tespit edilmesi • Belirlenen BT ihtiyaçlarının uygun bir yapı tarafından (örneğin; BT Yönlendirme Kurulu) değerlendirilerek onaylanıp onaylanmadığının belge incelemesi yoluyla tespit edilmesi • İhtiyaçlara ilişkin onaylama ve reddedilme kararları incelenerek, kararların, kurumun ilgili çalışma usul ve esaslarında belirtilen hususlara uygun şekilde alınıp alınmadığının tespit edilmesi
2. Projelerin onaylanmasına ilişkin kararlar alınırken kaynaklar ve beceriler dikkate alınıyor mu?	• Projeleri onaylayan yapının (örneğin; BT Yönlendirme Kurulu), karar alırken; - BT biriminin kapasitesi, - Kaynaklar, - Eğitim ihtiyacı, - Kullanıcıların yeni araç/sistem/uygulamayı kullanabilme yeterliliği gibi hususları dikkate alıp almadığının belge incelemesi ve mülakat yoluyla değerlendirilmesi

Konu	**BTY-2 Liderlik** Üst yönetim, iş ve BT hedeflerinin performansını uygun bir şekilde yönetiyor ve izliyor mu?
Kriter	İş ve BT hedefleri için performans ölçütleri oluşturularak BT Yönlendirme Kurulu veya eşdeğer yapıların periyodik olarak gözden geçirme toplantıları yoluyla gerekli önlemleri alması sağlanmalı; üst yönetime anahtar performans ölçütlerinin mevcut durumu hakkında bilgi verecek bir raporlama sistemi oluşturulmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumda iş ve BT'ye ilişkin hedeflerin performansının yönetilmesi ve izlenmesinden sorumlu bir yapı (örneğin, BT Yönlendirme Kurulu) bulunuyor mu?	• Kurumda iş ve BT hedeflerinin performansının yönetiminden ve izlenmesinden sorumlu bir yapı (örneğin, BT Yönlendirme Kurulu) bulunup bulunmadığının incelenmesi • BT Yönlendirme Kurulunun veya dengi yapının düzenli olarak toplanıp toplanmadığının ve kararlarının kayıt altına alınıp alınmadığının incelenmesi
2. İş ve BT'ye ilişkin performans ölçütleri belirleniyor mu?	• Örnek olarak seçilen projelerde performans ölçütleri incelenerek hem iş hem de BT sistemlerini kapsayacak şekilde oluşturulup oluşturulmadığının belirlenmesi
3. Proje durum raporları veya benzeri raporlar üretilerek performans ölçütleri izleniyor mu?	• Proje durum raporları ve ilgili diğer belgeler incelenerek projeye ilişkin maliyet, program ve performans göstergelerini ve bunlardan sapmaları içerip içermediğinin belirlenmesi • Örnek olarak seçilecek projelerde, üst yönetim tarafından gerçekleştirilen izleme faaliyetleri sonucunda gerekli düzeltme kararlarının alınıp alınmadığının belge incelemesi ve mülakat yoluyla belirlenmesi

Konu	**BTY-3 BT Yatırımları** Kurum BT yatırımlarını uygun şekilde yönetiyor mu?
Kriter	Kurum BT yatırım yönetimine ilişkin süreç ve prosedürlere sahip olmalı; projeler analizler çerçevesinde değerlendirilerek periyodik gözden geçirmeler neticesinde yatırım yönetiminin etkinliği değerlendirilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. BT yatırımlarının yönetimine ilişkin süreçler tanımlanmış mı?	• Mülakat ve belge incelemesi yoluyla, Kurumda BT yatırımlarının yönetimine ilişkin bir süreç, plan ve/veya prosedür bulunup bulunmadığının belirlenmesi
2. BT yatırımlarına ilişkin olarak stratejik planlama çerçevesinde gerekli değerlendirmeler yapılıyor ve dokümante ediliyor mu?	• BT yatırımlarının ulusal stratejik planlar, ulusal dönüşüm programları, üst politika belgeleri ve Kurumun stratejik planı-hedefleri ile ilişkisinin kurulup kurulmadığının incelenmesi • Kaynak verimliliğinin sağlanması ve mükerrerliğin önlenmesi amacıyla, Kurum bünyesindeki mevcut sistemler/projeler ile diğer kurumların benzer nitelikteki sistemleri/projelerinin değerlendirilip değerlendirilmediğinin incelenmesi
3. BT yatırımlarına ilişkin olarak fayda-maliyet analizleri yapılıyor mu?	• Fayda-Maliyet Analiz Raporları incelenerek bu raporların mevcut durumu olduğu gibi (faydaları olduğundan fazla, maliyeti ve süreyi de olduğundan az göstermeyecek şekilde) yansıtıp yansıtmadığının belirlenmesi
4. BT yatırımları belli kriterlere göre önceliklendiriliyor mu?	• Kurumun BT Projeleri Portföyü incelenerek, projelerin belirlenmiş olan kriterlere göre önceliklendirilip önceliklendirilmediğinin tespit edilmesi

5. BT yatırımlarına ilişkin "yap ya da satın al" kararları belirli kriterler temelinde alınıyor mu?	• BT yatırımlarına ilişkin olarak "yap ya da satın al" kararlarının yetenek, beceriler, maliyet, risk, vb. unsurlar temelinde alınıp alınmadığının belge incelemesi ve mülakat yoluyla belirlenmesi
6. BT yatırımlarının durumu izleniyor mu?	• Üretilen Proje Durum Raporları incelenerek maliyet ve takvim açısından izleme yapmaya uygun şekilde düzenlenip düzenlenmediğinin belirlenmesi • Başarısız olma ihtimali bulunan projeler incelenerek - kullanılan metodolojinin proje tipine uygun olup olmadığının, - projede kalite kontrol faaliyetlerinin uygulanıp uygulanmadığının belirlenmesi • Kurum yöneticileri ile görüşülerek belirlenen fayda veya performans kriterlerinin altında olduğu gerekçesiyle sonlandırılan projeler olup olmadığının tespit edilmesi

BT Stratejisi ve Planlama	
Denetim Hedefi	Kurumun, BT plan ve süreçlerini de içeren, kurum genel stratejisi ve amaç/hedefleri ile uyumlu bir BT stratejisinin olup olmadığını, risklerin ve kaynakların BT hedeflerine ulaşmada etkin bir şekilde yönetilip yönetilmediğini değerlendirmek
Referans	♦ Kamu İç Kontrol Standartları Tebliği / 6 ve 12 No'lu Standartlar ♦ COBIT 2019 / APO02 Yönetilen Strateji ♦ COBIT 2019 / APO12 Yönetilen Risk ♦ COBIT 2019 / EDM03 Garanti Edilmiş Risk Optimizasyonu
Konu	**BTY-4 BT Stratejisi** Kurum, BT faaliyetlerine rehberlik edecek bir BT stratejisine sahip mi?
Kriter	Kurumun, iş hedefleri doğrultusunda BT amaç ve ihtiyaçlarına yer veren ve iş ihtiyaçlarına cevap verecek BT kaynaklarının tanımlandığı, periyodik olarak gözden geçirilen ve güncellenen bir BT stratejik planı olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumun müstakil bir BT stratejisi var mı?	• Kurum BT stratejisi incelenirken aşağıdaki hususlar dikkate alınır: - Kurum strateji planı ve bilişim sistemleri strateji planı birlikte değerlendirilerek, kurum bilişim sistemlerinin kurum amaçları doğrultusunda, gerçekleştirilecek faaliyetleri ve başarı göstergelerini de içerecek şekilde geliştirilip geliştirilmediğinin incelenmesi, - BT stratejisinin üst yönetim tarafından onaylanmış ve yazılı halde mevcut olup olmadığının incelenmesi, - BT stratejisinin hazırlanmasında BT Yönlendirme Kurulu ya da eşdeğer bir yapının rolünün Kurul toplantı tutanakları ve BT strateji belgesi üzerinden incelenmesi, - Tanımlanan BT stratejisinin kurum bünyesinde paydaşlarla paylaşılıp paylaşılmadığının incelenmesi, - Mevzuattaki değişikliklerin düzenli olarak izlenerek kurum stratejilerinin güncellenip güncellenmediğinin incelenmesi.

Konu	**BTY-5 Risk Yönetimi** Kurum risklerini uygun bir şekilde yönetiyor mu?
Kriter	Kurumun risk yönetimine ilişkin bir politika ve planı olmalı, risklerin belirlenmesi ve yönetilmesi için gerekli kaynaklar tahsis edilmelidir. BT risklerinin yönetimi için genel risk değerlendirmesi ve stratejik planlarla uyumlu yönetişim süreçleri mevcut olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumda kurumsal risk yönetim planı/politikası veya eşdeğer bir belge var mı?	• Risk yönetim planının/politikasının veya benzeri dokümanların mevcudiyetinin ve aşağıdaki hususları kapsayıp kapsamadığının incelenmesi: - Riskleri anlama ve tanımlama - Riskleri önceliklendirme - Risklerin yönetimi - Risk kayıt sistemi - Yetki ve sorumluluklar • İlgili personelle görüşülerek risklere ilişkin alınması planlanan önlemlerin maliyet analizinin ve kaynak tahsisinin yapılıp yapılmadığının incelenmesi • Toplantı tutanaklarının incelenmesi yoluyla yeni risklerin belirlenerek analiz edilip edilmediğinin tespit edilmesi • İlgili personelle görüşülerek yapılan risk değerlendirmelerinin belirli aralıklarla gözden geçirilip geçirilmediğinin incelenmesi
2. BT'ye ilişkin risk değerlendirmesi yapılıyor ve belgelendiriliyor mu?	• BT risklerinin, genel yönetişim risk ve uyum (GRC) çerçevesinin bir parçası olacak şekilde değerlendirilip değerlendirilmediğinin ilgili dokümanlar yoluyla incelenmesi • BT risk kütüğünün bulunup bulunmadığının ve güncelliğinin sağlanıp sağlanmadığının belge incelemesi yoluyla belirlenmesi
3. Kurum üst yönetimi BT ve diğer riskler hakkında bilgilendiriliyor mu?	• Yönetim ile görüşülerek ve toplantı tutanakları incelenerek üst yönetimin BT ve diğer riskler konusunda bilgi sahibi olup olmadığının incelenmesi

Organizasyon, Standart, Politika ve Prosedürler	
Denetim Hedefi	Kurumun, BT hedeflerini karşılamaya yardımcı olacak organizasyon yapısına, standart, politika ve prosedürlere sahip olup olmadığını değerlendirmek
Referans	♦ COBIT 2019 / APO01 Yönetilen BT Yönetim Çerçevesi
Konu	**BTY-6 Organizasyon Yapısı** BT organizasyon yapısı, kurumun BT hedeflerini ve iş ihtiyaçlarını karşılamaya uygun mu?
Kriter	Kurumdaki BT yapılanması, organizasyon içinde mümkün olduğunca üst düzeyde olmalı, roller ve sorumluluklar açıkça tanımlanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumun müstakil BT birimi var mı?	• Kurumda müstakil bir BT biriminin olup olmadığı ile işlevleri yerine getirecek şekilde örgütlenip örgütlenmediğinin organizasyon şemaları incelenerek değerlendirilmesi • Organizasyon şemaları incelenerek BT biriminin stratejik düzeyde yapılanıp yapılanmadığının incelenmesi
2. Kurumda BT'ye ilişkin iş akışları, rol ve sorumlulukları ayrıntılı olarak tanımlayan dokümanlar var mı?	• Kurumda BT rol ve sorumluklarının ayrıntılı olarak düzenlendiği bir dokümanın var olup olmadığının incelenmesi • Personelin rol ve sorumluluklarının tutarlı olup olmadığının organizasyon şemaları ile görevlendirmelerin incelenerek değerlendirilmesi • Kadro yedeklemesinin yapılıp yapılmadığının organizasyon şemaları ile görevlendirmelerin incelenerek değerlendirilmesi • Görevler ayrılığı ilkesine uyulup uyulmadığının görev tanımları incelenerek, gözlem ve mülakat teknikleri kullanılarak incelenmesi • Bilgi işlem biriminin, iş akışlarına uygun şekilde yapılanıp yapılanmadığı ve işlerini yapıp yapmadığının incelenmesi

Konu	**BTY-7 Politika ve Prosedürler** Kurum, iş ve BT faaliyetlerine rehberlik edecek politika ve prosedürlere sahip mi?
Kriter	Kurum, iş ve BT faaliyetlerine rehberlik etmesi için uygun politika ve prosedürleri yazılı olarak belirlemeli ve ilgililerini bu konuda bilgilendirmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumda BT ile ilgili süreçlerde uyulması gereken kuralları belirleyen standart, politika ve prosedürler var mı?	• Kurumun aşağıda örnekleri verilen genel politika ve prosedürlerin içerisinde BT'ye ilişkin hususların varlığının incelenmesi: - Standartlara Uyum Politikası - Kişisel Verilerin İşlenmesi, Saklanması ve İmhası Politikası - Belgeleme ve Belge Tutma Politikaları - Kaynak Tahsis Politikası - Dış Kaynak Kullanımı Politikası - Kalite Güvence Politikası - İletişim Politikası

	- Karar Alma ve Onaylama Prosedürü • Politika ve prosedürlerin aşağıdaki hususlar göz önünde bulundurularak değerlendirilmesi: - Yazılı halde mevcut olup olmadığı - Üst yönetim tarafından onaylanıp onaylanmadığı - Anlaşılır bir dille yazılıp yazılmadığı - İlgili bütün personelin erişimine açık olup olmadığı - Periyodik olarak veya gerektiğinde güncellenip güncellenmediği - Temel alınan yasal düzenlemeler ve standartlar, kapsam ve yetki, rol ve sorumluluklar, ihtiyaç duyulan kaynak ve araçlar, prosedürlerle bağlantı, uyulmaması halinde uygulanacak kuralların belirtilip belirtilmediği • Örnekleme yoluyla seçilecek personelle politika ve prosedürlere ne ölçüde uyulduğunu anlamak için mülakat yapılması

İnsan Kaynakları ve Eğitim	
Denetim Hedefi	Kurum tarafından yeterince nitelikli/eğitimli personel istihdam edilip edilmediğini, personelin uygun kaynaklara erişiminin olup olmadığını değerlendirmek
Referans	♦ COBIT 2019 / APO07 Yönetilen İnsan Kaynakları
Konu	**BTY-8 İnsan Kaynakları ve Eğitim** Kurum, mevcut ve geleceğe ilişkin insan kaynağı ve diğer kaynak ihtiyaçlarını uygun şekilde yönetiyor mu?
Kriter	Kurum, iş ihtiyaçları doğrultusunda, mevcut ve gelecekteki insan kaynakları ihtiyaçlarını karşılamak için bir plana sahip olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurum insan kaynakları ve eğitim politikalarına sahip mi?	• BT Stratejik Planında mevcut duruma ve geleceğe ilişkin insan ve diğer kaynak gereksinimlerine yer verilip verilmediğinin incelenmesi • Kurumun insan kaynakları ve eğitim politikasının - Kurum üst yönetim tarafından onaylanıp onaylanmadığının - Belirli aralıklarla güncellenip, tüm personele duyurulup duyurulmadığının incelenmesi • İnsan kaynakları ve eğitim politikalarının aşağıdaki hususları içerip içermediğinin incelenmesi - Kurumun faaliyetlerini etkin ve verimli bir şekilde yerine getirebilmesini sağlayacak insan kaynağının niteliklerinin belirlenmesi, seçilmesi ve işe alınması ile eğitimi - Kritik pozisyonların beklenmedik/acil durumlarda veya personelin uzun süreli devamsızlığı halinde boş kalmamasına ilişkin düzenlemeler - Personelin işinin niteliğinde meydana gelen her türlü gelişme ve değişmelerden geri kalmaması için gereken bilgi ve becerileri kazandırmayı amaçlayan eğitim programlarının tespit edilip uygulanması - Kurumda gerçekleştirilen işlerin kapsamı ve insan kaynağı gereksinimi hakkında bilgi toplanması ve bu bilgiyi değerlendirmek üzere iş analizleri yapılması ile değişen koşullara uygun şekilde iş tanımları hazırlanması - Etik ilkelere ve mesleki kurallara uyum

2. Personelin bilgi ve becerilerinin arttırılmasına yönelik eğitim programları yapılıyor mu?	• Eğitimlerin, ilgili tüm birimlerin katılımıyla gerçekleştirilen eğitim ihtiyaç analizlerine dayalı olarak yürütülüp yürütülmediği ve düzenli olarak yapılıp yapılmadığının belge incelemesi ve mülakat yöntemi ile belirlenmesi

Uygunluk	
Denetim Hedefi	Kurumun kendi oluşturduğu politika ve prosedürlere, yasal ve diğer düzenlemelere uyumu güvence altına alacak mekanizmalar kurup kurmadığını değerlendirmek
Referans	♦ TS ISO/IEC 27002 / 18.1 Yasal ve Sözleşmeye Tabi Gereksinimlere Uyum ♦ COBIT 2019 / MEA03 Yönetilen Dış Gereksinimlerle Uyum
Konu	**BTY-9 Uygunluk Mekanizmaları** Kurum, belirlediği politika ve prosedürlerin uygulamasına ilişkin etkin izleme ve değerlendirme mekanizmaları kurmuş mu?
Kriter	Kurum, belirlenmiş bütün politika ve prosedürlerin izlenmesini sağlayacak iç denetim, kalite kontrol gibi mekanizmalara sahip olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. İç denetim birimi bilişim sistemlerini denetliyor mu?	• İç denetim birimi tarafından yapılan bilişim sistemleri denetiminin etkinliğinin aşağıdaki hususlar dikkate alınarak incelenmesi: - İç denetim raporlarının tamamın üst yönetime sunulup sunulmadığı - İç denetim raporlarında önerilere yer verilip verilmediği - Bu öneriler üzerine uygulamada gerekli değişiklik ve düzenlemelerin yapılıp yapılmadığı (Raporlarda yer alan önerilerin yüzde kaçının uygulamaya geçirildiği) - İç denetim çalışmalarının planlama, inceleme ve belgeleme açısından yeterli kalitede olmasını sağlayacak gözetim ve kalite kontrol mekanizmalarının kurulup kurulmadığı - İç denetim biriminde çalışan personele bilişim sistemlerinin denetimi konusunda eğitim verilip verilmediği
2. Kurumda, kalite kontrol/güvence ile proje yönetim ofisleri var mı?	• Organizasyon şemaları incelenerek kurumun BT hizmetleri ile projelerinin başarı ile yürütülmesini sağlamaya yönelik kalite kontrol/güvence ve proje yönetim ofislerinin varlığı ile etkinliğinin belge inceleme/mülakat yoluyla değerlendirilmesi
3. Kurumda bilişim sistemlerinin yürürlükteki düzenlemelere uygunluğu açısından denetlenmesine ilişkin prosedürler oluşturulmuş mu?	• Mevzuata uygunluk denetimine ilişkin prosedürlerinin aşağıdaki hususları içerip içermediğinin incelenmesi: - Görevli birim - Yapılacak denetimin sıklığı - Raporlamanın formatı - Raporların sunulacağı yer - Bulguların değerlendirilmesi • En son ne zaman mevzuata uygunluk denetimi yapıldığının tespit edilmesi • Denetimin kapsamının yeterli olup olmadığının incelenmesi • Denetim bulgularının raporlanıp raporlanmadığının bu bulgular ışığında belirlenen faaliyetlerin ve bu faaliyetlerin ne ölçüde gerçekleştirildiğinin incelenmesi

Ek-8.2:
Sistem Geliştirme ve Edinim
Önerilen Kontrol Değerlendirme Matrisi

Gereksinimlerin Geliştirilmesi ve Yönetimi	
Denetim Hedefi	Kurumun BT sistemlerine ilişkin gereksinimleri belirleme, önceliklendirme ve yönetme süreçlerinin etkinliğini değerlendirmek
Referans	♦ COBIT 2019 / BAI02 Yönetilen Gereksinim Tanımları ♦ COBIT 2019 / BAI03 Yönetilen Çözüm Tanımlama ve Oluşturma
Konu	**SGE-1 Gereksinimlerin Belirlenmesi** Kurum BT sistemleri için kullanıcı gereksinimlerini belirliyor mu?
Kriter	Kurumun yeni BT sistemlerine ya da ek işlevlere yönelik gereksinimleri toplama, inceleme ve gruplandırma süreçleri tanımlı olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Gereksinimlerin belirlenmesine yönelik süreçler tanımlanmış mı?	• Gereksinimlerin belirlenmesine yönelik düzenlemeler incelenerek kullanıcı talep ve ihtiyaçlarının alınması, incelenmesi ve gruplandırılmasına ilişkin süreçlerin tanımlanıp tanımlanmadığının tespit edilmesi
2. Gereksinimlerin belirlenmesine ilgili tarafların katılımı sağlanıyor mu?	• Gereksinimlerin belirlenmesine ilişkin düzenlemeler ve örnek olarak seçilecek uygulamalar incelenerek gereksinim belirleme süreçlerine iş süreç sahiplerinin, kullanıcıların, teknik destek personelinin, bilgi güvenliği temsilcilerinin ve ilgili diğer paydaşların dâhil edilip edilmediğinin tespit edilmesi

Konu	**SGE-2 Gereksinimlerin Yönetimi** Toplanan gereksinimler uygun şekilde yönetiliyor mu?
Kriter	İş ve kullanıcı ihtiyaçlarının en doğru ve maliyet etkin şekilde karşılanması amacıyla geliştirilecek/edinilecek sisteme ilişkin gereksinimler belgelendirilmeli, analiz edilmeli ve izlenmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Gereksinimler dokümante ediliyor mu?	• Gereksinimlerin talep sahibi kişi/birim, tarih, öncelik, maliyet, riskler ve diğer unsurları içerecek şekilde dokümante edilip edilmediğinin incelenmesi • Gereksinimler tespit edilirken bir ön değerlendirme faaliyetinin yürütülüp yürütülmediğinin ve benzer ya da mükerrer gereksinimlerin gruplanıp gruplanmadığının incelenmesi
2. Gereksinimler analiz ediliyor mu?	• Belge incelemesi ve ilgililerle mülakat yaparak gereksinimlerin değerlendirilmesinde ve önceliklendirilmesinde maliyet, iş ihtiyaçları, bilgi güvenliği, acil durumlar ve yeni görev ve sorumluluklar verilmesi gibi kriterlerin göz önüne alınıp alınmadığının belirlenmesi • Gereksinimler hakkında iş süreç sahipleri ve paydaşlar tarafından yapılan değerlendirme ve yorumlar incelenerek analiz ve karar safhalarında bütün görüşlerin değerlendirmeye alınıp alınmadığının belirlenmesi

	• Gereksinimlerin karşılanmasına ilişkin olarak yöntem (adam kiralama, birlikte geliştirme ve çıktı taahhütlü-tamamen karşı taraf geliştirmesi gibi) değerlendirmesi yapılıp yapılmadığının incelenmesi
3. Gereksinimlerin izlemesi yapılıyor mu?	• Gereksinim izlenebilirlik matrisleri incelenerek kabul edilen gereksinimlerin bir geliştirme veya edinim projesine atanıp atanmadığının ve ilgili proje içerisinde izlenip izlenmediğinin belirlenmesi

Proje Yönetimi ve Kontrolü	
Denetim Hedefi	Kurumun sistem geliştirme ve edinim projelerine ilişkin yönetim ve kontrol faaliyetlerinin etkinliğini değerlendirmek
Referans	♦ COBIT 2019 / BAI01 Yönetilen Programlar ♦ COBIT 2019 / BAI11 Yönetilen Projeler
Konu	**SGE-3 Proje Yönetimi** Sistem geliştirme ve edinim projeleri bir plan dâhilinde yürütülüyor mu?
Kriter	Onaylanmış her sistem geliştirme ve edinim projesinin yürütülmesine rehberlik edecek bir proje yönetim planı (veya dengi bir düzenleme) bulunmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Projenin yönetilmesine ilişkin proje yönetim planı (veya dengi düzenleme) var mı?	• Proje yönetim planında (veya dengi düzenlemede) projenin tanımı, kapsamı, maliyeti, takvimi, riskleri ve yönetim yapısının yer alıp almadığının ve iç ve dış paydaşların belirlenip belirlenmediğinin incelenmesi • Planın üst yönetim tarafından onaylanıp onaylanmadığının ve paydaşların yorumlarına yer verilip verilmediğinin incelenmesi • Sürüm/değişiklik kaydı incelenerek planın zaman içerisinde ortaya çıkan değişiklikler uyarınca güncellenip güncellenmediğinin belirlenmesi • Edinim projelerinde ve yüklenici eli ile yürütülen geliştirme projelerinde bir planın veya yüklenicinin gözetiminden sorumlu olacak kişilerin listesinin olup olmadığının incelenmesi • Proje yöneticileri ile mülakat yapılarak hangi sistem geliştirme yaşam döngüsü yönteminin kullanıldığının belirlenmesi
2. Proje yönetimine ilişkin görevlendirmeler yapılıyor ve organizasyon şeması belirleniyor mu?	• Kurum tarafından bir proje yöneticisi görevlendirilip görevlendirilmediğinin, yetkilerinin ve sorumluluklarının tanımlanıp tanımlanmadığının ve bu görevlendirmenin ilgili tüm taraflara bildirilip bildirilmediğinin belge incelemesi yolu ile tespit edilmesi • Geliştirmenin (tamamen veya kısmen) yüklenici tarafından gerçekleştirildiği durumlarda, yüklenici tarafında işin ana sorumlusunun belirlenip belirlenmediğinin ve ilgili taraflara bildirilip bildirilmediğinin belge incelemesi yolu ile tespit edilmesi • Projenin organizasyon şeması incelenerek proje ekibinde yer alan Kurum (ve varsa yüklenici firma) çalışanlarının kimlikleri, pozisyonları, görev ve sorumlulukları (kalite güvence, test, geliştirme, kurulum, destek, vb.) ve sahip olmaları gereken özelliklerin açık bir şekilde tanımlanıp tanımlanmadığının belirlenmesi • Yüklenici eli ile yürütülen projelerde proje yönetimine ilişkin temel faaliyetlerin yüklenici tarafından değil, işin asıl sahibi olan Kurum tarafından yerine getirilip getirilmediğinin incelenmesi

3. Proje kapsamı belirleniyor ve dokümante ediliyor mu?	• Proje kapsamı belirlenirken - Yapılacak işlerin belirlenerek alt parçalara ayrılıp ayrılmadığın, - Her bir alt parça için sorumlu kişilerin/birimlerin, öngörülen tamamlanma süresinin, önce gelen/takip eden ve bağlantılı görevlerin/işlerin, ihtiyaç duyulan personelin yetkinlik seviyesinin ve sayısının tanımlanıp tanımlanmadığının incelenmesi • Proje kapsam bildiriminde - Proje çıktılarının kabulü için yerine getirilmesi gereken koşulların ve kabul kriterlerinin, - Geliştirilen/edinilen sisteme işletim, bakım ve kullanıcı desteği verilip verilmeyeceğinin, (verilecek ise) desteğin kapsam ve içeriğinin, - Lisanslama ve sahipliğe ilişkin hususların, - Proje kapsamı dışında bırakılan hususların yer alıp almadığının belge incelemesi yoluyla tespit edilmesi
4. Projeye ilişkin değişiklik taleplerinin değerlendirilmesi ve onaylanması ya da reddedilmesi amacıyla değişiklik kontrolü gerçekleştiriliyor mu?	• Değişiklik önerilerinin hangi süreçler takip edilerek oluşturulacağının, hangi proje ve/veya kurum yetkilileri tarafından nasıl değerlendirileceğinin ve kabul veya reddedileceğinin ilgili proje veya kurum belgelerinde belirtilip belirtilmediğinin incelenmesi • Değişiklik önerilerinin yazılı olarak kayda alınıp alınmadığının incelenmesi • Değişiklik önerilerinin proje ve ürün kapsamı, süre, maliyet, riskler, yazılım ekibi, müşteri kurumlar, kullanıcılar ve diğer paydaşlar üzerindeki etkilerine ilişkin değerlendirme yapılıp yapılmadığının incelenmesi • Yalnızca onaylanan değişikliklerin gerçekleştirilmesinin sağlanıp sağlanmadığının incelenmesi • Onaylanan değişiklikler sonucunda ilgili proje belgelerinde gerekli güncelleme ve uyarlamaların gerçekleştirilip gerçekleştirilmediğinin incelenmesi
5. Proje için bir takvim hazırlanıyor mu?	• Proje bünyesinde gerçekleştirilecek aktiviteler için süre tahminleri ile başlangıç ve bitiş tarihlerini gösteren bir çizelgenin/takvimin hazırlanıp hazırlanmadığının incelenmesi • Hazırlanan çizelgenin/ takvimin, söz konusu aktiviteler arasındaki (öncüllük-ardıllık gibi) mantıksal ilişkileri ve bağımlılıkları gösterip göstermediğinin ve süreç içerisinde gerektiğinde güncellenip güncellenmediğinin incelenmesi
6. Projenin kaynak ihtiyacı belirleniyor mu?	• Proje bünyesindeki faaliyetleri yerine getirebilmek için kullanılacak kaynakların (insan kaynağı, araç-gereç, tedarik malzemesi ve diğer materyaller) tür, nitelik ve miktarı belirlenerek maliyet tespitinin gerçekleştirilip gerçekleştirilmediğinin incelenmesi
7. Projeye ilişkin riskler belirleniyor ve dokümante ediliyor mu?	• Risklerin başlangıçtan itibaren belirlenerek sınıflandırıldığı ve gerçekleşme ihtimalleri ile yol açacakları etki göz önüne alınarak derecelendirildiği bir risk listesinin/kütüğünün oluşturulup oluşturulmadığının incelenmesi • Risklerin gerçekleşmeleri halinde ne yapılacağının/nasıl bir yol takip edileceğinin ortaya konduğu risk yanıt planlarının hazırlanıp hazırlanmadığının incelenmesi • Risk değerlendirmelerinin süreç içerisinde gerektiğinde güncellenip güncellenmediğinin incelenmesi
8. Proje iletişiminin nasıl yürütüleceği belirleniyor mu?	• İletişim yönetiminde aşağıdaki hususların ele alınıp alınmadığının incelenmesi: - Hangi bilgilerin, kim tarafından, hangi gerekçeyle, hangi zamanlama ile ve kimlere iletileceği

	- İletişimin yöntemi/formatı - Gizli bilgilerin paylaşılması konusunda yetkilendirme yapabilecek olan personelin kimliği - Alt kademe çalışanlarca çözümlenemeyen meselelerin daha üst kademelere intikal ettirilmesine ilişkin havale süreci - Üst yönetimin proje gidişatı hakkında bilgilendirilmesine yönelik süreç - Ortak terminoloji sözlüğü - Eğer mevcut ise proje internet sitesi ile proje yönetim yazılımının kullanımına yönelik detaylar

Konu	**SGE-4 Projenin Kontrolü** Yürütülen projeler etkin şekilde kontrol ediliyor mu?
Kriter	Projeler maliyet, zaman ve performans gerekliliklerine uygunluk açısından izlenmeli ve kontrol edilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Projede izleme ve kontrol faaliyetlerini gerçekleştirmek üzere bir birim/ekip görevlendiriliyor mu?	• Mülakat ve belge incelemesi yapılarak kurum tarafından projelerde bir izleme ve kontrol birimi/komisyonu görevlendirilip görevlendirilmediğinin belirlenmesi
2. Projenin ilerlemesi izleniyor, ölçülüyor, gözden geçiriliyor ve raporlanıyor mu?	• Projeye ilişkin çalışma performansı bilgilerinin (durum raporları, bilgi notları, öneriler, tahminler, vb.) toplanarak ilgililerine raporlanıp raporlanmadığının ve düzenli aralıklarla yapılan gözden geçirme toplantılarında değerlendirilip değerlendirilmediğinin belge incelemesi yoluyla belirlenmesi • Proje maliyet ve zaman temel çizgilerinin proje durum raporları ile karşılaştırılması ve sapma olup olmadığının değerlendirilmesi • Proje yöneticisi ile mülakat yaparak ve raporları inceleyerek varsa önemli sapmalar için uygun düzeltici eylemlerin alınıp alınmadığının belirlenmesi • Proje yönetim ekibi ile mülakat yaparak ve yüklenici ile yapılan toplantıların tutanaklarını inceleyerek tedarikçi eliyle yürütülen proje faaliyetlerine ilişkin izlemenin sıklık ve etkinliğinin değerlendirilmesi • Tedarikçi ile yapılan hizmet seviyesi anlaşması ya da sözleşme incelenerek sözleşme koşullarının (örneğin; tedarikçi tarafından periyodik gözden geçirme faaliyeti yürütülmesi, durum ve ilerleme raporlarının sunulması, risk yönetimi faaliyetlerinin gerçekleştirilmesi, vb.) yerine getirilip getirilmediğinin tespit edilmesi • Kurumun sözleşme/ihale biriminin sorumlusu ile mülakat yapılarak hizmet seviyesi anlaşmalarının bulunmadığı durumlarda yüklenicinin gözetiminin nasıl sağlandığının belirlenmesi

