

Taslak

Kamu BT Denetimi Rehberi

İç Denetim Koordinasyon Kurulu

Ekim 2013

TASLAK

İçindekiler

Bilgi Teknolojileri Denetim Rehberi Hakkında.....	4
Giriş.....	4
Rehberin Yapısı ve Özellikleri	5
1. Bilgi Teknolojileri Denetimi Temel Kavramlar	7
1.1. Temel prensipler.....	7
1.2. BT denetiminin uygulama alanları.....	7
1.3. Mesleki etik kurallar	9
1.4. BT Denetimi Yetkinlik Modeli	11
1.5. Sertifikasyonlar.....	12
1.6. Uluslararası Standartlar ve Çerçevesler	14
2. BT DENETİM METODOLOJİSİ	15
2.1. BT Denetim Metodolojisine Giriş	15
2.2. Planlama	21
2.3. Yürütme.....	45
2.4. Raporlama ve İzleme	53
3. BT KURUM SEVİYESİ KONTROLLERİ VE YÖNETİŞİM SÜREÇLERİ DENETİMİ	59
3.1. KURUM SEVİYESİ KONTROLLER	60
3.2. BT YÖNETİŞİM SÜRECİ DENETİMİ	67
4. BİLGİ TEKNOLOJİLERİ YÖNETİM SÜREÇLERİ DENETİMİ	74
4.1. DEĞİŞİKLİK YÖNETİMİ	75
4.2. GÜVENLİK HİZMETLERİ YÖNETİMİ.....	93
4.3. YARDIM MASASI, OLAY VE PROBLEM YÖNETİMİ	116
4.4. BT OPERASYON VE YEDEKLEME YÖNETİMİ	134
4.5. SÜREKLİLİK YÖNETİMİ.....	143
4.6. BT ALTYAPI VE YAZILIM EDİNİM, KURULUM VE BAKIMI	158
4.7. BT HİZMET YÖNETİMİ	175
4.8. RİSK YÖNETİMİ	185
5. UYGULAMA KONTROLLERİNİN DENETİMİ	196
5.1. Uygulama kontrolleri.....	196

5.2. Uygulama kontrolleri – BT genel kontrolleri ilişkisi.....	200
6. BT ALTYAPI GENEL KONTROLLERİ.....	203
6.1. İŞLETİM SİSTEMLERİ	204
6.2. VERİTABANI SİSTEMLERİ.....	228

TASLAK

Bilgi Teknolojileri Denetim Rehberi Hakkında

Giriş

Bilgi teknolojileri (BT) ve iletişim alanındaki gelişmeler, özellikle de İnternet kullanımının yaygınlaşması ve bilgi toplumuna geçiş sürecindeki gereklilikler kamu sektörünü önemli şekilde etkilemektedir. Kamu kurum ve kuruluşları, teknolojideki söz konusu gelişmelere paralel olarak hızlı bir değişim sürecinden geçmektedir. Bu çerçevede hem diğer kurumlara hem de doğrudan vatandaşa verilen hizmetlerde özellikle son dönemde önemli ilerlemeler kaydedilmiştir.

BT dönüşüm süreci, hizmetlerin daha hızlı ve etkin bir şekilde verilmesine imkân vermekle birlikte, sistemlerin daha karmaşık bir yapıya bürünmesine yol açmış, bu da elektronik ortama alınan bilgilerin maruz kalabileceği riskler sebebiyle iç kontrol mekanizmalarının oluşturulması ve BT alanında etkin denetim faaliyetlerinin yürütülmesi ihtiyacını doğurmuştur. Tüm bunlara ek olarak bilgi güvenliği, BT ve iş sürekliliği, BT varlık yönetimi, mobil bilişim, bulut bilişim ve sosyal medya risk yönetimi gibi gündemde olan ve kamu kurumları için yüksek risk taşıyan konular BT denetimlerini daha da önemli hale getirmiştir.

Bu çerçevede, işlemlerini büyük ölçüde bilgi teknolojilerine dayalı olarak gerçekleştiren kamu kurumlarının, bilgi teknolojileri kullanımından kaynaklanan riskleri değerlendirebilmesi, bilgi teknolojilerine ilişkin iç kontrollerin etkinliği hakkında bir değerlendirmede bulunabilmesi ve ayrıca mali, performans ve uygunluk denetimlerinden daha anlamlı sonuçlar elde edebilmesi amacıyla BT denetim yöntemlerinden yararlanılmaktadır. En son 7 Şubat 2013 tarihinde değişikliğe uğramış olan “İç Denetçilerin Çalışma Usul ve Esasları Hakkında Yönetmelik” madde 7’de belirtildiği üzere, elektronik bilgi sistemleri ve e-Devlet hizmetlerinin yönetim ve sistem güvenilirliğinin gözden geçirilmesi de iç denetim alanlarından biridir.

İşbu Bilgi Teknolojileri Denetim Rehberi (Rehber), T.C. Maliye Bakanlığı İç Denetim Koordinasyon Kurulu’nun (İDKK) koordinasyonunda, 5018 sayılı Kamu Mali Yönetim ve Kontrol Kanunu’na uygun olarak, kamu idarelerinde Bilgi Teknolojileri Denetimi gerçekleştirilmesi sırasında izlenmesi ve uygulanması gereken prosedürler ve denetim adımları ile ilgili bir yöntem sunmaktadır. Rehber’in amacı, kamu kurum ve kuruluşlarında etkin Bilgi Teknolojileri Denetimleri gerçekleştirilebilmesine yardımcı olmaktır. Rehber, bilgi teknolojileri denetiminin planlama aşamasından, denetimin uygulanmasına ve sonuçların raporlanmasına kadar yapılması gerekenlere dair bir bakış açısı ve yöntem sunmaktadır.

Rehber’in hazırlanmasında, Türkiye’de BT denetimi alanında mevcut durumda yürürlükte bulunan düzenlemeler ve BT ile ilgili ülke ve dünya çapında kabul edilmiş çerçevelerden ve standartlardan yararlanılmış olup, kamu denetim ihtiyaçları ve BT denetim kapasitesi gözetilerek özellikle pratik ve uygulanabilir bir düzenleme yapılması gözetilmiştir.

Rehberin Yapısı ve Özellikleri

Rehberin yapısı

Denetim rehberi altı ana bölümden oluşmakta olup, ifade edilen bölümler denetçilerin ihtiyaçlarını modüler olarak sağlayacak şekilde tasarlanmıştır. Bu çerçevede;

- Bölüm 1’de; BT Denetimi Temel Kavramları konusunda bilgilendirici bir nitelik taşımaktadır. Bu bölümde BT denetimi ile ilgili temel prensipler, uygulama alanları, etik kurallar, kabul görmüş yetkinlikler, sertifikasyonlar ve yararlanılabilecek uluslararası standartlar ve çerçevelere değinilmektedir. Ayrıca bu bölüm altında BT denetiminin diğer denetim türleri ile olan ilişkisi ve bu tür denetimlerde BT denetiminin oynayabileceği rol hakkında bilgiler verilmektedir.
- Bölüm 2’de; BT Denetimi Metodolojisi’ne yer vermektedir. Bu bölümde öncelikle BT denetimini ilgilendiren kontrol tipleri ve bunların birbiriyle olan ilişkisine değinilmiştir. Sonrasında denetim öncesi gerçekleştirilmesi gereken çalışmalardan planlamaya, risk analizinden denetimin yürütülmesine ve raporlanmasına kadar kullanılabilecek yöntem ve araçlar hakkında bilgi verilmektedir.
- Bölüm 3’te; BT Yönetişim Süreçlerine ilişkin denetim yaklaşımı ele alınmakta, bu doğrultuda kurum seviyesi kontroller ile yönetişim kontrollerine ve bunlar ile ilgili denetim adımlarına yer verilmektedir.
- Bölüm 4’de; BT Yönetim Süreçlerine ilişkin denetim yaklaşımı ele alınmakta ve bu süreçlere ait BT genel kontrollerine ve ilgili denetim adımlarına yer verilmektedir.
- Bölüm 5’te; Uygulama Kontrollerine ilişkin detaylı bilgiler verilmekte ve söz konusu kontrollerin denetlenmesine ilişkin yöntemler üzerinde durulmaktadır.
- Bölüm 6’da; BT yönetim süreçleri kapsamında veya tek başına yürütülecek güvenlik denetimlerinde BT altyapısı seviyesinde değerlendirilmesi gereken BT genel kontrollerine ve bunlara ilişkin denetim adımlarına yer verilmektedir.

Rehberin özellikleri

Rehber, İDKK tarafından Eylül 2013’te yayınlanan “Kamu İç Denetim Rehberi” göz önünde bulundurularak hazırlanmış olup, özellikle söz konusu rehberde ele alınan iç denetim yaklaşımının ve ortak terminolojinin gözetilmesine azami özen gösterilmiştir. Buna paralel olarak Rehber, ağırlıklı olarak bilgi teknolojilerine özgü hususlara yoğunlaşmış olup, genel yaklaşımla ilgili tekrarlardan mümkün olduğunca kaçınılmıştır.

Rehberde uluslararası kabul görmüş risk tabanlı bir denetim yaklaşımı benimsenmiş olup, söz konusu yaklaşımda denetlenen kurumun bilgi teknolojilerinden kaynaklanan risk düzeyi dikkate alınarak BT denetim kapsamı belirlenmektedir. BT denetim kapsamı, BT Yönetişim Süreçleri, BT Yönetim Süreçleri ve BT Altyapısı olarak üç temel grupta ele alınmaktadır.

BT denetimlerinin önemli bir alanını oluşturan BT Yönetim Süreçleri, Rehber içerisinde uluslararası standart ve çerçevelerden faydalanılarak belirlenmiştir. Bu çerçevede özellikle ISACA (Information

Systems Audit and Control Association – Bilgi Sistemleri Denetim ve Kontrol Derneği) tarafından yayınlanan COBIT 4.1 ve COBIT 5 çerçevelerinden yararlanılmıştır. Bununla birlikte pratikte sıklıkla birlikte denetlenen süreçler bir arada gruplanarak denetçinin istifadesine sunulmuştur. Rehber içerisinde her bir sürecin ve alanın denetimi için aşağıdaki detaylara yer verilmiştir:

- Sürecin ve sürece ilişkin ana kontrol hedefinin tanımı
- Sürecin BT denetimi açısından önemi
- Süreçte yer alan temel kontroller
- Kontrollerin süreç içerisindeki akışına ilişkin örnek şema
- Sürece ilişkin risk ve kontrol eşleşmeleri
- Her bir kontrole ilişkin denetim adımları
- Ek kaynaklar

Belirtilen detaylar, her kurumda genel anlamda uygulanması mümkün olabilecek temel ve yaygın denetim adımlarını içermekle birlikte Rehber'deki yaklaşım, gerektiğinde ilave risk ve kontrollerin ele alınmasına, belirtilenlerden farklı denetim adımlarının ve tekniklerinin uygulanmasına ve ilave kaynaklara başvurulabilmesine imkân tanıyacak şekilde hazırlanmıştır. Böyle bir ihtiyaç duyulması halinde Rehber içerisinde ilgili yerlerde referans olarak belirtilen standartlara ve çerçevelere başvurulması mümkündür.

Rehberin kullanımı ile ilgili olarak aşağıdaki hususlara dikkat edilmesi önerilmektedir:

- BT denetimi birçok noktada denetçinin profesyonel yargısını, bilgi birikimini ve tecrübesini kullanmasını gerektirmektedir. Denetçinin, denetim hedefleri, yürürlükteki mevzuat, uygulanan uluslararası standartlar ve çerçeveler, denetlenenin ortamı ve şartlarına göre ve mesleki tecrübesi çerçevesinde oluşturduğu yargılara dayanarak denetim sürecini planlaması, yönetmesi ve sonlandırması beklenmektedir. Bu sebeplerden dolayı bu Rehber kullanılarak yürütülecek bilgi sistemleri denetimlerinin uygun düzeyde bir gözetim altında gerçekleştirilmesi, denetimlerin ihtiyaç ve hedeflere uygun olarak sonuçlanması adına önem taşımaktadır.
- Rehber, BT denetimine konu olabilecek alanlarla ilgili geniş bir perspektif sunmakla birlikte, kamunun mevcut BT denetimi kapasitesi göz önüne alınarak özellikle başlangıç ve üstü seviye hedef alınmış ve Rehber'in ilk planda uygulanabilir olmasına dikkat edilmiştir. Bu çerçevede, Rehber'in kullanılmasıyla kapsamdaki bilgi teknolojileri süreçleri ve faaliyetleri üzerinde genel bir değerlendirmeye ulaşılabilmekle birlikte, gerektiğinde daha kapsamlı bir güvence için ilgili bölümlerde belirtilen diğer kaynakların kullanılması ve denetim adımlarının denetim amacına uygun olarak detaylandırılması konusu, yetkin bir BT denetçisi tarafından değerlendirilmelidir.
- Rehberin etkin bir şekilde uygulanması için denetimi gerçekleştirecek denetçinin iç denetim tecrübesine sahip olmasının yanı sıra, temel düzeyde bir BT denetimi eğitimini de tamamlaması beklenmektedir. Rehberdeki daha ileri düzey konular için ileri düzey ve uygulamalı eğitimlerin ve ayrıca eğitim amaçlı pilot denetimlerin de gerçekleştirilmesi önerilir. Rehber bir denetim yöntemi sunmakta olup, Rehber'i kullanacak denetçiler ve okuyucuların almaları gereken eğitimleri ve denetimde saha tecrübesini tek başına ikame etme amacını taşımamaktadır. Rehberin etkin kullanımı için birinci bölümde de bahsi geçen yetkinliklere sahip olmak tavsiye edilmektedir.

1. Bilgi Teknolojileri Denetimi Temel Kavramlar

1.1. Temel prensipler

Bir kurumun hedeflerine ulaşması açısından, yararlanılan bilgi teknolojilerinin kurumun faaliyetlerini ne ölçüde destekleyebildiğinin ve ayrıca bilgi teknolojilerinden kaynaklanan risklerin iç kontrollerle ne derece kontrol altına alınabildiğinin anlaşılması önemlidir. Bu değerlendirmenin yapılması BT iç kontrol ortamının denetlenmesi ile mümkün olabilir. Özellikle düzenleyicilerden vatandaşa kadar çok geniş bir paydaş yelpazesine sahip olan kamu kurumlarında, BT iç kontrollerinin etkinliği konusundaki hassasiyet artış göstermekte ve bu da BT denetimine olan talebi arttırmaktadır.

BT denetimlerinin niteliği, zamanlaması ve kapsamı, belirlenen denetim hedefine göre değişmektedir. Denetim hedefi, mali süreçleri etkileyen BT kontrollerinin denetlenmesi, belirli bir konu hakkında mevzuata uygunluğun tespiti, bilgi güvenliği ile ilgili açıkların tespiti, kurumdaki bilgi sistemleri performansının değerlendirilmesi ya da diğer özel hususları değerlendirmek ile ilgili olabilir. Söz konusu hedefler doğrultusunda BT denetimleri tek başına gerçekleştirilebileceği gibi diğer denetim alanları ile beraber de yürütülebilir.

1.2. BT denetiminin uygulama alanları

1.2.1. Sistem denetimi

İDKK tarafından hazırlanan Kamu İç Denetimi Rehberi'ne göre sistem denetimi, denetlenen birimin faaliyetlerinin ve iç kontrol sisteminin; organizasyon yapısına katkı sağlayıcı bir yaklaşımla analiz edilmesi, eksikliklerinin tespit edilmesi, kalite ve uygunluğunun araştırılması, kaynakların ve uygulanan yöntemlerin yeterliliğinin ölçülmesi suretiyle değerlendirilmesidir.

Sistem denetiminde, denetlenen birimin faaliyetleri ve bir bütün olarak iç kontrol sistemi, aşağıdaki unsurlar ışığında değerlendirilir:

- Kamu kaynaklarının etkili, ekonomik ve verimli bir şekilde yönetilmesi,
- Kamu idarelerinin faaliyetlerinde kamu politikalarına ve tüm yasal düzenlemelere uyum göstermesi,
- Karar vericilere doğru ve zamanlı bilgi sağlanması için düzenli, zamanında ve güvenilir, rapor ve bilgi üretilmesi,
- Tüm karar ve işlemlerde usulsüzlük ve yolsuzlukların önüne geçilecek yapının kurulması,
- Kurum kaynaklarının kötüye kullanıma ve kayıplara karşı korunması ve israfın önüne geçilmesi.

Uygulamada iç kontrol sisteminin bir bütün olarak değerlendirilmesine yönelik gerçekleştirilen sistem denetimlerinde, BT denetimlerine sıklıkla yer verilmektedir. Bu husus, Rehber'in 2. bölümünde daha detaylı ele alındığı üzere, iç kontrol sistemini oluşturan kritik BT işlevselliklerinin, diğer bir deyişle süreç

akışları üzerinde bilgi teknolojilerine bağımlı olarak yürüyen kontrollerin sürekli ve tutarlı olarak çalışmasını destekleyen bir BT kontrol ortamına ihtiyaç duymasıyla açıklanır. Söz konusu BT kontrol ortamının etkin olmaması, sistem denetiminde incelenen süreç kontrolleri ile ilgili güvence alınmasına ilişkin farklı stratejilerin kullanılmasını gerektirebilir. Öte yandan BT kontrol ortamının etkin olarak değerlendirilmesi durumunda, buradan sağlanan güvence ile süreç kontrollerinde yürütülecek çalışmalarda ve harcanacak eforda tasarruf edilmesi mümkün olabilir. Bu çerçevede BT kontrollerinin denetlenmesi, iç kontrol sistemi üzerindeki denetim stratejisini etkileyen önemli bir faktördür.

1.2.2. Performans denetimi

İDKK tarafından hazırlanan Kamu İç Denetimi Rehberi'ne göre performans denetimi, yönetimin bütün kademelerinde gerçekleştirilen faaliyet ve işlemlerin planlanması, uygulanması ve kontrolü aşamalarındaki etkililiğin, ekonomikliğin ve verimliliğin değerlendirilmesidir.

BT denetimi çerçevesinde gerçekleştirilebilecek çalışmalar, öncelikle denetlenen kurumun BT yapısının anlaşılması ve BT sistemlerinin kurumun performans hedeflerinin karşılanması doğrultusundaki öneminin belirlenmesi hususunda katkı sağlayabilir.

Performans denetimlerinin içerdiği amaçlar çerçevesinde, bilgi teknolojilerine ilişkin planlama, yürütme ve kontrol faaliyetlerine ilişkin incelemelere de ihtiyaç duyulabilir. Özellikle bilgi teknolojileri hizmet seviyelerinin belirlenmesi ve bunların karşılanma durumları, BT planlama süreci, performans ölçümü ve BT risk yönetimi faaliyetleri bu çerçevede ilk akla gelen konulardır. Bu çerçevede ayrıca bilgi sistemlerindeki ve BT kontrollerindeki zayıflıklar ve eksiklikler tespit edilerek, bunların kurum performansını üzerindeki etkisi de değerlendirilebilir. BT yönetimi kontrolleri üzerinde gerçekleştirilecek bir değerlendirme ise, genel olarak değer üretimi konusuna odaklanarak performans denetiminin sonuçlarına katkı sağlayabilir.

1.2.3. Mali denetim

BT denetimleri, mali denetimleri desteklemek amacı ile de gerçekleştirilebilir. Buradaki amaç ve uygulama alanı, sistem denetimleriyle büyük oranda benzerlik içermektedir. Literatürde mali denetimlerle birlikte yürütülen iç kontrol sistemi denetimlerine genel olarak "bütünleşik denetim" adı verilmiştir. Bilgi teknolojilerine ilişkin kontroller, iç kontrol sisteminin önemli bir parçası olduğu için, söz konusu bütünleşik denetimlerde de BT kontrollerinin incelenmesi önemli bir yer tutar.

Mali denetimlerde özellikle muhasebe süreci başta olmak üzere mali denetim için kritiklik arz eden iş süreçlerine ait önemli BT uygulamaları ve BT bileşenleri denetlenmektedir. Mali denetimde kullanılan verilerin doğruluğu ve bütünlüğüne yönelik olarak gerçekleştirilen bu değerlendirmeler neticesinde, sistem denetimlerine benzer şekilde BT ortamından bir güvence sağlamak mümkün olabilir. Bu da denetim riskinin yeniden değerlendirilmesine ve mali denetimin niteliğini, zamanlamasını ve kapsamını etkiler.

1.2.4. Uygunluk denetimi

İDKK tarafından hazırlanan Kamu İç Denetimi Rehberi'ne göre uygunluk denetimi, kamu idarelerinin faaliyet ve işlemlerinin ilgili kanun, tüzük, yönetmelik ve diğer mevzuata uygunluğunun incelenmesidir.

Uygunluk denetimlerinde, ilgili mevzuat uyarınca BT kontrol ortamına ait belirli bir konunun denetlenmesi ya da sistem ve mali denetimlerde olduğu gibi ilgili iç kontrol sistemi ile ilgili bir güvence oluşturulmasına yönelik bir çalışma yürütülmesi mümkündür. Her iki durumda da BT denetimi için öngörülen yaklaşımdan istifade edilebilir. Ayrıca Bilgi Güvenliği Yönetim Sistemi (BGYS) gibi belirli standartlar uyarınca gerçekleştirilmesi gereken iç denetimler de bilgi teknolojileri denetimini içeren birer uygunluk denetimi olarak ele alınabilir.

1.2.5. Güvenlik denetimi

Bilgi teknolojileri denetimi, kurumun bilgi güvenliği kontrollerini değerlendirmek amacı ile de gerçekleştirilebilir. Bu çerçevede güvenlik denetimi, BT denetimlerinin belirli bir amaca özgü türlerinden biri olarak ele alınabilir. Güvenlik denetimleri; sistem, performans, uygunluk ya da mali denetimlere girdi sağlayabileceği gibi tek başına da kurumun bilgi teknolojileri altyapısı ve kontrol ortamının değerlendirilmesinde kullanılabilir.

Güvenlik denetimlerinde, kurumun bilgi güvenliği politikasından hareketle, kullanıcı ve yetkilendirme yönetimi, sistem güvenlik konfigürasyonlarının uygunluğu, denetim izlerinin oluşturulması ve takibi, güvenlik olaylarının yönetimi, vb alanlarda değerlendirme çalışmaları yürütülür. Çalışmalar sistemlere ilişkin veritabanı, işletim sistemi, ağ katmanı gibi teknik bileşenler üzerinde gerçekleştirildiği gibi, ayrıca bilgi güvenliği farkındalığı ve BT kullanıcılarının eğitilmesi gibi konuları da kapsar. Pratikte güvenlik denetimlerinde ele alınan konuların bir bölümü, sistem denetimi başta olmak üzere diğer denetim türlerinde de kapsam içerisinde değerlendirilmektedir.