Uygulama Geliştirme	
Denetim Hedefi	Tasarım ve kodlama süreçlerinin etkin olarak yönetilip yönetilmediğini değerlendirmek
Referans	♦ COBIT 2019 / BAI03 Yönetilen Çözüm Tanımlama ve Oluşturma ♦ TS ISO/IEC 27002 / 9.4.5 Program Kaynak Koduna Erişim Kontrolü ♦ TS ISO/IEC 27002 / 14.2.6 Güvenli Geliştirme Ortamı ♦ 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi / Tedbir 13
Konu	**SGE-5 Tasarım** Tasarım faaliyetleri uygun şekilde gerçekleştiriliyor mu?
Kriter	Tasarım dokümanları geliştirilerek sistemin tüm boyutlarıyla ele alınması sağlanmalı, bilgi güvenliği ve birlikte çalışabilirlik hususları göz önüne alınmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Tasarım dokümanları oluşturuluyor mu?	• Tasarım çalışmaları kapsamında aşağıdaki hususların ele alınıp alınmadığının incelenmesi: - İş akış diyagramlarının oluşturulması - İş kuralları, istisna ve muafiyetlerin belirlenmesi - Veri akış diyagramlarıyla gösterilen iş prosedürlerinin tanımlanması - Veri öğelerinin isimlerinin, cinslerinin, değer aralıklarının, kaynaklarının ve erişim yetkilerinin kurumsal veri sözlüğüne uygun şekilde belirlenmesi - Veri tabanında yer alan tablolar arasındaki ilişkiyi gösteren mantıksal veri yapısının çıkartılması - Veri saklama (verinin saklanma şekli), konumlandırma (verinin saklanacağı yer), çekme (veriye ulaşılması ve elde edilmesi için yapılması gerekenler) ve aktarım (geliştirilecek yazılımın daha önceden kullanılan bir yazılımın yerine geçeceği durumlarda) kurallarının tanımlanması - Kullanıcıların çalışacakları önyüzlerin tasarımları hakkında detayların belirlenmesi - Performans kriterleri ve test stratejilerinin belirlenmesi - Hata ve felaket kurtarmaya ilişkin ihtiyaç ve düzenlemelerin belirlenmesi - Yedekleme ve arşivlemeye ilişkin plan ve prosedürlerin tespit edilmesi - Denetim ve kontrol izleri bağlamında yapılacakların tespit edilmesi - İşletim sistemi, veri tabanı ve ağ ihtiyaçlarının belirlenmesi - Kurumdaki mevcut sistemler ile entegrasyonun nasıl sağlanacağının belirtilmesi - Yazılım tarafından sağlanacak verilerin dışa nasıl açılacağının ve dış sistemlerle entegrasyonun nasıl gerçekleştirileceğinin tespit edilmesi • Kullanıcıların, BT uzmanlarının, paydaşların ve ilgili yönetim birimlerinin tasarım sürecindeki rol ve sorumluluklarının belirlenip belirlenmediğinin incelenmesi • Tasarım faaliyetlerinin gerçekleştirilmesi, takibi ve güncellenmesi için bir araç kullanılıp kullanılmadığının incelenmesi
2. Tasarım çalışmalarında bilgi güvenliği gerekleri göz önüne alınıyor mu?	• Kurum bilgi güvenliği temsilcilerinin/ekibinin tasarım çalışmalarında yer alıp almadığının incelenmesi • Tasarım çalışmaları esnasında aşağıda yer verilen hususların ele alınıp alınmadığının belge incelemesi yoluyla tespit edilmesi:

	- Kurumun bilgi güvenliği politikaları ve prosedürleri ile uyum - Veriler ve çıktıların güvenlik sınıflandırmaları (“Tasnif Dışı”, “Hizmete Özel”, “Özel”, “Gizli”, vb.) - Kullanıcıların erişim kontrol prosedürleri - Güvenli oturum açma prosedürleri - Ayrıcalık destek programlarının kullanımı - …
3. Tasarım çalışmalarında diğer sistemlerle etkileşim ve birlikte çalışabilirlik hususları değerlendiriliyor mu?	• Belge incelemesi ve ilgililerle mülakat yapılarak Kurumun sahip olduğu diğer sistemler ve diğer Kurumların ilgili sistemleri ile etkileşim ve birlikte çalışabilirlik hususlarının değerlendirilip değerlendirilmediğinin incelenmesi

Konu	**SGE-6 Kodlama** Kodlama işlemleri uygun şekilde gerçekleştiriliyor mu?
Kriter	Kodlama işlemleri belirli prosedürler çerçevesinde ve güvenli yazılım geliştirme kurallarına uygun şekilde gerçekleştirilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kodlama işlemleri belirlenen prosedürler çerçevesinde yürütülüyor mu?	• Kodlama işlemlerine ilişkin prosedürlerin aşağıdaki hususları kapsayıp kapsamadığının incelenmesi: - Kodların nerede saklanacağı - Kodlara kimlerin nasıl erişeceği - Kullanılacak fonksiyonların özellikleri - İsimlendirme kuralları - Yorum-açıklama satırları - Versiyon takibi/kontrolünün nasıl yapılacağı • Kod yazımında isimlendirme kurallarına uyulup uyulmadığının incelenmesi • Kod parçalarının ne amaçla kullanıldığına yönelik açıklayıcı bilgi sağlamak amacıyla kod yazımında yorum satırlarına yer verilip verilmediğinin incelenmesi • Kod üzerinde gerçekleştirilen yenilik ve değişikliklerin takibi amacıyla sürüm kontrolünün sağlanıp sağlanmadığının incelenmesi
2. Güvenli kodlama gereksinimlerine uyuluyor mu?	• Güvenli kodlama gereksinimlerinin sağlanmasına yönelik süreçlerle ilgili olarak: - Kaynak kodların bulunduğu ortamlara sadece yetkili kişilerin erişip erişmediğinin incelenmesi - Kaynak kodların bulunduğu ortamlara erişimlerin kaydedilip edilmediği ve bu kayıtların saklanıp saklanmadığının incelenmesi - Kaynak kodların yazılımcı veya diğer kullanıcı bilgisayarlarına indirilmesine imkân tanınıp tanınmadığının incelenmesi - Kaynak kodlar yazılımcı veya diğer kullanıcı bilgisayarlarına indirilebiliyorsa, indirme kayıtlarının tutulup tutulmadığı ve kod bütünlüğünün sağlanıp sağlanmadığının incelenmesi - Yazılım ekibinin, geliştirdiği kodları güvenlik açıklıkları yönünden değerlendirmeye tabi tutup tutmadığının incelenmesi

Uygulama Edinim (Tedarik)	
Denetim Hedefi	Kurumun tedarik faaliyetlerini yürürlükteki mevzuata ve kendi düzenlemelerine uygun olarak gerçekleştirip gerçekleştirmediğini değerlendirmek
Referans	♦ COBIT 2019 / BAI03.04 Çözüm Bileşenlerini Tedarik Edin ♦ COBIT 2019 / APO10 Yönetilen Tedarikçiler
Konu	**SGE-7 Plan ve Prosedürler** Kurumda tedarik faaliyetlerinin gerçekleştirilmesine ilişkin bir plan ya da prosedür bulunuyor mu?
Kriter	Tedarik faaliyetleri (ihtiyaç/talep dokümanlarının ve şartnamelerin hazırlanması, tekliflerin alınması ve değerlendirilmesi, yüklenicinin seçimi, sözleşmenin imzalanması, vb.) yürürlükteki mevzuata ve Kurumun bu alandaki düzenlemelerine uygun şekilde gerçekleştirilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumun bir tedarik planı veya prosedürü var mı?	• Tedarik planı veya prosedürü incelenerek kullanıcıların süreçlere dâhil edilmesi, tekliflerin rekabetçi bir şekilde alınması, sözleşme öncesinde mümkün olan alanlarda piyasa araştırması yapılması ve yüklenici seçiminin objektif kriterlere dayanması gibi hususları içerip içermediğinin belirlenmesi • Sözleşme/ihale biriminde görev yapan personel ile mülakat yapılarak satın alma/ihale dosyasının tamlığını nasıl sağladıklarının (örneğin, kullanıcıların, paydaşların ve uygun olduğu durumlarda uzmanların görüşlerinin alınması) değerlendirilmesi • Kullanıcılar veya iş süreç sahipleri ile mülakat yapılarak gereksinimler oluşturulurken kendilerine danışılıp danışılmadığının ve ihale dokümanlarındaki teknik gereksinimler hakkında onaylarının alınıp alınmadığının belirlenmesi • Belge incelemesi ve ilgililerle mülakat yapılarak çözüm alternatiflerinin karşılaştırmalı şekilde değerlendirilerek sonuçlarının ilgililerine sunulup sunulmadığının belirlenmesi
2. Tedarik süreçlerinin mevzuata uygunluğu sağlanıyor mu?	• Kurumun sözleşme/ihale biriminin sorumlusu ile mülakat yapılarak ve seçilecek örnekler incelenerek tedarik süreçlerinin yürürlükteki yasa ve düzenlemelere uygun şekilde yürütülüp yürütülmediğinin belirlenmesi

Konu	**SGE-8 Yüklenicilerin Seçimi** Yüklenicilerin seçiminde uygun kriterler kullanılıyor mu?
Kriter	Yüklenicilerin seçiminde tarafsız olunmalı ve önceden belirlenmiş olan kriterler kullanılmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Yüklenicilerin seçimine yönelik süreçler etkin şekilde yürütülüyor mu?	• Belge incelemesi ve ilgililerle mülakat yapılarak yüklenicilerin seçiminin rekabet, şeffaflık ve hesap verebilirliği sağlayan bir şekilde gerçekleştirilip gerçekleştirilmediğinin belirlenmesi • Yüklenici puanlama matrisi ya da dengi belge incelenerek seçim kriterleri ile tutarlı olup olmadığının belirlenmesi

	• Belge incelemesi ve ilgililerle mülakat yapılarak yüklenici firma ile sözleşme imzalanmadan önce sözleşme taslağı hakkında kurumun hukuk biriminden görüş alınıp alınmadığının belirlenmesi • Belge incelemesi yapılarak yüklenicinin teklifi ile imzalanan sözleşme arasında tutarsızlık bulunup bulunmadığının belirlenmesi

Kalite Güvence ve Test	
Denetim Hedefi	Sistem geliştirme ve edinim faaliyetleri kapsamındaki kalite güvence ve test süreçlerinin etkinliğini değerlendirmek
Referans	♦ 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi / Tedbir 13 ♦ TS ISO/IEC 27002 / 14.2.6 Güvenli Geliştirme Ortamı ♦ TS ISO/IEC 27002 / 12.1.4 Geliştirme, Test ve İşletim Ortamlarının Birbirinden Ayrılması ♦ TS ISO/IEC 27002 / 14.3 Test Verisi ♦ COBIT 2019 / BAI03.06 Kalite Güvence Uygulayın ♦ COBIT 2019 / BAI03.07 Çözüm Testi İçin Hazırlık Yapın ♦ COBIT 2019 / BAI03.08 Çözüm Testlerini Gerçekleştirin
Konu	**SGE-9 Kalite Güvence** Kurumda sistem geliştirme ve edinime yönelik kalite güvence faaliyetleri yürütülüyor mu?
Kriter	Sistem geliştirme ve edinime ilişkin kalite güvence faaliyetleri rolleri ve sorumlulukları belirlenmiş bir birim/ekip tarafından ve tanımlanmış olan süreç ve prosedürlere göre yürütülmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Sistem geliştirme ve edinim faaliyetlerinde kalite güvencesine yönelik süreç ve prosedürler tanımlanmış mı?	• Kalite güvencesine yönelik süreç ve prosedürlerde aşağıdaki hususların yer alıp almadığının incelenmesi: - Ölçülebilir, net ve anlaşılır bir şekilde ifade edilmiş kalite ölçütleri - Takip edilecek ölçümler-metrikler - Paydaşlar tarafından belirlenen ve üzerinde uzlaşılan kalite hedefleri - Kalite gözden geçirmelerinin türleri, sorumluları, katılımcıları ve takvimi
2. Sistem geliştirme ve edinim faaliyetlerinde bir ekip tarafından kalite güvencesine yönelik çalışmalar yürütülüyor mu?	• Kalite güvence politikası/planı incelenerek örnek olarak seçilecek sistem geliştirme ve edinim faaliyetlerinde kalite güvence çalışmalarından sorumlu bir ekibin bulunup bulunmadığının belirlenmesi • Görevler ayrılığı ilkesi uyarınca, kalite güvence çalışmaları kapsamında görev alan personel ile sistem geliştirme ve edinim faaliyetlerini yürüten personelin ayrı kişiler olup olmadığının proje organizasyon şeması ve ilgili dokümanlar üzerinden incelenmesi • Kalite güvence prosedürleri incelenerek ve kalite güvence ekibi ile mülakat yapılarak - Gereksinim tanımlama dokümanı, kullanıcı kılavuzları, vb. belgelerin gözden geçirilip geçirilmediğinin, - Tasarım ve diğer konulara ilişkin değerlendirme toplantılarına iştirak edilip edilmediğinin incelenmesi • Kalite güvence ekibi tarafından hazırlanan raporlar incelenerek hangi hususların tespit edildiğinin (proje ekibinin proje planına, benimsenen

	sistem geliştirme yaşam döngüsüne ve ilgili değerlendirmelere uyup uymadığı, vb.) ve kime raporlandığının belirlenmesi • Tespit edilen hususlara yönelik düzeltici ve önleyici eylemler ve/veya değişiklik talepleri kararlaştırılıp kararlaştırılmadığının belge incelemesi yoluyla tespit edilmesi

Konu	**SGE-10 Test** Geliştirilen/edinilen BT sistemleri üzerinde testler planlanıyor ve gerçekleştiriliyor mu?
Kriter	Geliştirilen ve edinilen sistemler üzerinde gerçekleştirilecek testler planlanmalı, planlandığı şekilde uygulanmalı ve sistem, test sonuçlarına göre kabul veya reddedilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Gerçekleştirilecek testler planlanıyor mu?	• Test planı incelenerek aşağıdaki hususlara yer verilip verilmediğinin belirlenmesi: - Test ortamı ve buna ilişkin donanım ve yazılım özellikleri - Test verisi - Test ekibi, roller ve sorumluluklar - Detaylı test adımları, test senaryoları - Kabul kriterleri - Test sonuçlarının belgelenmesi ve saklanması - Hata ve problemlerin çözümü • Test planı incelenerek ve ilgililerle mülakat yapılarak; - İşlevsellik, - Performans, - Kapasite, - Mevcut altyapı ve diğer uygulamalar ile entegrasyon/birlikte çalışabilirlik, - Güvenlik konularına ilişkin testlerin planlanıp planlanmadığının belirlenmesi
2. Test ortamı bulunuyor mu?	• Belge incelemesi, ilgililerle mülakat (ve gerekli görüldüğünde teknik inceleme) yapılarak; - Test ortamının geliştirme ve ürün ortamlarından fiziksel ve mantıksal olarak ayrıştırılıp ayrıştırılmadığının, - Test ortamının dışarıdan erişime kapatılıp kapatılmadığının, - Test ortamına erişimlerin kayıt altına alınıp alınmadığının, - Canlı ortamda (geliştirme ve ürün ortamlarında) test yapılmasının engellenip engellenmediğinin, - Test ortamının mevcut teknolojik koşulları, kullanıcı tiplerini, işlem tiplerini ve iş süreçlerini gerçeğe yakın bir biçimde yansıtıp yansıtmadığının, - Test ortamında gerçek verilerin kullanılıp kullanılmadığının, kullanılıyor ise anonimleştirme ve maskeleme gibi yöntemlerin uygulanıp uygulanmadığının belirlenmesi
3. Geliştirilen/edinilen sistem plana uygun şekilde test ediliyor mu?	• Test tutanakları incelenerek - Test planında öngörülen testlerin gerçekleştirilip gerçekleştirilmediğinin,

	- Yazılımı geliştiren ve test eden personelin ayrı kişiler olup olmadığının, - Test sonuçlarının ilgililerine iletilip iletilmediğinin belirlenmesi • Belge incelemesi ve ilgililerle mülakat yapılarak hata ve problemlerin çözümüne ve ilgili bileşenin tekrar test edilmesine yönelik çalışma yürütülüp yürütülmediğinin belirlenmesi • Gözlem ve ilgililerle mülakat yapılarak test faaliyetlerinin gerçekleştirilmesi ve takibi için bir araç kullanılıp kullanılmadığının incelenmesi

Kurulum ve Değişiklikler	
Denetim Hedefi	Geliştirilen/edinilen sistemlerde kurulum, yapılandırma, değişiklikler ve kurulum sonrası izlemeye ilişkin süreçlerin etkinliğini değerlendirmek
Referans	♦ 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi / Tedbir 12 ♦ COBIT 2019 / BAI03.05 Çözümler Oluşturun ♦ COBIT 2019 / BAI03.10 Çözümleri Koruyun ♦ COBIT 2019 / BAI07 Yönetilen BT Değişiklik Kabulü ve Geçişi
Konu	**SGE-11 Kurulum ve Yapılandırma** Geliştirilen/edinilen sistemlerin kurulumuna ve yapılandırılmasına yönelik süreçler tanımlanıyor ve uygulanıyor mu?
Kriter	Geliştirilen/edinilen sistemler belgelendirilmeli, kurulumuna ve yapılandırılmasına yönelik gereklilikler tanımlanarak uygulanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Geliştirilen/edinilen sistemler ilgili kullanıcılar tarafından işlevsellik, tasarım, kalite ve performans açılarından kabul testine tabi tutuluyor mu?	• İlgililerle mülakat ve belge incelemesi yapılarak kullanıcı kabul test senaryoları ve kabul kriterleri oluşturulurken son kullanıcıların sürece katılıp katılmadığının belirlenmesi • Belge incelemesi, mülakat ve gözlem yapılarak kabul testlerinin test ortamında gerçekleştirilip gerçekleştirilmediğinin belirlenmesi • Test sonuçlarının dokümante edilip edilmediğinin belge incelemesi yoluyla belirlenmesi • Test tutanakları incelenerek, kullanıcı kabul testlerinin - Yazılım ekibinden bağımsız son kullanıcılar tarafından gerçekleştirilip gerçekleştirilmediğinin, - Sonuçlarının ilgililerine raporlanıp raporlanmadığının incelenmesi • Belge incelemesi ve mülakat yapılarak testler sonucunda onay verilmeyen hususlara yönelik gerekli düzeltme ve iyileştirmelerin yapılıp yapılmadığının ve yeniden test edilip edilmediğinin belirlenmesi
2. Edinilen yazılımın kullanım amacına uygun olmayan bir özellik ve arka kapı açıklığı içermediğine dair üretici ve/veya tedarikçiden taahhütname alınıyor mu?	• Belge incelemesi yapılarak, edinilen yazılımın kullanım amacına uygun olmayan bir özellik ve arka kapı açıklığı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) içermediğine dair üretici ve/veya tedarikçiden taahhütname alınıp alınmadığının belirlenmesi

3. Geliştirilen/edinilen sistemlerin uygulamaya alınmasına yönelik süreçler tanımlanıyor mu?	• Belge incelemesi yapılarak uygulamaya alma süreçlerinde aşağıdaki hususların ele alınıp alınmadığının tespit edilmesi: - Uygulamaya alma adımlarının belirlenmesi - Uygulamaya alma takviminin belirlenmesi - Uygulamaya alma süreçlerindeki roller ve sorumlulukların tanımlanması - Uygulamaya alma sonrasında izleme ve gözden geçirme faaliyetlerinin gerçekleştirilmesi
4. Geliştirilen/edinilen sistemlerin ilgili diğer BT bileşenleri ile uyumunu sağlamaya yönelik çalışmalar yapılıyor mu?	• Belge incelemesi ve ilgililerle mülakat yapılarak kurumdaki ilgili BT bileşenlerinin geliştirilen/edinilen sistemin tasarımına, kalite ve bilgi güvenliği ihtiyaçlarına uygun şekilde yapılandırılıp yapılandırılmadığının belirlenmesi
5. Geliştirilen/edinilen sistemler kullanılabilirlik, yönetim, destek ve bakım açısından belgelendiriliyor mu?	• Belge incelemesi yapılarak geliştirilen/edinilen sistemin tüm bileşenlerinin (kullanılabilirlik, yönetim, destek ve bakım açısından) aşağıdaki hususları kapsayacak şekilde belgelendirilip belgelendirilmediğinin belirlenmesi: - Kurulum kılavuzu - İşletim talimatları - Yönetim talimatları - Kullanıcı kılavuzları - Süreç tasarımına ilişkin akış şemaları ve tanımlamalar - Arayüz tanımlamaları - Kaynak kodu ve prosedürlerine ilişkin yorumlar - Diğer uygulamalar ve BT altyapısı ile ilişkiler
6. Geliştirilen/edinilen sistemlere ilişkin bakım, destek, iş sürekliliği ve eğitim konularında planlama yapılıyor mu?	• Belge incelemesi yapılarak geliştirilen/edinilen sistemle ilgili bakım faaliyetlerinin planlanıp planlanmadığının belirlenmesi • Belge incelemesi ve gözlem yapılarak geliştirilen/edinilen sistemle ilgili sorulara cevap verilmesi ve gelen hata ve önerilerin kayıt altına alınması amacıyla bir talep ve destek yönetim sistemi kurulup kurulmadığının belirlenmesi • Belge incelemesi yapılarak kurumun iş sürekliliği ve felaket kurtarma planlamasında geliştirilen/edinilen sistemin uygulamaya alınması nedeniyle gerekli değişiklik ve uyarlamaların gerçekleştirilip gerçekleştirilmediğinin belirlenmesi • Belge incelemesi ve ilgililerle mülakat yapılarak geliştirilen/edinilen sistemin işletilmesi ve kullanılmasına yönelik gerekli eğitimlerin planlanıp planlanmadığının ve temin edilip edilmediğinin belirlenmesi
7. Kurulumu gerçekleştirilen sistemlerin yönetimine ve işletilmesine ilişkin sorumlulukların ilgili iş birimine devri gerçekleştiriliyor mu?	• Belge incelemesi ve ilgililerle mülakat yapılarak uygulamaya alınan sistemin yönetiminin kullanıcılara/iş sahiplerine devredilip edilmediğinin belirlenmesi • Belge incelemesi ve ilgililerle mülakat yapılarak uygulamaya alınan sistemin destek hizmetinin bilgi işlem birimine devredilip edilmediğinin belirlenmesi
8. Geliştirilen sistem daha önceden kullanılan bir sistemin yerine geçecekse veri aktarım prosedürleri belirleniyor mu?	• Belge incelemesi ve ilgililerle mülakat yapılarak verinin aktarımında aşağıdaki hususların dikkate alınıp alınmadığının tespit edilmesi: - Aktarılacak verinin belirlenmesi - Veri aktarımında kullanılacak yöntemin belirlenmesi - Aktarma işlemlerinin sırasının planlanması - Aktarmaya ilişkin görev ve sorumlulukların belirlenmesi - Aktarım işlemlerinin izlenmesi, kaydedilmesi ve raporlanması - Aktarılması mümkün olmayacak verinin belirlenmesi ve raporlanması

	- Aktarım sonrası önceki sistemdeki verinin silinmesi
9. Devreye alınan yeni sistem ve yerine geçeceği mevcut sistem birlikte çalıştırılıyor ve elde edilen sonuçlar değerlendiriliyor mu?	• Belge incelemesi ve ilgililerle mülakat yapılarak birlikte çalıştırma işlemlerinin yapılıp yapılmadığının, elde edilen çıktılar arasında uyumluluğun sağlanıp sağlanmadığının ve çıktılar arasında uyumsuzluk varsa nedenlerinin araştırılıp araştırılmadığının tespit edilmesi

Konu	**SGE-12 Kurulum Sonrası İzleme** Geliştirilen/edinilen sistemlerde kurulum sonrası izleme gerçekleştiriliyor mu?
Kriter	Geliştirilen/edinilen sistem uygulamaya alındıktan sonra izlenmeli ve değerlendirilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Geliştirilen/edinilen sistem, gereksinim belirleme safhasında tanımlanan özellikler/yetenekler (ve varsa bunlardan sapmalar) açısından gözden geçiriliyor mu?	• Gözden geçirme faaliyetlerinin aşağıdaki hususları karşılayıp karşılamadığının belge incelemesi ve mülakat yoluyla belirlenmesi - İş amaçlarına uygunluk - Kullanıcı beklentilerini karşılama - Teknik koşulları karşılama - Beklenmeyen durumlar/etkiler - Maliyetler ve faydalar • Gözden geçirme faaliyetlerinde kullanılacak başarı kriterlerinin belirlenmesinde ilgili iş süreci ve/veya talep sahiplerinin yer alıp almadığının belge incelemesi ve mülakat yoluyla belirlenmesi

Konu	**SGE-13 Değişiklikler** Geliştirilen/edinilen sistemlerde/uygulamalarda gerçekleştirilen değişiklikler yönetiliyor mu?
Kriter	Geliştirilen/edinilen sistemlerde/uygulamalarda yalnızca yetkilendirilmiş ve onaylanan değişikliklerin gerçekleştirilmesi sağlanmalı ve gerçekleştirilen değişikliklerin kaydı tutulmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Yetkisiz değişikliklerin yapılmasını önleyecek mekanizmalar oluşturulmuş mu?	• Değişiklikleri yapabilecek kullanıcıların yetkilendirilmesine yönelik bir süreç tanımlanıp tanımlanmadığının belge incelemesi yoluyla tespit edilmesi • Değişiklik yapma yetkisine sahip olan kullanıcıların listesinin düzenli olarak gözden geçirilip geçirilmediğinin incelenmesi • Geliştirme ve ürün (canlı) ortamlarının birbirinden ayrılıp ayrılmadığının belge incelemesi ve mülakat yoluyla belirlenmesi • Çalışan uygulamanın kodlarının değiştirilmemesini sağlayacak önlemler (canlı ortama erişimlerin kısıtlanması, kaynak kodun özetinin saklanması, kaynak kodun konfigürasyon yönetim aracında bulunan sürüm numarasının (build number) saklanması, vb.) alınıp alınmadığının belge/kayıt incelemesi ve mülakat yoluyla belirlenmesi

2. Gerçekleştirilen değişikliklerin kaydı tutuluyor mu?	• Yapılan değişiklikler için (işletim sistemi, ağ veya uygulama seviyesinde) iz kaydı tutulup tutulmadığının belge/kayıt incelemesi ve mülakat yoluyla belirlenmesi

Ek-8.3:
BT İşletimi
Önerilen Kontrol Değerlendirme Matrisi

Hizmet Seviyesi Yönetimi	
Denetim Hedefi	Kurumun, BT hizmetlerinin üzerinde anlaşma sağlanan iç HSA'lara veya sözleşmelere göre yürütülmesinin takibini yapıp yapmadığını değerlendirmek
Referans	♦ COBIT 2019 / APO09.03 Hizmet Sözleşmelerini Tanımlayın ve Hazırlayın ♦ ITIL V4 / Hizmet Yönetimi Uygulamaları 5.2.15 Hizmet Seviyesi Yönetimi
Konu	**İB-1 Temel Parametreler** İş birimleri ile BT birimi arasında düzenlenen iç HSA'lar temel hizmet kriterlerini içeriyor mu?
Kriter	HSA'lar iyi uygulama örneklerinde yer verilen (iş süreç sahipleri ile BT destek ekibi arasındaki sorumluluk dağılımı, iş hedefleri, hizmet teklif ve ölçütleri, problem türleri tanımı, yardım masası sorumlulukları gibi) hususları içermelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Hizmet seviyeleri yazılı olarak belirleniyor mu? (HSA'lar var mı?)	• Sunulan BT hizmetleri için hizmet sağlayıcılarla düzenlenmiş yazılı HSA'lar olup olmadığının belge incelemesi yoluyla belirlenmesi • Süreç sahiplerinin HSA'larda imzasının olup olmadığının incelenmesi
2. HSA'lar gerekli temel bilgileri içeriyor mu?	• HSA'ların gerekli kriterleri/hususları kapsayıp kapsamadığının incelenmesi (detaylı ve ölçülebilir hizmet seviyesi hedefleri, kapsam dâhilinde olan/ olmayan sistem ve hizmetler, hizmet kalitesi, uygulama düzeyinde destek ve sorun giderme, sistemin erişilebilirliği, yardım masası saatleri, problemin ciddiyetine bağlı olarak yanıt ve çözüm süreleri, bakım takvimi, vb.)
3. Düzenlenen HSA'lara ilişkin kullanıcıların farkındalığı var mı?	• Düzenlenen HSA'lardan, hizmetlerden faydalanan birimlerde ve BT biriminde çalışan tüm kullanıcıların haberdar olup olmadığının mülakatlar yoluyla incelenmesi

Konu	**İB-2 Uygunluk** BT hizmetlerinin HSA'lar çerçevesinde yürütülüp yürütülmediğinin takibi için uygun mekanizmalar oluşturulmuş mu?
Kriter	HSA'lar uygulanmalı, izlenmeli ve gerektiğinde değiştirilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. BT hizmetlerinin, HSA'lara uygun biçimde sunulup sunulmadığı izleniyor ve raporlanıyor mu?	• HSA'lara uyulduğunun teyidi için; BT personeli ile görüşülmesi ve aşağıdaki hususların incelenmesi: - Yardım masası personelinin performans ölçümleri - İzleme araçlarının kullanılması - Destek görevi önceliklendirmesi - Ağ ve uygulama için temel/dayanak toplanması

	- Yanıt süresine ilişkin veriler - Yedekleme sıklığı - Yedeklenen verilerin test edilmesi • Yapılan izlemeler sonucu oluşturulan yazılı ve periyodik raporların var olup olmadığının, varsa tüm paydaşlarla paylaşılıp paylaşılmadığının incelenmesi • BT birimi tarafından günlük olarak veya belirli zaman aralıklarıyla üretilen raporlar/trend grafikleri incelenerek; - Üzerinde anlaşma sağlanan göstergelerin hepsinin izlenip izlenmediğinin - Hangi göstergelerin ölçüldüğünün ve yönetime periyodik olarak rapor edildiğinin belirlenmesi • Yardım masası faaliyet raporlarının yönetim tarafından dikkate alınıp alınmadığının ve raporlarda yer alan kritik hususların, satın alma kararları ile HSA'ların periyodik gözden geçirmelerinde değerlendirilip değerlendirilmediğinin belge incelenmesi yoluyla belirlenmesi • HSA'larda belirlenen operasyonel parametreler karşılanmadığında BT birimi tarafından ya da -BT destek hizmetinin dış kaynak kullanımı yoluyla alınması halinde- kurum yönetimi tarafından hangi eylemlerin yerine getirildiğinin incelenmesi
2. HSA'lar gerektiğinde değiştirilebiliyor mu?	• HSA'lar içerisinde yer alan hedefler ve koşullardan geçerli olmayanların HSA'lardan kaldırılıp kaldırılmadığının, güncellenen hedefler olup olmadığının yazılı HSA'lar karşılaştırılarak incelenmesi

Konu	**İB-3 Etkililik** BT hizmet yönetimi, kurum iş hedeflerini karşılamaya yardımcı oluyor ve kullanıcıların memnuniyetini sağlıyor mu?
Kriter	BT hizmetlerinde, iş ihtiyaç ve hedefleri doğrultusunda belirlenen performans ölçütlerine ulaşılmalı ve kullanıcıların memnuniyeti sağlanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kullanıcı memnuniyeti ölçülüyor mu?	• Kullanıcı memnuniyetinin anket ve diğer yöntemlerle ölçülüp ölçülmediğinin belge incelemesi ve mülakat yoluyla belirlenmesi • Gerçekleştirilen ölçümlerin sonuçlarının düzenli olarak raporlanıp raporlanmadığının ve ilgililerce değerlendirilip değerlendirilmediğinin belge incelemesi ve mülakat yoluyla belirlenmesi • Kullanıcılar ile görüşülerek yardım masası ve BT destek birimi tarafından sağlanan hizmetin kalitesinden memnun olup olmadıklarına ilişkin bilgi edinilmesi
2. İzleme sonuçları dikkate alınarak hizmet sunumuna uygun olmayan durumlar ve hedeflerden sapmalar belirlenip gerekli iyileştirme faaliyetleri yapılıyor mu?	• Yönetim tarafından periyodik olarak HSA parametrelerinin ve hizmet kalitesi unsurlarının gözden geçirilip geçirilmediğinin kontrol edilmesi • Bildirilen sorunlar için geliştirilen çözüm süresinin HSA'larda belirlenen eşik değerden daha az olup olmadığının incelenmesi • Yardım masası raporlarının incelenerek kritik hizmetlere ilişkin sorunların kullanıcılar tarafından bildirilmeden önce önlenip önlenmediğinin belirlenmesi • BT birimi ile hizmetlerden faydalanan birimler tarafından, izleme raporlarında belirtilen hizmet servislerine ilişkin gerçekleştirilebilecek iyileştirme faaliyetlerinin planlanıp planlanmadığının ve belirlenen iyileştirme faaliyetlerinin bir sonraki değerlendirme toplantısında takip

	edilip edilmediğinin mevcut yazılı gözden geçirme toplantı kayıtlarından incelenmesi

Kapasite Yönetimi	
Denetim Hedefi	Sistem performans ve kapasitesinin mevcut ve ilerideki iş ihtiyaçlarını karşılamasını sağlamaya yönelik faaliyetlerin etkinliğini değerlendirmek
Referans	♦ COBIT 2019 / BAI04 Yönetilen Erişilebilirlik ve Kapasite ♦ TS ISO/IEC 27002 / 12.1.3 Kapasite Yönetimi ♦ ITIL V4 / Hizmet Yönetimi Uygulamaları 5.2.3 Kapasite ve Performans Yönetimi
Konu	**İB-4 Parametreler** İş birimleri ve BT birimi arasında yapılmış ve BT hizmetleri için operasyonel parametrelerin seçimine temel oluşturacak yazılı bir anlaşma veya düzenleme var mı?
Kriter	Kurumun sistem performans ve kapasitesine ilişkin kriterler ölçülebilir belirlenmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumda kapasite planlaması yapılıyor mu?	• İlgili plan (düzenleme) veya BT biriminin kullandığı işletim rehberi incelenerek söz konusu belgelerin üst yönetim tarafından gözden geçirilerek imzalanıp imzalanmadığının belirlenmesi • Kapasite planlamasına ilişkin uygulamalar incelenmek ve kapasite sorumlularıyla görüşme yapılmak suretiyle planın aşağıdaki hususlar dikkate alınarak yapılıp yapılmadığının değerlendirilmesi: - Kapasite yönetimi sorumlusunun belirlenmesi - Kapasite ve performans durumunun düzenli olarak izlenmesi, ölçülmesi ve değerlendirilmesi - İş planlarının, senaryoların ve hizmet kullanım eğilimlerinin özeti - Hizmet öncelik durumu ve iş kritikliği - Kullanıcı talepleri ve kapasite talep yönetimi - Yasal, düzenleyici, sözleşmesel ve organizasyonel gereksinim değişikliklerinin, kapasiteye ve performansa potansiyel etkilerinin dikkate alınması - Gelecekte gerekli olacağı düşünülen ve kurum hedefleriyle uyumlu kapasite tahminlerinin yapılması (ilave kapasite ihtiyacı gibi) - Kapasite tahminlerinde insan kaynakları ve tesis kapasitesinin de dikkate alınıp alınmadığı - Bu tahminlerin yapılmasında işlem hacmi, veri kayıtları, ağ, işlemci, bellek ve disk kullanımı gibi hususların dikkate alınması - Hizmet kapasite artırımı için takvim, eşik değerler ve maliyetler - Yeni teknolojilerin kapasite ve performans üzerindeki potansiyel etkileri - Acil durumlarda iş sürekliliğinin sağlanabilmesi amacıyla bilgi işleme kapasitesinin göz önünde bulundurulması (Ör: felaket anında iş yükü tahminleri ve kapasite gereksinimleri gibi)
2. Kapasite planı düzenli aralıklarla güncelleniyor mu?	• Belge incelemesi yoluyla, Kurumda BT ihtiyaçları doğrultusunda kapasite planlamasının düzenli aralıklarla güncellenip güncellenmediğinin belirlenmesi