1.3. Mesleki etik kurallar

Etik kurallar, bireylerin ve kuruluşların davranışlarını düzenleyen ilkeleri ve beklentileri belirtir. Risk yönetimi, kontrol ve yönetim konularında denetim ya da güvence çalışmalarının güven üzerine kurulu olmasından dolayı, BT denetçisinin de birincil görevi çalışmalarında etik kurallara uygun hareket etmektir. Bu konuda BT denetçisinin diğer denetçilerden herhangi bir farkı olmadığı belirtilmelidir.

İç denetçilerin uyması gereken etik kurallar, 5018 sayılı Kamu Mali Yönetim ve Kontrol Kanununun 67'inci maddesinin (k) bendinde İç Denetim Koordinasyon Kurulu'nca belirlenen hükme bağlanmıştır. Buna göre BT denetçisi mesleğini icra ederken dürüstlük, tarafsızlık, nesnellik, bağımsızlık, gizlilik, yetkinlik gibi etik kurallara uymalı ve bu kuralların uygulanmasını desteklemelidir.

Bilgi sistemleri denetçisi denetim faaliyetlerini gerçekleştirirken Başbakanlık tarafından yürütülen 14.09.2010 tarihinde 27699 sayılı Resmi Gazete'de yayınlanan Denetim Görevlilerinin Uyacakları

Mesleki Etik Davranış İlkeleri Hakkında Yönetmelik çerçevesinde belirtilen maddelerle uyumlu davranmalıdır. Bu yönetmelik dışında denetçi, Uluslararası İç Denetim Enstitüsü (IIA) tarafından oluşturulan Etik Kuralları ve ISACA tarafından oluşturulan Profesyonel Etik Kuralları'nı da dikkate almalıdır (The Institute of Internal Auditors, 2009), (ISACA, 2004). Bu kurallardan yola çıkarak, BT denetçisi aşağıda listelenen etik kurallara ve bağımsızlık ilkesine uygun hareket etmelidir:

- BT denetçisi tüm mesleki hayatı boyunca sorumluluk ve doğruluk duygusuyla hareket etmelidir.
- BT denetçisi, kanun dışı bir faaliyete bilerek veya isteyerek taraf olmamalı, hukukun ve mesleğin gerektirdiği özel durum açıklamalarını yapmalıdır.
- BT denetçisi, görev alanındaki sorunları ve konuları ele alma konusunda bağımsız ve tarafsız olmalıdır.
- BT denetçisi tutarlı olarak dürüst davranmalıdır. Bu, kendisine ve yaptığı denetime güven duyulmasını sağlamaktadır.
- BT denetçisi, değerlendirmelerini olumsuz etkileyebilecek veya bu şekilde algılanabilecek hiçbir faaliyet veya ilişki içerisine girmemeli, yalnızca elde ettiği kanıtlara dayalı sonuçları denetim standartlarına uygun olarak birleştirerek ve değerlendirerek doğru ve nesnel denetim raporları hazırlamalıdır.
- BT denetçisi, mesleki veya yasal zorunluluk olmadıkça, elde ettikleri bilgilerin değerinin korunmasına ve gizliliğine özen göstermeli, gereken onay ve yetkileri almadan denetlenen kurum hakkındaki bilgileri başkalarıyla paylaşmamalıdır.
- BT denetçisi, denetimi gerçekleştirebilecek bilgi ve beceriye sahip olmalıdır ve sadece görevin gerektirdiği bilgi, beceri ve tecrübeye sahip olduğu işleri üstlenmelidir. Bilgi sistemleri denetçisi sahip olduğu profesyonel yetkinlikleri sürekli geliştirmekle sorumludur.
- BT denetimi bir ekip çalışması halinde gerçekleştiriliyorsa BT denetçisi ekip üyelerinin profesyonel etik kurallarına uygun şekilde çalıştıklarından emin olmalıdır. BT denetçisi, denetim süresince karşılaştığı her sorunla profesyonel etik kurallarına ve denetim standartlarına uygun şekilde mücadele etmelidir.
- BT denetçisi çıkar çatışmalarından kaçınmalı, baskıcı, hakaret edici ve tehdit edici uygulamalarda bulunmamalıdır.
- Profesyonel etik kurallarına veya denetim standartlarına uymayan BT denetçisi hakkında disiplin işlemleri başlatılmalıdır.
- Uyulması gereken etik kurallar profesyonel denetçilerin taleplerine ve gelişmelere göre güncellenir. BT denetçisi etik kurallardaki değişiklikleri takip etmekle sorumludur.

Denetimde bağımsızlık ilkesi

BT denetçisi, denetimle ilgili tüm konularda, tutum ve davranışıyla denetlenenden bireysel ve kurumsal olarak bağımsız olmalıdır. Denetim ancak bu şekilde tarafsız şekilde tamamlanır. Bilgi sistemleri denetçisinin denetlenen alanda doğrudan kontrolü varsa veya denetlenen alanda doğrudan kontrolü olan kişilere rapor verme sorumluluğu varsa, denetçi bağımsızlığını kaybeder. Eğer BT denetçisi bir durumun veya ilişkinin bağımsızlığını etkilediğini fark ederse, mümkün olduğunca kısa sürede yöneticilerini bilgilendirmelidir.

BT denetçisinin bağımsızlık şartını sağlamadan denetime devam ettiği durumlar olması halinde, bu durumlar yönetime açıklanmalı ve raporlanmalıdır. Denetim alanından bağımsız olunup olunmadığı

hususunu, bilgi güvenliği denetçisi, yönetim veya denetim komitesi tarafından belirli aralıklarla kontrol edilmelidir. Bu kontrollerde şahsi ilişkiler, mali kazançlar, öncelikli iş görevleri ve sorumlulukları dikkate alınmalıdır (ISACA, 2004), (ISACA, 2008).

1.4. BT Denetimi Yetkinlik Modeli

BT denetimi konusunda iç denetime ilişkin genel yetkinliklere büyük ölçüde ihtiyaç duyulmakla birlikte, bir takım ilave yetkinliklerin de gerektiği şüphesizdir. Bunların başında, BT denetimine özgü teknik yetkinlikler gelmektedir. Teknik yetkinlikler ağırlıklı olarak bilgi teknolojileri süreçleri ve kontrollerine ilişkin teknik bilgiler ve bunlar üzerinde gerçekleştirilebilecek denetim yöntemleri ile ilgilidir. Ayrıca BT denetçisinin denetlenen kuruma ve iş süreçlerine ilişkin riskler ve kontrollerle ilgili bir anlayış geliştirmiş olması da kritiktir.

BT denetçisi için teknik yetkinlik tek başına yeterli değildir. Özellikle bilgi teknolojileri gibi gelişmekte olan ve henüz denetim kapasitesinin yüksek olmadığı bir alanda, ikna kabiliyeti, mülakatlar/görüşmeler gerçekleştirme, insanlarla iyi ilişkiler kurma ve sunum yapma gibi becerilere de yoğun olarak ihtiyaç duyulmaktadır. Uygulamada bu becerilerin teknik yetkinlikler kadar önemli olduğu görülmektedir.

BT denetçisinin denetimle ilgili görevi ve sorumluluklarına bağlı olarak ihtiyaç duyacağı bilgi ve beceriler zaman içerisinde değişmektedir. Dolayısıyla ilgili yetkinliklerin sürdürülmesi ve yenilerinin kazanılması için sürekli eğitim yaklaşımının takip edilmesi önemlidir. BT denetimi ile ilgili birçok sertifika programı sürekli eğitim kavramını zorunlu kılmaktadır.

Ekip olarak yürütülen BT denetimlerinde bütün ekip üyelerinin gerçekleştirecekleri çalışma için uygun seviyelerde yetkinliklere sahip olması, ekip üyeleri arasında görev dağılımı yapılırken her denetim alanı için gerekli profesyonel ve teknik bilgi ve beceriye sahip olan BT denetçisinin görevlendirilmesine özen gösterilmelidir.

Aşağıda BT denetimine ilişkin teknik yetkinliklere ve daha sonra tüm iç denetçiler için anlamlı olan teknik olmayan yetkinliklere yer verilmiştir.

1.4.1. Teknik Yetkinlikler

X ISACA kurumunun bilgi sistemleri denetçileri için düzenlediği CISA sertifikasyon sınavında da kapsandığı şekilde, bilgi sistemleri denetimleri gerçekleştirecek kişilerin aşağıdaki konularda teknik yetkinliklere sahip olması beklenmektedir.

- Bilgi Sistemleri Denetimi Süreci: Kurum bilgi sistemlerinin korunması ve kontrol altında tutulması için BT denetim standartları ile uyumlu bir denetim hizmetinin sağlanması.
- Bilgi Sistemlerinin Yönetimi ve Yönetişimi: Kurumun hedeflerine ulaşması ve kurum stratejisinin desteklenmesi için gerekli liderlik, kurumsal yapı ve süreçlerin mevcut olduğunun güvencesinin sağlanması.

- Bilgi Sistemlerinin Edinimi, Geliştirilmesi ve Kurulması: Edinim, geliştirme, test etme ve kurulma yöntemlerinin kurum stratejileri ve hedefleri ile uyumlu olduğunun güvencesinin sağlanması.
- Bilgi Sistemlerinin İşletimi, Bakımı ve Desteklenmesi: Bilgi sistemleri operasyonlarının, bakım ve destek süreçlerinin, kurum stratejileri ve hedefleri ile uyumlu olduğunun güvencesinin sağlanması
- Bilgi Varlıklarının Korunması: Kurumun güvenlik politikalarının, standartlarının ve prosedürlerinin bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini (kullanılabilirliğini) koruduğunun sağladığının güvencesinin verilmesi.

1.4.2. Teknik Olmayan Yetkinlikler

Bilgi sistemleri denetçisinden beklenen teknik olmayan yetkinlikler IIA'nın İç Denetçi Yetkinlik Çerçevesi modelinde aşağıdaki şekilde belirlenmiştir (The Institute of Internal Auditors, 2010).

- Etki (nüfuz) ve iletişim
 - Nüfuzunu etkili kullanma ve geliştirme
 - Açık ve ikna edici mesajlar vererek ve aktif dinleyerek, etkin bir şekilde iletişim kurma
 - Liderlik ve ekip çalışması
 - Kurumsal politika ve prosedürleri etkin bir şekilde uygular
 - İşe alma, seçme ve personel elde tutma politikalarını etkin olarak kullanır
 - Etkin olarak plan yapar, öncelikleri belirler ve ekibin geri kalanının performansını yönetir
 - Ekibe ve kuruma bağlılığın oluşması için teşvik eder ve yön gösterir
 - Ortak hedefler doğrultusunda ilişkiler kurar ve beraber çalışır
 - İşbirliği ile etkin bir biçimde çalışır
 - Ortak hedefler doğrultusunda ekip sinerjisi oluşturulur
- Değişiklik yönetimi
 - Değişime ve yeniliğe açıktır
- Anlaşmazlık çözümü
 - Anlaşmazlıkları müzakereler ile etkin olarak yönetir ve çözümler

1.5. Sertifikasyonlar

BT denetçilerinin alabileceği uluslararası kabul gören bazı sertifikasyonlar ve detaylarına aşağıda yer verilmektedir:

Uluslararası Sertifikalı Bilgi Sistemleri Denetçisi (Certified Information Systems Auditor):

BT denetimi konusunda uzmanlığın en önemli göstergelerinden biri olan CISA sertifikası, ISACA tarafından belirli koşulları sağlayan denetçilere verilmektedir. Bu sertifika ile bireyler, bilgi sistemlerinin denetim süreci, yönetimi ve yönetişimi, edinimi, geliştirilmesi ve kurulması, işletimi bakım ve

desteklenmesi ile bilgi varlıklarının korunması gibi konularda uluslararası düzeyde tanınırlar. Söz konusu konular ISACA'nın tanımladığı BT yetkinlik modeliyle birebir örtüşmektedir.