Konu	**İB-5 İzleme** Kurum, iş ihtiyaçları karşılamak için sistem performans verilerini gerçek zamanlı ve periyodik olarak topluyor ve gözden geçiriyor mu?
Kriter	Performans verileri, kapasite ve performansın etkin yönetimi için izlenmeli, değerlendirilmeli ve raporlanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Performans verileri toplanıyor mu?	• Sistem kapasitesi üzerinde etkisi olan unsurlara ilişkin durum raporları, ağ ve konfigürasyon bilgileri, sistem kaynaklarına erişilebilirlik, sisteme bağlanma ve cevap verme süreleri, trafik durum ve trend bilgileri ile performans bilgileri gibi bilgilerin kurum tarafından toplanıp toplanmadığının mülakat ve belge incelemesi yoluyla belirlenmesi
2. Hizmet ve kaynaklara ilişkin kapasite ve performans yeterliliği izleniyor ve raporlanıyor mu?	• BT hizmetleri ve bu hizmetleri oluşturan bileşenlere ilişkin kapasite ve performans eşik değerleri, alarmlar ve uyarılar belirlenip belirlenmediğinin incelenmesi • Kapasite yönetimi sorumlusu tarafından bu eşik değerlerle alakalı tahmin edilen ve gerçekleşen kaynak kapasite ve performans kullanımlarına ilişkin izleme yapılıp yapılmadığının ve sonuçların düzenli olarak raporlanıp raporlanmadığının değerlendirilmesi • Kurumdaki kapasite gereksiniminin söz konusu sistemin iş kritikliği dikkate alınarak ve önceliklendirme yapılmak suretiyle belirlenip belirlenmediğinin incelenmesi

Konu	**İB-6 Performans Verilerinin Analizi** Performans verileri, verimliliğin değerlendirilmesi ve kapasitede oluşabilecek sıkıntılara karşı alınabilecek önlemlerin belirlenmesinde kullanılıyor mu?
Kriter	Toplanan performans verileri periyodik olarak analiz edilerek, değişen ihtiyaç ve koşullar çerçevesinde kapasite sorunlarının çözümü planlanmalı ve gerekli iyileştirmeler gerçekleştirilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Performans verileri analiz edilerek gerekli iyileştirme faaliyetleri gerçekleştiriliyor mu?	• İzleme verilerinin analizinde aşağıdaki hususların oluşup oluşmadığının irdelenmesi ve eğer oluşmuş ise düzeltici iyileştirme faaliyetlerinin (iş yükünü değiştirme, görevleri önceliklendirme, kaynak arttırma, talep azaltma vb. gibi) yapılıp yapılmadığının değerlendirilmesi - Altyapıdaki darboğazlar ve etkin noktalar - Uygunsuz iş yükü dağılımları - Uygunsuz veri tabanı indeksleri - Verimsiz hafıza kullanımları - İşlem oranındaki beklenmeyen artışlar - Uygulama tasarımlarındaki verimsizlikler - Sistem mimarisindeki hatalı tasarımlar - Ağ yapılandırması ve konfigürasyon hataları

Olay ve Problem Yönetimi	
Denetim Hedefi	Kurumun olay ve problem yönetimine ilişkin politika ve prosedürlerinin etkinliğini değerlendirmek
Referans	♦ COBIT 2019 / DSS02 Yönetilen Hizmet Talepleri ve Olayları ♦ COBIT 2019 / DSS03 Yönetilen Problemler ♦ ITIL V4 / Hizmet Yönetimi Uygulamaları 5.2.5 Olay Yönetimi ♦ ITIL V4 / Hizmet Yönetimi Uygulamaları 5.2.8 Problem Yönetimi
Konu	**İB-7 Politikaların Varlığı ve Farkındalığı** Kurumun yazılı bir olay ve problem yönetimi politikası ve kullanıcıların bu konuda farkındalığı var mı?
Kriter	Kurumda, olay ve problem yönetimine ilişkin etkin politikalar ve prosedürler olmalı; kullanıcılar bunlardan haberdar edilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Olay yönetimine ilişkin politika ve prosedürler oluşturulmuş mu?	• Olay yönetimine ait politika ve prosedürlerin aşağıdaki hususları içerip içermediğinin incelenmesi: - Log kayıtları ve güvenlik yazılımları yoluyla gerekli bilginin toplanarak verinin düzenli olarak gözden geçirilmesinin sağlanması için log kayıt standart ve prosedürleri - Olayların tanımlanması, kaydının alınması, önceliklendirilmesi, desteğin sağlanması, olay sonrasında yürütülecek faaliyetler, yönetimin bilgilendirilmesi gibi aşamaların tanımlanması - Olay önceliklendirme yöntemlerinin ve/veya kriterlerinin tanımlanması - Yardım talebi çeşidine göre yardım türü modellerinin tanımlanması - Tanımlanmış risk kategorilerine göre anında çözülemeyen olaylar için bir üst merciiye iletme prosedürleri - Olay yönetimi için sadece tanımlanmış araçların kullanılması ve bu araçların kullanımı hakkında son kullanıcılara bilgilendirme yapılması - Olay analizinin yapılarak olay veri tabanına kaydının sağlanması - Çözüm sürecinde olayı takibe alan uyarı ve bilgilendirme sistemlerinin varlığı - Olayın tekrarlamasını önleyecek planların yapılması - Adli delillerin işlenmesine yönelik hükümler - Bilgi güvenliği ihlal olaylarının tespiti ve raporlanması süreci - İhlal olayında dâhili ve harici kişi ya da kuruluşlarla iletişim ve kontrollü kurtarma dâhil olmak üzere müdahale prosedürleri - Güvenlik ihlallerini işleyen çalışanlar ile ilgili işlemler için yürürlükteki resmi bir disiplin müeyyidesine atıf yapılması • Bilgi güvenliği ihlali olaylarına yönelik müdahale faaliyetlerinin aşağıdaki hususları içerip içermediğinin belirlenmesi: - Bilgi güvenliği ihlal olaylarının türlerinin, hacimlerinin ve maliyetlerinin ölçeklendirilmesini ve izlenmesini sağlayacak bir mekanizmanın olması - Kanıt olarak kullanılabilecek bilginin teşhisi, toplanması, edinimi ve korunmasına yönelik prosedürlerin varlığı - İhlalin ortaya çıkmasından sonra olabildiğince kısa sürede delil toplanması - Gereken hallerde bilgi güvenliği adli bilişim analizi yapılması - İlgililerine bilgi güvenliği ihlal olayının bildirilmesi

	- İhlal olayına sebebiyet veren bilgi güvenliği zayıflıklarının ele alınması - İhlal olayının resmi olarak kapatılması ve kayıt edilmesi
2. Problemlerin sınıflandırması ve raporlanması için gerekli politika ve prosedürler tanımlanıyor ve uygulanıyor mu?	• Problem yönetimine ait politika ve prosedürlerin aşağıdaki hususları içerip içermediğinin incelenmesi: - Durum ya da olayların, problem olarak tanımlanması için gerekli kriterler - Problemin tespit edilmesi, sınıflandırılması, önceliklendirilmesi, ilgili personele aktarılması, çözümün sağlanması, problem sonrası yürütülecek faaliyetler, yönetimin bilgilendirilmesi gibi aşamaların tanımlanması - Problemlerin sınıflandırmasına ilişkin yöntemlerin tanımlanması - Problem önceliklendirme kriterlerinin tanımlanması - Problem analizinin yapılarak problem veri tabanına kaydının sağlanması - Çözülmemiş durumda olan problemlerin düzenli olarak takibinin yapılması ve ilgili yönetim birimine raporlanması
3. Olay ve problem yönetimine ilişkin oluşturulan politika ve prosedürler hakkında kullanıcı farkındalığı oluşturulmuş mu?	• Tüm çalışanlar ve yükleniciler için, herhangi bir güvenlik olayının olabildiğince hızlı bir şekilde raporlanması konusunda farkındalık eğitimlerinin verilip verilmediğinin incelenmesi

Konu	**İB-8 Beceriler ve Kaynaklar** Olay ve problemlere müdahale için gerekli ekip, kaynak ve araçlar bulunuyor mu?
Kriter	Olay ve problemlere müdahale için yeterli bilgi ve beceriye sahip üyelerden oluşan ekipler oluşturulmalı, uygun araçlar kullanılmalı, gerekli kaynaklar tahsis edilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurum, olay ve problemlere müdahale için bir ekip oluşturmuş mu?	• Ekibin olay ve problemlerin araştırılması için yetkisinin olup olmadığının incelenmesi • Ekip üyelerinin ağlar, işletim sistemleri ve güvenlik konularında uzmanlıklarının ve iş süreçlerinin incelenmesi • Kurum içinde bilgi güvenliği ihlal olaylarını ele alacak yetkili personelin olup olmadığının incelenmesi • Gerçekleşen problemlere ilişkin kök nedenleri değerlendirmek için bilgi kaynakları ve veri tabanlarından yararlanarak durumu analiz edecek uzmanların görevlendirilip görevlendirilmediğinin incelenmesi • Olay ve problemlerin araştırılması için uygun personelin atanıp atanmadığının belirlenmesi için vaka raporlarının gözden geçirilmesi
2. Olay ve problem yönetimi için kayıt analizi araçları kullanılıyor mu?	• Kullanılan olay yönetim araçları incelenerek siber olayların korelasyon kuralları doğrultusunda tespiti ve detaylı analizi için kayıt analizi araçları (örneğin; SIEM - güvenlik bilgileri ve olay yönetimi) kullanılıp kullanılmadığının tespit edilmesi • Kayıt analiz araçları kullanılıyor ise - 5651 sayılı yasaya uygun biçimde ve kayıtların değişmezliğini sağlamak için kriptografik algoritmalar kullanılıp kullanılmadığının - Aracın yapılandırmasının düzenli olarak gözden geçirilip geçirilmediğinin - Tutulan kayıtların düzenli olarak izlenip izlenmediğinin tespit edilmesi

Konu	**İB-9 Müdahalelerin Etkinliği** Kurumun belirlediği strateji, politika ve prosedürler olay ve problemlere etkili bir şekilde müdahale edilmesini sağlıyor mu?
Kriter	Kurum, olay ve problemlere belirlediği politika ve prosedürlere uyarak uygun ekip ve araçlarla etkili bir şekilde müdahalede bulunmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Olay ve problemler, belirlenen politika ve prosedürler dâhilinde mi çözümlenmektedir?	• Denetim dönemi boyunca açılmış olay ve problem kayıtları içerisinden örneklem yoluyla seçilecek olay ve problemlerin ilgili politika ve prosedürlerde belirtildiği şekliyle kayıt altına alınarak takibinin sağlanıp sağlanmadığının incelenmesi • Sık tekrar eden sorunların nedenlerinin araştırılmasında olay ve problem yönetimi veri tabanındaki bilgilerden yararlanılıp yararlanılmadığının araştırılması • Önemli olayların tekrarlanmasını önlemek için kullanıcılara güncellenen eğitimlerin verilmesi gibi olay sonrası faaliyetlerin yürütülüp yürütülmediğinin incelenmesi • Örnek olarak seçilen olay ve problemlerin ancak ilgili paydaşların onayı ile "çözümlendi/tamamlandı/giderildi vb." durumuna alınıp alınmadığı • Olay müdahale ekibince çözümü sağlanan tüm olaylar için detaylı kayıt tutulup tutulmadığının ve buna ilişkin olarak veri tabanında bilgi güncellemesi yapılıp yapılmadığının incelenmesi
2. Olay ve problemlerin çözümünü hızlandıracak yardım masası kurulmuş mu?	• Problemlerin çözümünü hızlandıracak yardım masasının işleyişi ile ilgili olarak aşağıdaki hususların incelenmesi: - Yardım masası yönetim sürecinin belirlenip, talep sınıflandırma yöntemleri ve modellerinin tanımlanıp tanımlanmadığı - Yardım masası için bir eğitim programı uygulanıp uygulanmadığı - Yardım masasında görev alan personelin eğitim, sertifika ve iş tecrübeleri dikkate alınarak yeterliliklerinin değerlendirilmesi - Yardım masasının sorunların çözülmesi veya bunun başarılamaması durumunda ilgili uzman personele yönlendirilebilecek şekilde yapılandırılıp yapılandırılmadığı - Örnekleme yoluyla seçilen kullanıcılarla görüşme yapılarak yardım masasından alınan desteğin yeterliliğinin değerlendirilmesi - Açık durumdaki problemlerin listesi temin edilerek, bu problemlerin durumlarının BT yönetiminin ve kullanıcıların haberdar olması için yardım masasına raporlanıp raporlanmadığı

Değişiklik Yönetimi	
Denetim Hedefi	Kurumun, BT sistemleri ve uygulamalarına yönelik tüm değişikliklerin kontrollü bir şekilde yürütülmesini sağlayacak bir değişiklik yönetim sürecine sahip olup olmadığını değerlendirmek
Referans	♦ COBIT 2019 / BAI06 Yönetilen BT Değişiklikleri ♦ COBIT 2019 / BAI07 Yönetilen BT Değişim Kabul ve Geçişi ♦ TS ISO/IEC 27002 / 12.1.2 Değişiklik Yönetimi ♦ TS ISO/IEC 27002 / 14.2.2 Sistem Değişiklik Kontrolü Prosedürleri ♦ ITIL V4 / Hizmet Yönetimi Uygulamaları 5.2.4 Değişiklik Kontrolü
Konu	**İB-10 Politika** Kurumun, değişiklik döngüsü boyunca uygun kontrolleri içeren, onaylanmış bir değişiklik yönetim politikası var mı?
Kriter	Kurum, BT varlıkları ve süreçlerini etkileyebilecek değişikliklerin kontrollü ve etkin bir şekilde gerçekleştirilmesini sağlayacak politika ve prosedürlere sahip olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumun onaylanmış bir değişiklik yönetimi politikası veya prosedürü/ standardı var mı?	• Kurumdaki değişiklik yönetimine ilişkin sürecin bilgi güvenliği de dahil olmak üzere incelenmesi ve ilgili politika/prosedür belgelerinin aşağıdaki hususları içerip içermediğinin değerlendirilmesi: - Değişikliklerin planlanması ve takvimi - Değişiklik taleplerinin yazılı olarak sunulması ve talep analizi - Personelin görev ve sorumlulukları, görevler ayrılığı ilkesi ve iletişim - Önerilen değişiklikler için resmi onay ve değerlendirme prosedürleri - Değişiklik gerekçeleri ve faydaları - Değişimin maliyeti - Etki ve risk analizi ile önceliklendirme - Değişiklik yapmamanın etkileri - Tedarikçilerin ve sözleşmelerin değişim sürecine olan etkisi - Önemli değişikliklerin tanımlanması ve kaydedilmesi - Değişikliklerin sınıflandırılması - Bir olayı çözmek için gerekli değişikliklerin hızlı ve kontrollü uygulanmasını sağlamak için acil değişiklik süreci - Devreye alma ve dönüşüm planı - Değişiklik kabul testleri için test planı ve bir test ortamı oluşturulması - Testlerin yapılması ve kabul kriterleri - Bilgi güvenliği gereksinimlerinin karşılandığının doğrulanması - Canlı (üretim) ortamına geçiş süreci - İlgili tüm personele değişiklik detaylarının bildirilmesi - Devreye alma sonrası gözden geçirme - Canlı sistemin izlenmesi - Başarısız değişikliklerin ve öngörülmeyen olayların onarılması ya da sona erdirilmesi için sorumlulukları da içeren geri dönüş prosedürleri - Değişikliklerin takibi, belgelenmesi, raporlanması, analizi ve etki değerlendirmesi - Değişiklik sonrası yeni istihdam gereksiniminin değerlendirilmesi

	• Değişiklik yönetiminin planlanması, değişiklik taleplerinin değerlendirilmesi, önceliklendirilmesi ve yetkilendirilmesinin Kurum üst yönetimi tarafından gerçekleştirilip gerçekleştirilmediğinin incelenmesi
2. Değişikliğe karar verilmesinde ve önceliklendirmede etki ve risk analizi yapılıyor mu?	• Değişikliklere ilişkin etki ve risk analizinde Kurumun değişiklik politikası/prosedürü dikkate alınarak aşağıdaki hususların varlığının incelenmesi: - İş amaç ve süreçlerine olası etkileri - Altyapı bileşenlerine olası etkileri - Hizmet edinenlere ve kullanıcılara olası etkileri - Diğer hizmetlere ve uygulamalara olası etkileri - Mevcut planlara (kapasite planı, hizmet sürekliliği planları, vb.) olası etkileri - Bilgi güvenliğine ve bilgi güvenliği unsurlarına etkileri - Kurum kontrolünde olmayan bileşenlere olası etkileri - Planlanmış mevcut değişiklikler - Değişiklik yapmamanın olası etkileri - Gelecekteki kaynak gereksinimleri - BT eğitiminin gerekliliği - Testlerin gerekliliği - Hizmet kesinti süreleri - Geri dönüş süreleri • Kurum tarafından iç ya da dış mevzuattan kaynaklanabilecek ve BT süreçlerini ilgilendiren değişikliklerin, sürekli olarak takip edilip edilmediğinin, izlendiğinin ve önceliklendirme için dikkate alınıp alınmadığının incelenmesi • İş süreçlerinin planlı bir şekilde desteklenmesi ve yeterli değişiklik kayıtlarının yer alması için sisteme yönelik tüm değişikliklerin yetkilendirilmiş, test edilmiş, dokümante edilmiş ve kontrol edilmiş olarak yapılıp yapılmadığının incelenmesi

Konu	**İB-11 Geri Dönüş Prosedürleri** BT birimi, gerektiğinde önceki versiyona geri dönüşü sağlıyor mu?
Kriter	Değişiklikler sonucunda istenmeyen bir etki görülmesi halinde etkilenen alanların iyileştirilmesine, önceki versiyona dönmeye yönelik prosedürler tanımlanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Değişiklik sonucunda ortaya çıkması muhtemel istenmeyen etkilerin telafisi için geri dönüş prosedürleri belirlenmiş mi?	• Değişiklik sonucunda istenmeyen etkilerin ortaya çıkması halinde söz konusu durumun öncelikli olarak ele alınıp alınmadığının belge inceleme veya mülakat yoluyla incelenmesi • Kurumun ihtiyaç olması halinde değişiklikten önceki versiyonlara dönmeyi organize edecek şekilde değişiklik sürecini yürütüp yürütmediğinin iş akış süreçleri incelenmek suretiyle tespit edilmesi • Değişiklik yönetimine ilişkin dokümanlar incelenerek değişikliğin istenmeyen etkilerinin ortaya çıktığı durumlar için (acil durumlar dahil) yedekleme, düzeltme, konfigürasyon ve erişim logları, test ve uygulama gibi prosedürlerin varlığının araştırılması

Konu	**İB-12 Acil Durum Değişiklikleri** Acil durum değişiklikleri yeterli düzeyde kontrol ediliyor mu?
Kriter	Acil durum değişiklikleri için ayrı prosedürler belirlenmeli, uygulanmalı ve değişikliklerin kontrollü bir şekilde gerçekleştirilmesi sağlanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Acil durum değişiklikleri için istisnai/farklı nitelikteki prosedürler belirlenmiş mi?	• Acil durumlar için acil durum değişiklik prosedürlerinin dokümante edilip edilmediğinin ve önceden karşılaşılan durumlar için bilişim personelinin bu prosedürlere ne derecede uygun işlem yaptıklarının incelenmesi • Acil değişiklik prosedürlerinde, acil değişiklerde uygulanacak aşamaların, takip ve kayıt süreci ile gerekli olabilecek ek erişim/yetkilendirme mekanizmasının belirtilip belirtilmediğinin incelenmesi
2. Standart değişiklik yönetimi prosedürlerinin uygulanmadığı hallerde acil durum değişiklikleri yeterli düzeyde kontrol ediliyor ve izleniyor mu?	• Değişiklik için tüm ek/acil erişim düzenlemelerinin, değişiklik uygulandıktan sonra uygun şekilde yetkilendirildiğinin, belgelendiğinin ve iptal edildiğinin incelenmesi • Acil durum değişiklikleri gerçekleştirildikten sonra söz konusu duruma neden olan etmenlerin belirlendiğinin ve değişiklik yönetimi personeli ile mülakat yapılmak suretiyle acil değişiklik prosedürlerinin uygulamada takip edilip edilmediğinin incelenmesi • Toplam değişiklikler içinde standart dışı acil durum değişikliklerinin yüzdesinin hesaplanması ve değişiklikten sonra yetkilendirilmemiş olan acil değişikliklerin sayısının belirlenmesi

Konu	**İB-13 Değişiklik Kapanışı ve Dokümantasyonu** Değişiklik uygulandıktan sonra ilgili sistemlerin ve kullanıcı belgelerinin güncellenmesi için uygun süreçler izleniyor mu?
Kriter	Değişiklikler gerçekleştirildikten sonra, yeni sistem izlenmeli, analiz edilerek raporlanmalı ve yeni duruma uygun olarak varlık envanteri, kullanıcı kılavuzları, eğitim materyalleri gibi değişikliğin etkilediği tüm belgeler güncellenmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Değişiklikten sonra yeni sistemin izlenmesini ve raporlanıp analiz edilmesini sağlayan kontroller oluşturulmuş ve değişikliğin kapanışı gerçekleştirilmiş mi?	• İzleme ve raporlama prosedürlerinin aşağıdaki hususları karşılayıp karşılamadığının incelenmesi: - İş amaçlarına ve planlara/prosedürlere uygunluk - Değişiklik başarı oranı - Değişiklik tamamlanma süresi - Kullanıcı beklentilerini karşılama - Teknik koşulları karşılama • Değişikliklerin gerçekleştirilmesini müteakip yeni duruma uygun olarak; - BT varlık portföyü ve envanterinin - İş süreçlerinin - Operasyonel prosedürlerin, - Konfigürasyon bilgilerinin, - Kullanıcı uygulama dokümanlarının, - Yardım ekranlarının ve eğitim materyallerinin güncellenip güncellenmediğinin incelenmesi

Ek-8.4:
Dış Kaynak Kullanımı
Önerilen Kontrol Değerlendirme Matrisi

Dış Kaynak Kullanımı Politikası	
Denetim Hedefi	Kurumun dış kaynak kullanımı konusunda yeterli politikasının olup olmadığını değerlendirmek
Referans	♦ COBIT 2019 / APO10 Yönetilen Tedarikçiler ♦ Bilgi ve İletişim Güvenliği Rehberi / 3.5.3. Tedarikçi İlişkileri Güvenliği ♦ TS ISO/IEC 27002 / 15 Tedarikçi İlişkileri İçin Bilgi Güvenliği Politikası
Konu	**DKK-1 Dış Kaynak Kullanımı Politikası** Kurum tarafından dış kaynak kullanımına ilişkin politikalar belirlenmiş mi?
Kriter	Dış kaynak kullanımına ilişkin kurum politikası (dış kaynak kullanımına konu olacak hizmetler, kısıtlamalar, tedarik, güvenlik, iş sürekliliği, denetim ve izleme gibi temel unsurları kapsayacak şekilde) belirlenmiş olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumun dış kaynak kullanımı konusunda bir politikası var mı?	• Dış kaynak kullanımına ilişkin politika belgelerinin onaylanıp onaylanmadığının incelenmesi • Dış kaynak kullanımı veya satın alma belgelerinde üst yönetimin onay sürecine dâhil olup olmadığının incelenmesi • Dış kaynak kullanımı politika belgesinde, kurumun dışarıdan temin edebileceği ya da edemeyeceği kurum varlıkları ve hizmetler hakkında, bilgiye yer verilip verilmediğinin incelenmesi • Kurum tarafından, dış kaynak kullanımı hizmetlerine ve tedarikçilere ilişkin risklerin belirlenip belirlenmediğinin, tedarikçilerin kuruluş merkezinin Türkiye'de bulunmasına ilişkin bir düzenleme olup olmadığının incelenmesi • Kurumun, iş devam ederken yüklenicinin değişme veya işi bırakma olasılığına ilişkin riskleri belirleyip belirlemediğinin, işin kurum tarafından devralınmasına ilişkin düzenleme olup olmadığının incelenmesi • Dış kaynak kullanımına ilişkin süreçlerde uyulacak mevzuat veya kurum düzenlemelerine atıf yapılıp yapılmadığının incelenmesi • Politika belgesinde, güvenlik, denetim ve izleme mekanizmalarının belirlenip belirlenmediğinin incelenmesi

Tedarik	
Denetim Hedefi	Kurumun hizmet gereksinimlerini belirlemeyi ve yüklenici seçimini uygun bir şekilde yönetip yönetmediğini değerlendirmek
Referans	♦ 4734 Sayılı Kamu İhale Kanunu ♦ 4735 Sayılı Kamu İhale Sözleşmeleri Kanunu ♦ Kamu İhale Genel Tebliği ♦ Kamu İhale Uygulama Yönetmelikleri ve Tip Sözleşmeler ♦ TÜBİTAK BİLGEM YTE - İşletim ve Bakım Rehberi / 5.3.2.2 İhtiyacın Belirlenmesi ve Uygun Tedarikçilerin Seçilmesi ♦ COBIT 2019 / APO10.02 Tedarikçileri Seçin
Konu	**DKK-2 Tedarik Süreci** Gerekli tedarik süreçleri takip edilmiş ve uygun yüklenici seçimi yapılmış mı?
Kriter	Kurum, hizmet gereksinimlerinin tanımlanarak doğru ve eksiksiz biçimde aktarılmasını ve uygun yüklenici seçimini sağlayacak süreçlere sahip olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Tedarik süreçleri tanımlanmış mı?	• Tedarik edilecek ürün, hizmet ya da işlerle ilgili ihale sürecini gerçekleştiren Kurumun ve yaptırılacak işin 4734 sayılı Kamu İhale Kanunu kapsamında olup olmadığının belirlenmesi ve kapsamda olmayan kurumlar için tedarik süreçlerini içerecek bir düzenlemenin var olup olmadığının incelenmesi
2. Gereksinimler belirlenmiş mi?	• Alınacak hizmet kapsamında, gereksinimleri açık şekilde tanımlayan şartnamenin veya iş tanımlama dokümanının incelenmesi • Kullanıcı gereksinimlerinin dikkate alınıp alınmadığının incelenmesi
3. Tedarik sürecine ilişkin hazırlanması gereken dokümanlar hazırlanmış mı?	• Kurum/dış kaynak kullanımına konu iş 4734 sayılı Kanun kapsamında ise, hazırlanması gereken ve aşağıda sıralanan belgelerin doğruluk ve tamlık açısından incelenmesi: - Harcama talimatı - Yaklaşık maliyet hesap cetveli - Fayda-maliyet analizi - İlan veya ihaleye davet - İstekli listesi - Başvuru ve teklifler - Değerlendirme belgesi - Karar ve tutanaklar - Onay belgesi - İdari şartname - Teknik şartname - Sözleşme tasarısı - İlgili mevzuat gereğince hazırlanması zorunlu diğer belgeler • Kurum/dış kaynak kullanımına konu iş 4734 sayılı Kanundan istisna ya da muaf ise, tabi olunan düzenlemeler gereğince oluşturulması istenen dokümanların varlığının araştırılması • Şartname veya iş tanımlama dokümanında, hizmetin özelliklerinin net ve anlaşılır bir biçimde yazılıp yazılmadığının ve belirli bir marka, model,

	patent veya ürün ismi kullanmaktan kaçınılarak tarafsız bir şartname oluşturulup oluşturulmadığının incelenmesi
4. Uygun yüklenici seçimi yapılmış mı?	• 4734 sayılı Kanun kapsamındaki dış kaynak kullanımlarında; tedarik sürecinin yürütülmesinde ve yüklenici seçiminde aşağıdaki hususların dikkate alınıp alınmadığının incelenmesi: - Yüklenici seçim sürecinin temel ihale ilkeleri ve yürürlükteki düzenlemelere uygun, saydam, rekabetçi, objektif, güvenilir, gizli, ihtiyaçların uygun şartlarla ve zamanında karşılanmasını ve kaynakların verimli kullanılmasını sağlayacak şekilde yapılıp yapılmadığı - İhale komisyonunda karar verici olarak görev alan üyeler ile sözleşme tasarısı ve teknik şartnameleri hazırlayan/inceleyen personelin konusunda uzman ve nitelikli olup olmadığı - Tedarike ilişkin yaklaşık maliyetin ayrıntılı miktar ve fiyat araştırması yapılmak suretiyle gerçekçi ve gizli bir biçimde tespit edilip edilmediği - İhaleye ilişkin ilanın/ihaleye davetin şeffaf, rekabeti sağlayacak şekilde yapılıp yapılmadığı - Uygun yüklenicinin seçimine yönelik kriterlerin uygulamada esas alınıp alınmadığı - İhaleye teklif veren isteklilerin yeterli olup olmadıkları (yeterli seviyede teminata, mali/idari yapıya ve iş deneyim belgesine sahip olup olmadığı gibi) - İsteklilerin ihalelere katılmaktan yasaklı olup olmadıkları - Gereksinimlerin karşılanmasında yerli ürün ve hizmet kullanımının teşvik edilmesi amacıyla mevzuatta yer alan yerli istekliler lehine fiyat avantajı uygulanıp uygulanmadığı - Yeterliliği sağlayan ve ekonomik açıdan en avantajlı teklifi veren isteklinin seçilip seçilmediği - İhale kararlarının ihale yetkilisince onaylanıp onaylanmadığı ve var ise itiraz/şikâyet süreçlerinin sonuçlandırılıp sonuçlandırılmadığı • 4734 sayılı Kanun kapsamında olamayan dış kaynak kullanımlarında, seçim süreçlerinin dış kaynak kullanım politikasına uygunluk açısından incelenmesi • Yüklenici seçiminin 4734 sayılı Kanun hükümlerine göre (en uygun teklif kriteri) yapılamadığı durumda, seçimin aşağıdaki kriterler esas alınarak bir puanlama usulüne göre yapılıp yapılmadığının incelenmesi: -Teklif kapsamında sunulan destek, eğitim, vb. gibi yan unsurlar - Yüklenicinin referansları - Yüklenicinin geçmiş başarıları - Yüklenicinin kabiliyetleri, sahip olduğu sertifikalar - Yüklenicinin büyüklüğü ve finansal durumu - Yüklenicinin bulunduğu (destek verdiği) bölge
5. Satın alma ile ilgili kararlar uygun yönetim düzeyinde alınıyor mu?	• Tedarik ile ilgili kararların uygun yönetim düzeyinde onaylanıp onaylanmadığının tespiti için Kurum yönetimi ve ilgili çalışanlar ile görüşme yapılması

Tedarikçilerin Yönetimi	
Denetim Hedefi	Kurumun tedarikçiyi yönetip yönetemediğini ve hizmete ilişkin performans değerlerinin hedeflenen düzeyden sapması durumunda uygun önlemleri alıp almadığını değerlendirmek
Referans	♦ 4734 Sayılı Kamu İhale Kanunu ♦ 4735 Sayılı Kamu İhale Sözleşmeleri Kanunu ♦ Kamu İhale Genel Tebliği ♦ Kamu İhale Uygulama Yönetmelikleri ve Tip Sözleşmeler ♦ TÜBİTAK BİLGEM YTE - İşletim ve Bakım Rehberi / 5.3.2.3 Sözleşmelerin Oluşturulması ve Yönetilmesi ♦ TÜBİTAK BİLGEM YTE - İşletim ve Bakım Rehberi / 5.3.2.4 Tedarikçilerin İzlenmesi ♦ TS ISO/IEC 27002 / 15.1.2 Tedarikçi Anlaşmalarında Güvenliği İfade Etme ♦ TS ISO/IEC 27002 / 15.1.3 Bilgi ve İletişim Teknolojileri Tedarik Zinciri ♦ TS ISO/IEC 27002 / 15.2.1 Tedarikçi Hizmetlerini İzleme ve Gözden Geçirme ♦ COBIT 2019 / APO10.03 Tedarikçi İlişkilerini ve Sözleşmelerini Yönetin ♦ COBIT 2019 / APO10.05 Tedarikçi Performansını ve Uyumunu İzleyin ♦ COBIT 2019 / DSS01.02 Dış Kaynaklı BT Hizmetlerini Yönetin
Konu	**DKK-3 Tedarikçi Yönetimi** Kurum tedarikçilerle sözleşme yapma sürecini ve sözleşmenin uygulanmasını uygun şekilde yönetiyor mu?
Kriter	Tedarikçiden alınacak hizmete ilişkin koşullar, hedefler, roller ve sorumluluklar netleştirilerek karşılıklı anlaşmaya varılması ve uyumlu olarak hayata geçirilmesi sağlanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Yüklenici ile kurumun taleplerini karşılayacak kapsamda yazılı bir sözleşme düzenlenmiş mi?	• Yüklenici ile alınacak hizmete ilişkin koşullar, hizmet seviyesi, hedefler, roller ve sorumlulukları kapsayan yazılı bir sözleşmenin yapılıp yapılmadığının incelenmesi • Sözleşmenin Kurumun tabi olduğu mevzuata uygunluğunun değerlendirilmesi • Şartname ve sözleşme hükümlerinin birbirleriyle uyumlu, tam ve tutarlı olup olmadığının incelenmesi • Sözleşme hazırlanırken belirlenen hizmet seviyelerinin, hizmet seviyesi anlaşmasına uyumlu olup olmadığının incelenmesi
2. Yüklenici, sunmakta olduğu hizmetler için alt yüklenicilerden yararlanıyorsa, bunlara ilişkin riskler sözleşmede belirlenmiş mi?	• Yüklenicinin alt yükleniciler ile yaptığı sözleşmenin incelenmesi • Sözleşmede, yüklenicinin alt yükleniciler ile ilgili sorumluluğu üstlenip üstlenmediğinin incelenmesi

3. Sözleşmede Kuruma hizmetlerin takibini sağlayacak gözetim ve izleme yetkisi tanımlanıyor mu ve izleme yapılıyor mu?	• Sözleşmede kurumun hizmet seviyesini izleme yetkisinin tanımlanıp tanımlanmadığının incelenmesi • Ortaya çıkabilecek hizmet eksikliğini tespit etmek için izleme raporlarının (durum veya ilerleme raporlarının) gözden geçirilmesi • Üçüncü taraflara yaptırılan dış denetim ve iç denetim raporlarının incelenmesi • Kurum tarafından izleme faaliyetlerini değerlendirmek için izleme raporlarının, yüklenici ile yapılan yazışmaların ve olay müdahale raporlarının incelenmesi
4. Kurumun aldığı hizmetler için yerinde inceleme yapma yetkisi var mı?	• Kurum tarafından gerçekleştirilen hizmet alımlarında (örneğin; veri merkezi hizmeti) sözleşme veya şartnamelerde Kurumun yerinde inceleme yapabilme yetkisinin olup olmadığının incelenmesi
5. Sözleşme hükümleri uygulanmadığı takdirde, sözleşmede buna ilişkin yaptırım hükümlerine yer verilmiş mi?	• Yaptırımlara ilişkin hükümlerin (örneğin; hizmet seviyesi) yer alıp almadığının tespiti için sözleşmenin gözden geçirilmesi • Yüklenici hizmetlerinin sağlanmasında eksiklikler tespit edildiğinde, yükleniciyle iletişime geçilerek uygun eylemlerin gerçekleştirildiğinin ve gerekli yaptırımların uygulanıp uygulanmadığının incelenmesi
6. Kurum ile yüklenici arasında iletişim mekanizmaları belirlenmiş mi?	• Kurum ve yüklenici arasında, hangi iletişim araç ve mekanizmalarının kullanılacağının belirlenip belirlenmediğinin ve etkinliğinin belge incelemesi ve mülakatla belirlenmesi

Veri Hakları	
Denetim Hedefi	Kurumun veri koruma gereksinimlerinin tanımlanıp tanımlanmadığını ve bunların sözleşmenin bir parçası olup olmadığını değerlendirmek
Referans	⬩ Bilgi ve İletişim Güvenliği Rehberi / 3.5.3. Tedarikçi İlişkileri Güvenliği ⬩ TÜBİTAK BİLGEM YTE - İşletim ve Bakım Rehberi / 5.3.2.4 Tedarikçilerin İzlenmesi ⬩ TS ISO/IEC 27002 / 13.2.4 Gizlilik ya da İfşa Etmeme Anlaşmaları ⬩ TS ISO/IEC 27002 / 15.1.2 Tedarikçi Anlaşmalarında Güvenliği İfade Etme ⬩ COBIT 2019 / APO01.07 Bilgi (Veri) ve Sistem Sahipliğini Tanımlayın ⬩ COBIT 2019 / DSS01.02 Dış Kaynaklı BT Hizmetlerini Yönetin
Konu	**DKK-4 Veri Koruma ve Veri Yönetimi** Kurumun, veri koruma ve erişim hakları sözleşme ile uygun bir şekilde belirlenmiş mi?
Kriter	Kurumun veri koruma ve erişim hakları tanımlanmış olmalı ve ilgili gerekliliklere yüklenicinin uyması sağlanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurum verileri tanımlanmış mı?	• Verilerin, işlem verilerini ve verileri destekleyen programları/yazılımları kapsayacak şekilde tanımlanıp tanımlanmadığının incelenmesi
2. Kurumun veri koruma ve erişim gereksinimleri tanımlanmış mı?	• Kurum verilerinin korunması ve erişim haklarına ilişkin hususların belirlenip belirlenmediğinin incelenmesi
3. Veri koruma ve erişim hakları hizmet sözleşmesine	• Sözleşme ya da şartnamelerde kurumun kendi verisine erişim ve kullanım haklarının bulunup bulunmadığının incelenmesi

dâhil ediliyor ve izlemesi yapılıyor mu?	• Sözleşme ya da şartnamelerde yüklenicinin kurum verisini korumasına ilişkin hükümlerin olup olmadığının incelenmesi • İlgili olan bütün bilginin kapsama alınıp alınmadığını belirlemek amacıyla yüklenici ile yapılan gizlilik sözleşmesinin gözden geçirilmesi • Yüklenicinin Kurum verisinin korunmasına ilişkin yükümlülüklerini yerine getirip getirmediğine yönelik olarak bağımsız denetim, iç denetim, vb. çalışmalar yürütülüp yürütülmediğinin incelenmesi • İzleme raporları, olay müdahale raporları, yazışmalar, vb. belgeler incelenerek Kurum tarafından izleme faaliyeti yürütülüp yürütülmediğinin belirlenmesi

Yurtdışı Hizmet Sağlayıcı	
Denetim Hedefi	Kurumun yurtdışı hizmet sağlayıcılar ile sözleşme yapmaya ilişkin bir stratejisinin olup olmadığını belirlemek
Referans	♦ COBIT 2019 / APO10.04 Tedarikçi Riskini Yönetin
Konu	**DKK-5 Yurtdışı Tedarikçi Yönetimi** Kurum yurtdışından dış kaynak kullanımı sağlarken, yurtdışı tedarikçi ile ilgili ortaya çıkabilecek sorunların farkında mı?
Kriter	Dış kaynak kullanımı politikasının yurtdışı kuruluşlarından sağlanan dış kaynak kullanımıyla ilgili hükümleri açıkça belirlenmiş ve mevzuata uyum sağlanmış olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurum, yurtdışından sağladığı dış kaynak kullanımı nedeniyle ortaya çıkabilecek sorunları değerlendiriyor mu?	• Kurumun, yurtdışından sağladığı dış kaynak kullanımıyla ilgili riskleri belirleyip belirlemediğinin incelenmesi • Yurtdışından sağlanan dış kaynak kullanımıyla ilgili risklere ilişkin fayda maliyet analizinin değerlendirilmesi • Tedarikçiye ilişkin güvenlik araştırmasının yeterli düzeyde yapılıp yapılmadığının incelenmesi
2. Yurtdışından kaynak kullanımında mevzuata uyum sağlanıyor mu?	• Yurtdışından kaynak kullanımında ulusal güvenlik stratejileri ve diğer mevzuata uyumun değerlendirilmesi • Yurtdışı kaynak sağlayıcısının Türkiye'de merkezi bulunması, destek hizmeti vermesi, veri koruma, denetim ve izleme, gizlilik, veri tabanlarının yurtdışında olması durumu, ulusal güvenlik, kişisel verilerin korunması vb. konularının değerlendirilmesi • Yurtdışı kaynak sağlayıcısının kendi ülkesinde tabi olduğu hükümlerin incelenmesi • Türkiye ile ilgili yurtdışı hizmet sağlayıcı arasında ikili anlaşma olup olmadığının incelenmesi.

İş Bilgisinin ve İş Sahipliğinin Korunması	
Denetim Hedefi	Kurumun iş bilgisi ve iş süreç sahipliğini koruyup korumadığını değerlendirmek
Referans	♦ COBIT 2019 / APO01.06 Bilgi (Veri) ve Sistem Sahipliğini Tanımlayın ♦ COBIT 2019 / APO10.04 Tedarikçi Riskini Yönetin ♦ COBIT 2019 / DSS01.02 Dış Kaynaklı BT Hizmetlerini Yönetin
Konu	**DKK-6 İş Bilgisi ve İş Sahipliği** Kurum dış kaynak kullanımı yoluyla yürüttüğü hizmetleri kendi başına sağlama kapasitesine sahip mi?
Kriter	Kurum iş bilgisini ve iş süreçlerinin sahipliğini korumalı ve yüklenicinin hizmeti aksatması ya da sağlayamaması durumunda önemli faaliyetlerine kendi kaynakları ile devam edebilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. İş süreci sahipliği iyi tanımlanmış ve belgelenmiş mi?	• Süreç, veri ve uygulama yazılımının sahipliğinin kurum tarafından sözleşme ile hüküm altına alınıp alınmadığının incelenmesi
2. Dış kaynak kullanımından kaynaklanan iş bilgisi kaybını ve tedarikçiye bağımlılığı önleyecek tedbirler kurum tarafından alınmış mı?	• Veri, uygulama yazılımı, sistem tasarımı açısından iş bilgisinin iyi belgelenip, personelin eğitim vb. yöntemler ile periyodik şekilde bilgi kapasitelerinin güncellenip güncellenmediğinin incelenmesi • Kurum ve personelinin, tedarikçi tarafından gerçekleştirilen önemli sistem güncelleme faaliyetlerine dâhil olup olmadığını değerlendirilmesi • Yüklenici tarafından gerçekleştirilen sistem güncellemelerine ilişkin detaylı dokümantasyonun Kuruma verilip verilmediğinin incelenmesi • Sistem ve verilerin sahipliği ile ilgili olarak yüklenici ile herhangi bir olay veya anlaşmazlık olup olmadığının incelenmesi • Önemli olaylarda, kurum ve yüklenicinin işi ortaklaşa yönetip yönetemediğini tespit etmek için yüklenici ile toplantı tutanaklarının gözden geçirilmesi
3. İşin kuruma devir süreci belirlenmiş mi?	• Hizmet akdinin sona ermesi veya sonlandırılması durumunda, yazılım, donanım, veri, iş süreç ve bilgileri, vb. BT varlıklarının kuruma devri için gerekli süreçlerin sözleşmede belirlenip belirlenmediğinin incelenmesi

Maliyet Kontrolü ve Yönetimi	
Denetim Hedefi	Kurumun dış kaynak kullanımını uygun maliyet ile sağlayıp sağlamadığını değerlendirmek
Referans	♦ 4734 Sayılı Kamu İhale Kanunu ♦ 4735 Sayılı Kamu İhale Sözleşmeleri Kanunu ♦ Kamu İhale Genel Tebliği ♦ Kamu İhale Uygulama Yönetmelikleri ve Tip Sözleşmeler ♦ TÜBİTAK BİLGEM YTE - İşletim ve Bakım Rehberi / 5.3.2.2 İhtiyacın Belirlenmesi ve Uygun Tedarikçilerin Seçilmesi ♦ COBIT 2019 / APO06.03 Bütçeleri Oluşturun ve Koruyun ♦ COBIT 2019 / APO10.02 Tedarikçileri Seçin ♦ COBIT 2019 / APO10.05 Tedarikçi Performansını ve Uyumunu İzleyin
Konu	**DKK-7 Fayda Maliyet Analizi** Kurum, dış kaynak kullanımına ilişkin maliyetleri gerçekçi bir şekilde değerlendiriyor mu?
Kriter	Dış kaynak kullanımında fayda maliyet analizi gerçekçi bir şekilde yapılmalı ve hizmetin uygun maliyet ile karşılanması sağlanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Dış kaynak kullanımı için tüm maliyetler belirlenmiş mi? (Gelecekte ortaya çıkabilecek muhtemel maliyetler dâhil)	• Tüm maliyetlerin kurum tarafından belirlenip ve ilgili paydaşlar tarafından incelenip, onaylandığının değerlendirilmesi • Tüm maliyetlerin sözleşmeye yansıtılıp yansıtılmadığının ve gelecekteki maliyetler de dâhil olmak üzere hiçbir gizli maliyetin olup olmadığının incelenmesi
2. Kurum maliyet fayda analizi yapıp, analiz sonucuna göre ortaya çıkan en uygun seçeneği tercih etmiş mi?	• Seçim ve maliyet sürecine ilişkin belgelerin incelenmesi • Kurumun taahhüdünden önce tüm maliyetlerin fayda-maliyet analizine tabi tutulup tutulmadığının gözden geçirilmesi • Sözleşmedeki tahmini ve gerçek harcamaların incelenmesi ve karşılaştırılması
3. Dış kaynak kullanımı konusunda Kurum ile ilişkilendirilen belirli sorumluluklar var mı ve bunların içinde kritik maliyet unsurları bulunuyor mu?	• Dış kaynak kullanımına ilişkin harcamaların kuruma ait bütçe ile karşılaştırılması
4. Ek veya artan maliyetler Kurumdan mı tahsil ediliyor?	• Belirli faaliyet alanlarının maliyetinde değişiklik olması durumunda hizmet sağlayıcının performansının gözden geçirilmesi • Hizmet sağlayıcıdan gelen ek maliyet taleplerine karşı kurumun bu maliyet artışı için aldığı aksiyonların incelenmesi

Hizmet Seviyesi Anlaşması	
Denetim Hedefi	Kurumun, tedarikçi ile tüm unsurları ve gereksinimleri detaylandıran bir hizmet seviyesi anlaşması yapıp yapmadığını ve bu anlaşmaya uyumu takip edip etmediğini değerlendirmek
Referans	♦ TÜBİTAK BİLGEM YTE - İşletim ve Bakım Rehberi / 5.7.2 ♦ COBIT 2019 / APO09.03 Hizmet Sözleşmelerini Tanımlayın ve Hazırlayın ♦ COBIT 2019 / APO09.05 Hizmet Anlaşmalarını ve Sözleşmelerini Gözden Geçirin ♦ COBIT 2019 / APO10.03 Tedarikçi İlişkilerini ve Sözleşmelerini Yönetin ♦ COBIT 2019 / APO10.05 Tedarikçi Performansını ve Uyumunu İzleyin
Konu	**DKK-8 Hizmet Seviyesi Anlaşmasının Yeterliliği** Kurum tedarikçi ile tüm gereksinimleri kapsayan bir hizmet seviyesi anlaşması yapmış mı?
Kriter	Hizmet seviyesi anlaşması, tedarikçiyi teknik ve diğer gereksinimlere göre izleme ve kontrol etme hususunda bir temel oluşturmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurum ve tedarikçi arasında ayrıntılı bir hizmet seviyesi anlaşması yapılmış mı?	• Hizmet seviyesi anlaşmasının varlığının ve tüm kullanıcı gereksinimlerinin hizmet düzeyi gereksinimlerine dönüştürülüp dönüştürülmediğinin incelenmesi
2. Hizmet seviyesi anlaşması, kurum ile hizmet sağlayıcı arasındaki tüm rolleri ve sorumlulukları tanımlayacak kadar ayrıntılı mı?	• Anlaşmada Kurumun ve hizmet sağlayıcının rollerinin ve sorumluluklarının açıkça tanımlanıp tanımlanmadığının incelenmesi
3. Hizmet seviyesi anlaşması özenle uygulanıyor mu?	• Performans seviyeleri için parametrelerin açıkça tanımlandığının ve hizmet seviyesi anlaşmasına dâhil edilip edilmediğinin incelenmesi
4. Kurumun, hizmet seviyesi anlaşmasının uygulanmasını izlemek için bir yöntemi var mı?	• Kurum ve hizmet sağlayıcı arasında hizmet seviyesi izleme yöntemi varlığının incelenmesi • Hizmet seviyesi anlaşmasındaki parametrelerin yüklenici tarafından rapor edildiğini ve Kurum içindeki ilgili personel tarafından gözden geçirilip geçirilmediğini değerlendirmek için yüklenicilerin durum raporlarının gözden geçirilmesi
5. Hizmet seviyesi anlaşmasının istisnalarını belirleyen mekanizma var mı?	• Hizmet seviyesi anlaşmasında meydana gelecek sapmalar için kurum tarafından alınan önlemlerin incelenmesi

Güvenlik	
Denetim Hedefi	Dış kaynak kullanımı sırasında güvenliğe ilişkin gereksinimlerin ele alınıp alınmadığını ve bunlara uyulup uyulmadığını değerlendirmek
Referans	♦ Hizmet İşleri Genel Şartnamesi / Madde 13 ♦ Bilgi ve İletişim Güvenliği Rehberi / 3.5.3 Tedarikçi İlişkileri Güvenliği ♦ TÜBİTAK BİLGEM YTE - İşletim ve Bakım Rehberi / 5.3.2.4 Tedarikçilerin İzlenmesi ♦ TS ISO/IEC 27002 / 15.1.2 Tedarikçi Anlaşmalarında Güvenliği İfade Etme ♦ TS ISO/IEC 27002 / 13.2.4 Gizlilik ya da İfşa Etmeme Anlaşmaları ♦ COBIT 2019 / DSS01.02 Dış Kaynaklı BT Hizmetlerini Yönetin
Konu	**DKK-9 Güvenlik Gereksinimlerinin Tanımlanması** Kurum dış kaynak kullanımında bilgi güvenliğine ilişkin gereksinimlerin uygulanmasını sağlıyor mu?
Kriter	Kurum, tedarikçilere bilgi güvenliği gereksinimlerini aktarmalı ve uygulamasını izlemelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurum tarafından dış kaynak kullanımına ilişkin güvenlik gereksinimleri belirlenmiş ve hizmet sağlayıcı tarafından yerine getirilmesini sağlayacak mekanizmalar oluşturulmuş mu?	• Güvenlik gereksinimlerinin Kurum tarafından belirlenip, tedarik sözleşmesi veya hizmet seviyesi anlaşmasına dâhil edilip edilmediğinin incelenmesi • Kurumun, tedarikçi tarafından veri, uygulama yazılımı ve donanımdaki değişiklikleri yetki dâhilinde yapıp yapmadığının doğrulanması
2. Kurumun, tedarikçinin güvenlik gereksinimlerine uyup uymadığını izlemek için bir yöntemi var mı?	• Kurumun, erişim günlüklerini inceleyerek, dışarıdan sağlanan verilere, uygulama yazılımına ve donanıma erişim konusunda bir güvencesi olup olmadığının doğrulanması • Kurumun yüklenici tarafından uygulamaya konan güvenlik mekanizmaları konusunda güvence sahibi olup olmadığının doğrulanması • Kurumun tedarikçiden düzenli rapor alıp almadığını ve izleme raporlarındaki bilgilere göre hareket edip etmediğinin doğrulanması • Bilgi güvenliği ile ilgili olarak yüklenicilerle ve çalıştırdığı personeli ile yazılı gizlilik sözleşmeleri yapılıp yapılmadığının incelenmesi

Yedekleme ve Felaket Kurtarma Planlarına Uyum	
Denetim Hedefi	Dış kaynak kullanımı durumunda, tedarikçinin Kurumun iş sürekliliği ve felaket kurtarma planlarına uyumunun sağlanıp sağlanmadığını değerlendirmek
Referans	♦ COBIT 2019 / DSS01.02 Dış Kaynaklı BT Hizmetlerini Yönetin ♦ COBIT 2019 / DSS04.04 İş Sürekliliği Planını (BCP) ve Felaket Müdahale Planını (DRP) Uygulayın, Test Edin ve Gözden Geçirin ♦ COBIT 2019 / DSS04.07 Yedekleme Düzenlemelerini Yönetin
Konu	**DKK-10 Yedekleme ve Kurtarma Prosedürleri** Dış kaynak kullanımı hizmetleri uygun şekilde yedeklenip bunlara ilişkin felaket kurtarma çözümleri belirlenmiş mi?
Kriter	Tedarikçi, iş sürekliliği ve felaket kurtarma planlarına ilişkin yükümlülüklerini yerine getirmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Tedarikçi, iş sürekliliği ve felaket kurtarma planları için sözleşme veya hizmet seviyesi anlaşmasında belirlenen yükümlülüklerini karşılıyor mu?	• Tedarikçinin veriler, uygulamalar ve hizmetler için iş sürekliliği ve felaket kurtarma planlarını uyguladığından emin olmak için sözleşme veya hizmet seviyesi anlaşmasının gözden geçirilmesi • Tedarikçinin, iş sürekliliği ve felaket kurtarma planları faaliyetlerine ilişkin prosedürlerin periyodik olarak test edildiğini doğrulayan bağımsız veya iç denetim raporlarının hazırlanıp hazırlanmadığını gözden geçirmek için sözleşme veya hizmet seviyesi anlaşmasının gözden geçirilmesi • Periyodik olarak yapılan testlerin sözleşme koşullarına ve/veya hizmet seviyesi anlaşmasına uygun olarak yürütüldüğünden emin olmak için hizmet sağlayıcıdan gönderilen raporların incelenmesi • İş sürekliliği ve felaket kurtarma planları faaliyetlerine ilişkin prosedürlerin güncellenip güncellenmediğini kontrol etmek için periyodik raporların gözden geçirilmesi

Ek-8.5:
İş Sürekliliği Yönetimi
Önerilen Kontrol Değerlendirme Matrisi

İş Sürekliliği Politikası	
Denetim Hedefi	Kurumda etkili bir iş sürekliliği politikası olup olmadığını değerlendirmek
Referans	♦ COBIT 2019 / DSS04.01 İş Sürekliliği Politikasını, Amaçlarını ve Kapsamını Tanımlayın
Konu	**İSFKP-1 İş Sürekliliği Politikası** Kuruluşun iş sürekliliği için acil durum planı ve politikası var mı?
Kriter	Kurumun onaylanmış, yayınlanmış ve benimsenmiş bir acil durum planı ve acil durum operasyonlarının tüm alanlarını kapsamlı bir şekilde tanımlayan ve eğitim gereksinimlerini ve test programlarını belirleyen bir politikası olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumun, iş sürekliliğine ilişkin bir politikası var mı?	• İş sürekliliği Politikasının kurumun genel BT politikalarıyla tutarlı olduğundan emin olmak için belge incelemesi • İş Sürekliliği planlamasında kurumun genel süreklilik amaçlarının belirlenmiş olup olmadığının incelenmesi • BT politikasının, Kurumun acil durum hedeflerini, acil durum planlaması için örgütsel çerçeve ve sorumlulukları tanımlayarak iş sürekliliğinin gerekliliklerini ele aldığını değerlendirmek için politika belgesinin incelenmesi • Koşullar değiştiğinde politikanın ne sıklıkta güncellendiğini belirlemek için inceleme yapılması • Politikanın kim tarafından onayladığının ve en son ne zaman dağıtıldığının belirlenmesi • Politikanın kurum içinde yeterince anlaşılıp anlaşılmadığını değerlendirmek için kurum çalışanlarından örnek grupla mülakat yapılması

İş Sürekliliği Organizasyonu	
Denetim Hedefi	Yeterli bir iş sürekliliği ekibinin mevcut olup olmadığını değerlendirmek
Referans	♦ COBIT 2019 / DSS04.01 İş Sürekliliği Politikasını, Amaçlarını ve Kapsamını Tanımlayın
Konu	**İSFKP-2 İş Sürekliliği Fonksiyonu** Bir iş sürekliliği ekibi veya eşdeğer bir işlevde oluşturulmuş bir organizasyon var mı?
Kriter	İş sürekliliği sürecini yürüten bir iş sürekliliği ekibi mevcut olmalı ve ekibin görev ve sorumluluk alanları açıkça belirlenmiş olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Üst yönetimce iş sürekliliği kapsamındaki faaliyetlerin yürütülmesinden sorumlu bir ekip oluşturulmuş mu?	• Üst yönetimde iş sürekliliği sorumluluğunun yeterli düzeyde sahiplendiğinin ve üstlenildiğinin değerlendirilmesi için belge incelemesi (Örneğin, yönetim kurtarma düzeyini ve aciliyetini belirlemiş ve bunu, politika üzerinde yansıtmış mı?) • Kurum üst yöneticileriyle görüşülerek kurum iş sürekliliği organizasyon planlaması hakkında aşağıdaki hususların varlığının araştırılması: - Kurum iş sürekliliğine yönelik politikaların uygulanmasında sorumlulukların belirlenmiş olması - Kurumda iş süreklilik planlaması faaliyetlerini yürütecek ekipte kimlerin yer aldığını gösteren listelerin olması - İş süreklilik planlamasını yürütecek kişilerin görev tanımlarının yapılmış olması • Belge incelemesi ve ilgili personelle mülakat yapılarak, kurumun tüm kritik alanlarının iş sürekliliği ekibine dağıtılmış olup olmadığının değerlendirilmesi • Tüm kritik birimlerin felaket kurtarma için ekip üyeleri atadıklarını ve rollerinin açık bir şekilde ortaya konduğunu değerlendirmek için belge incelemesi • Kurumun her bir kritik birimi/departmanı için iş sürekliliği ekibinden örnek bir çalışan grubuyla iş sürekliliğindeki rollerini bildiklerini değerlendirmek için mülakat yapılması

Risk ve İş Etki Değerlendirmesi	
Denetim Hedefi	Risk değerlendirmesi ve iş etki analizi yapılıp yapılmadığını ve bir risk yönetim sisteminin yürürlükte olup olmadığını değerlendirmek
Referans	♦ COBIT 2019 / DSS04.02 İşletme Esnekliğini Koruyun
Konu	**İSFKP-3 Risk Değerlendirmesi** Kurum tarafından risk değerlendirilmesi ve iş etki analizi yapılıyor mu?
Kriter	Risk değerlendirmesi ve iş etki analizi yapılmış, kritik veriler, uygulama yazılımları, işlemler ve kaynaklar tanımlanmış ve önceliklendirilmiş olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Risk değerlendirmesi gerçekleştirilmiş mi?	• Risk değerlendirmesinin yapıldığının, olası tehditlerin ve bunların etkilerini belirlendiğinin belge incelemesiyle değerlendirilmesi • Tüm fonksiyonel alanların risk değerlendirmesinde dikkate alındığından emin olmak için belge incelemesi. • İlgili paydaşların risk tanımlama sürecine dahil edildiklerini görmek için belge incelemesi • Risk değerlendirme ekibi ile görüşme yapılarak ve hazırladıkları raporlar incelenerek, risk değerlendirmesi yapılırken aşağıdaki hususların ele alınıp alınmadığının incelenmesi: - Risk yönetimi sürecinde tüm öncelikli iş süreçlerinin ele alınmış olması - Yapılan analizlerde nelerin risk olarak görüldüğü ve risk seviyelerinin tespit edilmiş olması - Yapılan risk analizlerinde olası tehditler ve kurum üzerinde yaratabileceği zarar ya da aksaklıkların öngörülmüş olması - Sistemin yeniden kurulması ve çalıştırılması için gerekli zaman sürelerinin ele alınmış olması - Üçüncü kişiler marifetiyle yürütülen işlerin olası aksama durumlarının ele alınmış olması - Yapılan risk değerlendirmelerinin düzenli olarak gözden geçirilmesi
2. İş etki analizi yapılmış mı?	• İş etki analizi yapılırken aşağıdaki hususlara uyulup uyulmadığının değerlendirilmesi: - Etki analizi yapılırken bütün iş birimlerinin yöneticilerine danışılmış olması - İş etki analizinin tüm fonksiyonel alanları kapsaması - Bütün iş süreçlerinin belirlenmiş olması - Bu süreçlerde birbiriyle bağımlı çalışanların tespitinin yapılması ve kritik iş süreçlerinin önceliklendirilmiş olması - Kritik veri ve işlerin üst yönetim ve ilgili personelin katılımıyla belirlenmesi - İlgili paydaşların iş etki analiz sürecine dâhil edilmiş olması - Kurum işlerinden hangilerinin süreklilik için kritik olduklarının belirlenmiş olması - Aksayan işler ve veri kayıplarının onarılmasının yaklaşık maliyetlerinin belirlenmiş olması - Kurum kaynaklarından öncelikle kurtarılması ya da desteklenmesi gerekenlerin belirlenmiş olması

	- Olası iş etkilerinin değerlendirilmesinden sonra felaketten kurtarma hedeflerinin (RTO, RPO) belirlenmesi - Kurtarılacak sistemlerin bir listesinin istenildiğinde elde edilebilmesi - Kurtarma hedeflerini karşılayacak personel, varlık ve hizmetlerin minimum gereksinimlerinin tespit edilmesi - İş etki analizi sonuçlarının üst yönetimle paylaşılması ve mutabık kalınması

Konu	**İSFKP-4 Risk Yönetimi** İş sürekliliğine ilişkin risk yönetim çerçevesi belirlenmiş mi?
Kriter	Riski azaltma ve izleme süreçleri de dâhil olmak üzere bir risk yönetim süreci oluşturulmuş ve acil durum kurtarma öncelikleri belirlenmiş olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. İş sürekliliği için risk yönetim süreci oluşturulmuş mu?	• Risk yönetim sürecinin risk değerlendirme, iş etki analizi ve izleme gibi tüm önemli hususları içerip içermediğinin tespiti için belge incelemesi • Risk yönetim sürecinde üst yönetim de dâhil olmak üzere ilgili personelin rol ve sorumluluklarının farkında olup olmadığının tespiti için mülakat ve belge incelemesi • Üst düzey yönetim dâhil olmak üzere tüm ilgili personelin riskleri izlediğinden ve riskleri azaltmak için gerekli adımları attıklarından emin olunması için görüşme yapılması, belge incelemesi • Artık risklerin kurum üzerinde önemli bir etkisi bulunmadığını değerlendirmek için belge incelemesi • Acil durum önceliklerinin belirlenmesi ve olası kesinti senaryolarının etkisinin yeterince ele alındığını değerlendirmek için belge incelemesi yapılması • Risklerin belirlendiğini, riskleri azaltma faaliyetlerin tanımlandığını, risklerin periyodik olarak izlendiğini ve güncelleştirildiğini belirlemek için toplantı tutanaklarının ve risk kütüğünün gözden geçirilmesi

İş Sürekliliği ve Felaket Kurtarma Planı	
Denetim Hedefi	İş sürekliliği planının donanım, veri, uygulama yazılımı ve veri merkezi (kurtarma) için yedekleme ve kurtarma planları içerip içermediğini ve uygun şekilde uygulanıp uygulanmadığını değerlendirmek
Referans	♦ COBIT 2019 / DSS04.02 İşletme Esnekliğini Koruyun
Konu	**İSFKP-5 İş Sürekliliği ve Felaket Kurtarma Planı** Kurumun yazılı bir iş sürekliliği ve felaket kurtarma planı var mı?
Kriter	Kurumun bir iş kesintisinden sonra ya da iş yoğunluğunun arttığı dönemlerde işin sürdürülmesi ya da iş süreçlerinin yeniden kazanılması için gerekli eylem adımlarını içeren yazılı bir planı olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumda yazılı bir iş süreklilik planı var mı? İş sürekliliği planına dahil yada bundan ayrı olarak bir felaket kurtarma planı var mı?	• Planların, kurtarma planlaması maliyetinin planla azaltılması hedeflenen riskin maliyetini geçmeyecek şekilde dizayn edilmiş olduğunun doğrulanması • Planların, icrasının gerektiği durumlarda birkaç çalışanın uzmanlığı veya bilgisine bağlı olmayacak şekilde detaylı ve anlaşılır hazırlanmış olmasının değerlendirilmesi • Tüm çalışmaların, yazışmaların ve plan evraklarının belgelendirilerek dosyalarda saklanıp saklanmadığının ve mevcut planın birkaç kopyasının farklı bir yerde güvenli olarak tutulup tutulmadığının belirlenmesi için gözlem yapılması ve belgelerin incelenmesi • Kesintiye uğrayan iş süreçlerinin ne kadar süre sonra çalışır hale getirileceğine dair hedef sürenin planda belirtilmiş olması • Planlarda iş kesintisi sonrası kurumun kabul edebileceği veri kaybı için maksimum sürenin belirlenmesi • Yedeklerden geri dönüşte ve felaket kurtarmada görevli personelin rollerinin ve sorumluluklarının açıkça belirlendiğinin doğrulanması • İlgili tüm personele planın uygulanması konusunda hizmet içi eğitim verilip verilmediğinin eğitim belgelerinden incelenmesi ve örnek personel grubuyla alınan eğitim ile ilgili görüşme yapılması
2. İş sürekliliği ve felaket kurtarma planları güncelleniyor mu?	• İş sürekliliği ve felaket kurtarma planlarının güncelliğini değerlendirmek için belge incelemesi • İş sürekliliği ve felaket kurtarma planlarının son versiyonlarının ilgili herkese ulaştırıldığının doğrulanması

Yedekleme	
Denetim Hedefi	Kurumun yedekleme politikasının olup olmadığını ve yedekleme işlemlerinin uygun şekilde yapılıp yapılmadığını değerlendirmek
Referans	♦ COBIT 2019 / DSS04.07 Yedekleme Düzenlemelerini Yönetin
Konu	**İSFKP-6 Yedekleme** Yedekleme işlemlerine ilişkin politikalar belirlenerek uygun şekilde yedekleme işlemleri yapılıyor mu?
Kriter	Bir felaket sonrası iş süreçlerinin yeniden kazanılması için gerekli olan sistem, veri ve uygulamaların yedekleri alınmış olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumun yazılı bir yedekleme politikası var mı?	• Yedekleme politikasının aşağıdaki hususlar yönünden değerlendirilmesi: - Yedeklerin hangi sıklıkla alınacağının belirlenmiş olması - Yedeklerin alınması, transferi, saklanması ve kontrol edilmesine yönelik temel ilkelerin belirlenmiş olması - Yedeklerden geri dönüş testlerinin ne zaman ve ne şekilde yapılacağının belirlenmiş olması - Hizmet sürekliliği ihtiyaç seviyesine göre uzak yedekleme birimlerinin sıcak, ılık ya da soğuk site şekilde kurulacağının ele alınmış olması • Yedeklenen kayıtların tekrar istenmesi ve kullanılmasına yönelik prosedürlerin varlığının incelenmesi • Yedekleme araçlarının hangilerinin ne sıklıkla çalışma alanı dışına gönderileceğinin belirlenmiş olduğunun doğrulanması
2. Yedekleme işlemleri düzenli olarak yapılıyor mu?	• Veri dosyaları ve uygulamaların yedeklerinin düzenli olarak alınmakta olduğunun doğrulanması • Yedeklenen veri dosyalarının içerikleri ve konumlarının listelendiğinin doğrulanması • Yedekleme araçlarının doğru etiketlenmiş olduğunun incelenmesi • Yedekleme araçlarında muhafaza edilen veri dosyaları ve uygulamaların sistemin yeniden kurulması için gerekli nitelikte bilgi içerip içermediklerinin ilgililerle görüşme yapılarak tespit edilmesi • Kurtarma faaliyetleri dışardan mal ve hizmet tedarikini zorunlu kılacaksa, ilgili tedarikçilerle anlaşmaların yapılmış olduğunun doğrulanması
3. Düzenli olarak yedekten geri dönüş testleri yapılıyor mu?	• Yedekten geri dönüş testlerinin bir plana bağlı olarak yürütülüp yürütülmediğinin incelenmesi • Yedekten geri dönüş testlerinin sonuçlarının dokümante edilerek ilgililerine raporlanıp raporlanmadığının incelenmesi • Yedekten geri dönüş testlerinin sonuçları üzerine yedekleme prosedürlerinde gerekli olan düzeltme/güncelleme işlemlerinin gerçekleştirilip gerçekleştirilmediğinin incelenmesi
4. Alınan yedekler, kurum bilişim sisteminin bulunduğu coğrafi mekândan farklı ve güvenli bir ortamda muhafaza ediliyor mu?	• Yedekleme araçlarının kurum bilişim sisteminin bulunduğu coğrafi mekândan farklı güvenli bir ortamda saklanmakta olduğunun doğrulanması • Hizmet sürekliliği ihtiyaç seviyesine göre uzak yedekleme birimlerinin sıcak, ılık ya da soğuk site karakterlerinden kurum politikasında belirtilmiş olana göre dizayn edilmiş olduğunun incelenmesi