Sertifikalı Risk ve Bilgi Sistemleri Kontrolleri Uzmanı (Certified in Risk and Information Systems Control):

Risk tanımlama, risk değerlendirme, risk yanıtlama, risk izleme, bilgi sistemleri kontrol tasarımı ve kontrolü gibi konularda tecrübesi olan BT profesyonelleri için tasarlanan bu sertifika ISACA tarafından verilmektedir (ISACA, 2013) .

Sertifikalı İç Denetçi (Certified Internal Auditor):

İç denetçiler için uluslararası geçerliliği olan en önemli sertifikadır. Bireylerin iç denetim alanında mesleki profesyonelliklerini gösterebildikleri bir ölçüt olan sertifika, Uluslararası İç Denetim Enstitüsü(IIA) tarafından verilmektedir. CIA sertifikasına sahip olan bireyler, iç denetim biriminin yönetim, risk ve kontrol konularındaki rolü, iç denetim görevinin yürütülmesi, iş analizi ve bilgi teknolojisi, stratejik yönetim, müzakere ve örgütsel davranış gibi iş yönetim becerileri konularında uluslar arası düzeyde tanınırlar (The Institute of Internal Auditors, 2013).

Sertifikalı Bilgi Sistemleri Güvenlik Uzmanı (Certified Information Systems Security Professional):

CISSP sertifikası kimlik tanıma, saldırı tespitleri, yazılım geliştirme güvenliği, iş sürekliliği ve felaket kurtarma planları, şifreleme, bilgi güvenliği ve risk yönetimi, bilgisayar suçları, yönetsel sorumluluklar gibi konulara yönelik olarak bağımsız bir kuruluş olan Uluslararası Bilgi Sistemleri Güvenliği Sertifikasyon Konsorsiyumu (ISC) tarafından verilmektedir. CISSP, en önemli uluslararası bilgi güvenliği sertifikalarındandır.

Sertifikalı Bilgi Gizliliği Uzmanı (Certified Information Privacy Professional):

CIPP sertifikası gizli bilginin toplanması ve kullanılması, kurum yazılımlarının yüklenmesi veya kaldırılması gizlilik kuralları, sistem ve ağ donanımının korunması gibi konulara yönelik olarak geliştirilen ilk küresel gizlilik sertifikasıdır. CIPP sertifikası Uluslararası Gizlilik Uzmanları Birliği (IAPP) tarafından verilmektedir. Bu sertifika ile bireyler BT ürünlerinin ve servislerinin geliştirilmesi, test edilmesi, canlı ortama geçirilmesi ve denetlenmesi sırasında kurum verisinin güvenliliği ve gizli tutulması konusunda bir anlayışa sahip olurlar (IAPP, 2013).

Sertifikalı Bilgi Güvenliği Yöneticisi (Certified Information Security Manager):

CISM sertifikası Bilgi ISACA tarafından verilmektedir. CISM sertifikasına sahip kişiler bilgi güvenliği yönetimi, risk yönetimi, bilgi güvenliği program geliştirme, bilgi güvenliği program yönetimi ve olay yönetimi konularında bilgi ve tecrübe sahibidirler.

Küresel Bilgi Güvencesi Sertifikası (Global Information Assurance Certification):

GIAC bilgi güvenliği çalışanlarının yeteneklerini tescillemek adına kurulmuş bir organizasyondur. Bu doğrultuda, bilgi güvenliği çalışanları; güvenlik yönetimi, adli bilişim, yönetim, denetim, yazılım güvenliği, hukuk ve güvenlik uzmanlığı konularında sertifikalar vermektedir.

Kurumsal BT Yönetişim Sertifikası (Certified in the Governance of Enterprise IT):

CGEIT sertifikası ISACA tarafından verilmektedir. CGEIT kurum BT yönetişimi çerçevesi, stratejik yönetim, fayda gerçekleştirme, risk optimizasyonu, kaynak optimizasyonu gibi konulara yönelik olarak geliştirilen bir sertifikadır.

Risk Yönetimi Güvence Sertifikası (Certification in Risk Management Assurance)

CRMA sertifikası IIA tarafından verilmektedir. CRMA risk güvencesi, yönetim süreçleri, kalite güvence, ya da kontrol öz değerlendirme konularında sorumluluğu veya tecrübesi olan iç denetçiler ve risk yönetimi uzmanları için tasarlanmıştır (The Institute of Internal Auditors, 2013).

1.6. Uluslararası Standartlar ve Çerçevesler

Rehber hazırlanırken gerekli noktalardan aşağıdaki çerçeve, standart ve referanslardan faydalanılmış ve ilgili bölümlerde kaynak olarak gösterilmiştir. Söz konusu kaynaklar bir BT denetçisi için gerektiğinde başvurulmak üzere kullanılabilir ilave kaynaklar için önemli bir başlangıç noktası teşkil etmektedir.

- COBIT 5 (ISACA, 2012)
- COBIT 4.1 (ISACA, 2007)
- IT Assurance Guide Using COBIT 4.1 (IT Governance Institute, 2007)
- ITAF (ISACA, 2008)
- ITAF 2nd Edition (ISACA, 2013)
- ISACA Denetim Kılavuzları
- The Institute of Internal Auditors – Guide to the Assessment of IT Risk (GAIT)
- The Institute of Internal Auditors – Global Technology Audit Guides (GTAG)
- The Institute of Internal Auditors – Uygulama Kılavuzları
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) – Enterprise Risk Management
- ISO 2700x ailesi
- Tübitak – Bilgem Kılavuzları
- IT Infrastructure Library v3 (UK Cabinet Office, 2011)
- ISO 22301 (International Standards Organization, 2012)

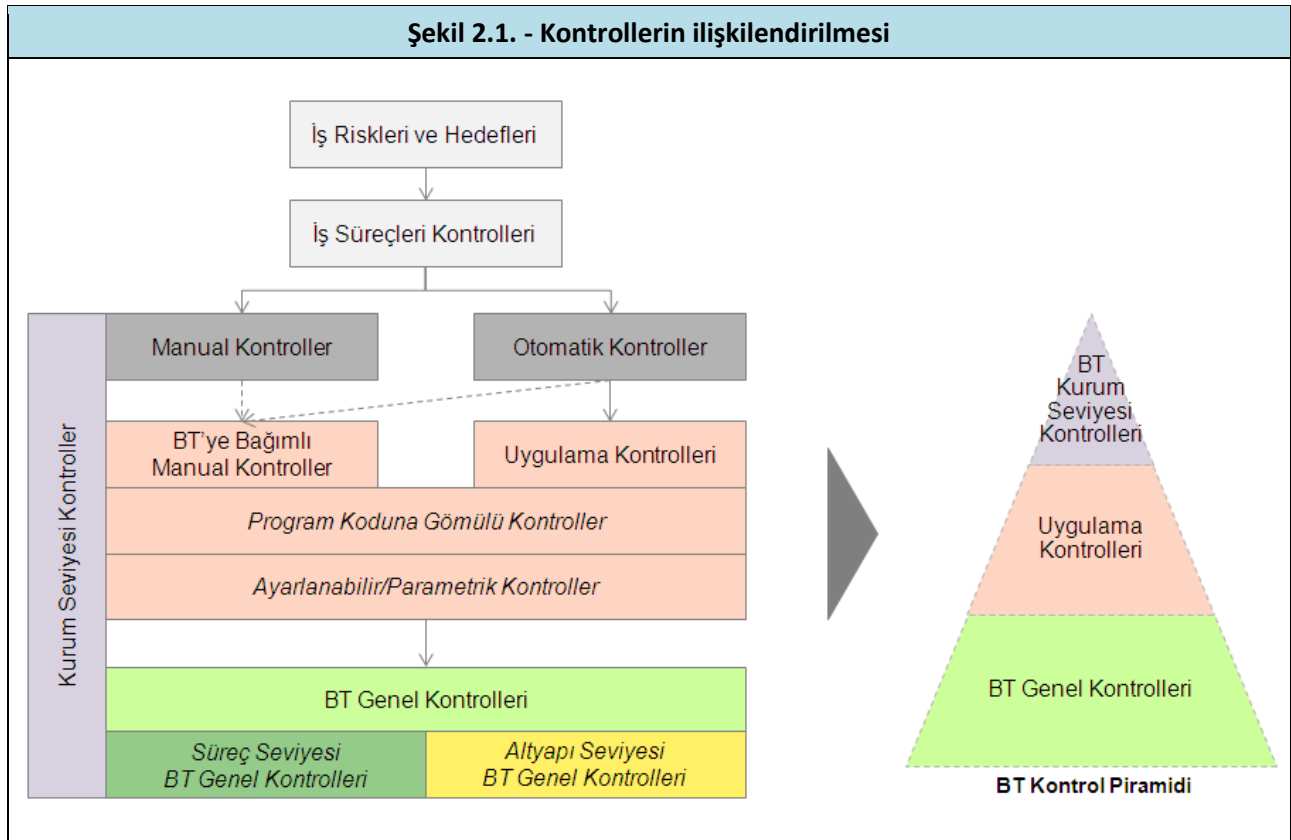
2. BT DENETİM METODOLOJİSİ

2.1. BT Denetim Metodolojisine Giriş

2.1.1. Kontrollere ilişkin ön bilgi

Rehber’de açıklanan BT denetim metodolojisinin doğru anlaşılabilmesi açısından, öncelikle iç kontrol sistemi içerisinde yer alan değişik kontrol türlerinin hatırlanmasında ve özellikle BT ile ilgili kontrollerin konumlandırılmasının yapılmasında yarar görülmektedir.

İç kontrol sistemi içerisinde yer alan farklı kontrol türlerine ve bunların birbiriyle olan ilişkilerine ait şekle aşağıda yer verilmektedir:



Şekilde görüldüğü üzere iç kontrol sisteminin iş risklerini ve hedeflerini karşılayabilmesi açısından, iki ana kontrol grubu (manual ve otomatik kontroller) ile tüm kontrol yapısını destekleyen kurum seviyesi kontroller grubunun varlığı söz konusudur. Bu yapı içerisinde otomatik kontroller ve BT genel kontrolleri,

bilgi teknolojilerine bağımlı olarak çalıştıklarından doğrudan BT denetimi konusunu oluştururlar. Ayrıca bilgi teknolojilerine ilişkin kurum seviyesi kontroller de BT denetimi içerisinde ele alınır.

BT denetimi içerisinde ele alınan kontrol türlerine ilişkin açıklamalara aşağıdaki bölümlerde yer verilmektedir.

BT Kurum Seviyesi Kontrolleri

Kurum seviyesi kontroller, genel tanımı itibariyle kurum yönetiminin yönergelerinin ve talimatlarının eksiksiz uygulandığına dair makul bir güvence sağlanması için kuruma ve personelin tümüne yaygın şekilde tasarlanmış olan iç kontrollerdir. BT kurum seviyesi kontrolleri de söz konusu alanlarda bilgi teknolojileri ile ilgili üst seviye kontrolleri ifade etmekle birlikte, aynı zamanda BT yönetimi ile ilgili hususlara da değinir.