Çevresel Kontroller	
Denetim Hedefi	Kurumun yedekleme konusunda uygun çevresel kontrollere sahip olup olmadığını değerlendirmek
Referans	♦ TS ISO/IEC 27002 / 11 Fiziksel ve Çevresel Güvenlik ♦ COBIT 2019 / DSS01.04 - Çevreyi Yönetin
Konu	**İSFKP-7 Çevresel Kontrol Mekanizmaları** Çevresel kontrol mekanizmaları uygun şekilde tasarlanıp uygulanıyor mu?
Kriter	Yedekleme alanlarında elektrik, yangın, su, nem, sıcaklık kaynaklı çevresel tehditler için uygun kontrol mekanizmaları oluşturulmuş olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Yedekleme alanında çevresel kontroller tasarlanmış ve uygulamaya konulmuş mu?	• Yedekleme alanlarında aşağıdaki kontrol prosedürlerinin varlık ve etkinliğinin belge incelemesi ve gözlem yapılarak değerlendirmesi; - Kesintisiz güç kaynağının mevcut olması - Yangından koruma sistemlerinin yeterli olması - Nem, sıcaklık ve voltaj limitlerinin kontrol altında tutulması - Sel felaketini önleyecek sistemlerin yeterli düzeyde olması - Çevre kontrollerinin mevzuata uygunluğu - Çevre kontrollerinin tüm personel tarafından benimsenip, uygulanması

Test	
Denetim Hedefi	İş sürekliliği ve felaket kurtarma prosedürlerinin test edilip edilmediğini değerlendirmek
Referans	♦ COBIT 2019 / DSS04.04 İş Sürekliliği Planını ve Felaket Müdahale Planını Uygulayın, Test Edin ve Gözden Geçirin
Konu	**İSFKP-8 Test Faaliyetleri** İş sürekliliği ve felaket kurtarma planları test ediliyor mu?
Kriter	İş sürekliliği ve felaket kurtarma planları uygun şekilde ve düzenli olarak test faaliyetlerine tabi tutulmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. İş sürekliliği ve felaket kurtarma planları düzenli olarak test ediliyor mu?	• Testlerin zamanında ve doğru aralıklarla gerçekleştirilip gerçekleştirilmediğini öğrenmek için belge incelemesi yapılması • İş sürekliliği politikasında öngörülen kriterlere göre testlerin yapıldığını değerlendirmek için belge incelemesi • Testlerin risk senaryolarına dayalı olarak yapılıyor olduğunun doğrulanması • Test sonrası varılan sonuçlara dayalı önerilerin takip edilmeleri için uygun makamlara iletildiğinin belgeler üzerinden incelenmesi • Test sonuçlarına dayalı tavsiyelerin takip edildiğinin ve iş sürekliliği planı ve felaket kurtarma planının güncellendiğinin belgeler üzerinden değerlendirilmesi

	• Planın, iş süreçlerinde önemli değişiklikler yapıldığında veya kilit görevlerdeki değişimlerden sonra tam olarak test edilip edilmediğinin incelenmesi

Güvenlik	
Denetim Hedefi	İş sürekliliği ve felaket kurtarma planının veri, uygulama yazılımı, donanım ve veri merkezinin güvenliğini sağlayıp sağlamadığını değerlendirmek
Referans	♦ COBIT 2019 / DSS04.03 Bir İş Sürekliliği Müdahalesi Geliştirin ve Uygulayın
Konu	**İSFKP-9 Güvenlik Tedbirlerinin Etkinliği** Yedekleme ve felaket kurtarma ile ilgili uygun güvenlik tedbirleri alınıyor mu?
Kriter	Yedekleme ve felaket kurtarma faaliyetleri sırasında veri, uygulama yazılımı, donanım ve veri merkezi güvenliği sağlanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Yedekleme ve felaket kurtarma faaliyetleri sırasında veri, uygulama yazılımı, donanım ve veri merkezi için güvenlik tedbirleri alınmış mı?	• Yedekleme araçlarının transferleri ile ilgili riskleri minimize edecek tedbirlerin alınmış olduğunun doğrulanması • Yedekleme araçlarının saklandığı yerlerin mantıksal veya fiziksel erişiminin güvenli olduğunun doğrulanması • Yedeklerin alındığı araçların olası her türlü tehlikeden korunacak şekilde özel yerlerde saklandığının doğrulanması • Yedekleme ve veri kurtarma işlemi sırasında veri dosyalarının, uygulama yazılımının ve donanımın sayı ve durumunun korunup korunmadığının doğrulanması • Veri, uygulama yazılımı ve donanımın yedekleme veya felaket kurtarma işlemi sırasında herhangi bir değişiklik geçirip geçirmediğinin, uygulama yazılımı ve veri ile ilgili dosyaların boyutu ve kayıt sayılarının kontrol toplamlarının incelenmesi yoluyla doğrulanması • Erişim kontrol logları (fiziksel ve mantıksal) üzerinden herhangi bir güvenlik ihlalinin olup olmadığının incelenmesi

Dış Kaynak Kullanımında Yedekleme ve Felaket Kurtarma	
Denetim Hedefi	Dış kaynak kullanımında, tedarikçilerin, iş sürekliliği ve felaket kurtarma planlarına uyumunun sağlanıp sağlanmadığını değerlendirmek
Referans	♦ COBIT 2019 / DSS04.03 Bir İş Sürekliliği Müdahalesi Geliştirin ve Uygulayın
Konu	**İSFKP-10 Dış Kaynak Kullanımında Tedarikçilerin Uyumu** Dış kaynak kullanımında tedarikçilerin kurumun iş sürekliliği ve felaket kurtarma politikalarına uyumu sağlanıyor mu?
Kriter	Tedarikçi ile yapılan sözleşme veya hizmet seviyesi anlaşmalarında, kurumun iş sürekliliği ve felaket kurtarma planlarına uyumuna ilişkin hususlara yer verilmeli, dış kaynak kullanım hizmetleri uygun şekilde yedeklenmeli ve bunlara felaket kurtarma çözümlerinin uygulanması sağlanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Dış kaynak kullanım sözleşmelerinde, iş sürekliliği ve felaket kurtarma ile ilgili hususlara yer verilmiş mi?	• Örnek seçilen dış kaynak kullanım sözleşmeleri incelenerek, iş sürekliliği ve felaket kurtarma ile ilgili aşağıdaki hususlara yer verilip verilmediğinin değerlendirilmesi; - İş sürekliliği için kurumun belirlediği prosedürlere uyum taahhüdü - Felaket durumunda dış tedarikçinin izleyeceği adımlar - İş akdinin sona ermesi veya sonlandırılması durumunda iş sürekliliğinin sağlanmasına ve varlıkların kuruma devrine ilişin hükümler - Hizmet sağlayıcının el değiştirmesi durumunda iş sürekliliğinin nasıl sağlanacağına ilişkin hususlar • Kurumun iş sürekliliği ve felaket kurtarmaya ilişkin belirlediği kuralların dış kaynak kullanım sözleşmelerine yansıtılıp yansıtılmadığının incelenmesi
2. Dış kaynak kullanımında tedarikçilerin kurumun iş sürekliliği ve felaket kurtarma planlarına uyumu sağlanıyor mu?	• Dış tedarikçiden alınan hizmetin yedekleme ve veri kurtarma işlemleri sırasında veri dosyalarının, uygulama yazılımının ve donanımın - Sayı ve durumunun korunup korunmadığının, - Herhangi bir değişikliğe uğrayıp uğramadığının tedarikçi tarafından kayıtların sayısı ve dosya boyutu ile ilgili kontrol toplamları üzerinden incelenip incelenmediğinin Kurum tarafından denetlendiğinin doğrulanması • Kurumun, dış hizmet sağlayıcıdaki erişim kayıtlarını (fiziksel ve mantıksal) güvenlik ihlali olup olmadığı açısından incelediğinin doğrulanması • Kurumun, dış tedarikçinin yedekleme ve felaket kurtarma testlerini yapıp yapmadığı noktasında gözetim ve izleme faaliyeti yürütüp yürütmediğinin incelenmesi

Ek-8.6:
Bilgi Güvenliği
Önerilen Kontrol Değerlendirme Matrisi

Risk Değerlendirmesi	
Denetim Hedefi	Bilgi güvenliği ile ilgili bütün risklerin tanımlanıp tanımlanmadığını ve uygun bir risk azaltma stratejisinin uygulamaya konup konmadığını değerlendirmek
Referans	♦ Kamu İç Kontrol Standartları Tebliği / Standart: 6 Risklerin Belirlenmesi ve Değerlendirilmesi ♦ COBIT 2019 / APO12 Yönetilen Risk ♦ COBIT 2019 / EDM03 Güvence Altına Alınan Risk Optimizasyonu
Konu	**BG-1 Değerlendirme Mekanizması** Kurumda bilgi güvenliği risklerinin değerlendirilmesine yönelik bir mekanizma bulunuyor mu?
Kriter	Kurum iyi dokümante edilmiş ve etkin şekilde işletilen bir bilgi güvenliği risk değerlendirme mekanizmasına sahip olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Bilgi güvenliği risklerinin değerlendirilmesine ilişkin süreçler tanımlanmış mı ve uygulanıyor mu?	• İlgili düzenlemeler ve belgeler incelenerek ve üst yönetim ve operasyon seviyesindeki çalışanlar ile mülakat yapılarak; - Risk değerlendirme faaliyetleri bünyesindeki tanımlama, önceliklendirme, yanıtlama/karar verme ve kaydetme süreçlerinin nasıl yürütüleceğinin tanımlanıp tanımlanmadığının, - Risk değerlendirme faaliyetlerine hangi birimlerin/çalışanların katılacağının ve görev ve sorumluluklarının neler olduğunun açık ve net bir şekilde belirlenip belirlenmediğinin, - Risk değerlendirmesinin düzenli aralıklarla (veya şartlar değiştiğinde yeniden) gerçekleştirilerek güncellenip güncellenmediğinin, - Kurumda yeni sistemlerin devreye alınması, sistemlerde yükseltmeler yapılması veya yeni versiyonlara geçilmesi planlandığında risk değerlendirmesi yapılıp yapılmadığının tespit edilmesi. • Kurumun BT varlıklarının ve sistemlerinin -gerektiğinde diğer varlıklar ve sistemler ile olan ilişkilerini/bağlantılarını da içerecek şekilde- varlık grupları itibariyle listelenerek dokümante edilip edilmediğinin incelenmesi • Kritik bilginin erişilemez hale gelmesi, kaybedilmesi, bozulması ya da gizliliğinin ihlalinin sonuçlarına yönelik bir iş etki analizi gerçekleştirilip gerçekleştirilmediğinin belge incelemesi yoluyla tespit edilmesi. • Kurum tarafından gerçekleştirilen risk değerlendirmesinin yeterince kapsamlı bilgiye dayanıp dayanmadığının (örneğin; risk değerlendirmesi yapılırken Kurumun olay yönetimi sisteminden alınan veri ve raporların kullanılıp kullanılmadığının) belge incelemesi yoluyla tespit edilmesi • Olay ve problem müdahale raporları ile önceki risk dokümanları ve kütükleri birlikte incelenerek risk değerlendirmesinin etkinliğinin değerlendirilmesi • Kurumda risk değerlendirmesine ilişkin prosedürlerin ve dokümanların tanımlanmamış/hazırlanmamış olması durumunda, örnek olarak seçilecek iş

	ve işlemler incelenerek operasyonel süreçlerin içinde etkin telafi edici kontroller kurulup kurulmadığının belirlenmesi

Konu	**BG-2 Kapsam** Bütün önemli riskler değerlendirme kapsamına alınmış mı?
Kriter	Bilgi güvenliğine ilişkin bütün önemli iç ve dış riskler uygun şekilde tanımlanmalı ve muhtemel etkileri ve sonuçları değerlendirilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Risk değerlendirmesi sonucunda bir risk kütüğü hazırlanmış mı?	• Risk kütüğü incelenerek Kurum sistemleri, iş süreçleri ve altyapısına ilişkin temel risklerin aşağıdaki bilgileri içerecek şekilde tanımlanıp tanımlanmadığının belirlenmesi: - Varlığın adı, ait olduğu varlık grubu, sahibi, bulunduğu yer - Tehdidin ve riskin tanımı - Etkilenecek varlıklar ve muhtemel sonuçlar - Riskin sahibi - Riskin (gerçekleşme olasılığı, gizlilik-bütünlük-erişilebilirlik açısından değeri, işe etkisi ve varlık değeri uyarınca hesaplanan) değeri/puanı - Risk seviyesi (örneğin; düşük, orta, yüksek, çok yüksek) - Risk kabul seviyesi/puanı - Risk kararı (örneğin; azaltma, kabul, izleme, kaçınma, transfer) - Mevcut kontroller - Seçilen/ilave kontroller - Bir sonraki gözden geçirme tarihi - Kontrol sonrası/artık risk değeri/puanı

Konu	**BG-3 Risk Azaltma Faaliyetleri** Kurumda risk azaltma faaliyetleri gerçekleştiriliyor mu?
Kriter	Risklerin azaltılması için risk değerlendirme dokümanlarında belirlenmiş olan faaliyetler gerçekleştirilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Risk değerlendirmesi sonucunda karar verilen azaltma faaliyetleri yerine getiriliyor mu?	• Olay ve problem müdahale raporları incelenerek risk değerlendirme dokümanlarında tanımlanmış olan bilgi güvenliği risklerinin önlenmesi, tespit edilmesi ve kontrolüne yönelik uygun prosedürlerin uygulamaya konup konmadığının belirlenmesi • Olay ve problem müdahale raporlarının eksik olabileceği göz önüne alınarak diğer kurumsal dokümanların da (örneğin; yıllık faaliyet raporları, diğer periyodik raporlar, vb.) incelenmesi • Kurumda iyi tanımlanmış/düzgün işleyen bir risk değerlendirme mekanizması bulunmuyorsa aşağıdaki hususların incelenmesi: - Ne tür telafi edici kontrollerin kurulduğu - Düzgün işleyen bir risk değerlendirme mekanizmasının varlığı halinde mevcut telafi edici kontrollere kıyasla daha etkin şekilde azaltılabilecek riskler sebebiyle herhangi bir güvenlik olayının yaşanıp yaşanmadığı

Bilgi Güvenliği Politikası	
Denetim Hedefi	Kurumda bilgi güvenliği alanındaki düzenlemelerin yeterliliğini ve etkinliğini değerlendirmek
Referans	♦ TS ISO/IEC 27002 / 5 Bilgi Güvenliği Politikaları ♦ COBIT 2019 / APO13 Yönetilen Güvenlik ♦ 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ♦ Bilgi ve İletişim Güvenliği Rehberi / 2. Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci ♦ 6698 sayılı Kişisel Verilerin Korunması Kanunu ve İlgili Mevzuat ♦ Bilgi ve İletişim Güvenliği Rehberi / 4.1 Kişisel Verilerin Güvenliği
Konu	**BG-4 Bilgi Güvenliği Politikası** Kurumun bir bilgi güvenliği politikası ve ilgili tamamlayıcı dokümanları var mı?
Kriter	Kurum, tüm operasyonel riskleri kapsayan ve Kurum faaliyetleri için önemli olan bütün bilgi varlıklarına kayıp, zarar ve kötüye kullanıma karşı makul bir koruma sağlayan bir bilgi güvenliği politikasına ve ilgili tamamlayıcı dokümanlara sahip olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumda bilgi güvenliği alanında üst (stratejik) yönetim seviyesinde bir farkındalık ve destek mevcut mu?	• Kurumun BT Stratejisinde (ve diğer stratejik yönetim dokümanlarında) bilgi güvenliğinin öneminin ve bilgi güvenliğine ilişkin mevzuat ve düzenlemelere uyumun yeterince vurgulanıp vurgulanmadığının belge incelemesi yoluyla belirlenmesi • Kurumda yazılı bir BT Stratejisi bulunmaması halinde üst yönetim, birim yöneticileri ve çalışanlar ile mülakat yapılarak bilgi güvenliğinin stratejik önemine ilişkin farkındalık seviyelerinin ve değerlendirmelerinin öğrenilmesi • Bilgi güvenliğine ilişkin istihdam, eğitim ve yatırım ihtiyacının tanımlanıp tanımlanmadığının incelenmesi
2. Kurumun yazılı bir bilgi güvenliği politikası var mı?	• Bilgi güvenliği politika belgesinin aşağıdaki hususlar dikkate alınarak incelenmesi: - Amacının ve kapsamının açık bir şekilde ifade edilip edilmediği - İlgili güvenlik tedbirlerine uyulmaması durumunda, karşılaşılabilecek risklerin ve uygulanacak yaptırımların belirtilip belirtilmediği - Üst yönetim tarafından onaylanıp onaylanmadığı - Tüm personel tarafından anlaşılabilecek bir dille yazılıp yazılmadığı - Tüm personele duyurulup duyurulmadığı - Tüm personelin erişimine açık olup olmadığı - Uygun yönetim kademeleri tarafından düzenli aralıklarla gözden geçirilip geçirilmediği
3. Bilgi güvenliği politikasında tanımlanan hedef ve gereksinimler doğrultusunda ilgili tamamlayıcı dokümanlar hazırlanmış mı?	• Bilgi güvenliği politikasının aşağıdaki alanlar (ve denetlenen Kurumun sahip olduğu bilişim alt yapısı ve sistemler göz önüne alınarak ilgili olabilecek diğer alanlar) açısından tamamlayıcı nitelikteki dokümanlar (politika, prosedür, talimat, plan, liste, vb.) ile desteklenip desteklenmediğinin incelenmesi: - Kural ve düzenlemelere uyulmasını sağlamaya yönelik uygulamalar, yaptırımlar - Risk yönetimi

	- Varlık yönetimi - Veri sınıflandırması - İnsan kaynakları güvenliği - Fiziksel ve çevresel güvenlik - Ağ yönetimi ve güvenliği - Sunucu yönetimi ve güvenliği - Veri tabanı yönetimi ve güvenliği - Erişim yönetimi ve kontrolü - Parola kullanımı - İnternet kullanımı - E-posta kullanımı - Yazılım kullanımı - Mobil cihaz kullanımı - Kötü niyetli yazılımlardan korunma - Güvenlik açıklarının tespit edilmesi ve yönetimi - Kriz/acil durum yönetimi - Güvenli yazılım geliştirme - Değişim yönetimi - Yedekleme ve bakım - Kişisel verilerin güvenliği - Bulut bilişim - … • Bahse konu dokümanların düzenli aralıklarla (veya şartlar değiştiğinde) gözden geçirilerek güncellenip güncellenmediğinin incelenmesi
4. Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulmuş mu?	• BGYS Sertifikasının güncel/geçerli olup olmadığının belirlenmesi • BGYS sertifikasının belgelendirme sürecinin TÜRKAK tarafından akredite edilen bir belgelendirme kuruluşu aracılığıyla gerçekleştirilip gerçekleştirilmediğinin incelenmesi • BGYS kapsamında aşağıdaki süreçlerin tanımlanarak ilgili faaliyetlerin yerine getirilip getirilmediğinin incelenmesi: - İzleme, ölçme, analiz ve değerlendirme - İç tetkik - Yönetimin gözden geçirmesi - Uygunsuzluk ve düzeltici faaliyet - Sürekli iyileştirme
5. Tanımlanan bilgi güvenliği gerekliliklerinin yerine getirilmesi yönetim tarafından izleniyor ve gerekli önlemlerin alınması sağlanıyor mu?	• Olay raporları incelenerek çalışanlar ve dış paydaşlar tarafından ilgili dönemde gerçekleştirilen bilgi güvenliği ihlallerinin sayısının belirlenmesi ve politikanın uygulama etkinliğinin değerlendirilmesi • Güvenlik olay raporları ve izleme dokümanları incelenerek çalışanlar güvenlik politikalarını ihlal ettiğinde Kurum tarafından hangi eylemlerin gerçekleştirildiğinin belirlenmesi
6. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberine uyum çalışmaları yerine getiriliyor mu?	• Belge incelemesi ve mülakat yöntemleri kullanılarak; Bilgi ve İletişim Güvenliği Rehberine uyum çalışmaları çerçevesinde aşağıdaki çalışmaların 31.01.2021 tarihi itibariyle tamamlanıp tamamlanmadığının belirlenmesi: - Rollerin ve sorumlulukların atanması, - Kurum varlık gruplarının ve kritiklik derecelerinin tanımlanması, - Her bir varlık grubu için mevcut durum ve boşluk analizi çalışmalarının yapılması, - Telafi edici kontrollerin dokümante edilmesi,

	- Rehber uygulama yol haritasının hazırlanması. • Belge incelemesi ve mülakat yoluyla; kritiklik derecesi "1" olarak belirlenen varlık grupları özelinde uygulanması gereken temel seviye tedbirlerin 31.07.2022 tarihi itibariye yerine getirilip getirilmediğinin belirlenmesi.

Konu	**BG-5 Gizliliğin ve Mahremiyetin Korunması** Kurum, bilginin gizliliğini ve mahremiyetini koruyor mu?
Kriter	Kurumun bilgi güvenliği politikasında belirlenen ihtiyaçlarını uygun şekilde yansıtan ve iç paydaşlar ile üçüncü taraflar nezdinde gizli bilginin korunmasını sağlayan düzenlemeler bulunmalıdır. Kişisel verilerin korunmasına ilişkin yasal gereklilikler karşılanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurum personeline bilgi güvenliği gereklerine uyum konusunda taahhütname/ sözleşme imzalatılıyor mu?	• İşe başlatma prosedürü incelenerek personele bilgi güvenliğine ilişkin rollerini ve sorumluluklarını içeren taahhütname/sözleşme imzalatılıp imzalatılmadığının belirlenmesi • Çalışmakta olan personelin anılan nitelikteki taahhütnameleri/sözleşmeleri imzalamasının sağlanıp sağlanmadığının belge incelemesi yoluyla belirlenmesi
2. Dış paydaşlar ve yükleniciler ile yapılan sözleşmeler bilgi güvenliği ile ilgili hükümler içeriyor mu?	• Dış paydaşlar ve yükleniciler ile yapılan sözleşmelerdeki hüküm ve koşullar incelenerek, yüklenicilerin kurum bilgi varlıklarını nasıl kullanacağına ve bilgi sistemlerine ve hizmetlerine nasıl erişeceğine ilişkin süreçlerin, güvenlik kısıtlamalarının ve yükümlülüklerinin tanımlanıp tanımlanmadığının belirlenmesi • Yükleniciler tarafından herhangi bir bilgi güvenliği ihlalinin gerçekleştirilip gerçekleştirilmediğinin ve varsa bu tür ihlaller karşısında Kurum tarafından hangi eylemlerin yerine getirildiğinin incelenmesi
3. Kurum tarafından kişisel veri envanteri oluşturulmuş mu?	• Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirdikleri kişisel veri işleme faaliyetlerini; - Kişisel veri işleme amaçları ve hukuki dayanağını, - Veri kategorisini, - Aktarılan alıcı grubunu, - Kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, - Yabancı ülkelere aktarımı öngörülen kişisel verileri, - Veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları kişisel veri envanterinin oluşturulup oluşturulmadığının ve belirli periyotlarda güncellenip güncellenmediğinin incelenmesi
4. Kurumda kişisel veri saklama ve imha politikası var mı?	• Kişisel veri saklama ve imha politikasının kişisel veri işleme envanteri ile uyumlu şekilde hazırlanıp hazırlanmadığının incelenmesi • Kişisel veri saklama ve imha politikasının aşağıdaki hususlar göz önünde bulundurularak değerlendirilmesi: - Yazılı halde mevcut olup olmadığı - Üst yönetim tarafından onaylanıp onaylanmadığı - Tüm personel tarafından anlaşılır bir dille yazılıp yazılmadığı - İlgili bütün personelin erişimine açık olup olmadığı - Politika değişiklik geçmişi gözden geçirilerek periyodik olarak veya gerektiğinde güncellenip güncellenmediği

	• Örnekleme yoluyla seçilecek personelle kişisel veriler ile ilgili politika ve prosedürlere ne ölçüde uyulduğunu anlamak için gözlem/mülakatlar yapılması
5. Kurum, veri sorumluları siciline kayıt yaptırmış mı?	• Kurumun, işlemekte olduğu kişisel verilerle ilgili kategorik bazda bilgi girişi yapacağı bir kayıt sistemi olan Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) kayıt yaptırıp yaptırmadığının incelenmesi.
6. Kurumda kişisel verilerin güvenliğinin sağlanmasına yönelik tedbirler alınıyor mu?	• Kurumda, kişisel verilerin güvenliği ile ilgili olarak Bilgi ve İletişim Güvenliği Rehberinde aşağıdaki başlıklar altında yer verilen hususların gereğinin yerine getirilip getirilmediğinin incelenmesi: - Kayıt Yönetimi - Erişim Kayıtları Yönetimi - Yetkilendirme - Şifreleme - Yedekleme, Silme, Yok Etme ve Anonim Hale Getirme - Aydınlatma Yönetimi - Açık Rıza Yönetimi - Kişisel Veri Yönetim Sürecinin İşletilmesi

Bilgi Güvenliği Örgütlenmesi	
Denetim Hedefi	Kurumda etkin bir bilgi güvenliği örgütlenmesinin bulunup bulunmadığını değerlendirmek
Referans	♦ TS ISO/IEC 27002 / 6 Bilgi Güvenliğinin Organizasyonu ♦ COBIT 2019 / APO13 Yönetilen Güvenlik ♦ 11 Kasım 2013 Tarihli ve 28818 Sayılı Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ
Konu	**BG-6 Örgütlenme Yapısı** Kurumda etkin bir bilgi güvenliği örgütlenmesi var mı?
Kriter	Bilgi güvenliği politikası çerçevesinde ilgili roller ve sorumluluklar açık şekilde tanımlanarak dokümante edilmeli ve görevlendirmeler gerçekleştirilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Bilgi güvenliğe ilişkin rol ve sorumluluklar tanımlanarak görevlendirmeler gerçekleştirilmiş mi?	• Bilgi güvenliğinden sorumlu bir birim ya da ekibin oluşturulup oluşturulmadığının incelenmesi • Bilgi güvenliği fonksiyonu ile BT operasyonları arasında "görevler ayrılığının" uygun şekilde sağlanıp sağlanmadığının incelenmesi • Üst yönetim, birim yöneticileri, BT personeli ve Kurumun BT altyapısını kullanan bütün kullanıcılar için bilgi güvenliğine ilişkin rol ve sorumlulukların resmi olarak ve açık şekilde belirtilip belirtilmediğinin incelenmesi • İhtiyaç duyulan düzenlemelerin tanımlanmasına ve faaliyetlerin gerçekleştirilmesine yönelik bir önceliklendirme ve karar alma mekanizmasının olup olmadığının incelenmesi
2. Kurumda Siber Olaylara Müdahale Ekibi (SOME) mevcut mu?	• İlgili mevzuatları uyarınca kurulması öngörülen SOME'nin mevcut olup olmadığının incelenmesi • SOME iletişim bilgilerinin güncel olup olmadığının incelenmesi

	• Siber olaylara müdahale planlarının; uygulanması gereken akış, rol ve sorumlulukları içerecek şekilde dokümante edilip edilmediğinin incelenmesi • SOME'nin yeni gelişen tehditler karşısında düzenli eğitim ve tatbikat yapıp yapmadığı hususlarının belge üzerinden incelenmesi • Siber olaylardan sonra Siber Olay Müdahale Raporlarının düzenlenip düzenlenmediğinin incelenmesi

Konu	**BG-7 Eşgüdüm** Kurumun farklı birimlerindeki bilgi güvenliği uygulamaları koordine ediliyor mu?
Kriter	Bilgi güvenliği faaliyetlerinde sorumluluk çatışması, uyumsuzluk ya da açıkta kalan alanlar olmamalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Bilgi güvenliğine ilişkin kural, süreç ve prosedürlerin Kurum genelinde uygulanmasında eşgüdüm sağlanıyor mu?	• Belge incelemesi, uygulamanın gözlemlenmesi ve çalışanlar ile mülakat yapılması yoluyla Kurumdaki farklı departmanlar/birimler tarafından takip edilen bilgi güvenliği kural, süreç ve prosedürleri arasında çatışma/ çakışma/boşluk olup olmadığının belirlenmesi • Yöneticilerin (varsa) eşgüdüm sorunlarının farkında olup olmadığının ve inceleme ve eşgüdüm faaliyetlerine nezaret edip etmediğinin belirlenmesi

Varlık Yönetimi	
Denetim Hedefi	BT varlıklarının güvenliğinin uygun şekilde sağlanıp sağlanmadığını değerlendirmek
Referans	⬧ Bilgi ve İletişim Güvenliği Rehberi / 3.1.1 Donanım Varlıklarının Envanter Yönetimi ⬧ Bilgi ve İletişim Güvenliği Rehberi / 3.1.2 Yazılım Varlıklarının Envanter Yönetimi ⬧ TS ISO/IEC 27002 / 8 Varlık Yönetimi ⬧ COBIT 2019 / BAI09 Yönetilen Varlıklar ⬧ 5846 sayılı Fikir ve Sanat Eserleri Kanunu ve İlgili Mevzuat
Konu	**BG-8 Varlık Yönetimi** Kurum, bilgi güvenliğini destekleyen uygun bir varlık yönetimi sistemine sahip mi?
Kriter	Kurumun bilgi varlıkları ilgili standartlar, çerçeve belgeler ve iç düzenlemelere uygun şekilde korunmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumda donanım varlıklarının envanteri tutuluyor mu?	• Kurumun donanım varlık envanteri incelenerek, varlıkların; - Varlık grubu, varlık türü, - Marka, model, seri numarası, - (Varsa) destek alınan tedarikçi sözleşme bilgileri (bakım süresi, kapsamı, vb.), - Kullanan kişi ve kullanıldığı yer

	bilgilerini de içerecek şekilde yer alıp almadığının belirlenmesi • Varlık envanterinin tam ve güncel olup olmadığını tespit etmek için örnekleme yoluyla seçilen varlıklar ile envanter bilgilerinin karşılaştırılması
2. Kurumda yazılım varlıklarının envanteri tutuluyor mu?	• Kurumda kullanılan tüm yazılımların (işletim sistemleri, donanım yazılımları, üçüncü parti yazılımlar, uygulama yazılımları, vb.) güncel bir listesinin aşağıdaki bilgileri içerecek şekilde tutulup tutulmadığının belge incelemesi ve mülakat yoluyla belirlenmesi: - Yazılımların adı, sürümü, yayımcısı, - Lisans bilgileri ve edinim tarihi, - Üreticisi tarafından sunulan destek hizmetinin devam edip etmediği, - (Varsa) destek alınan tedarikçi sözleşme bilgileri (bakım süresi, kapsamı, vb.), - Yazılımın yüklendiği donanımlar. • Kurumun sahip olduğu lisansların durumlarını takip edebileceği bir mekanizma olup olmadığının incelenmesi • Kurum tarafından "onaylı yazılım listesi" oluşturulup oluşturulmadığının incelenmesi
3. Kurum lisanslı yazılım kullanımına ilişkin yasal gerekliliklere uyuyor mu?	• Lisanslı yazılım alınması, lisans kayıtlarının tutulması, lisanssız yazılımların silinmesi ve periyodik denetimlerin yapılması hususlarında gerekli kontrollerin incelenmesi
4. Kurumun bilgi varlıklarına sahip/sorumlu atamaları yapılmış mı?	• Örnekleme yoluyla seçilen bilgi varlıklarının belli bir bireyin veya birimin yönetim sorumluluğuna verilip verilmediğinin incelenmesi
5. Kurumun bilgi varlıkları güvenlik gereksinimleri açısından sınıflandırılmış mı?	• Bilgi varlıklarının, tanımlı bir prosedür uyarınca ve yapılan risk değerlendirmesi çerçevesinde; - yasal gereksinimler, - değer, - kritiklik, - yetkisiz ifşa ve değiştirilmeye karşı hassasiyet açısından sınıflandırılıp sınıflandırılmadığının incelenmesi • Örnekleme yoluyla seçilecek bilgi varlıklarının yaşam döngüleri boyunca (elde edilme, kullanılma, saklanma, iletilme, silinme ve imha) güvenlik sınıflandırmasına uygun şekilde hareket edilip edilmediğinin belirlenmesi
6. Varlıkların kabul edilebilir kullanımına, elden çıkarılmasına ve yeniden kullanımına ilişkin süreç ve kurallar yazılı şekilde tanımlanmış mı?	• İlgili belgeler incelenerek BT donanım ve yazılımlarına ilişkin "kabul edilebilir kullanım politikası" oluşturulup oluşturulmadığının belirlenmesi • Kurum tarafından satın alınan ve kullanıcı bilgisayarlarında kullanılacak olan sabit disklerin, sistemlere dâhil edilmeden önce, veri kurtarmaya imkân sağlamayacak şekilde güvenli silme işlemine tabi tutulup tutulmadığının belge incelemesi ve mülakat yoluyla belirlenmesi • Varlıkların elden çıkarılmasına ve yeniden kullanımına ilişkin prosedürler incelenerek; - Varlıkların yok edilmesine veya yeniden kullanılmasına yönelik yetkilendirmelerin uygun şekilde gerçekleştirilip gerçekleştirilmediğinin, - Varlıklar yok edilmeden veya yeniden kullanılmadan önce içindeki verilerin veri kurtarmaya imkân sağlamayacak şekilde güvenli silme işlemine tabi tutulmasını öngören hükümler bulunup bulunmadığının ve - Varlıkların fiziksel imhasına yönelik süreçlerin tanımlanıp tanımlanmadığının belirlenmesi

	• Örnekleme yapılarak kullanımdan çıkarılacak ya da yeniden kullanıma verilecek varlıklar ile ilgili olarak belirtilen düzenlemelerin uygulanıp uygulanmadığının incelenmesi
7. İşten ayrılan veya görev yeri/tanımı değişen personelden kuruma ait varlıklar geri alınıyor mu?	• İşten ayrılan veya görev yeri/tanımı değişen personelden kullanmakta oldukları Kurum varlıklarının geri alınmasına ilişkin süreçlerin tanımlanıp tanımlanmadığının incelenmesi • Örnekleme yoluyla seçilen işten ayrılan veya görev yeri/tanımı değişen personelden Kuruma ait varlıkların geri alınıp alınmadığının kayıtlardan incelenmesi

İnsan Kaynakları Güvenliği	
Denetim Hedefi	Bilişim sistemlerinde ortaya çıkabilecek çalışan (ve kullanıcı) kaynaklı hata, ihmal ve suiistimalleri önlemeye yönelik süreç ve mekanizmaların etkinliğini değerlendirmek
Referans	♦ TS ISO/IEC 27002 / 7 İnsan Kaynakları Güvenliği ♦ Bilgi ve İletişim Güvenliği Rehberi / 3.5 Personel Güvenliği ♦ COBIT 2019 / APO07 Yönetilen İnsan Kaynakları
Konu	**BG-9 Çalışanların Sorumlulukları** Çalışanların bilgi güvenliği ile ilgili rol ve sorumluluklarını yerine getirmeleri sağlanıyor mu?
Kriter	Yüklenici firma personeli ve hassas bilgiyi kullanan bütün kullanıcılar da dâhil olmak üzere tüm çalışanların bilgi güvenliği gereklerine uyumunu sağlayacak etkin düzenleme ve mekanizmalar bulunmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. BT biriminde kritik pozisyonlarda görev üstlenecek (yüklenici personeli dâhil) çalışanların işe alımında güvenlik soruşturması gerçekleştiriliyor mu?	• Güvenlik soruşturması yapılması gerekli olan kritik rollerin tanımının uygun şekilde yapılıp yapılmadığının incelenmesi • Örnek olarak seçilecek BT personelinin işe başlama belgeleri incelenerek güvenlik soruşturmalarının gerçekleştirilip gerçekleştirilmediğinin belirlenmesi
2. Personelin bilgi güvenliğine ilişkin rol ve sorumlulukları tanımlanmış mı?	• Kurum çalışanlarının ve yüklenici personelinin bilgi güvenliğine ilişkin rollerinin ve sorumluluklarının açık şekilde tanımlanarak dokümante edilip edilmediğinin belge incelemesi yoluyla tespit edilmesi • Kurum personeli ve üçüncü taraf çalışanları ile mülakat yapılarak kurumsal bilgi varlıklarının korunmasına ilişkin sorumluluklarını bilip bilmediklerinin incelenmesi
3. Personelin bilgi güvenliği gereklerine uyumu izleniyor mu?	• Personelin bilgi güvenliğine ilişkin düzenlemelere, etik kurallara ve mesleki iyi uygulamalara uyumunu kontrol etmek için Kurum tarafından denetim/izleme faaliyetleri yürütülüp yürütülmediğinin incelenmesi
4. İşten ayrılan veya görev yeri/tanımı değişen personelin erişim yetkilerinin kaldırılmasına/ güncellenmesine ilişkin düzenlemeler/ mekanizmalar var mı?	• İşten ayrılma prosedürü incelenerek ayrılan personelin - Kurum sistem ve uygulamalarına erişim yetkilerinin kaldırılmasına ve - E-posta hesaplarının kapatılmasına ilişkin tanımlı bir sürecin bulunup bulunmadığının belirlenmesi • (Varsa) tanımlanmış olan sürecin örnekleme yoluyla seçilen işten ayrılan personel için işletilip işletilmediğinin incelenmesi

	• Görev yeri/tanımı değişen personelin erişim yetkilerinin (ve varsa kullanıcı ayrıcalıklarının) yeni durumlarına göre zamanlı şekilde güncellenip güncellenmediğinin incelenmesi
5. Kritik pozisyonlarda görev yapan BT personeline yönelik düzenlemeler mevcut mu?	• BT biriminde kritik pozisyonlarda görev yapan çalışanlar için zorunlu izin kullandırılmasına ilişkin düzenlemelerin bulunup bulunmadığının incelenmesi • BT birimi çalışanlarının son 5 yıla ilişkin izin kullanım durumları incelenerek hiç izin kullanmayan personel olup olmadığının belirlenmesi • BT personeline ilişkin görevlendirme, rotasyon ve işten çıkarma prosedürlerinin kişiye bağımlılığı azaltacak şekilde düzenlenip düzenlenmediğinin ve bu çerçevede ne tür bilgi aktarım mekanizmalarının kullanıldığının incelenmesi

Konu	**BG-10 Eğitim** Çalışanların bilgi güvenliği alanındaki yetkinliklerini artırmaya yönelik eğitimler düzenleniyor mu?
Kriter	Uygun kapsamda ve düzenli aralıklarla kurumsal bilgi güvenliği eğitimleri gerçekleştirilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Tüm çalışanlara yönelik düzenli bilgi güvenliği eğitimleri gerçekleştiriliyor mu?	• Eğitim plan ve tutanakları incelenerek (danışmanlar, yükleniciler, geçici personel ve gerektiğinde tedarikçiler de dâhil olmak üzere) Kurumun BT kaynaklarının tüm kullanıcılarına yönelik düzenli bilgi güvenliği eğitimleri gerçekleştirilip gerçekleştirilmediğinin belirlenmesi • Eğitim programlarının içeriği incelenerek Kurumun güvenlik politikaları temelinde ilgili iç kontrol çerçevelerinin ve güvenlik gereksinimlerinin kapsama dâhil edilip edilmediğinin belirlenmesi (örneğin; güvenlik gereksinimlerine uymamanın etkisi, Kurum kaynaklarının ve tesislerinin uygun kullanımı, olay yönetimi, çalışanların bilgi güvenliğine ilişkin sorumlulukları, vb.) • Çalışanlarla mülakat yapılarak Kurum tarafından düzenlenen eğitimlere katılıp katılmadıklarının ve bilgi güvenliğinin ve gizliliğin korunmasına ilişkin sorumluluklarını açık şekilde anlayıp anlamadıklarının belirlenmesi • Eğitim materyallerinin ve programlarının düzenli olarak gözden geçirilip geçirilmediğinin incelenmesi • (Varsa) Kurumun eğitim politikası incelenerek eğitim ihtiyaçları belirlenirken Kurumun kritik gereksinimlerinin eğitim ve farkındalık programlarına yansıtılmasının sağlanıp sağlanmadığının belirlenmesi

Fiziksel ve Çevresel Güvenlik	
Denetim Hedefi	Kurumun tesislerinin ve bilgisayar alan ve varlıklarının yetkisiz fiziksel erişime ve çevresel tehlikelere karşı etkin şekilde korunup korunmadığını değerlendirmek
Referans	♦ Bilgi ve İletişim Güvenliği Rehberi / 3.6 Fiziksel Mekânların Güvenliği ♦ TS ISO/IEC 27002 / 11 Fiziksel ve Çevresel Güvenlik ♦ COBIT 2019 / DSS05.05 BT Varlıklarına Fiziksel Erişimi Yönetin ♦ COBIT 2019 / DSS01.04 Çevreyi Yönetin ♦ COBIT 2019 / DSS01.05 Tesisleri Yönetin
Konu	**BG-11 Politika ve Prosedürler** Yetkisiz fiziksel erişimi engellemeye ve çevresel tehlikelerden korunmaya yönelik düzenlemeler mevcut mu?
Kriter	Kurum, tesislerinin ve bilişim sistemlerinin fiziksel ve çevresel güvenliğine ilişkin yazılı güvenlik politikasına ve prosedürlerine sahip olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Yetkisiz fiziksel erişim ve çevresel tehlikeler ile ilgili yazılı güvenlik politikası ve prosedürler oluşturulmuş mu?	• Fiziksel ve çevresel güvenlikle ilgili politika ve prosedürlerin aşağıda belirtilen hususları içerip içermediğinin incelenmesi: - Tesisler ve bilgisayar alanlarının fiziksel güvenlik sınırları - Bilişim sistemlerinin bulunduğu ortamların, donanım ve teçhizatın ve personelin konumunu gösteren güncel yerleşim planları - Tesislere ve bilgisayar alanlarına erişim yöntemleri - Giriş-çıkış kontrolleri ve personel güvenliği - Geçici personel ve ziyaretçilerle ilgili hususlar - Alarmların ve diğer sızma tespit araçlarının kullanımı - Olağanüstü durumlarda tahliye - BT varlıklarının tesis dışına çıkarılması - "Temiz masa" ve "temiz ekran" politikaları - Çevresel güvenliğe ilişkin kontrol düzenlemeleri • Fiziksel ve çevresel güvenlikle ilgili politika ve prosedürlerin güncel bir risk analizine dayanıp dayanmadığının ve BT varlıklarının güvenlik sınıflandırması ile uyumlu şekilde hazırlanıp hazırlanmadığının incelenmesi

Konu	**BG-12 Fiziksel Erişim** Kurum tesislerine ve bilgisayar alanlarına yalnızca yetkilendirilmiş personelin erişebilmesi sağlanıyor mu?
Kriter	Kurum tesislerine ve bilgisayar alanlarına (sistem odaları, veri depolama alanları, ağ teçhizatı, çalışma alanları, vb.) fiziksel erişimin yetki dâhilinde gerçekleştirilmesini sağlayacak önlemler alınmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurum tesislerine ve binalarına yetkisiz fiziksel erişimi önlemeye yönelik tedbirler alınmış mı?	• Yetkisiz kişilerin tesis ve binalara zorla girmesini engelleyecek fiziksel önlemlerin (örneğin; duvarla çevirme, bariyer koyma, kapıların ve pencerelerin kilitli tutulması, vb.) bulunup bulunmadığının gözlem ve saha incelemesi yoluyla belirlenmesi

	• Tesis ve binaların kritik noktalarını görüntüleyen ve kayıtları makul bir süre boyunca saklayan bir güvenlik kamera kayıt sisteminin bulunup bulunmadığının saha ve belge incelemesi yoluyla tespit edilmesi • Tesis ve binalarda uygun sızma tespit sistemlerinin (örneğin; hırsız alarmı, kamera kayıt sistemi, projektör, vb.) kurulup kurulmadığının ve bakımlarının ve testlerinin düzenli olarak yapılıp yapılmadığının saha ve belge incelemesi yoluyla tespit edilmesi • Tesis ve binalara sızma olayı gerçekleşmesi halinde takip edilen sürecin ilgili düzenlemeler ve talimatlar üzerinden incelenmesi • Güvenlik olay kayıtları incelenerek sızma girişimlerinin zamanında tespit edilip edilmediğinin belirlenmesi • Yetkisiz kişilerin tesislere giriş yapabildiği teslimat ve yükleme alanları gibi noktalarda fiziksel bariyerler ve güvenlik görevlilerinin bulunup bulunmadığının ve bu yerlerin güvenlik kameralarıyla izlenip izlenmediğinin saha incelemesi yoluyla belirlenmesi • Kurum tesislerine ve binalarına giriş-çıkışlarda kimlik tanımlama ve doğrulamaya yönelik bir mekanizma (kart okuyucu, biyometrik tanımlayıcı, güvenlik görevlisi kontrolü, vb.) bulunup bulunmadığının ve giriş-çıkışların kaydının tutulup tutulmadığının saha ve belge incelemesi yoluyla tespit edilmesi • Ziyaretçi kayıtlarının; ziyaret tarihi, giriş-çıkış saati, ziyaretçinin hangi birime geldiği, kiminle görüşeceği, hassas alanlara giriş yetkisi verilip verilmediği, güvenlik görevlisinin refakat edip etmediği gibi hususları içerecek şekilde tutulup tutulmadığının belge incelemesi yoluyla tespit edilmesi • İşten ayrılma prosedürü incelenerek Kurumdan ayrılan personelin tesislere ve binalara fiziksel erişiminin kaldırılmasına yönelik bir süreç bulunup bulunmadığının belirlenmesi • Kurumdan ayrılan personel arasından örnekleme yöntemiyle belirlenenlerin fiziksel erişimlerinin kaldırılıp kaldırılmadığının incelenmesi
2. Kurumun bilgisayar alanlarına yetkisiz fiziksel erişimi önlemeye yönelik tedbirler alınmış mı?	• Bilgisayar alanlarının; - Fiziksel olarak sınırlandırılıp sınırlandırılmadığının, - Sadece yetkili personelin erişimine açık olup olmadığının, - Giriş ve çıkışların kaydının tutulup tutulmadığının ve kayıtları makul bir süre boyunca saklayan bir güvenlik kamera kayıt sistemi tarafından izlenip izlenmediğinin gözlem, mülakat ve belge incelemesi yoluyla tespit edilmesi • Bilgisayar alanlarına fiziksel erişim yetkisinin kim tarafından ve nasıl tanındığının bilgi güvenliği gerekliliklerine uygunluk açısından incelenmesi • Örnek olarak seçilecek personelin fiziksel erişim yetkilerinin görev tanımlarına uygun olup olmadığının incelenmesi • Bilgisayar alanlarına erişim haklarının düzenli olarak gözden geçirilerek güncellenip güncellenmediğinin incelenmesi • Kuruma mal ve hizmet sağlayanların bilgisayar alanlarına erişiminin sadece gerektiğinde, yetki dâhilinde ve izlenmek kaydıyla sınırlandırılıp sınırlandırılmadığının incelenmesi • Bilgisayar alanlarına sızma olayı gerçekleşmesi halinde takip edilen sürecin ilgili düzenlemeler ve talimatlar üzerinden incelenmesi • Güvenlik olay kayıtları incelenerek sızma girişimlerinin zamanında tespit edilip edilmediğinin belirlenmesi • Kâğıtlar ve taşınabilir depolama ortamları için “temiz masa” ve bilgi işleme araçları için “temiz ekran” politikaları oluşturulup oluşturulmadığının incelenmesi

	• Teçhizat, bilgi ve yazılımların Kurum dışına çıkarılmasına yönelik süreçlerin tanımlanıp tanımlanmadığının incelenmesi • Kabloların yetkisi olmayan cihazlara takılmasını engellemek için teknik tarama ve fiziksel kontrollerin gerçekleştirilip gerçekleştirilmediğinin incelenmesi
3. Elektromanyetik Bilgi Kaçaklarından Korunma Yöntemleri (TEMPEST) uygulanıyor mu?	• Belge incelemesi, mülakat ve gözlem yoluyla, TEMPEST kapsamında; - Sistem odası/veri merkezinde kullanılan tüm gizlilik seviyeli bilgi işleyen cihazların hangi odalarda/bölümlerde kullanıldığını gösteren bir liste tutulup tutulmadığının - Sistem odası/veri merkezinde kullanılan tüm gizlilik seviyeli bilgi işleyen cihazların TEMPEST onayları olup olmadığının - TEMPEST onayı bulunan cihazların envanterinin tutulup tutulmadığının - Sistem odası/veri merkezindeki cihazların bulunduğu odalarda/bölümlerde elektromanyetik bilgi kaçaklarına karşı TEMPEST tesisat kurallarına/ilgili mevzuatlara uygun önlemler (örneğin; zırhlı kablolama sistemleri ve elektromanyetik kalkan kullanımı) alınıp alınmadığının belirlenmesi

Konu	**BG-13 Çevresel Güvenlik** Kurumun bilgisayar alanları çevresel tehlikelerden korunuyor mu?
Kriter	Bilgisayar alanlarının yangın, su, elektrik, iklimlendirme ve temizlik ile ilgili çevresel tehlikelerden korunmasına ilişkin kontrol düzenlemeleri oluşturulmalı ve uygulanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Yangın tehlikesine karşı gerekli önlemler alınıyor mu?	• Yangın tehlikesine karşı aşağıdaki faaliyetlerin gerçekleştirilip gerçekleştirilmediğinin belge ve saha incelemesi, gözlem ve mülakat yoluyla tespit edilmesi: - Yangından korunmaya ve kurtarmaya ilişkin bir prosedür hazırlanması ve ilgili personelin görev ve sorumluluklarının belirlenmesi - Bilişim sistemleri açısından kritik alanların yangına dayanıklı malzemeler kullanılarak inşa edilmesi - Sistem odasının yüksek patlayıcı özelliği olan yakıt deposu gibi alanlardan uzakta konumlandırılması - Yanıcı maddelerin (atık kâğıt, kimyasallar, kırtasiye, temizlik sıvıları) bilgisayar teçhizatlarından uzakta tutulması - Gerekli alanlarda duman detektörlerinin kullanılması - Otomatik yangın söndürme ve önleme sistemlerinin kurulması - Uygun yangın söndürme araçlarının tesis edilmesi (Örneğin; elektrik yangınlarında kullanılmak üzere uygun yangın söndürme teçhizatlarının bulundurulması) - Yangın söndürme ve önleme sistemlerinin testlerinin ve bakımlarının düzenli olarak yapılması - Yıldırımdan korunma önleminin binalar için uygulanması ve yıldırımdan korunma filtrelerinin tüm güç ve iletişim hatlarına takılması - Personelin; yangın alarmının, yangın detektörlerinin, elektrik anahtarlarının ve acil bir durumda kullanılabilir olan diğer araçların varlığı ve kullanımı konusunda bilgilendirilmesi - Daha önce yaşanmış yangın vakaları varsa, bunlar hakkında düzenlenmiş raporlarda önerilen önlemlerin alınması

2. Su kaynaklı tehlikelere karşı gerekli önlemler alınıyor mu?	• Su kaynaklı tehditlerden korunmak için aşağıdaki faaliyetlerin gerçekleştirilip gerçekleştirilmediğinin belge ve saha incelemesi yoluyla tespit edilmesi: - Bilişim sistemlerinin su basması riskinin yüksek olduğu zemin ve altı katlar ile su boruları veya su tanklarının etrafında veya ıslak zeminlerin (lavabo, mutfak, banyo, vb.) bitişiklerinde konumlandırılmaması - Su tesisatında yasal gereksinimlerle uyumlu ekipmanların kullanılması - Su ve kanalizasyon tesisatlarının bakımlarının düzenli olarak yapılması - Su sızıntılarına karşı su/nem detektörleri kullanılması, testlerinin ve bakımlarının düzenli olarak yapılması - Daha önce yaşanmış su kaynaklı vakalar varsa, bunlar hakkında düzenlenmiş raporlarda önerilen önlemlerin alınması
3. Elektrik kaynaklı tehlikelere karşı gerekli önlemler alınıyor mu?	• Elektrik kaynaklı tehditlerden korunmak için aşağıdaki faaliyetlerin gerçekleştirilip gerçekleştirilmediğinin belge ve saha incelemesi yoluyla tespit edilmesi: - Sistem odasının manyetik alanların yoğun olduğu trafo gibi cihazlardan uzak yerlerde konumlandırılması - Elektrik tesisatında ve kablolamada yasal gereksinimlerle uyumlu ekipmanların kullanılması - Güç kaynaklarında ve jeneratörlerde gücün devamlılığını sağlamak için alternatifli çoklu besleyicilerin kullanılması - Kesintisiz güç kaynakları ve jeneratörlerin testlerinin ve bakımlarının düzenli olarak yapılması - Alternatif güç kablolaması ve diğer düzenleyicilerin kurulduğu alanların anti-statik zemin kaplamasının yapılması - Bilgi işlem tesislerindeki güç ve iletişim hatlarının yer altından (ya da yeterli alternatif korumaya sahip şekilde) döşenmesi ve periyodik bakımlarının yapılması
4. İklimlendirme ile ilgili tehlikelere karşı gerekli önlemler alınıyor mu?	• Sıcaklık ve nem gibi iklimlendirme sisteminden kaynaklanabilecek tehditlerden korunmak için aşağıdaki faaliyetlerin gerçekleştirilip gerçekleştirilmediğinin belge ve saha incelemesi yoluyla tespit edilmesi: - Havalandırma ve klima sistemlerinin uygun noktalarda konumlandırılması - Havalandırma ve klima sistemlerinde yasal gereksinimlerle uyumlu ekipmanların kullanılması - Havalandırma ve klima sistemlerine sadece yetkili kişilerin müdahale etmesinin sağlanması - Havalandırma ve klima sistemlerinin bakımlarının düzenli olarak yapılması
5. Temizlik ile ilgili tehlikelere karşı gerekli önlemler alınıyor mu?	• Toz, çöp, haşere gibi temizlik zafiyetinden kaynaklanabilecek tehditlerden korunmak için aşağıdaki faaliyetlerin gerçekleştirilip gerçekleştirilmediğinin belge ve saha incelemesi yoluyla tespit edilmesi: - Bilgi işlem alanlarında uygun yerlere uyarı levhaları konulması, çöp kutusu yerleştirilmesi - Bilgi işlem alanlarının uygun şekilde temizlenmesi, çöplerinin ve atıklarının düzenli olarak toplanması - Çöp karıştırma saldırısını önlemek için sertifikası güncel kâğıt imha makinesi kullanılması - Haşereyle mücadele için düzenli olarak ilaçlama faaliyetleri yapılması

Erişim	
Denetim Hedefi	Kurumda sistem ve uygulamalara erişimin etkin şekilde yönetilip yönetilmediğini değerlendirmek
Referans	♦ 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi / Tedbir 15 ♦ Bilgi ve İletişim Güvenliği Rehberi / 3.2.1 Kimlik Doğrulama ♦ Bilgi ve İletişim Güvenliği Rehberi / 3.2.2 Oturum Yönetimi ♦ Bilgi ve İletişim Güvenliği Rehberi / 3.2.3 Yetkilendirme ♦ TS ISO/IEC 27002 / 9 Erişim Kontrolü ♦ COBIT 2019 / DSS05.04 Kullanıcı Kimliğini ve Mantıksal Erişimi Yönetin
Konu	**BG-14 Politika ve Prosedürler** Erişim yönetimine ilişkin politika ve prosedürler hazırlanmış mı?
Kriter	Kurum, bilişim sistemlerine ve uygulamalara erişimi düzenleyen politika ve prosedürlere sahip olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumda erişim kontrolüne ilişkin yazılı politika ve prosedürler var mı?	• Erişim ile ilgili politika ve prosedürlerde aşağıdaki hususların ele alınıp alınmadığının belge incelemesi yoluyla tespit edilmesi: - Kullanıcıların ve sistem yöneticilerinin rol ve sorumlulukları - Kullanıcıların oluşturulması ve kaldırılması - Varsayılan olarak özellikle açık olması gerekenler dışındaki tüm sistem ve uygulamalara erişimin kimlik doğrulama ile sağlanması - Erişim haklarının verilmesi ve iptal edilmesi - Ayrıcalıklı erişim haklarının yönetimi - Erişim haklarının ve ayrıcalıklarının periyodik olarak gözden geçirilmesi - Parolaların oluşturulması ve kullanılmasında uyulması gereken kurallar - Güvenli oturum açma prosedürleri - Erişim kayıtlarının tutulması ve izlenmesi - Yetkisiz erişimlerin raporlanması

Konu	**BG-15 Erişim Haklarının ve Ayrıcalıkların Yönetimi** Kurum sistem ve uygulamalarına güvenli erişim sağlanıyor mu?
Kriter	Kullanıcıların oluşturulmasına, kaldırılmasına, erişim haklarının ve ayrıcalıklarının verilmesine, yönetilmesine, izlenmesine ve geri alınmasına yönelik süreçler tanımlanmalı ve yetkisiz erişimi önleyecek mekanizmalar uygulanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kullanıcıların oluşturulmasına ve kaldırılmasına ilişkin süreçler tanımlanmış mı ve uygulanıyor mu?	• Kullanıcıların oluşturulmasına ve kaldırılmasına ilişkin süreçlerin tanımlanıp tanımlanmadığının belge incelemesi yoluyla tespit edilmesi • İşletim sistemleri ve uygulama programlarındaki varsayılan kullanıcı kimliklerinin kullanılıp kullanılmadığının, yönetici ve misafir hesaplarının kapatılıp kapatılmadığının incelenmesi • Kullanıcılar için izlenebilirliği ve sorumluluk tespitini sağlayacak şekilde tek ve benzersiz kimliklerin oluşturulup oluşturulmadığının belge ve kayıt incelemesi yoluyla belirlenmesi

	• Örnekleme yöntemiyle seçilecek kullanıcıların oluşturulmasına ilişkin süreç ve belgeler incelenerek talebin yazılı olarak iletilip iletilmediğinin ve yetkili makam tarafından onaylanıp onaylanmadığının tespit edilmesi • Örnek olarak seçilecek kullanıcılar ile mülakat yapılarak ortak/paylaşımlı kullanıcı kimliklerinin kullanılıp kullanılmadığının incelenmesi • Kurumdan ayrılan personel arasından örnekleme yöntemiyle belirlenenlerin kullanıcı kimliklerinin hemen kaldırılıp kaldırılmadığının belge ve kayıt incelemesi ve mülakat yoluyla tespit edilmesi • Belirli bir süre kullanılmayan, bir iş süreci veya kurum personeli ile ilişkilendirilemeyen tüm hesapların otomatik olarak devre dışı bırakılıp bırakılmadığının belge ve kayıt incelemesi ve mülakat yoluyla tespit edilmesi
2. Kullanıcıların erişim haklarının verilmesi ve iptal edilmesine ilişkin süreçler tanımlanmış mı ve uygulanıyor mu?	• Erişim haklarının verilmesi ve iptal edilmesine ilişkin süreçlerin tanımlanıp tanımlanmadığının belge incelemesi yoluyla tespit edilmesi • Erişim haklarının verilmesi ve iptal edilmesine ilişkin süreçlerde görevlerin ayrılığı ilkesinin gözetilip gözetilmediğinin belge incelemesi yoluyla belirlenmesi • Örnekleme yöntemiyle seçilecek kullanıcılara erişim hakları verilmesine ilişkin süreç ve belgeler incelenerek - Talebin yazılı olarak iletilip iletilmediğinin, - Talep edilen erişim haklarının ilgili görev tanımlarına referans verilerek "bilmesi gereken" ilkesi uyarınca gerekçelendirilip gerekçelendirilmediğinin ve açıkça tanımlanıp tanımlanmadığının, - Yetkili makam tarafından onaylanıp onaylanmadığının tespit edilmesi • Kurum dışından verilen erişim yetkisinin sınırlı olarak ve belirli bir süre için tanımlanıp tanımlanmadığının, bu tarz erişimlerin çok faktörlü kimlik doğrulaması ile gerçekleştirilip gerçekleştirilmediğinin ve erişim yolunun şifreli ve güvenli olup olmadığının belge ve kayıt incelemesi yoluyla tespit edilmesi • Verilen erişim haklarının kaydının merkezi olarak tutulup tutulmadığının belge ve kayıt incelemesi yoluyla tespit edilmesi • Kullanıcıların erişim haklarının düzenli olarak gözden geçirilip geçirilmediğinin belge incelemesi ve mülakat yoluyla tespit edilmesi • Görev yeri/tanımı değişen personel arasından örnekleme yöntemiyle belirlenenlerin erişim haklarının güncellenip güncellenmediğinin belge ve kayıt incelemesi yoluyla değerlendirilmesi
3. Ayrıcalıklı erişim haklarının tahsis edilmesi ve kullanımına ilişkin süreçler tanımlanmış mı ve uygulanıyor mu?	• Ayrıcalıklı erişim haklarının verilmesi ve kullanılmasına ilişkin süreçlerin tanımlanıp tanımlanmadığının belge incelemesi yoluyla tespit edilmesi • Ayrıcalıklı erişim haklarının hangi kullanıcılara hangi gerekçelerle tahsis edileceğinin ve hangi koşullarda sona ereceğinin ilgili düzenlemelerde belirlenip belirlenmediğinin incelenmesi • Ayrıcalıklı erişim haklarının kaydının merkezi olarak tutulup tutulmadığının belge ve kayıt incelemesi yoluyla tespit edilmesi • Ayrıcalıkların, doğrudan kullanıcılara verilmek yerine kullanıcıların atanmış/ait oldukları rollere/profillere/gruplara tanımlanıp tanımlanmadığının incelenmesi • Ayrıcalıklı erişim haklarının günlük işler için kullanılandan farklı bir kullanıcı kimliğine tahsis edilip edilmediğinin incelenmesi • Ayrıcalıklı erişim hakkına sahip kullanıcıların günlük işlerini yapmak için ayrıcalıklı kullanıcı kimliklerini kullanmamalarının sağlanıp sağlanmadığının işlem kayıtları üzerinden incelenmesi

	• Ayrıcalıklı kullanıcıların gerçekleştirdikleri işlemlerin kayıtlarının tutulup tutulmadığının ve düzenli olarak gözden geçirilip geçirilmediğinin belge incelemesi yoluyla tespit edilmesi • Kullanıcıların ayrıcalıklı erişim haklarının düzenli olarak gözden geçirilip geçirilmediğinin belge incelemesi ve mülakat yoluyla tespit edilmesi
4. Yazılı bir parola politikası var mı ve uygulanıyor mu?	• Parola politikasının aşağıdaki hususları içerip içermediğinin incelenmesi: - Parola oluşturma kuralları ➢ Güvenli bir minimum karakter uzunluğunun bulunması ➢ Alfabetik, sayısal ve özel karakterlerin karışık kullanılması ➢ Alfabetik karakterlerde büyük ve küçük harflerin karışık kullanılması ➢ Her kullanıcının kendine özel ve kendisi tarafından tanımlanmış bir parola kullanması ➢ Kullanıcılara otomatik olarak verilen ilk parolanın saldırılara dirençli, benzersiz ve sınırlı geçerlilik süresine sahip olması ➢ Kullanıcıların basit, yaygın olarak kullanılan veya kolay tahmin edilebilir parolalar oluşturmasının engellenmesi ➢ Farklı sistemler ve uygulamalar için farklı parolaların kullanılması - Parola koruma kuralları ➢ Kullanıcı parolalarının kriptografik algoritmalar kullanılarak korumalı parola dosyalarında saklanması ➢ Parola dosyalarına yetkisiz erişim denemelerinin raporlanması ➢ Parolaların kullanıcılara güvenli bir yolla ulaştırılması ➢ Kullanıcıların parolalarını başkalarıyla paylaşmaması, kâğıtlara ya da elektronik ortamlara kaydetmemesi ➢ Görevden ayrılan personelin bildiği/kullandığı parolaların hemen değiştirilmesi - Parola değiştirme kuralları ➢ Kullanıcıların ilk girişten sonra parolalarını değiştirmeye zorlanması ➢ Uygulama programlarının varsayılan parolalarının kurulumu takiben hemen değiştirilmesi ➢ Belirli periyotlarla parola değiştirme zorunluluğu olması ➢ Önceden kullanılan parolaların belli bir süre (örneğin; 12 ay) boyunca yeniden kullanımının engellenmesi ➢ Unutulmuş parola işlevinin eski parolayı kullanıcıya göndermemesi, parola sıfırlama fonksiyonuna yönlendirmesi, belirlenen yeni parolayı açık metin olarak iletmemesi ➢ Parola değiştirme fonksiyonunun en az eski parola, yeni parola ve yeni parolanın yinelenmesi adımlarından oluşması • Parola politikasının uygulanmasının ağ yönetim sistemi ve işletim sistemleri tarafından zorunlu tutulup tutulmadığının incelenmesi • Örnekleme yoluyla seçilen uygulamalarda parola politikası ile belirlenen kurallara uyulup uyulmadığının incelenmesi • Örnekleme yoluyla seçilen kullanıcılar ile mülakat yapılarak parola politikası ile belirlenen kurallar hakkında bilgi sahibi olup olmadıklarının tespit edilmesi
5. Sistem ve uygulamalara erişimde güvenli oturum açma prosedürleri tanımlanmış mı ve uygulanıyor mu?	• Kurum sistem ve uygulamalarında güvenli oturum açma prosedürlerinin tanımlanıp tanımlanmadığının belge incelemesi yoluyla tespit edilmesi • Örnek olarak seçilecek Kurum sistem ve uygulamalarında oturum açılarak aşağıdaki gerekliliklerin sağlanıp sağlanmadığının incelenmesi: - Oturum açma başarıyla tamamlanana kadar sistem ve uygulama tanımlayıcılarının görüntülenmemesi

	- Bilgisayara sadece yetkili kullanıcıların erişim sağlaması gerektiğini belirten genel bir uyarı mesajının görüntülenmesi - Yetkisiz kullanıcılara yardım edebilecek hiçbir bilgi ve yardım mesajının görüntülenmemesi - Parola giriş alanlarının kullanıcı girdilerini yansıtmayacak şekilde ayarlanması - Girilen bilgilerde bir hata ya da eksiklik olması durumunda hangi bilginin doğru ve yanlış olduğunun belirtmemesi - Oturumun başarıyla açılmasının ardından en son başarılı oturum açmanın tarih ve saatinin ve en son başarılı oturum açmadan bu yana gerçekleşen bütün başarısız oturum açma denemelerinin detaylarının görüntülenmesi - Aynı kullanıcı için eşzamanlı aktif oturum sayısının sınırlandırılması - Oturum anahtar değerlerinin yeterince uzun, eşsiz ve rasgele olması - Oturum anahtar değerlerinin URL'lerde veya hata mesajlarında tutulmaması - Kullanıcının, parolasını değiştirdikten veya hesabı kilitlendikten sonra tüm aktif oturumların sonlandırılması - Tanımlanan bir hareketsizlik süresi sonrasında oturumun sonlandırılması • Örnek olarak seçilecek Kurum sistem ve uygulamalarında gerçekleşen başarılı ve başarısız oturum açma girişimlerinin kayıtlarının tutulup tutulmadığının kayıt incelemesi yoluyla tespit edilmesi • Örnek olarak seçilecek Kurum sistem ve uygulamalarında oturum açma denemeleri yapılarak kaba kuvvet saldırılarına karşı korumaya (örneğin; CAPTCHA kullanılması, başarısız oturum açma girişimlerinin sayısının sınırlandırılması, sonraki oturum açma denemelerine izin vermeden önce zamanın geciktirilmesi, belli yetkilendirmeler olmadan sonraki denemelerin reddedilmesi, vb.) sahip olup olmadıklarının incelenmesi • Paket çözümleme araçları kullanılarak örnek olarak seçilecek Kurum sistem ve uygulamalarında oturum açma esnasında parolaların ağ üzerinden açık metin olarak iletilip iletilmediğinin incelenmesi • Kritik uygulamalarda ek güvenlik sağlamak amacıyla; - Oturum açmada parola girişine ilaveten başka yöntemler (örneğin, güvenilir konumdan/kaynaktan erişim, token cihazı, parmak izi okuyucu, tek kullanımlık şifre, vb.) kullanılıp kullanılmadığının ve - Oturum sürelerinin kısıtlanıp kısıtlanmadığının belirlenmesi
6. Erişim kayıtları tutuluyor ve izleniyor mu?	• Sistem yöneticileri ve kullanıcılar ile görüşme yapılarak, ilgili belge ve kayıtlar incelenerek ve veri analiz yöntemleri kullanılarak aşağıdaki hususların varlığının/etkinliğinin değerlendirilmesi - Tüm sistemlerde ve ağ cihazlarında kayıt mekanizmasının etkinleştirilmesi - Kayıtların, bilgi güvenliği gereksinimleri ve ilgili mevzuat gereği kabul edilebilir süre boyunca cihaz üzerinde veya harici sistemlerde tutulması, yetkisiz erişime ve değişime karşı korunması - Kayıtların, muhafazaları için tanımlanan kabul edilebilir sürenin sona ermesi ile birlikte güvenli bir şekilde yok edilmesi - Sistem yöneticisi, operatörler ve kullanıcıların faaliyetlerinin kayıt altına alınması, kayıtların korunması ve düzenli olarak gözden geçirilmesi - Sistem iz kayıtlarının; olay açıklaması, olay kaynağı, olay zamanı, kullanıcı/sistem bilgisi, kaynak adresleri, hedef adresleri ve işlem detayları bilgilerini içerecek şekilde tutulması ve bütünlüğünün zaman damgası ile korunması - Kayıtlarda zaman damgalarının tutarlı olması için ağa bağlı tüm sistemlerin (sunucular, iş istasyonları, güvenlik ürünleri, ağ aygıtları, vb.)