BT yönetimi kavramı literatürde BT organizasyon yapıları, sorumluluklar, liderlik, BT yatırım ve yönlendirmesiyle ilgili karar verme hakkı ve BT ile iş stratejilerinin uyumlaştırılması gibi bir dizi farklı konu ile ilişkilendirilmiştir. COBIT çerçevesinde BT yönetimi, kurumun amaçlarının bir uzlaşma çerçevesinde belirlenebilmesi için paydaş ihtiyaçlarının, koşulların ve alternatiflerin değerlendirilmesi, önceliklendirme ve karar verme mekanizmaları sayesinde kuruma yön verilmesi ve nihayetinde kararlaştırılan yön ve amaçlara uyumun ve performansın izlenmesi unsurlarını kapsamaktadır. Bu niteliği ile konuya ilişkin kontroller de yukarıdaki şekilde belirtilen BT kontrol piramidinin en tepe noktasını oluşturmaktadır.

COBIT çerçevesi, özellikle COBIT 5 versiyonu ile birlikte, BT yönetim ve yönetim süreçleri ile ilgili net bir ayrıma gitmiştir. Bu husus BT denetçisinin kontrollerin niteliğini doğru algılayabilmesi açısından önem arz etmektedir. Bu çerçevede BT yönetimi, yukarıda da belirtildiği üzere genel anlamda kurumu yönlendiren bir katman olarak düşünülebilir. BT yönetimi ise kurumun amaçlarına ulaşabilmesi için yönetim organları tarafından belirlenen yönün takip edilebilmesini sağlayan aktivitelerin planlanması, geliştirilmesi, işletilmesi ve izlenmesi faaliyetlerini içerir. Bu yönüyle BT yönetimine ilişkin kontroller aşağıda görüleceği üzere ağırlıklı olarak BT genel kontroller grubunda değerlendirilmektedir.

Otomatik Kontroller

Otomatik kontroller, bilgi sistemlerinin kendilerinden beklenen faaliyetleri doğru ve tam olarak yerine getirmesi için sahip olmaları gereken işlevsellikleri içermektedir. “Kritik BT işlevselliği” olarak da adlandırılan bu işlevsellikler, hesaplama, limit kontrolleri, onay yetkileri ve raporlama gibi, iş risklerini doğrudan etkileyebilen ve denetçinin ilgi alanına giren konuları içermektedir. İç kontrol sisteminde iş hedeflerine ulaşılmasını ve iş risklerinin karşılanmasını sağlayan kritik BT işlevselliği, uygulama kontrolleri ve BT’ye bağımlı manual kontroller yardımıyla sağlanır.

- *Uygulama kontrolleri*

Uygulama kontrolleri, kritik BT işlevselliğinin yerine getirilmesini sağlayan ve kurumun bilgi sistemleri tarafından otomatik olarak yerine getirilen kontrol prosedürlerini içermektedir. Uygulama kontrolleri kabaca beş grup olarak ele alınmaktadır:

- Kaynak Veri Hazırlığı ve Yetkilendirme: Uygulama veri girişinde kaynak belge kontrolleri, veri giriş yetkileri, vb.
- Kaynak Verilerin Toplanması ve Girilmesi: Kaynak belgelerin zamanlılığı, tamlığı ve doğruluğu, veri giriş yetkileri, veri girişi hata takibi ve düzeltmeleri, vb.
- Doğruluk, Tamlık ve Orijinallik Kontrolleri: Kaynak veri girişi sırasında giriş, düzeltme ve raporlamalar, veri girişine ait görevler ayrılığı, vb.
- Veri İşleme Bütünlüğü ve Doğrulaması: Veri işlem bütünlüğünün sağlanması, işlemlere ilişkin denetim izlerinin oluşturulması, hata kontrolleri, vb.
- Çıktı Kontrolü, Mutabakatı ve Hata Yönetimi: Çıktıların kontrolü, çıktı transfer kontrolleri, çıktıların saklanması, vb.

Uygulama kontrolleri, ilgili BT uygulamasının program koduna gömülmüş olabilir. Bu durumda kontrolün işleyişine ilişkin değişiklikler ancak program kodunda yapılabilecek değişiklikler ile mümkün olabilir. Bu da genelde değişiklik yönetimi sürecinin bir konusudur. Bazı durumlarda ise uygulama kontrollerine ilişkin unsurlar, program kodunda bir değişiklik yapmaksızın, parametrik olarak ayarlanabilir. Bu durumda da ilgili parametrelere erişim yetkileri kritik bir hal alır.

Uygulama kontrollerinin nasıl çalıştığının anlaşılması ve denetlenmesi çoğu kez bilgi teknolojilerine ilişkin detaylar içerebildiğinden, pratikte uygulama kontrolleri genelde iç denetçiler ve BT denetçileri tarafından beraber ele alınmaktadır.

- *BT'ye bağımlı manual kontroller*

BT'ye bağımlı manual kontroller, hem manual hem de otomatik unsurları beraber taşıyan kontrollerdir. Bu konuda sıklıkla verilen örneklerden biri, bilgi sistemi tarafından hazırlanan bir kontrol raporunun ilgili yönetici tarafından elle gözden geçirilerek onaylanmasına ilişkindir. Örnekte kontrol raporunun hazırlanması, bilgi sistemleri tarafından otomatik olarak gerçekleştirildiği için, raporun tamlığı ve doğruluğu kritik BT işlevselliğinin tam ve doğru çalışmasına bağlıdır. Dolayısıyla kontrolün bu unsuru bir uygulama kontrolü gibi ele alınır. Öte yandan yöneticinin raporu kontrol etmesi ve onaylaması bilgi sistemlerine bağlı olmadan yürütüldüğü için kontrolün bu unsuru bir manual kontrol gibi değerlendirilir. Denetimde her iki unsur da kendi metodolojileri çerçevesinde ayrı ayrı değerlendirilir. Bu çerçevede BT'ye bağımlı manual kontrollerin otomatik unsurları, uygulama kontrollerine benzer şekilde ele alınmaktadır. Rehber'de genel olarak uygulama kontrolü kavramından bahsedilirken BT'ye bağımlı manual kontrollerin bu unsuru da kastedilmektedir.

BT Genel Kontrolleri

Rehber'in de önemli bir bölümünü oluşturan BT genel kontrolleri, bilgi teknolojilerinden beklenen kritik işlevselliklerin sürekli ve düzgün çalışmasını destekleyecek prosedürleri içermektedir. BT genel kontrolleri literatürde en dar anlamıyla aşağıdaki unsurları kapsamaktadır (COSO, 1992; ITGI, 2006):

- Uygulama sistemlerinin geliştirilmesi ve bakımına ilişkin kontroller
- Sistem yazılımı kontrolleri
- Erişim güvenliği kontrolleri
- Veri merkezi operasyonlarına ilişkin kontroller

Söz konusu minimum kapsam birçok denetim hedefi için yeterli olabilmekle birlikte, BT genel kontrolleri pratikte daha geniş bir alanda değerlendirilmektedir. Bu çerçevede BT genel kontrolleri, BT yönetim süreçleri ile ilişkili tüm kontrolleri ifade etmektedir. Kurumun amaçlarına ulaşabilmesi için belirlenen yönün takip edilebilmesini sağlayan tüm BT aktivitelerinin planlanması, geliştirilmesi, işletilmesi ve izlenmesine ilişkin faaliyetler, BT genel kontrolleri kapsamında değerlendirilmektedir.

BT genel kontrollerinin BT denetim metodolojisi açısından en önemli özelliklerinden biri, bilgi teknolojilerinden beklenen kritik işlevselliklerin ya da uygulama kontrollerinin sürekli ve düzgün çalışmasını desteklemeleridir. Diğer bir deyişle, denetlenen bir uygulama kontrolünün bilgi sistemi üzerinde sürekli ve düzgün çalışabilmesi, BT genel kontrollerinin etkinliğine bağlıdır. Uygulama kontrolleri ise Şekil 2.1'de de belirtildiği üzere, iç kontrol sisteminin önemli unsurlarından biri olmasından dolayı, BT genel kontrolleri doğrudan ve dolaylı olarak iç kontrol sistemi üzerinde belirleyici bir niteliğe sahiptir. Bu nedenle BT genel kontrollerinin “yaygın” (pervasive) (ITGI, 2006) bir niteliğe sahip olduğu belirtilir.

BT genel kontrollerinin uygulama kontrollerinin çalışmasını destekleyebilmesi hususu, denetim stratejisinin belirlenmesi açısından oldukça önemlidir. Teoride, uygulama kontrolünün kendinden beklenen işlevselliği yerine getirebilme durumunun, BT genel kontrollerinin bir bütün olarak etkin olması durumunda hiç değişmeden devam ettiği kabul edilir. Böyle bir durumda BT kontrol ortamı, uygulama kontrolünün sürekli ve düzgün çalışmasını sağlayacak etkinliğe sahiptir. Dolayısıyla uygulama kontrollerinin denetimi için gerçekleştirilecek prosedürlerin niteliği, zamanlaması ve kapsamında değişikliğe gidilmesi ve pratikte önemli tasarrufların sağlanması mümkündür. Öte yandan BT genel kontrolleri bir bütün olarak etkin olmadığında, bunun denetimler üzerinde önemli sonuçları olabilir. Bu hususa Rehber'in 5.2. bölümünde yer verilmiştir.

BT genel kontrolleri, uygulanabilirliği arttırabilmek açısından Rehber'de iki alt grup olarak ele alınmıştır. Buna göre:

- Süreç seviyesi BT genel kontrolleri, BT yönetim süreçleri üzerinde bulunan genel kontrollerden oluşur.
- Altyapı seviyesi BT genel kontrolleri ise, BT uygulamaları, veritabanları, işletim sistemleri ve ağ katmanları üzerinde yer alan teknik genel kontrolleri içerir. Söz konusu teknik genel kontroller de

aslen süreç seviyesi kontrollerin ayrılmaz bir parçası olmakla birlikte, BT denetim planının hazırlanması, BT denetçilerine görev dağılımının yapılabilmesi ve saha çalışmaları hususlarında önemli bir pratiklik sağladığından, ayrı bir grup olarak incelenmiştir.

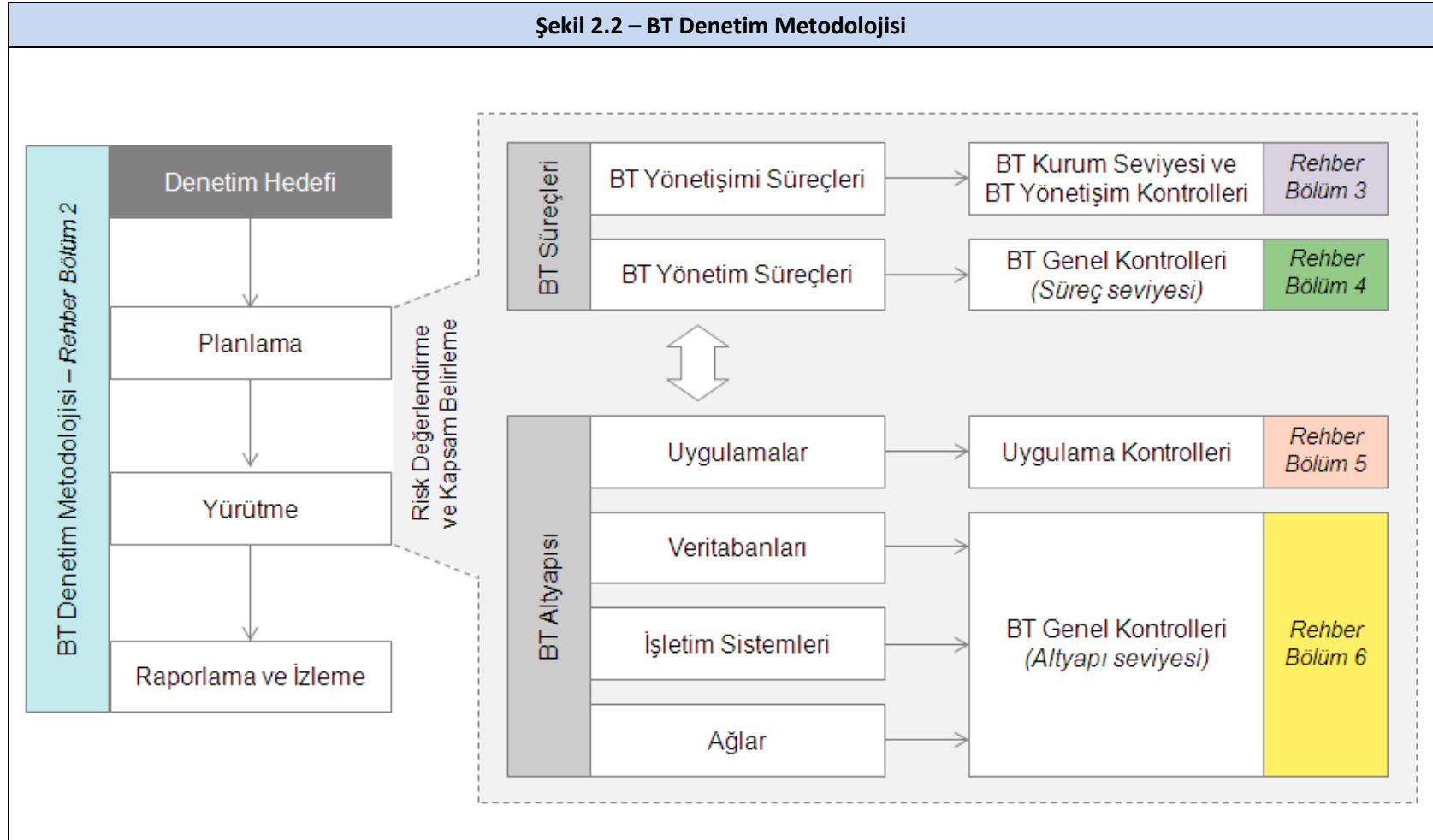
2.1.2. BT Denetim Metodolojisi: Büyük Resim

BT denetim metodolojisinin ana adımlarına, BT denetiminin konusu olan unsurlara ve bir önceki kısımda belirtilen kontrol türlerinin metodolojideki yerlerine işaret eden genel bir şemaya bir sonraki sayfada yer verilmektedir.

Şekilde görüldüğü üzere BT denetim metodolojisi, denetim hedefine uygun olarak “Planlama”, “Yürütme” ve “Raporlama ve İzleme” şeklinde üç ana adımdan oluşmaktadır. Planlama adımında yer alan risk değerlendirme ve kapsam belirleme çalışmalarının tamamı ve dolayısıyla BT denetim çalışmalarının yürütülmesi, yukarıda bahsi geçen BT kontrol piramidinde yer alan üç temel BT kontrol grubuna odaklanmaktadır.

Şekil 2.2’de ayrıca her bir BT kontrol grubuna ilişkin detaylı denetim adımlarının, Rehber’in hangi bölümünde ele alındığı da renk kodlarıyla gösterilmiştir. Aynı renk kodları kontrollerin birbiriyle olan ilişkisinin gösterildiği Şekil 2.1’de de kullanılmıştır.

Rehber’in 2.2. bölümü ile beraber, BT denetimi metodolojisinin üç ana adımı ve bu adımlarda yer alan detay çalışmaların nasıl yürütüleceği ile ilgili konular ve denetimde kullanılacak çeşitli araçlar/formlar ele alınmaktadır.



2.2. Planlama

2.2.1. Denetim hedeflerinin anlaşılması

BT denetimi faaliyetinin etkin bir şekilde gerçekleştirilmesi için birinci şart, öncelikle denetim hedeflerinin net bir şekilde ortaya konulması ve anlaşılmasıdır. Özellikle ilk kez BT denetimi gerçekleştirilecek kurumlarda, BT denetiminin hangi amaçla yapılacağına bilinçli olarak belirlenmesi ve BT denetim ekibinin bu doğrultuda yönlendirilmesi kritiktir. Bu amaçla denetçinin olduğu kadar Kurum'un ve paydaşların denetimle ilgili beklentilerinin de tam olarak anlaşılması gereklidir. Bu adımda bahsi geçen paydaşlar; kurumun hizmet sunduğu vatandaşlar, kurum yönetimi, personel, tedarikçiler ve diğer kamu kurumları olmak üzere, kurumun faaliyet alanları ile ilişkili tüm unsurları ifade etmektedir. Denetimle ilgili hedefler arasında mevzuata uygunluk ya da belirli bir alandaki risklerin tespiti gibi ihtiyaçların yanı sıra süreç iyileştirme ve önemli dönüşüm projelerinin etkilerinin ölçülmesi gibi farklı beklentiler de yer alabilir.

Denetim hedeflerinin belirlenmesi açısından, planlama aşamasından detaylı denetim çalışmalarına kadar denetimi her anlamda etkileyebilecek iç ve dış etkenler de bu aşamada değerlendirme kapsamına alınmalıdır. Örnek olarak; yeni teknolojilerin geliştirilmesi, yeni bir BT hizmeti ihtiyacının doğması, mevzuatla gelen zorunlu değişiklikler ya da BT bütçesini küçülebilecek olası mali kriz öngörülerini bu etkenlerden bazılarıdır.

Denetim hazırlıkları başlatılırken öncelikle kurum fonksiyonları, paydaş beklentileri, Kurum'un organizasyonel yapısı, teknolojik değişiklikler, yasal mevzuat, iş ihtiyaçları ve kuruma ve faaliyet alanına özgü risklerin bütününe ifade eden risk evreni, geçmiş dönemlerde tespit edilen denetim bulgularının mevcut durumları ile son denetim döneminden sonra gerçekleşen ve BT ortamını etkileyebilecek önemli değişiklikler hakkında bilgi alınmalıdır. Denetim planı oluşturulurken denetim hedeflerine uygun BT hedeflerinin belirlenmesi ve bu hedeflerle ilişkilendirilebilen denetim çalışmalarının risk faktörlerine göre planlanması önemlidir. Bu noktada her bir kamu kurumunun faaliyet amacı ve hedefinin, boyutunun, sunduğu hizmetin ve etkilendiği diğer faktörlerin birbirinden farklı nitelikte olduğu dikkate alınmalıdır.

Denetim hedefleri doğrultusunda karar verilen denetim alanı her ne olursa olsun bu denetim faaliyetinin bütüncül bir yaklaşımla ve etkin bir şekilde gerçekleştirilmesi adına denetim alanını etkileyen bilgi teknolojileri unsurlarının ve BT denetimi için entegrasyon noktalarının anlaşılması büyük önem taşır. Örneğin, sistem denetimlerinde süreçlerin işletilmesi için kullanılan kritik sistemlere erişim ve görevler ayrılığı, uygunluk denetimlerinde mevzuata uyum açısından BT risklerinin boyutu ve etkileri, mali denetimde mali tabloların oluşturulması için kullanılan bilgi sistemlerinin veri akışını tam ve doğru şekilde sağlayıp sağlamadığı, performans denetiminde BT yatırımlarının BT stratejileri ile uyumu, güvenlik denetiminde ise veritabanı ve işletim seviyesindeki güvenlik parametrelerinin konfigürasyonuna yönelik unsurlar öne çıkabilir. Bu unsurlar, denetim hedefi ve denetim alanları dikkate alınarak belirli bir risk değerlendirme ve planlama süreci takip edildikten sonra denetim kapsamına dâhil edilirler.

Özetle, BT denetimlerinin kurumlara katkı sağlayacak bir amaca hizmet etmesi için, yapılan denetimin teknik seviyesi ve denetim alanı ne olursa olsun, kurum hedefleri ile paralel ve onları destekleyici bir anlayışla gerçekleştirilmesi gerekir. Bu sebeple her ne kadar teknik yapısı ve karmaşıklığı ile farklılıkları ön plana çıksa da BT denetimleri de diğer tüm denetimler gibi tek bir amaca hizmet etmektedir. Bu da, kurum hedefleri ve paydaş beklentilerinin karşılanmasıdır.

2.2.2. BT ortamının anlaşılması

Ön araştırmanın yapılması

Kamu İç Denetim Rehberi'nde de belirtildiği üzere, denetçiler denetim çalışmasını yürütecekleri kurum ile ilgili belirli konuları denetime başlamadan önce anlamaya yönelik bir araştırma ve bilgi toplama faaliyeti gerçekleştirmelidir. Bu sayede denetim çalışmalarının daha verimli ve etkin olması sağlanabilecektir. Ön araştırmanın yapılması sırasında aşağıda belirtilen konularda bilgiler toplanır, gerekli ön analizler yapılır ve kayıt altına alınır.

- *Kurum ile ilgili temel mevzuatın anlaşılması*

Kurumun faaliyet göstermekte olduğu alan için yayımlanmış ve yürürlükte olan kanun, yönetmelik, tebliğ, genelge ve benzeri nitelikte olan mevzuat uyarınca BT fonksiyonu ile ilgili olarak uygulanması ve uyulması gereken prensip ve kuralların araştırılması ve analiz edilmesi, denetim çalışmalarına ilişkin kapsamın belirlenmesine doğrudan etki edebilecek alanların belirlenmesine yardımcı olacak ve aynı zamanda mevzuat açısından gerekli bir husus denetim kapsamı dışında bırakılmasına engel olacaktır.

- *Kurum iş süreçlerinin anlaşılması*

Denetçi, kurumun faaliyet gösterdiği alanda yürütülen çalışmaları, bunlara ilişkin süreç ve/veya iş akışlarını, ilgili faaliyet alanındaki görev, rol ve sorumlulukları ve BT'nin bu faaliyet ve süreçlerdeki rolünü genel itibarıyla anlamak adına mevcut durumda hazır bulunan belge ve dokümanları inceleyerek gerekli bilgileri edinmeye çalışır. Söz konusu bilgilerin bir bölümü kurumun hazırlamış olabileceği Stratejik Plan ve Faaliyet Raporu gibi kaynaklarda bulunabilir.

- *Önceki denetim raporlarının incelenmesi*

Denetlenecek alanda ya da BT ile ilgili başka bir alanda daha önceden yapılmış iç denetim çalışmalar ve kurum yönetimi tarafından dışarıdan hizmet olarak alınan denetim ya da değerlendirme benzeri çalışmalara ilişkin raporların ve varsa bu raporlarda kuruma iletilmiş olan bulgulara ilişkin alınan düzeltici ya da önleyici faaliyetlerin anlaşılması, kurum bünyesinde iyileştirme ihtiyacı olan alanların önceden anlaşılmasına ve denetim kapsamının buna yönelik revize edilmesine olanak verecektir.

Açılış toplantısının yapılması

Ön araştırma sonrasında denetim faaliyetine başlamadan önce denetçi denetlenecek kurumdaki ilgili üst yöneticiler, denetlenecek iş birimin yöneticisi/yöneticileri, BT birimi yöneticileri ve sorumluları ve ilgili diğer sorumlu personelin katılacağı bir açılış toplantısı yapar. Bu toplantının amacı Kamu İç Denetim Rehberi'inde de belirtilen aşağıdaki hususlar üzerinde bilgi paylaşımı yapmak ve görüş birliğine varmaktır:

- Denetimin amacı ve kapsamı,
- Denetim yöntemi,
- Denetim sonuçlarının ne şekilde paylaşılacağı,
- Denetimin tahmini süresi,
- Denetime yardımcı olacak personel ve çalışanlardan beklentiler,
- Birimin denetimden beklentileri,
- Denetim ekibi ile birim arasındaki iletişimin nasıl gerçekleştirileceği,
- Denetimin sağlayacağı faydalar.