	düzenli olarak zaman bilgisinin alındığı; yedekli yapıda ve senkronize zaman sunucusunun kullanılması - Kayıt tutan sistemlerde yeterli depolama alanının tahsis edilmesi, depolama alanının doluluk oranının düzenli olarak kontrol edilmesi - Analiz ve inceleme amacıyla kayıtların merkezi bir kayıt yönetim sisteminde toplanması ve düzenli olarak yetkili personel tarafından gözden geçirilmesi - Kayıt tutma veya gönderme işlemi sırasında hata oluştuğunda uyarı mekanizmalarının aktif edilmesi ve izlenmesi - Kayıtların periyodik olarak yetkisiz faaliyetler için gözden geçirilmesi • Kayıt alma mekanizmalarının devre dışı bırakılıp bırakılmadığının veya kayıtların değiştirilip değiştirilmediğinin tutulan kayıtlar üzerinden sistem ve yardımcı sistem araçları kullanılarak incelenmesi • Yetkisiz erişim teşebbüslerine ilişkin yönetime rapor sunulup sunulmadığının, sunulan raporlarda belirtilen hususlara ilişkin olarak işlem yapılıp yapılmadığının incelenmesi

Ağ Yönetimi ve Güvenliği	
Denetim Hedefi	Kurum ağının etkin şekilde yönetilerek güvenliğinin sağlanıp sağlanmadığını değerlendirmek
Referans	♦ Bilgi ve İletişim Güvenliği Rehberi / 3.1.6 Ağ Güvenliği ♦ Bilgi ve İletişim Güvenliği Rehberi / 3.1.11 Sızma Testleri ve Güvenlik Denetimleri ♦ TS ISO/IEC 27002 / 13.1 Ağ Güvenliği Yönetimi ♦ 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ♦ COBIT 2019 / DSS05.02 Ağ ve Bağlantı Güvenliğini Yönetin
Konu	**BG-16 Politika ve Prosedürler** Ağ yönetimi ve güvenliğine ilişkin politika ve prosedürler mevcut mu?
Kriter	Kurum, ağ yönetimi ve güvenliğine ilişkin yazılı politikalara ve alt düzenlemelere sahip olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumda ağ yönetimi ve güvenliğine ilişkin yazılı politika ve prosedürler var mı?	• Ağ yönetimine ve güvenliğine ilişkin politika ve prosedürlerde aşağıdaki hususların ele alınıp alınmadığının belge incelemesi yoluyla tespit edilmesi: - Yöneticilerin ve kullanıcıların görevleri ve sorumlulukları - Kimlik denetimi ve yetkilendirme - Kablosuz iletişim - Sanal özel ağ (VPN) kullanımı - Uzaktan erişim - Yönetim protokolleri ve kriptolama - İnternet ve e-posta kullanımı - Yöneticilerin ve kullanıcıların internet ortamından dosya indirmelerine ilişkin kural ve sınırlamalar - Ağ trafiğinin izlenmesi ve kaydedilmesi - Ağ kapasitesinin izlenmesi

Konu	**BG-17 Güvenlik Yapılandırmaları ve Sıkılaştırma Tedbirleri** Ağ güvenliğini sağlamaya yönelik yapılandırmalar ve sıkılaştırma tedbirleri gerçekleştiriliyor mu?
Kriter	Ağın güvenli ve etkin bir şekilde yönetilmesi ve kullanılmasına ilişkin yapılandırmalar ve sıkılaştırma tedbirleri (dokümantasyon, yedeklilik, güncelleme, segmentasyon, yetkilendirme, erişim, kayıt alma, izleme, uzaktan erişim, e-posta, vb. konuları kapsayacak şekilde) gerçekleştirilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurum ağı dokümante ediliyor mu?	• Belge/kayıt incelemesi ve mülakat yoluyla; - Kurum ağlarının fiziksel ve mantıksal topolojilerinin dokümante edilip edilmediğinin - Mevcut donanım ve yazılım envanteri ile ağ topolojilerinin eşleşip eşleşmediğinin - Kurum ağ ve güvenlik cihazlarına ait yapılandırmaların (ağ trafiğini düzenleyen kurallara ait tanımlar, kullanılma amacı ve kuralı tanımlayan kişi bilgisi yer alacak şekilde) dokümante edilip edilmediğinin ve güncelliğinin sağlanıp sağlanmadığının tespit edilmesi
2. Kullanılan ağ ve güvenlik cihazlarında yedeklilik ve yük paylaşımı sağlanıyor mu?	• Kurum ağ mimarisine ilişkin dokümanlar incelenerek ve mülakat yapılarak, ağ ve güvenlik cihazlarının - Yedekli yapıda ve - Yük paylaşımlı olarak çalışıp çalışmadığının belirlenmesi
3. Kullanılan ağ ve güvenlik cihazlarının güncelliği sağlanıyor mu?	• Belge/kayıt incelemesi ve mülakat yoluyla; - Güncel ve üretici desteği devam eden ağ ve güvenlik cihazlarının kullanılıp kullanılmadığının - Ağ ve güvenlik cihazlarının sürümlerinin güncelliğinin düzenli olarak kontrol edilip edilmediğinin - Gerekli güncelleştirmelerin ve yayımlanan güvenlik yamalarının yüklenip yüklenmediğinin belirlenmesi
4. Kurum ağı bilgi güvenliği gereksinimleri doğrultusunda katmanlara ayrılmış mı?	• Kurum ağ mimarisine ilişkin dokümanlar incelenerek ve mülakat yapılarak - Kablolu ve kablosuz ağların ayrılıp ayrılmadığının - İstemcilerin yer aldığı ağlar ile sunucu/uygulamaların yer aldığı ağların ayrılıp ayrılmadığının - Sunucu ağında istemcilerin yer almamasının sağlanıp sağlanmadığının - Yönetimsel işlemler için ayrı yönetim ağları kullanılıp kullanılmadığının - İnternete açık olarak çalışan sunucuların (uygulama sunucusu, web sunucu, e-posta sunucuları, vb.) DMZ (DeMilitarized Zone) gibi ayrı bir bölgede tutulup tutulmadığının belirlenmesi
5. Kurum ağından ayrı bir misafir ağı oluşturulmuş ve güvenliği sağlanmış mı?	• Belge/kayıt incelemesi ve mülakat yoluyla; - Misafir ağının kurum ağı ile fiziksel ve/veya mantıksal olarak izole edilip edilmediğinin - Misafir cihazlarının yalnızca misafir ağına erişimlerinin mümkün kılınıp kılınmadığının - Misafirlerin, misafir ağına bağlanırken kimlik bilgilerini doğrulayan mekanizmalar kullanılıp kullanılmadığının

	- Misafirler tarafından misafir ağı üzerinden yapılan tüm erişimlerin kayıt altına alınıp alınmadığının tespit edilmesi
6. Kurum ağında yönetim ve yapılandırmaya ilişkin yetkilendirmeler ve erişimler bilgi güvenliği gereklerine uygun şekilde gerçekleştiriliyor mu?	• Belge/kayıt incelemesi ve mülakat yoluyla; - Kurum ağ ve güvenlik cihazlarında yönetim ve yapılandırma işlemlerini yapabilecek kullanıcıların yetkilendirilmesine yönelik bir süreç tanımlanıp tanımlanmadığının - Yönetim ve yapılandırma yetkisine sahip olan kullanıcıların listesinin düzenli olarak gözden geçirilip geçirilmediğinin - Ağ ve güvenlik cihazlarının yönetiminin, çok faktörlü kimlik doğrulama mekanizmaları kullanılarak şifreli ağ trafiği üzerinden yapılıp yapılmadığının tespit edilmesi
7. Kurum ağ trafiği bilgi güvenliği gereklerine uygun şekilde yönetiliyor mu?	• Belge/kayıt incelemesi ve mülakat yoluyla; - İnternetten gelen veya internete giden tüm ağ trafiğinin, yetkisiz bağlantıları engellemek için uygulama katmanında filtreleme ve kimlik doğrulaması yapılarak iletilip iletilmediğinin - Kurumdaki sistemlerin, kurum tarafından onaylanmayan web sitelerine bağlanmasını engelleyen ağ tabanlı URL filtrelerinin uygulanıp uygulanmadığının - URL sınıflandırma servisleri kullanılıp kullanılmadığının, bu servislerin kullandığı listelerin güncel tutulup tutulmadığının, kategorilendirilmemiş sitelerin varsayılan olarak engellenip engellenmediğinin - Kurum ağ sınırlarından sadece izin verilen kaynaklardan izin verilen hedeflere, izin verilen port ve protokoller ile trafik akışının sağlanıp sağlanmadığının - Ağda kritik verinin taşınmasında güvenli protokollerin (VPN teknolojileri, SSL/TLS, vb.) kullanılıp kullanılmadığının ve kritik verinin ayrıca şifrelenerek taşınıp taşınmadığının belirlenmesi
8. Kurum internet ortamında konusu suç oluşturan içeriklere erişimi önleyici tedbirleri alıyor mu?	• 5651 sayılı yasa ve ilgili mevzuat uyarınca, konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak amacıyla içerik filtreleme sistemi kullanılıp kullanılmadığının incelenmesi
9. Kurumda ağ erişimleri ve ağ trafiği izleniyor ve kayıt altına alınıyor mu?	• Bakınız: BG-15 Erişim Haklarının ve Ayrıcalıkların Yönetimi / 6 • Belge/kayıt incelemesi ve mülakat yoluyla; - Ağ sınır cihazlarındaki bağlantı trafiği, kullanıcı işlemleri gibi bilgilerin kayıt altına alınıp alınmadığının - Kurum tarafından gerekli görülen durumlarda, belirlenen kaynaklar ve hedefler arasındaki tüm ağ trafiğinin izlenebilmesi için kayıt mekanizmaları oluşturulup oluşturulmadığının tespit edilmesi
10. Yer sağlayıcı trafik bilgisi ve internet toplu kullanım sağlayıcı erişim kayıtları tutuluyor mu?	• 5651 sayılı yasa ve ilgili mevzuat uyarınca, Kurum tarafından yer sağlayıcı trafik bilgisinin tutulup tutulmadığı ve tutulan trafik bilgisinin aşağıdaki hususları içerip içermediğinin incelenmesi: - Kaynak IP adresi - Hedef IP adresi - Bağlantı tarih-saat bilgisi - İstenen sayfa adresi - İşlem bilgisi (GET, POST komut detayları) - Sonuç bilgisi

	• Yer sağlayıcı trafik bilgilerinin zaman damgası ile damgalanarak 6 ay saklanıp saklanmadığının ve gizliliğinin temin edilip edilmediğinin incelenmesi • 5651 sayılı yasa ve ilgili mevzuat uyarınca, Kurum tarafından internet toplu kullanım sağlayıcı erişim kayıtlarının tutulup tutulmadığı ve tutulan erişim kayıtlarının aşağıdaki hususları içerip içermediğinin incelenmesi: - İç ağlarında dağıtılan IP adres bilgileri - Kullanıma başlama ve bitiş zamanı ve bu IP adreslerini kullanan bilgisayarların tekil ağ cihaz numarasını (MAC adresi) gösteren bilgiler - Hedef IP adresi - Bir veya birden fazla IP adresinin portlar aracılığı ile kullanıcılara paylaştırılması yöntemi ile sunulan internet erişim hizmetinde kullanıcıya tahsis edilen gerçek IP ve port bilgileri • İnternet toplu kullanım sağlayıcı erişim kayıtlarının elektronik ortamda kaydedilip 2 yıl süre ile saklanıp saklanmadığının incelenmesi
11. Ağ üzerinden gerçekleştirilebilecek saldırılardan korunmaya yönelik önlemler alınıyor mu?	• Belge/kayıt incelemesi ve mülakat yoluyla; - Sadece onaylı donanımların kurum ağına bağlanabilmesini sağlamak için kurum ağına bağlanan cihazlara kimlik denetimi yapılıp yapılmadığının - Ağ içerisinde veri akışını kontrol etmek, izlemek ve izinsiz ağ trafiğini takip etmek amacıyla ağ tabanlı veri sızıntısı önleme sistemlerinin kullanılıp kullanılmadığının - Saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit ve engelleme sistemlerinin kullanılıp kullanılmadığının - Kullanılan güvenlik sistemleri tarafından tespit edilen tehditlerin, saldırıların ve saldırı girişimlerinin raporlanıp raporlanmadığının ve analiz edilip edilmediğinin değerlendirilmesi
12. Kurum sistemlerine/sistem bileşenlerine uzaktan erişimde bilgi güvenliği gereklerine uyum sağlanıyor mu?	• Uzaktan erişim ile ilgili olarak aşağıdaki tedbirlerin alınıp alınmadığının belge incelemesi, gözlem ve mülakat yoluyla belirlenmesi: - İnternet ortamından kurum içi kaynaklara erişimde VPN teknolojilerinin kullanılması - Kuruma uzaktan bağlanacak cihazların; zararlı yazılımdan korunma, işletim sistemi ve uygulama güncelliği, vb. hususlar kapsamında kurum politikalarına uygunluğunun güvenli uzaktan bağlantı sağlayan sistemler üzerinden (VPN, vb.) kontrol edilmesi, Kurum politikasına uymayan cihazlara bağlantı izni verilmemesi - Sunuculara uzaktan yapılacak erişimlerde çok faktörlü kimlik doğrulama mekanizmalarının kullanılması - Veri tabanı sunucularına uzak bağlantıların mümkün olduğunca sınırlandırılması, yalnızca yetkili kullanıcıların ve/veya uygulamaların uzaktan erişimine olanak sağlanması - Kullanıcı bilgisayarlarında, bilgisayara ağ üzerinden erişim yetkisinin, sadece yönetici hesapları ve uzak masaüstü kullanıcıları veya grupları ile sınırlandırılması
13. E-posta kullanımında bilgi güvenliği gereklerine uyum sağlanıyor mu?	• E-posta kullanımı ile ilgili olarak aşağıdaki tedbirlerin alınıp alınmadığının belge incelemesi, gözlem ve mülakat yoluyla belirlenmesi: - E-posta içeriğindeki zararlı bağlantılara (URL) erişimin engellenmesi - Spam e-postaları engellemek üzere DNS tabanlı filtreleme ve kara liste yöntemlerinin uygulanması - İzinsiz ve/veya çalıştırılabilir dosya türleri içeren e-posta veya e-posta eklerinin engellenmesi - Kuruma dışarıdan gelen e-posta eklerinin çok katmanlı güvenlik analizinden (içerik analizi, beyaz liste/kara liste, imza tabanlı anti-virüs,

	anti-malware taramaları, vb.) geçirilmesi, bu aşamadan sonra hala kategorilendirilmemiş e-posta eklerinin kum havuzunda çalıştırılması - Kurum politikalarına göre gizlilik dereceli bilgi/veri içeren e-posta alışverişlerinin şifreli ve imzalı olarak yapılması, e-posta alışverişlerinin şifreli ve imzalı olarak yapıldığı durumda kullanılan sertifikaların kuruma özel olarak üretilmesi
14. Kurumda yıllık olarak sızma testi ve güvenlik denetimleri yapılıyor mu?	• Kurum sistemlerine yönelik yılda en az bir defa harici ve dâhili sızma testleri ve güvenlik denetimleri gerçekleştirilip gerçekleştirilmediğinin belge incelemesi ve mülakat yoluyla belirlenmesi • Test sonuçları uyarınca tespit edilen zafiyetlerin giderilmesine yönelik gerekli düzeltmelerin yapılıp yapılmadığının incelenmesi

İşletim Sistemleri Yönetimi ve Güvenliği	
Denetim Hedefi	Kurumda kullanılan işletim sistemlerinin sorunsuz ve güvenli şekilde çalışmasının sağlanıp sağlanmadığını değerlendirmek
Referans	⬧ Bilgi ve İletişim Güvenliği Rehberi / 5.1 İşletim Sistemi Sıkılaştırma Tedbirleri ⬧ Bilgi ve İletişim Güvenliği Rehberi / 3.1.8. İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi ⬧ TS ISO/IEC 27002 / 12 İşletim Güvenliği ⬧ COBIT 2019 / DSS05.03 Uç Nokta Güvenliğini Yönetin ⬧ COBIT 2019 / DSS05.01 Kötü Amaçlı Yazılımlara Karşı Korunun
Konu	**BG-18 Politika ve Prosedürler** İşletim sistemlerinin yönetimi ve güvenliğine ilişkin politika ve prosedürler mevcut mu?
Kriter	Kurum, işletim sistemlerinin yönetimi ve güvenliğine ilişkin yazılı politikalara ve alt düzenlemelere sahip olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumda işletim sistemlerinin yönetimine ve güvenliğine ilişkin yazılı politika ve prosedürler var mı?	• İşletim sistemlerinin yönetimine ve güvenliğine ilişkin politika ve prosedürlerde aşağıdaki hususların ele alınıp alınmadığının belge incelemesi yoluyla tespit edilmesi: - Yöneticilerin ve kullanıcıların görevleri ve sorumlulukları - Kurulum ve bakım - Kimlik denetimi ve yetkilendirme - Kullanıcı grupları ve profilleri - Versiyon yükseltmeleri ve yama geçişleri - Uzaktan erişim - Yönetici ve kullanıcı işlemlerinin izlenmesi ve kaydedilmesi

Konu	**BG-19 Güvenlik Yapılandırmaları ve Sıkılaştırma Tedbirleri** İşletim sistemlerinin güvenliğini sağlamaya yönelik yapılandırmalar ve sıkılaştırma tedbirleri gerçekleştiriliyor mu?
Kriter	İşletim sistemlerinin güvenli ve etkin bir şekilde yönetilmesi ve kullanılmasına ilişkin yapılandırmalar ve sıkılaştırma tedbirleri (güncelleme, yetkilendirme, erişim, kayıt alma, zararlı yazılımlardan koruma, şifreleme, vb. konuları kapsayacak şekilde) gerçekleştirilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kullanılan işletim sistemlerinin güncelliği sağlanıyor mu?	• Belge/kayıt incelemesi ve mülakat yoluyla; - Güncel ve üretici desteği devam eden işletim sistemlerinin kullanılıp kullanılmadığının - Kullanılan versiyonların güncelliğinin düzenli olarak kontrol edilip edilmediğinin ve gerekli güncelleştirmelerin ve yayımlanan güvenlik yamalarının yüklenip yüklenmediğinin - İşletim sistemi güncellemeleri için merkezi bir güncelleme sunucusu oluşturulup oluşturulmadığının - Yamaların yüklenmeden önce test ortamında uyumsuzluklara karşı test edilip edilmediğinin - Yamalar uygulanmadan önce sistemin yedeklemesinin yapılıp yapılmadığının - Uygulanan yamaların kaydının tutulup tutulmadığının - Zorunlu nedenlerden dolayı kullanılan güncel olmayan işletim sistemleri için telafi edici/ek güvenlik önlemlerinin alınıp alınmadığının değerlendirilmesi
2. Kullanıcıların erişimleri ve yetkileri bilgi güvenliği gerekleri doğrultusunda yönetiliyor mu?	• Belge/kayıt incelemesi ve mülakat yoluyla; - Kimlik doğrulama için merkezi kimlik yönetimi servisi kullanılıp kullanılmadığının - Son kullanıcıların, güvenlik sıkılaştırmaları kapsamında kurum tarafından uygulanması gerekli görülen konfigürasyonlara müdahale etmemesi ve beyaz listede bulunan programlar haricinde program kurmalarının engellenmesi için gerekli kullanıcılar dışında tüm kullanıcıların yerel yönetici hesaplarının devre dışı bırakılıp bırakılmadığının - Gerekli kullanıcılar için varsayılan olarak aynı tanımlanan yerel yönetici hesaplarının parolalarının değiştirilip değiştirilmediğinin tespit edilmesi
3. Gerçekleştirilen işlemler kayıt altına alınıyor mu?	• Bakınız: BG-15 Erişim Haklarının ve Ayrıcalıkların Yönetimi / 6 • Belge/kayıt incelemesi ve mülakat yoluyla; - Sistem zaman ve tarih ayarları, kullanıcı hesapları, ağ yapılandırması, erişim kontrolleri üzerinde yapılan değişikliklerin kayıt altına alınıp alınmadığının - Giriş ve çıkış bilgileri, yetkisiz dosya okuma denemeleri, dosya silme işlemleri ve sistem yöneticisi hareketlerinin kayıt altına alınıp alınmadığının belirlenmesi
4. Zararlı yazılımlardan korunmaya yönelik faaliyetler gerçekleştiriliyor mu?	• Belge/kayıt incelemesi ve mülakat yoluyla; - İstemci ve sunucu sistemlerinin tamamında zararlı yazılımdan korunma uygulamalarının kullanılıp kullanılmadığının - Zararlı yazılımdan korunma uygulamalarında en güncel yama dosyalarının bulunup bulunmadığının ve imza veri tabanının güncel olup olmadığının

	- Zararlı yazılımdan korunma uygulamalarına ait politikaların merkezi olarak yönetilip yönetilmediğinin - Zararlı yazılımlara karşı düzenli olarak tarama gerçekleştirilip gerçekleştirilmediğinin - Kurumdaki tüm bilgisayarların, taşınabilir diskleri otomatik olarak zararlı yazılım taramasından geçirecek şekilde yapılandırılıp yapılandırılmadığının - Kurumdaki tüm bilgisayarların, taşınabilir ortamlarda otomatik kod çalıştırılmasına izin vermeyecek şekilde yapılandırılıp yapılandırılmadığının - Tüm zararlı yazılım tespitlerinin, merkezi yönetim ve kayıt sunucularına iletilip iletilmediğinin değerlendirilmesi
5. İşletim sistemlerinin yapılandırılmasında gerekli sıkılaştırmalar gerçekleştirilmiş mi?	• Belge/kayıt incelemesi ve mülakat yoluyla; - Kritik bilgi içeren ve/veya işleyen makinelerde disk seviyesinde şifreleme yapılıp yapılmadığının - İşletim sistemi hata ve sorun bilgilerinin üretici ile paylaşılması özelliğinin pasif hale getirilip getirilmediğinin - Sunucularda kullanılmayan kablosuz ağ ara yüzlerinin pasif hale getirilip getirilmediğinin - Kritik sistemlerin taşınabilir depolama birimlerini desteklemeyecek şekilde yapılandırılıp yapılandırılmadığının, taşınabilir depolama birimleri takıldığında uyarı üretecek mekanizmaların aktif edilip edilmediğinin ve bu uyarıların izlenip izlenmediğinin tespit edilmesi

Veri Tabanı Yönetimi ve Güvenliği	
Denetim Hedefi	Kurumun veri tabanlarının etkin şekilde yönetilerek güvenliğinin sağlanıp sağlanmadığını değerlendirmek
Referans	♦ Bilgi ve İletişim Güvenliği Rehberi / 3.2.7 Veri Tabanı ve Kayıt Yönetimi ♦ Bilgi ve İletişim Güvenliği Rehberi / 5.2 Veri Tabanı Sıkılaştırma Tedbirleri ♦ TS ISO/IEC 27002 / 12 İşletim Güvenliği
Konu	**BG-20 Politika ve Prosedürler** Veri tabanlarının yönetimi ve güvenliğine ilişkin politika ve prosedürler mevcut mu?
Kriter	Kurum, veri tabanlarının yönetimi ve güvenliğine ilişkin yazılı politikalara ve alt düzenlemelere sahip olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kurumda veri tabanlarının yönetimi ve güvenliğine ilişkin yazılı politika ve prosedürler var mı?	• Veri tabanı yönetimine ve güvenliğine ilişkin politika ve prosedürlerde aşağıdaki hususların ele alınıp alınmadığının belge incelemesi yoluyla tespit edilmesi: - Yöneticilerin ve kullanıcıların görevleri ve sorumlulukları - Kurulum ve bakım - Kimlik denetimi ve yetkilendirme - Kullanıcılar ve kullanıcı şemaları - Kullanıcı profilleri ve kaynak kullanım limitleri

	- Versiyon yükseltmeleri ve yama geçişleri - Depolama ve yedekleme ayarları - Uzaktan erişim - Yönetici ve kullanıcı işlemlerinin izlenmesi ve kaydedilmesi

Konu	**BG-21 Güvenlik Yapılandırmaları ve Sıkılaştırma Tedbirleri** Veri tabanlarının güvenliğini sağlamaya yönelik tedbirler alınıyor mu?
Kriter	Veri tabanlarının güvenli ve etkin bir şekilde yönetilmesi ve kullanılmasına ilişkin yapılandırmalar ve sıkılaştırma tedbirleri (güncelleme, yetkilendirme, kayıt alma, şifreleme, vb. konuları kapsayacak şekilde) gerçekleştirilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kullanılan veri tabanı sistemlerinin güncelliği sağlanıyor mu?	• Belge/kayıt incelemesi ve mülakat yoluyla; - Güncel ve üretici desteği devam eden veri tabanı sistemlerinin kullanılıp kullanılmadığının - Kullanılan versiyonların güncelliğinin düzenli olarak kontrol edilip edilmediğinin ve gerekli güncelleştirmelerin ve yayımlanan güvenlik yamalarının yüklenip yüklenmediğinin değerlendirilmesi
2. Kullanıcılar ve yetkileri bilgi güvenliği gerekleri doğrultusunda yönetiliyor mu?	• Belge/kayıt incelemesi ve mülakat yoluyla; - Belirli bir süre boyunca kullanılmayan kullanıcıların tespit edilerek pasif hale getirilip getirilmediğinin - Roller gözden geçirilerek kullanılmayan rollerin kaldırılıp kaldırılmadığı/pasif hale getirilip getirilmediğinin - Kullanıcı hakları gözden geçirilerek gereksiz olarak tanımlanmış ve/veya ihtiyaç duyulmayan yetkilerin kaldırılıp kaldırılmadığının - Yetkilerin tanımlanmasında görevler ayrılığı ilkesinin gözetilip gözetilmediğinin - Kurulum ile gelen örnek verilerin (örnek tablolar, kayıtlar, kullanıcılar, vb.) veri tabanından silinip silinmediğinin - Kritik veri içeren tablo ve nesneler için tablo ve/veya nesne bazında yetkilendirme yapılıp yapılmadığının - Veri tabanı servislerini çalıştıran kullanıcılar için “en az yetki” prensibinin uygulanıp uygulanmadığı, ihtiyaç duyulmadığı takdirde yönetici yetkilerinin tanınmamasının sağlanıp sağlanmadığının - Veri tabanının çalıştığı işletim sistemi üzerinde; komut çalıştırma, yerel dosya okuma/yazma vb. işlemlere imkân sağlayabilecek ayrıcalıkların sınırlandırılıp sınırlandırılmadığının - Yedek dosyalarına yetkisiz kullanıcıların erişmesini engellemek için, dosya izinlerinin yapılandırılması, şifreleme, vb. yöntemler kullanılıp kullanılmadığının tespit edilmesi
3. Veri tabanı işlemlerinin kaydı tutuluyor mu?	• Bakınız: BG-15 Erişim Haklarının ve Ayrıcalıkların Yönetimi / 6 • Belge/kayıt incelemesi ve mülakat yoluyla; - İşlem ve denetim kayıtlarının alınıp alınmadığının - Kayıt dosyalarının güvenliğinin sağlanması amacıyla, kullanıcıların ilgili dosyalar üzerindeki yetkilerinin sınırlandırılması, kayıtların güvenli olarak farklı bir lokasyona kopyalanması, vb. yöntemlerin kullanılıp kullanılmadığının

	- Veri tabanı tarafından kullanılan sistem dosyalarının ve üretilen iz kayıtlarının aynı disk bölümü üzerinde bulunmamasının, farklı disk bölümlerinde tutulmasının sağlanıp sağlanmadığının belirlenmesi
4. Veri tabanlarında tutulan verinin gizliliğini sağlamaya yönelik tedbirler alınıyor mu?	• Belge/kayıt incelemesi ve mülakat yoluyla; - Veri tabanı sunucularında yer alan kritik verinin, depolama motoru (storage engine) ve/veya disk seviyesinde şifreleme gibi yöntemler ile güvenliğinin sağlanıp sağlanmadığının - Veri tabanı üzerinde yer alan özel nitelikli kişisel verilerin açık metin olarak tutulmamasının sağlanıp sağlanmadığının, ulusal ve/veya uluslararası standartlar tarafından kabul görmüş kriptografik yöntemlerden faydalanılarak saklanıp saklanmadığının - Veri tabanı sunucusu ile istemci arasındaki iletişimin şifreli trafik üzerinden sağlanıp sağlanmadığının tespit edilmesi

Ek-8.7:
Uygulama Kontrolleri
Önerilen Kontrol Değerlendirme Matrisi

Girdi	
Denetim Hedefi	Geçerli veri girişinin yetkili personel tarafından ve uygun şekilde yapılıp yapılmadığını değerlendirmek
Referans	♦ COBIT 2019 / DSS06.01 İş Süreçlerine Yerleştirilmiş Kontrol Faaliyetlerini Kurum Hedefleriyle Hizalayın ♦ COBIT 2019 / DSS06.04 Hataları ve İstisnaları Yönetin
Konu	**UK-1 Girdilerin Doğrulanması** Uygulamanın yeterli girdi doğrulama kontrolleri var mı?
Kriter	Girdi doğrulama kuralları kapsamlı olarak belirlenmeli, belgelendirilmeli, uygulamanın veri giriş ara yüzlerine tanımlanmalı ve düzenli aralıklarla güncellenmelidir. Girdi doğrulama kontrolleri sadece yetkili kişiler tarafından devre dışı bırakılabilmeli ve bu işlemlerin kaydı tutulmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Girdi verisinin doğrulanmasına ilişkin kriterler ve parametreler belirlenmiş mi?	• İş kuralları, gereksinim dokümanları ve uygulama ile ilgili diğer belgeler incelenerek ve iş süreç sahipleri ile görüşülerek; değerlendirmeye konu iş süreçlerinde hangi girdi doğrulama kurallarının yer alması gerektiğinin belirlenmesi • Belge incelemesi ve ilgililerle mülakat yapılarak; - Girdi doğrulama kriter ve parametrelerinin iş kuralları ile eşleşip eşleşmediğinin - Doğrulama kurallarının uygun şekilde tasarlanıp tasarlanmadığının ve dokümante edilip edilmediğinin belirlenmesi • Mülakat ve belge incelemesi (ve gerekli görüldüğünde uzman desteği yoluyla kod analizi) yapılarak; girdi verisine ilişkin doğrulama kriterleri ve parametrelerinin - Düzenli olarak gözden geçirilip geçirilmediğinin - Zamanında, uygun bir şekilde ve yetkili kişilerce güncellenip güncellenmediğinin belirlenmesi
2. Girdi doğrulama kontrolleri etkin şekilde çalışıyor mu?	• Uygulamanın kullanımı gözlemlenerek, uygulama test ortamında çalıştırılıp veri giriş ekranları/ara yüzleri denenerek ve BDDTA yardımıyla uygulama verileri analiz edilerek; aşağıda örnekleri verilen otomatik girdi doğrulama kontrollerinden gerekli olanların zamanında ve tam olarak çalışıp çalışmadığının belirlenmesi: - Üst limit kontrolü - Aralık kontrolü - Zorunlu alan kontrolü - Rakam kontrolü - Seri veya sıra kontrolü - Mükerrerlik kontrolü - Geçerlilik kontrolü

	- Makullük kontrolü - Tamlık kontrolü - Boşluk kontrolü • Çevrimiçi işleme (online processing) yapan sistemlerde, veri tabanında yer alan bilgilerin gizlilik ve bütünlüğünün korunması amacıyla, "*", "=", "or", "select" gibi veritabanı komut ve ifadelerinin çalıştırılabilir komut dizisi özelliğinden arındırılarak kabul edilip edilmediğinin belirlenmesi • Uygulamanın kullanımı gözlemlenerek, uygulama test ortamında çalıştırılıp veri giriş ekranları/ara yüzleri denenerek ve BDDTA yardımıyla uygulama verileri analiz edilerek; - Kurallara uymayan girişlerin reddedilip edilmediğinin - Gerekli hata mesajlarının üretilip üretilmediğinin belirlenmesi
3. Girdi doğrulama kontrollerinin devre dışı bırakılması yetki dâhilinde gerçekleştiriliyor ve kayıt altına alınıyor mu?	• Belge ve kayıtlar incelenerek ve gözlem yapılarak; - Girdi doğrulama kontrollerini devre dışı bırakma yetkisinin yalnızca yönetici (süpervizör) pozisyonundaki personele ve sınırlı sayıda durum için tanımlanıp tanımlanmadığının - Kontrollerin devre dışı bırakıldığı durumlarda, bu eylemlerin düzgün şekilde kayıt altına alınıp alınmadığının ve uygunluğunun/yerindeliğinin gözden geçirilip geçirilmediğinin belirlenmesi • Hata düzeltmeleri ve giriş iptallerine ilişkin belge ve kayıtlar incelenerek tanımlı prosedürlerin izlendiğinin doğrulanması

Konu	**UK-2 Kaynak Belgelerin ve Verilerin Yönetimi, Toplanması ve Girişi** Kaynak belgeler ile veri hazırlama ve giriş süreçleri uygun şekilde yönetiliyor mu?
Kriter	Veri hazırlama ve giriş prosedürleri yazılı olmalı ve kullanıcılara duyurulmalıdır. Kaynak belgeler imha edilene kadar kayıt altında tutulmalı, her işleme eşsiz ve sıralı bir numara atanmalıdır. Kaynak belgelerin asılları yasal gereklilikler veya politikalarda öngörülen süre boyunca saklanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Veri giriş işlemlerinin yapılmasına ilişkin tanımlanmış bir prosedür var mı?	• Aşağıdaki hususların varlığı incelenerek, veri hazırlama ve giriş işlemlerinin yapılmasına ilişkin prosedürlerin yeterince dokümante edilip edilmediğinin belirlenmesi: - Veri giriş şekli (manuel, online, vb.) - Veri giriş ara yüzlerine ilişkin tanımlamalar - Belge veya iş akışı ve zamanlaması - Kaynak belgelerin belirlenmesi, düzenlenmesi ve onaylanması ile bunlara ilişkin görev, yetki ve sorumluluklar - Belge düzenleme sürecinde hataların ve düzensizliklerin tespit edilmesi, raporlanması ve düzeltilmesi - Kaynak belgelerin saklanacağı süre - Kaynak belge olarak veri giriş formu kullanılıyorsa standart formların tespit edilmesi • Kullanıcılarla görüşme yapılarak; prosedürlere erişimlerinin olup olmadığının ve prosedürlerin anlaşılıp anlaşılmadığının belirlenmesi

2. Kaynak belgeler prosedürlerde tanımlandığı şekilde kullanılıyor ve yönetiliyor mu?	• İlgili belgeler incelenerek ve kullanıcılar ve program uygulamaları gözlemlenerek; - Prosedürlerde tanımlanmış olan kaynak belgelerin kullanılıp kullanılmadığının - Kaynak belgelerin standart bir içeriğe (örneğin; sıra numarası, tarih, önceden belirlenmiş giriş kodları, varsayılan değerler, vb.) sahip olup olmadığının ve uygun şekilde doldurulup doldurulmadığının - Kaynak belge düzeninin ve belgede girilmesi istenen verilerin, veri giriş ekranlarının formatıyla ve içeriğiyle uyumlu olup olmadığının - Önemli işlemler için önceden numaralandırılmış (örneğin; seri ve sıra numarası) standart veri giriş formlarının kullanılıp kullanılmadığının - İş birimlerinden veri giriş/işleme birimine gelen bütün kaynak belgelerin imha edilme bilgilerini de içerecek şekilde kayıtlarının tutulup tutulmadığının - İş birimleri ile veri giriş/işleme birimi arasında, gönderilen/gelen/girilen kaynak belgelerin sayıları üzerinden bir kontrol/teyit mekanizması kurulup kurulmadığının - Kaynak belgelerin gerekli olan süreler boyunca saklanıp saklanmadığının - Mükerrerliği önlemek amacıyla; ✓ Her işleme/kaynak belgeye eşsiz ve sıralı numaralar atanıp atanmadığının ✓ İşlem yapılan kaynak belgelerin işaretlenip işaretlenmediğinin ✓ Genel toplamların kontrol edilip edilmediğinin belirlenmesi • İlgililerle görüşülerek, program uygulamaları gözlemlenerek ve BDDTA kullanılarak; - Örnekleme yöntemiyle belirlenen sistem kayıtlarının kaynak belgeler ile karşılaştırılması, prosedürlere uyulup uyulmadığının belirlenmesi - Kaynak belge numaralarındaki sıraya uymama, boşluk ve mükerrerlik durumlarının tespit edilmesi ve bunların ne tür işlemlere konu olduğunun incelenmesi

Konu	**UK-3 Hata Yönetimi** Hata yönetimi konusunda yeterli prosedürler var mı?
Kriter	Uygulama, sorunları net ve öz bir şekilde tanımlayan bir hata mesajı mekanizmasına sahip olmalı, hata kayıtları düzenli olarak gözden geçirilmeli ve hatalı girişlere yönelik düzeltici önlemler, uygulamada işlem safhasına geçilmeden önce alınmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Hatalı ve kural dışı veri girişlerinin kaydı tutuluyor mu?	• Uygulamanın geliştiricileri ve yöneticileri ile görüşülerek ve belge incelemesi yapılarak; girdi doğrulama kontrollerini geçemeyen işlemlere uygulanan hata ve istisna yönetimine ilişkin politika ve prosedürlerin değerlendirilmesi • Program uygulamaları gözlemlenerek; girdi doğrulamasını geçemeyen bütün hata türleri için hata mesajı üretilip üretilmediğinin incelenmesi • Program uygulamaları gözlemlenerek; verinin girdi kontrollerince reddedilmesi halinde veri öğelerinin askı dosyalarına yazılıp yazılmadığının belirlenmesi • Askı dosyaları incelenerek; hata türü, giriş tarihi-saati ve girişi yapan kullanıcı/personel bilgilerinin tutulup tutulmadığının belirlenmesi

2. Hatalı veya kural dışı durumlara ait kayıtlar düzenli olarak gözden geçiriliyor ve düzeltici önlemler alınıyor mu?	• Yöneticiler ile görüşülerek ve belge incelemesi yapılarak; hatalı işlem kayıtlarının düzenli olarak gözden geçirilmesine ilişkin prosedürlerin - var olup olmadığının - uygulanıp uygulanmadığının - düzeltici önlemlerin başlatılmasına ilişkin hususları içerip içermediğinin belirlenmesi • Belge incelemesi, mülakat ve gözlem yapılarak; tekrar işlem sürecine girmeden önce askı dosyalarındaki verinin gözden geçirilerek yetkili personel tarafından düzeltilmesini/tekrar girilmesini sağlayan prosedürlerin mevcut olup olmadığının ve uygulanıp uygulanmadığının belirlenmesi • Belge incelemesi ve mülakat yapılarak; hata oranları çok yüksek olduğunda ve/veya düzeltici işlemler yapıldığında durumun bir üst merciye iletilmesine ilişkin prosedürlerin var olup olmadığının değerlendirilmesi

Konu	**UK-4 Yetki Yönetimi** Veri girişine ilişkin yetkilendirmeler uygun şekilde gerçekleştiriliyor ve yönetiliyor mu?
Kriter	İşlemler için yetki seviyeleri oluşturulmalı ve düzgün yapılandırılmış kontroller aracılığıyla işlemlerin bunlara uygun şekilde yapılması sağlanmalıdır. Veri girişi için görevler ayrılığı ilkesi esas alınmalı, bu ilkenin uygulanamadığı durumlarda telafi edici kontroller kurulmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Veri girişine ilişkin yetki seviyeleri tanımlanmış mı?	• Belge incelemesi ve mülakat yoluyla; sistem tasarımının önceden onaylanmış yetki listelerine uygun şekilde gerçekleştirilip gerçekleştirilmediğinin belirlenmesi • Yetki listeleri incelenerek; bütün işlem türleri için uygun yetki seviyelerinin tanımlanıp tanımlanmadığının belirlenmesi • Ana işlem sınıfları için veri giriş, düzeltme, kabul, ret ve iptal işlemleri ile ilgili yetkilendirme kural ve süreçlerinin uygun şekilde tasarlanıp tasarlanmadığının ve dokümante edilip edilmediğinin incelenmesi
2. Veri giriş işlemlerinin yetki dâhilinde yapılmasını sağlayacak tedbirler alınmış mı?	• Veri tabanında bulunan yetkilendirme kayıtları/denetim kütükleri BDDTA yardımıyla incelenerek ve ilgililerle görüşülerek; yetkilendirme/yetki değişikliği işlemlerinin tanımlanmış olan yetkilendirme kuralları ile uyumlu olup olmadığının incelenmesi • İlgililerle görüşülerek ve BDDTA kullanılarak; ana dosyalarda yer alan parametrelere ilişkin tüm veri girişlerinin ve değişikliklerinin yetki dâhilinde, zamanında ve doğru yapıldığının ve yıl içinde bu parametrelerin yetkisiz kişilerce veya suiistimale yönelik olarak değiştirilmediğinin teyit edilmesi • Farklı dönemlere ait kaynak belgelerin üzerindeki imzalarla yetkilendirme listelerinin karşılaştırılması ve işlemlerin yetki dâhilinde gerçekleştirilip gerçekleştirilmediğinin incelenmesi • Uygulama test ortamında çalıştırılarak yetki seviyelerinin uygun şekilde uygulanıp uygulanmadığının gözlemlenmesi • İlgililerle görüşülerek, program uygulamaları gözlemlenerek ve BDDTA kullanılarak; - Veri girişlerinin tamamlanıp onaylanmasından sonra kilitlenip kilitlenmediğinin ve sonrasında geriye dönük işlem yapılıp yapılamadığının tespit edilmesi - Verilerin silinemediğinin teyit edilmesi - Düzeltmelerin, üzerine yazma yöntemiyle yapılamadığının teyit edilmesi

3. Görevler ayrılığı ilkesi gözetiliyor mu?	• Uygulamanın bir görevler ayrılığı tablosunun olup olmadığının belirlenmesi • Görevler ayrılığı tablosu, kullanıcı listesi ve kullanıcılara tanımlanan özel erişim ayrıcalıkları incelenerek; önemli görevler/iş fonksiyonları ve bu kapsamda izin verilen işlemler için yeterli ayrımın yapılıp yapılmadığının belirlenmesi (örneğin; veri girişini yapan personel ile belgeyi doğrulayan personelin aynı olmaması) • Bilgilerin doğru ve eksiksiz kaydedilmesinin sağlanması amacıyla "çift imza", "kontrol edildi parafı" gibi kontrol mekanizmalarının oluşturulup oluşturulmadığının belirlenmesi • Görevler ayrılığının uygulanamadığı durumlar için telafi edici kontrollerin var olup olmadığının incelenmesi (örneğin; bu nitelikteki işlemlerin kayıt altına alınması ve düzenli olarak gözden geçirilmesi)

İşlem	
Denetim Hedefi	Uygulamanın işlem döngüsü boyunca, verinin bütünlüğünü, geçerliliğini ve güvenilirliğini sağlayıp sağlamadığını değerlendirmek
Referans	♦ COBIT 2019 / DSS06.01 İş Süreçlerine Yerleştirilmiş Kontrol Faaliyetlerini Kurum Hedefleriyle Hizalayın ♦ COBIT 2019 / DSS06.02 Bilgilerin İşlenmesini Kontrol Edin ♦ COBIT 2019 / DSS06.04 Hataları ve İstisnaları Yönetin
Konu	**UK-5 İş Süreçlerine İlişkin Kural ve Gereksinimlere Uyum** İş süreçlerine ilişkin kurallar ve gereklilikler uygulama içerisine uygun şekilde yerleştirilmiş mi?
Kriter	Uygulama, işlemleri iş süreçlerine ilişkin kurallara ve gerekliliklere uygun şekilde/beklendiği gibi gerçekleştirmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Uygulama için hazırlanmış ve iş sürecini tanımlayan bir iş ve zaman çizelgesi var mı?	• İş ve zaman çizelgesi incelenerek aşağıdaki bilgileri içerip içermediğinin belirlenmesi: - Yapılması gereken işler ve iş öncelikleri - İş uygulamalarındaki sıra akışı - Onay/kontrol işlemleri - Ulaşılması gereken bilgi ortamı ve dosyalar - İşlem sonrası süreç, örneğin; yeniden mutabakat ve beklenenden farklı çıktıların gözden geçirilmesi • Örnek olarak seçilen iş süreçlerine ilişkin iş ve zaman çizelgeleri incelenerek; çizelgelerin iş kurallarına uygun olarak, doğru bir sırayı takip edecek ve doğru bir zamanda doğru bilgi dosyalarına erişecek şekilde tasarlanıp tasarlanmadığının tespit edilmesi
2. Uygulama iş süreçleri ile uyumlu şekilde çalışıyor mu?	• Örnek olarak seçilen önemli işlemler canlı sistemle/ortamla eşlenik bir test sistemi/ortamında yeniden gerçekleştirilerek; işlemlerin iş süreçlerine ve kurallarına uygun şekilde ve zamanında gerçekleşip gerçekleşmediğinin incelenmesi • Örnek olarak seçilen işlemlerin doğru hesaplanıp hesaplanmadığının tespiti amacıyla hesaplamaların uygulama dışında yeniden yapılması ve elde edilen sonuçların uygulama çıktılarıyla karşılaştırılması

	• Verilere ilişkin akışın istenildiği gibi doğru bir şekilde gerçekleştiğini test etmek amacıyla -gerekirse uzman desteği alınarak- örnek olarak seçilen işlemler üzerinde aşağıdaki testlerin uygulanması: - Enstantane (snapshot) - İz sürme (tracing) - Haritalandırma (mapping) • Kritik işlemler için oluşturulan akışın tasarlandığı gibi çalışıp çalışmadığının incelenmesi amacıyla -gerekirse uzman desteği alınarak- kod analizi yapılması

Konu	**UK-6 İşlem Kontrolleri** Uygulama kontrolleri, işlemlerin bütünlüğünü ve tamlığını sağlıyor mu?
Kriter	Uygulama işlem safhasındaki hataları doğru şekilde tespit etmeli ve tanımlamalıdır. İşlem esnasında yaşanan beklenmedik kesintilerde dahi verinin bütünlüğü korunmalıdır. İşleme hatalarının ele alınmasına, askı dosyalarının gözden geçirilmesine ve çözümüne ilişkin yeterli bir mekanizma bulunmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Uygulamada işlemlerin tam ve doğru olarak yapılmasını sağlamaya yönelik otomatik kontroller var mı?	• Uygulamanın geliştiricileri ve yöneticileri ile görüşülerek ve belge incelemesi yapılarak; aşağıda örnekleri verilen işlem kontrollerinden hangilerinin yazılıma entegre edilerek kullanıldığının belirlenmesi ve kullanılan kontrollerin işlevsellik ve tasarım yönünden değerlendirilmesi: - Düzen ve biçim kontrolü - Sıra ve mükerrerlik kontrolleri - Denklik kontrolleri - Kontrol toplamları ve özet toplamları - Hesaplanmış miktarlarda makullük kontrolü - Hesaplanmış miktarlarda limit kontrolü • Veri işlemenin eksiksiz/tam gerçekleştiğinden emin olmak için mutabakatlar ve diğer belgeler incelenerek girdi sayımlarının çıktı sayımlarıyla uyumlu olup olmadığının belirlenmesi • İşlemler süreç boyunca izlenerek, mutabakatların dosya toplamlarının eşleşip eşleşmediğini etkili bir şekilde belirleyip belirleyemediğinin ve eşleşmeme halinde durumun raporlanıp raporlanmadığının incelenmesi • Kontrol dosyalarının işlem sayılarını ve parasal değerleri kaydetmek için kullanılıp kullanılmadığının incelenmesi • Kritik işlemler için oluşturulan kontrollerin tasarlandığı gibi çalışıp çalışmadığının incelenmesi amacıyla -gerekirse uzman desteği alınarak- kod analizi yapılması • Otomatik kontrollerin olmaması durumunda amaca uygun telafi edici kontrollerin olup olmadığının belirlenmesi
2. İşlemleri yeniden başlatma prosedürleri tanımlanmış mı?	• Uygulamanın geliştiricileri ve yöneticileri ile görüşülerek ve belge incelemesi yapılarak; gerektiğinde verilerin yedeklenmesi ve dosya kurtarma işlemlerinin başlatılması ile ilgili tanımlanmış bir prosedürün olup olmadığının belirlenmesi • İncelenen dönemde, kontroller onaylandıktan sonra sürecin yeniden başlatılmak zorunda olduğu kayıtlı vakaların tespit edilmesi ve onaylanma sürecinin doğru bir şekilde işletilip işletilmediğinin incelenmesi

	• Veri işlemedeki beklenmeyen kesintiler sırasında verilerin bütünlüğünü otomatik olarak korumak için yardımcı programların kullanılıp kullanılmadığının incelenmesi
3. Hata ve beklenmedik durum raporları üretiliyor ve yönetim tarafından düzenli olarak gözden geçiriliyor mu?	• Hata ve beklenmedik durum raporlarının temin edilmesi ve bütün sorunların makul bir süre içinde açıklığa kavuşturulup kavuşturulmadığının ve düzeltme işlemlerinin yönetim tarafından onaylanıp onaylanmadığının belirlenmesi • İşlem verilerinin girişiyle ilgili işlevsel açıklamalar ve tasarım bilgileri incelenerek; doğrulama kontrollerinden geçemeyen işlemlerin askı dosyalarına kaydedilip kaydedilmediğinin belirlenmesi • Askı dosyalarının doğru ve tutarlı bir şekilde üretilip üretilmediğinin ve kullanıcıların bu işlemler hakkında bilgilendirilip bilgilendirilmediğinin incelenmesi • Örnek olarak seçilen işlemler incelenerek; doğrulama kontrollerinden geçemeyen işlemlerin kaydedildiği askı dosyalarında yalnızca son hataların yer alıp almadığının ve kontrollerden geçemeyen önceki hatalı işlemlerin uygun şekilde düzeltilip düzeltilmediğinin belirlenmesi • Muhasebede denklik sağlanması gereken işlemlerde, denkliğin sağlanamadığı durumları tanımlayan raporların oluşturulduğunun, gözden geçirildiğinin, onaylandığının ve uygun personele dağıtıldığının doğrulanması • Örnek olarak seçilen veri giriş işlemleri uygun analiz ve araştırma araçlarıyla incelenerek geçerli işlemlerin hatalı olarak belirlendiği veya hataların tespit edilemediği durumların olup olmadığının değerlendirilmesi

Çıktı	
Denetim Hedefi	Çıktı bilgisinin kullanımdan önce tam ve doğru olmasının sağlanıp sağlanamadığını ve uygun şekilde korunup korunmadığını değerlendirmek
Referans	♦ COBIT 2019 / DSS06.01 İş Süreçlerine Yerleştirilmiş Kontrol Faaliyetlerini Kurum Hedefleriyle Hizalayın ♦ COBIT 2019 / DSS06.06 Bilgi Varlıklarını Koruyun
Konu	**UK-7 Çıktı Kontrolleri** Uygulama çıktısının doğruluk ve tamlığını sağlayacak kontroller oluşturulmuş mu?
Kriter	Çıktı kontrolleri; uygulama çıktısının, son kullanıcı işlemi dâhil olmak üzere müteakip işlemlerde kullanımından önce doğruluk ve bütünlüğünün onaylanmasını, düzgün şekilde izlenmesini, uygunluk ve doğruluk açısından gözden geçirilmesini ve bütünlük ve doğruluk kontrollerinin etkili olmasını sağlayacak şekilde tasarlanmış olmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Çıktıların üretilmesine ilişkin bir prosedür var mı?	• Çıktıların üretilmesine yönelik prosedürlerin incelenmesi ve aşağıda yazılı hususları kapsayıp kapsamadığının belirlenmesi: - Üretilmesi istenen veya beklenen çıktıların bir listesi ✓ Ödeme emri, çek gibi mali nitelikli evraklar ✓ Elektronik dosya ve veriler ✓ Elektronik dosya veya verinin saklandığı araçlar/ortamlar ✓ Yazılı raporlar - Çıktıların yasal zorunluluk gereği veya kurumun inisiyatifi ile belirlenmiş formatı - Çıktıların kim tarafından ne zaman üretileceği ve kimlere dağıtılacağı

	- Tanımlanmış iş ve zaman çizelgesi - Sürecin yürütülmesine ilişkin sorumluluklar - Elde edilen çıktıların saklanması ve güvenliğinin sağlanması
2. Çıktı üzerinde uygunluk, tamlık ve doğruluk kontrolleri yapılıyor mu?	• Fiziksel çıktılar üzerinde yürütülen kontrollerin etkinliğinin, aşağıda örnekleri verilen incelemeler yapılarak değerlendirilmesi: - Üretilen fiziksel çıktıların beklenen çıktı listesiyle karşılaştırılması - Fiziksel çıktı ile elektronik ortamdaki çıktının aynı olup olmadığının incelenmesi • Eğer muhasebe programı üzerinde inceleme gerçekleştiriliyorsa; BDDTA kullanılarak alınmış tüm yevmiye kayıtlarından hareketle mali tabloların yeniden üretilmesi ve belgelerde yer alan mali tablolarla karşılaştırılarak bir farklılığın olup olmadığının tespit edilmesi • Son kullanıcı uygulamalarında yeniden kullanılan elektronik çıktıların bir listesi alınarak, yeniden kullanılmadan ve yeniden işlenmeden önce çıktıların tamlık ve doğruluk açısından test edilip edilmediğinin gözlem ve mülakat yoluyla incelenmesi • Örnek olarak seçilen elektronik çıktılara ilişkin sürecin izi sürülerek, diğer işlemler gerçekleştirilmeden önce çıktıların tamlık ve doğruluğunun teyit edilip edilmediğinin incelenmesi • Raporların yayınlanmasından önce, veri bütünlüğünün sağlanması amacıyla çıktı toplu kontrol toplamları ile girdi toplu kontrol toplamları arasında mutabakat sisteminin oluşturulup oluşturulmadığının belirlenmesi • Çıktılar üzerinde tamlık ve doğruluk testleri yeniden gerçekleştirilerek etkili olup olmadıklarının belirlenmesi • Çıktıların üretilmesinde denklik ve mutabakat mekanizmalarının -ilgili dokümanlarda öngörüldüğü şekilde- işletilip işletilmediğinin incelenmesi • Çıktıların; program adı veya numarası, başlık veya açıklama, kapsadığı işlem dönemi, kullanıcı adı ve konumu, hazırlandığı tarih ve saat ve güvenlik sınıflandırması bilgilerini içerip içermediğinin incelenmesi • Raporların dağıtımından önce hataların günlüğe kaydedilmesine ve çözümlenmesine ilişkin prosedürlerin tanımlanıp tanımlanmadığının incelenmesi • Örnek olarak seçilen çıktı raporları incelenerek; - Çıktının makullüğünün ve doğruluğunun değerlendirilmesi - Hataların raporlanıp raporlanmadığının ve merkezi olarak kaydının tutulup tutulmadığının belirlenmesi
3. Hata ve beklenmedik durum raporları üretiliyor ve düzenli olarak gözden geçiriliyor mu?	• Yönetimle görüşme yapılarak sistem/uygulama programlarının hatalı çıktılarının nasıl raporlandığının ve kontrol edildiğinin belirlenmesi • Örnekleme yoluyla seçilen hata raporları incelenerek, hataların nedenlerinin, bu hataların neticesinde yapılan işlemlerin ve bunların tekrarlanmaması için alınan önlemlerin tespit edilmesi

Konu	**UK-8 Çıktının Dağıtılması ve Saklanması** Çıktılar doğru alıcılara ulaştırılıyor ve uygun şekilde korunuyor mu?
Kriter	Çıktılar, geçerli gizlilik sınıflandırması çerçevesinde yönetilmeli, doğru alıcılara dağıtılmalı ve mevzuatta öngörülen süre boyunca güvenli şekilde saklanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Çıktılar gizlilik derecelerine göre sınıflandırılıyor mu?	• Çıktıların gizlilik derecelerine göre sınıflandırılmasına ilişkin yazılı prosedürlerin olup olmadığının incelenmesi • Örnek olarak seçilen çıktıların/raporların - Uygun gizlilik etiketleri taşıyıp taşımadığının - Gizlilik derecelerine uygun şekilde dağıtılıp dağıtılmadığının belirlenmesi
2. Çıktıların doğru yere/ kullanıcıya dağıtılması sağlanıyor mu?	• Uygulayıcılarla görüşme yapılması ve örnek olarak seçilen çıktıların dağıtımına ilişkin süreçlerin incelenmesi suretiyle; - Çıktıların doğru alıcılara ve zamanında ulaştırılıp ulaştırılmadığının belirlenmesi - Çıktılar ulaştırılması beklenen alıcılarına beklenen zamanda ulaşmadığında yapılan işlemlerin incelenmesi • Hassas çıktıların gereken hallerde özel erişim kontrollü çıktı araçlarına gönderilmesi için yazılı prosedürlerin olup olmadığının kontrol edilmesi • Hassas bilginin dağıtım yöntemlerinin gözden geçirilmesi ve önceden belirlenmiş erişim haklarının düzgün şekilde uygulanmasını sağlayan mekanizmaların varlığının doğrulanması
3. Çıktıların güvenli ve yasal gerekliliklere uygun şekilde saklanması sağlanıyor mu?	• Bütün kâğıt ve elektronik çıktıların arşivleme, muhafaza ve depolama işlemlerinin gizlilik derecelerine ve mevzuatta öngörülen sürelere uygunluğunun belge incelemesi ve yerinde tespit yöntemiyle incelenmesi • Bütün manyetik çıktıların fiziksel ve çevresel güvenliği sağlanmış ortamlarda muhafaza edilip edilmediğinin belirlenmesi

Uygulama Güvenliği	
Denetim Hedefi	Uygulama bilgisinin kötüye kullanıma karşı uygun şekilde korunup korunmadığını değerlendirmek
Referans	♦ Bilgi ve İletişim Güvenliği Rehberi / 3.2.1 Kimlik Doğrulama ♦ Bilgi ve İletişim Güvenliği Rehberi / 3.2.2 Oturum Yönetimi ♦ Bilgi ve İletişim Güvenliği Rehberi / 3.2.3 Yetkilendirme ♦ TS ISO/IEC 27002 / 9 Erişim Kontrolü ♦ COBIT 2019 / DSS05.04 Kullanıcı Kimliğini ve Mantıksal Erişimi Yönetin ♦ COBIT 2019 / DSS06.03 Rolleri, Sorumlulukları, Erişim Haklarını ve Yetki Düzeylerini Yönetin ♦ COBIT 2019 / DSS06.05 Bilgi Olayları İçin İzlenebilirlik ve Hesap Verilebilirliği Sağlayın
Konu	**UK-9 Kullanıcıların Yönetimi** Uygulamanın kullanıcıları uygun şekilde yönetiliyor mu?
Kriter	Uygulamanın kullanıcıları tanımlı prosedürler dâhilinde oluşturulmalı ve kaldırılmalı, yetkileri görev tanımlarına uygun şekilde belirlenerek yönetilmeli ve mantıksal erişimlerinin güvenliği sağlanmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Kullanıcıların oluşturulmasına ve kaldırılmasına ilişkin süreçler tanımlanmış mı ve uygulanıyor mu?	• Bakınız: BG-15 Erişim Haklarının ve Ayrıcalıkların Yönetimi / 1
2. Kullanıcıların yetkileri görev tanımlarına uygun şekilde veriliyor ve yönetiliyor mu?	• Belge incelemesi, mülakat ve program uygulamalarının gözlemlenmesi yöntemleri kullanılarak ve gerekli görüldüğünde uzman desteğinden yararlanılarak; - Kullanıcıların yetkilerinin kendi görev tanımlarına ve "mümkün olan en kısıtlı yetki" prensibine uygun şekilde tanımlanıp tanımlanmadığının - Kullanıcıların uygulama içerisinde yetkilerinin olmadığı sayfalara, menülere ve yönetim ara yüzlerine erişip erişemediklerinin - Erişim kontrolleri için belirlenen kuralların (yetkisi özellikle verilmediyse) kullanıcılar tarafından değiştirilmesinin mümkün olup olmadığının belirlenmesi • Kritik işlemler ve bu işlemleri gerçekleştirmeye yetkili olan personel incelenerek görevler ayrılığı ilkesinin uygulanıp uygulanmadığının ve karşılıklı kontrollerin (uygulayan, onaylayan ve yetkilendirenin aynı kişiler olamaması gibi) kurulup kurulmadığının değerlendirilmesi • Kullanıcıların yetkilerinin görev tanımlarına uygunluğunun düzenli olarak gözden geçirilip geçirilmediğinin belge incelemesi ve mülakat yoluyla tespit edilmesi • Görev yeri/tanımı değişen personel arasından örnekleme yöntemiyle belirlenenlerin yetkilerinin güncellenip güncellenmediğinin belge ve kayıt incelemesi yoluyla değerlendirilmesi
3. Kullanıcıların uygulamaya mantıksal erişimlerinin güvenliğini sağlamaya yönelik mekanizmalar oluşturulmuş mu?	• Bakınız: BG-15 Erişim Haklarının ve Ayrıcalıkların Yönetimi / 2-5

Konu	**UK-10 İzleme Mekanizmaları** Uygulamanın izleme mekanizmaları amacına uygun şekilde oluşturulmuş mu?
Kriter	Kritik işlemlere ilişkin düzeltme, iptal ve yetkilendirmeler kayıt altına alınmalı, bu kayıtlar uygun şekilde tutulmalı ve muhafaza edilmeli, olağandışı (şüpheli) faaliyetlerin takibi amacıyla düzenli olarak gözden geçirilmelidir.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Uygulamada bir denetim izi mekanizması oluşturulmuş mu?	• Bakınız: BG-15 Erişim Haklarının ve Ayrıcalıkların Yönetimi / 6 • Denetim izi kayıtları, diğer belgeler, planlar, politikalar ve prosedürler incelenerek; - İşlemlerin (özellikle düzeltmeler, iptaller ve yüksek tutarlı işlemlerin) gecikme olmaksızın ve ayrıntılı şekilde gözden geçirilmesine uygun bir kayıt alma mekanizmasının olup olmadığının - Gerçekleştirilen her işleme özgün birer tanımlama bilgisi atanıp atanmadığının belirlenmesi • Erişim hakları ve erişim kayıtları incelenerek; - Denetim izi dosyalarına sadece yetkili personelin erişiminin olduğunun doğrulanması - Denetim izi mekanizmasını hangi çalışanların devre dışı bırakabileceğinin ya da kayıtları silebileceğinin belirlenmesi - Denetim izi dosyalarının ayrıcalıklı kullanıcılar tarafından gerçekleştirilebilecek değişikliklere karşı korunup korunmadığının tespit edilmesi • Denetim izi kayıtları, gözden geçirme belgeleri ve diğer belgeler incelenerek (ve gerekli görüldüğünde uzman desteği ve BDDTA yardımıyla işlemler ve betikler üzerinden süreç adımları takip edilerek); - Etkin bir gözden geçirme faaliyeti yürütülüp yürütülmediğinin ve - Olağandışı (şüpheli) faaliyetlerin tespit edilip edilemediğinin belirlenmesi

Konu	**UK-11 Veri Transferi** Veri transferi güvenli şekilde yapılıyor mu?
Kriter	Veri transferinden sorumlu personele rehberlik yapacak detaylı teknik bilgileri içeren prosedürler tanımlanmalı ve veri transferlerinin tam ve doğru olarak yapılmasını sağlayan manuel veya otomatik kontroller oluşturulmalıdır.
Kontrol Sorusu	**İnceleme Yöntemi**
1. Veri transferine ilişkin tanımlanmış bir prosedür ve teknik detayları içeren yazılı dokümanlar var mı?	• Veri transferine ilişkin sürecin incelenerek aşağıdaki hususları kapsayıp kapsamadığının belirlenmesi: - Görevliler, yetki ve sorumlulukları - Transfer edilecek dosya ve mesajlar - Transfer sürecinin altyapısına ait bilgiler, örneğin; ilgili programlar - Güvenlik ve veri işlemeye ilişkin konular - Transfer şeması ve sıklığı - İletinin başlatılması, alınması ve saklanması - Bilgi ortamı araçlarıyla yapılan aktarımlara ilişkin prosedürler - Transfer yönetimi yönergesi

	- Transferlerin izlenmesini sağlayan ara yüzlerin oluşturulması - Transferin başarı ile tamamlandığına dair kontroller - Hatalarla baş etme prosedürleri - Yeniden başlatma mekanizması - Acil durum ve felaket sonrası durumla baş etme işlemleri - Günlük tutulması ve saklaması • Veri transfer sürecinin kontrolünde kullanılan donanım ve yazılımlara ait dokümanların elde edilmesi ve bunların yeterli olup olmadıklarının değerlendirilmesi • Uygulama programlarına veri gönderilmesi veya alınmasına ilişkin detay bilgilerin temin edilmesi: - Veri akış yönü - Transfer edilen bilgilerin türü - Transfer edilen işlemlerin yaklaşık hacmi veya değeri • Yönetimle görüşme yapılarak veri transfer alt yapısının beklendiği şekilde çalışmasına ilişkin riskleri öngörüp öngörmediğinin tespit edilmesi • Tüm belgelerin güncellendiğinin ve muhafaza edildiğinin belirlenmesi
2. Veri transferinin tam ve doğru olarak yapılmasını güvence altına alan otomatik veya manuel kontroller var mı?	• Bilişim sistemleri personeli ile görüşme yaparak ve dokümanları gözden geçirerek veri transferinin tam ve doğru olarak gerçekleşmesini sağlayacak otomatik ve manuel kontrollerin aşağıdaki hususları kapsayıp kapsamadığının belirlenmesi: - Transfer edilen dosyaların üstünde büyüklüğü ve parasal değerine ilişkin bilgilerin yer alması - Elektronik olarak hedef veya kaynak dosya büyüklüğünün karşılaştırılması - Transferde doğru prosedürün uygulandığının kontrol edilmesi - Mesaj veya raporlara ilişkin transferin başarıyla gerçekleşip gerçekleşmediğine ilişkin aşağıda örnekleri verilen otomatik kontrollerden ilgili olanların oluşturulması: ✓ Döngü\yankı kontrolü ✓ Fazlalık kontrolü ✓ Eşlik kontrolü ✓ Mükerrerlik kontrolü ✓ Eşitlik kontrolü ✓ Hata kodu ✓ Ardışık işlem (dizi) kontrolü - Hata raporlarının üretilmesi • Uygulanan mantıksal ve fiziksel erişimlerinin yeterliliğinin test edilmesi amacıyla veri transferi yapılan örnek işlemlerin seçilmesi ve yetkili kişiler tarafından yapılıp yapılmadığının belirlenmesi • Verilerin, uygulama bileşenleri arasında şifreli olarak (gizliliği korunarak) iletilip iletilmediğinin değerlendirilmesi