Açılış toplantısında bunlara ilave olarak özellikle BT ortamındaki temel bileşenler (uygulamalar, sistemler, donanım, vb.), BT organizasyon yapısı, BT altyapısının entegrasyon seviyesi, BT altyapısının genel şematik yapısı ve dış ortamlarla olan bilgi alış verişi düzeyi gibi konular da tartışılarak ileriki bölümlerde yürütülecek anlayış geliştirme ve analiz aşamaları öncesi ön bilgi edinilebilir.

Açılış toplantısında görüşülen konular tutanak altına alınır, denetlenecek birim ile paylaşılır ve denetim dosyası içinde saklanır.

BT Organizasyonun Anlaşılması

Denetçi, BT biriminin kurumun genel organizasyon yapısı içerisindeki yerini, BT birimi yönetiminin kurum seviyesinde temsil seviyesini, BT biriminin kendi içerisindeki organizasyon yapılanmasını ve bunlara ilişkin ilişki, iletişim ve raporlama yapılarını inceleyerek BT organizasyonunu anlamalıdır. Söz konusu inceleme denetçiye kurum içerisinde BT'ye ilişkin faaliyetlerin organizasyon seviyesinde nasıl yürütüldüğü konusunda bilgi verebileceği gibi, denetim sırasında karşılaşılabilecek belirli aksaklıkların kök nedenlerinin belirlenmesinde yol gösterici de olabilecektir.

Üçüncü taraf hizmetlerin anlaşılması

Denetlenecek kurum bünyesinde BT faaliyetleri ile ilgili hizmetlerin bir bölümü belirli hizmet sağlayıcı firma, kurum ya da kuruluşlarca karşılanıyor olabilir. Böyle bir durumda dışarıdan alınan hizmetlerin niteliği, bu hizmetlerin kurumun BT ve genel iş faaliyetleri açısından sahip olduğu önem, ilgili hizmetlerin sunumuna ilişkin sözleşme ve/veya hizmet anlaşmalarının koşul ve şartları ile söz konusu hizmetlere olan bağımlılığın seviyesi, denetim çalışmaları açısından değerlendirilmeli ve gerektiği durumlarda söz konusu hizmetleri sağlayan firma, kurum ya da kuruluşlardan temsilcilerin de bilgi ve görüşlerine başvurulmalıdır.

BT envanterinin anlaşılması

BT envanteri, kurumun BT ortamında bulundurduğu tüm uygulama, yazılım, donanım, cihaz, lisans ve benzeri bileşenlere ilişkin listenin varsa temin edilmesi, özellikle uygulama ve yazılımların hangi iş süreçlerini ve faaliyet alanlarını desteklediğini anlamak açısından önem arz etmektedir. Bu anlamda uygulamalara yönelik olarak yapılacak bir envanter analizinde aşağıda belirtilen bilgiler özellikle aranmalı ve kayıt altına alınmalıdır:

- Uygulamanın adı ve kısa açıklaması,
- Uygulamanın desteklediği faaliyet alanları ve iş süreçleri
- Uygulamanın kurum içinde mi yoksa dışında mı geliştirildiği
- Uygulama ile ilgili varsa dışarıdan alınan hizmetlerin niteliği
- Uygulamanın üzerinde çalıştığı sunucu/işletim sistemi ve kullanmakta olduğu veritabanı sistemlerinin model ve sürüm bilgileri
- Uygulamanın üzerinde çalıştığı donanım (ör: AS/400 platformu)

Söz konusu envanter ileride bahsedilecek olan bilgi toplama formu aracılığı vasıtası ile kayıt altına alınıp yine rehberin ilerleyen bölümlerinde bahsedilecek olan risk değerlendirme ve kapsam belirleme adımlarına girdi olarak kullanılacaktır.

Yukarıda bahsedilmiş olan ve genel olarak BT ortamının anlaşılmasına yardımcı olacak bilgilerin bir bölümünün ileriki aşamalarda kullanılabilmesi açısından kayıt altına alınması gerekmektedir. Bu doğrultuda oluşturulmuş olan Bilgi Toplama Formu (Bkz: **Ek 1 – Bilgi Toplama Formu**), “Genel Bilgiler” ve “Teknik Bilgiler” adında iki ana bölümden oluşmaktadır. Bu formun amacı denetim saha çalışmalarına başlamadan önce denetlenenden planlama, kapsam belirleme ve risk analizi aşamaları için girdi sağlayacak verilere ulaşmaktır.

Formun “Genel Bilgiler” bölümünde kurumun organizasyonel ve mali yapısı hakkında bilgiler istenmektedir. “Teknik Bilgiler” bölümünde ise kurum BT birimine ve yapısına ilişkin bilgiler yer almaktadır.

Bilgi toplama formu denetlenen ile denetim öncesinde paylaşılır ve denetlenenden formda istenilen dokümanları ve bilgileri sağlaması istenir. Sağlanan bilgiler ile kurum hakkında genel bir görüş edinmenin yanında planlama, kapsam belirleme ve risk analizi alanlarında kullanılacak gerekli bilgiler edinilir.

2.2.3. Risk değerlendirmesinin yapılması

Denetim kapsamının denetim hedefleriyle uyumlu bir şekilde belirlenmesi ve denetim çalışmalarının planlanması aşamasında denetçi, denetim alanını önemlilik kavramı ile ölçeklendirebilmek için risk değerlendirmesinden faydalanır. Bu aşamada, Kurum’un hizmet alanları ve buna bağlı riskler hakkında bilgi sahibi olmak büyük önem taşımaktadır.

Bir kurumun iç denetim sürecini etkileyen şartlar zamanla değişebildiğinden, hiçbir risk değerlendirme yaklaşımı tek başına tüm şartlarda en ideal risk değerlendirme stratejisi olarak değerlendirilemez. Riskler, kurum'un süreç ve hedefleri göz önünde bulundurularak denetim çalışmalarının detay seviyesini belirlemek üzere değerlendirildiği gibi her bir BT katmanına özgü olmak üzere gizlilik, bütünlük ve erişilebilirlik yani bilgi güvenliği unsurlarıyla da değerlendirilir.

Değerlendirme sürecinde; kurum hedeflerinin karşılanmasında nelerin yanlış gidebileceği, ihmal edilebilecek konular ve yasal yükümlülüklerle uyumsuzluklar göz önünde bulundurulur. Değerlendirme sonucu ortaya çıkan risk puanı dikkate alınarak denetim için zorunlu tutulan kontrol hedeflerine ilave alanların ya da kontrol hedeflerinin de kapsama alınması mümkündür.

Risk değerlendirme aşaması genel itibariyle Kamu İç Denetim Rehberi'nde belirtilen temel risk faktörleri ve risk değerlendirme yaklaşımı göz önünde bulundurularak, Kurum'un karşı karşıya kaldığı bilgi teknolojileri risklerinin,

- Stratejik etki,
- Hizmetler/faaliyetler,
- Yasal uyum,
- BT kaynakları ve
- Organizasyon yapısı

gibi unsurlar çerçevesinde değerlendirilmesinden ibaret olacaktır. Yukarıda belirtilen risk unsurlarına ek olarak mali etkiler, sosyal etkiler, itibar etkileri ve varsa önceki denetim sonuçlarından kaynaklanan hususlar eklenebilir.

Bilgi teknolojilerinin kurum içerisindeki yeri ve önemi, kurumun yapısı ve karmaşıklığı, bilgi teknolojileri biriminin yapısı, kurumun organizasyon değişikliği beklentisi, stratejik öncelikler ve çeşitli dış etmenleri de dikkate alan risk değerlendirmesi, bilgi sistemleri denetim planlamasının yanı sıra kapsam belirleme sürecinin de en kritik adımlarından biridir. Bu yaklaşımın, denetim planlaması öncesinde benimsenmesi kaynakların etkin bir şekilde kullanılması için önemlidir. Denetim planlaması oluşturulurken gerçekleştirilen risk değerlendirmesi;

- Denetim prosedürlerinin içeriği, kapsamı ve zamanlaması,
- Denetlenecek alanlarının ve fonksiyonların belirlenmesi,
- Denetim için ayrılacak kaynak ve zamanın belirlenmesi

konularında yardımcı olur.

Denetim çalışmalarının planlanması ve denetimin kapsamının belirlenmesi amacıyla, denetim çalışmalarının detay seviyesi ve kapsama alınacak BT süreçleri ve uygulamalar için bir risk değerlendirmesi yapılmalıdır.

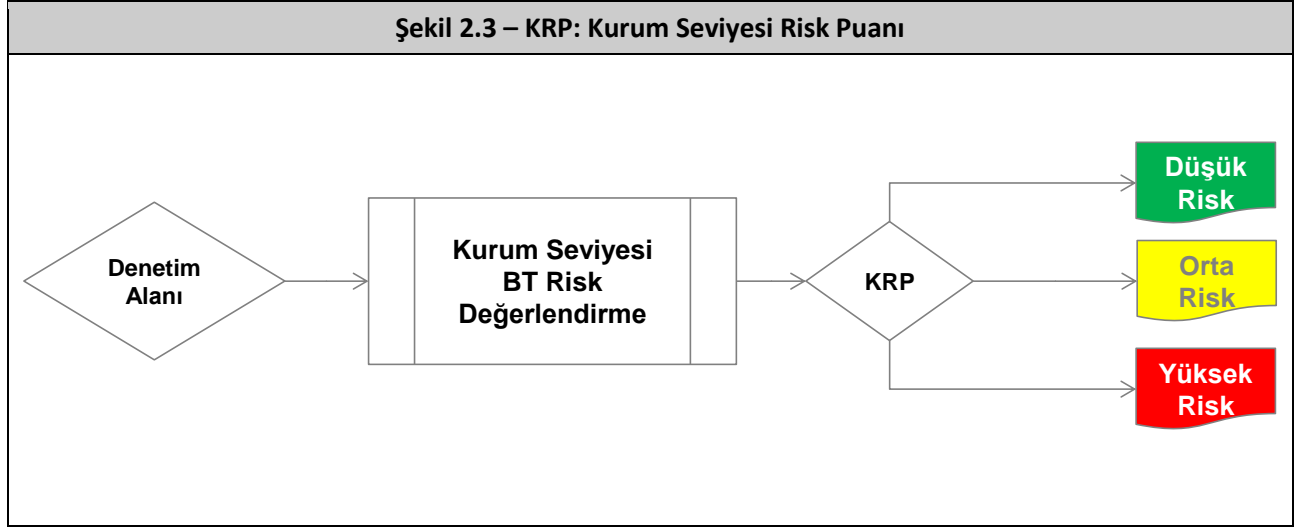
Risk değerlendirme çalışması için hazırlanmış olan Risk değerlendirme formu, hem kurum için geçerli BT risklerinin ölçeğinin anlaşılması hem de uygulamaların bireysel olarak risk seviyelerinin belirlenmesi için kullanılan iki ayrı bölümden oluşur (bkz. *Ek 2-Risk Değerlendirme Formu*).

Kurum seviyesi BT risk değerlendirmesi

Kurumun genelinde BT ile ilgili oluşabilecek risklerin değerlendirilmesinde kullanılacak olan *Kurumsal risk değerlendirme* formu, (1) “Stratejik etki”, (2) “Hizmetler/faaliyetler”, (3) “Yasal uyum/mevzuat”, (4) “BT kaynakları” ve (5) “Organizasyon yapısı” başlıkları altında toplam 31 sorudan oluşur. Bu sorulara verilecek cevaplar neticesinde kurumun kurumsal risk derecesini temsil eden ve 100 üzerinden hesaplanan bir değer – Kurum Risk Puanı (KRP) elde edilir. Söz konusu sorular genel itibariyle Kamu İç Denetim Rehberi’nde belirtilen temel risk faktörlerine ilişkin değerlendirmelere imkan sağlamakla birlikte kurumun faaliyet alanı ya da sunduğu hizmetler göz önünde tutularak özelleştirilebilir. KRP’si 40 ve aşağısı olan kurumlar neredeyse risksiz olarak değerlendirilebilirken, “100” değeri ise en yüksek seviyede riski işaret etmektedir. KRP’si 40 ile 70 arasında olan kurumlar Orta Riskli olarak değerlendirilir. Söz konusu puan aralıkları kurumun faaliyet alanına ve BT ortamının karmaşıklığına bağlı olarak değiştirilebilir.

Denetim alanına göre kapsam belirleme için kullanılacak yönlendirme tablolarına aşağıda yer verilmiştir.

Kurum seviyesi risk değerlendirme için önerilen risk seviyelerine ilişkin gösterim aşağıdaki şekilde verilmiştir.



Uygulama seviyesi BT risk değerlendirmesi

Kurum bünyesinde bulunan uygulamaların temel olarak faaliyetleri ve iş süreçlerini destekleme seviyeleri ve belirli teknik özellikleri açısından değerlendirilmesi sırasında kullanılacak olan *Uygulama seviyesi risk değerlendirme formu*, bir yandan kuruma ait uygulamaların kapsama alınma uygunluğunu da değerlendirmek amacıyla sorulmuş toplam 16 adet sorudan oluşmaktadır. Bu sorulara verilecek cevaplar neticesinde uygulama risk seviyesini temsil eden 100 üzerinden bir değer – Uygulama Risk Puanı (URP) elde edilir. Uygulama risk seviyesi 40 ve aşağısı olan uygulamalar neredeyse risksiz olarak değerlendirilebilirken, “100” değeri ise en yüksek seviyede riski işaret etmektedir. URP’si 40 ile 70 arasında hesaplanan kurumlar Orta Riskli olarak değerlendirilir. Söz konusu puan aralıkları kurumun faaliyet alanına ve BT ortamının karmaşıklığına bağlı olarak değiştirilebilir.

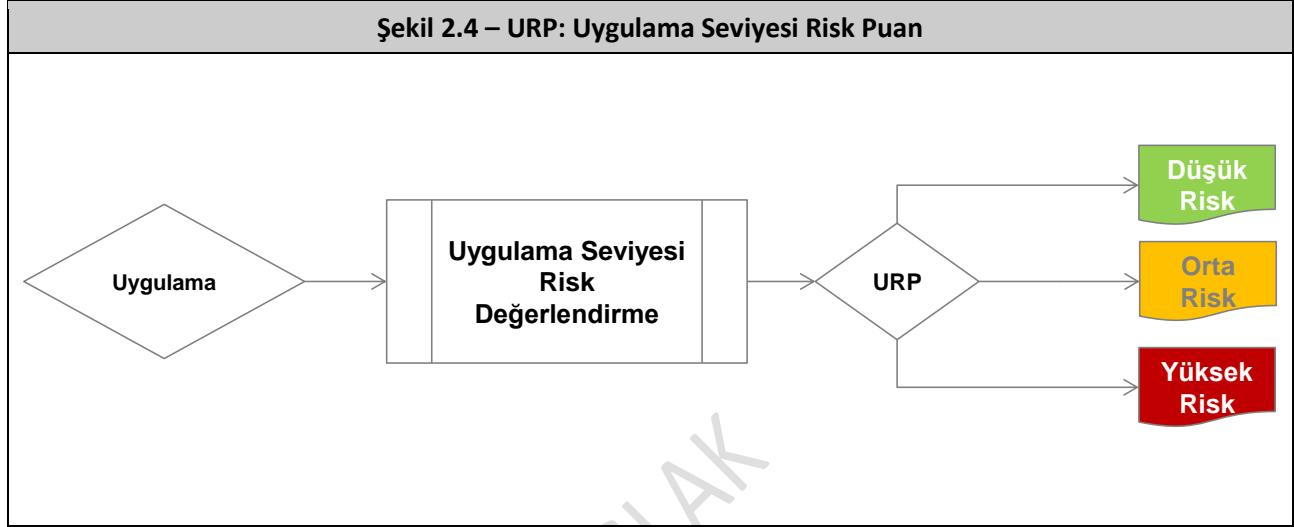
Denetim alanına göre kapsam belirleme için kullanılacak yönlendirme tablolarına aşağıda yer verilmiştir.

Risk değerlendirme formunun kapsamadığı ve kapsayamayacağı önceki denetim raporları, müfettiş raporları, yönetimin denetimden beklentisi, kaynak planlaması veya denetçinin dikkatine gelebilecek diğer hususlar ışığında risk seviyesi tekrar değerlendirilebilir ve gerekçesini belirtmek suretiyle kapsama yeni uygulamalar eklenebilir ya da var olan uygulamalar kapsamdan çıkarılabilir.

Uygulama seviyesinde risk değerlendirmesinden sonra kapsama alınacak uygulama envanterinin teknoloji envanter formu (bkz. *Ek 3 - Teknoloji Envanteri Formu*) içerisinde kayıt altına alınması gerekmektedir. *Teknoloji envanteri formu* denetçi tarafından doldurulmalıdır. Denetim hedefleri ve uygulama risk değerlendirmesi sonucu olarak kapsama alınan uygulamaların kurulu olduğu platformlar, işletim sistemleri, veritabanları ve uygulama ile ilgili süreç sahipleri bu envanter üzerinde kaydedilir.

Risk değerlendirme ve bir sonraki bölümde verilmiş olan denetim alanına göre kapsam belirleme için kullanılacak yönlendirme tablolarının kullanımı neticesinde belirlenecek kapsam uyarınca gerçekleştirilmesi gereken detay denetim adımları ve çalışmaları rehberin ilerleyen bölümlerinde sunulmuştur.

Uygulama seviyesi risk değerlendirme için önerilen risk seviyelerine ilişkin gösterim aşağıdaki şekilde verilmiştir.



2.2.4. Kapsamın belirlenmesi

Kapsam Belirlenmesine İlişkin Esaslar

Denetim kapsamına alınacak ve rehberin ilerleyen bölümlerinde detaylı olarak ele alınmış olan BT alanları, denetim stratejisi ve denetim planına uygun bir şekilde seçilecek olan denetim alanı ve gerçekleştirilecek risk değerlendirme sonuçları uyarınca belirli bir karar mekanizması üzerinden belirlenebileceği gibi, belirtilen alanların her biri müstakil olarak bir denetim alanı olarak seçilebilir. Kamu İç Denetim Rehberi'nde de belirtildiği üzere, denetim alanlarının oluşturulmasında, denetim konusu hususların kendi içerisinde tutarlı bir şekilde bir bütün olarak ele alınmasına dikkat edilir.

BT denetimi kapsamının, denetim stratejisi ve planı uyarınca seçilecek denetim alanına bağlı olarak ne şekilde belirlenebileceğine ilişkin karar mekanizmaları her bir denetim alanı için ayrı ayrı olarak aşağıdaki bölümde verilmiştir.

Denetim kapsamına alınacak ve rehberin ilerleyen bölümlerinde detaylı olarak ele alınmış olan BT alanları, denetim stratejisi ve denetim planına uygun bir şekilde seçilecek olan denetim alanı ve gerçekleştirilecek risk değerlendirme sonuçları uyarınca belirli bir karar mekanizması üzerinden belirlenebileceği gibi, belirtilen alanların her biri müstakil olarak bir denetim alanı olarak seçilebilir. Kamu İç Denetim Rehberi'nde de belirtildiği üzere, denetim alanlarının oluşturulmasında, denetim konusu hususların kendi içerisinde tutarlı bir şekilde bir bütün olarak ele alınmasına dikkat edilir.

Ařađıda belirtilen kapsam tabloları dıřında kalan Uygulama Kontrollerinin denetimi bařta Mali ve Sistem denetimlerinde olmak üzere belirli ölçüde deđerlendirme kapsamına alınır. Uygulama kontrollerinin dođası geređi kurumların faaliyet alanı ve uygulanan iř süreçleri ile iř uygulamaları kullanımı ve karmařıklıđı aısından farklılık göstermesinden dolayı, denetim kapsamına alınacak uygulama kontrolleri her denetimde deneti tarafından yukarıda belirtilen hususlar dikkate alınarak belirlenir ve uygulanır.

TASLAK

Mali Denetim Kapsamında Yürütülecek BT Denetimi Kapsamı

Mali denetim kapsamında Kurum Seviyesi Risk Değerlendirme ve Uygulama Risk Değerlendirme sonuçları uyarınca yürütülebilecek denetim çalışmaları için belirlenebilecek kapsama ilişkin yönlendirme aşağıda belirtilmiştir.

Kurum Seviyesi Risk Değerlendirme	Düşük Risk (KRP < 40)	Orta Risk (40 < KRP < 70)	Yüksek Risk (70 < KRP)
BT Kurum Seviyesi Kontrolleri	Kapsamda	Kapsamda	Kapsamda
BT Yönetişim Kontrolleri	Kapsamda değil	Kapsama alınması önerilir	Kapsamda
BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup	Zorunlu denetim adımları kapsamda	<ul style="list-style-type: none"> Zorunlu denetim adımları kapsamda Seçime bağlı denetim adımlarının kapsama alınması önerilir 	Zorunlu ve Seçime Bağlı denetim adımlarının tamamı kapsamda
BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 2. Grup	Denetlenen kurumun faaliyetlerine ya da denetim dönemi içinde sistem değişikliği olup olmadığına bağlı olarak seçilecek süreçler (ör: DS2, AI2) dışında kapsamda değil	<ul style="list-style-type: none"> Zorunlu denetim adımları kapsamda Denetlenen kurumun faaliyetlerine ya da denetim dönemi içinde sistem değişikliği olup olmadığına bağlı olarak seçilecek süreçler (ör: DS2, AI2) için Seçime Bağlı denetim adımları kapsamda 	Zorunlu ve Seçime Bağlı denetim adımlarının tamamı kapsamda

Uygulama Seviyesi Değerlendirme	Risk	Düşük Risk (URP < 40)	Orta Risk (40 < URP < 70)	Yüksek Risk (70 < URP)
İş Uygulamaları		BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen Zorunlu denetim adımlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim adımlarının tümü ve 2. Grup içinde belirtilen denetim adımlarından Zorunlu olanlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim adımlarının tümü ve 2. Grup içinde belirtilen denetim adımlarından Zorunlu olanlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır. Buna ilave olarak 2. Grup içinde belirtilen Seçime Bağlı denetim adımlarının ilgili iş uygulaması üzerinde yürütülebilecek olanların kapsama alınması da önerilir.
İşletim/Sunucu Sistemleri		Seçilen iş uygulamasının çalışma mantığına ve sunucu sistemi ile olan etkileşimine, sunucu sistemi seviyesindeki son kullanıcı hesabı sayısına ve sunucu sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınabilir.	Seçilen iş uygulamasının çalışma mantığına ve sunucu sistemi ile olan etkileşimine, sunucu sistemi seviyesindeki son kullanıcı hesabı sayısına ve sunucu sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımlarının kapsama alınması önerilir.	Seçilen iş uygulamasının çalışma mantığına ve sunucu sistemi ile olan etkileşimine, sunucu sistemi seviyesindeki son kullanıcı hesabı sayısına ve sunucu sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınır.
Veritabanı Sistemleri		Seçilen iş uygulamasının çalışma mantığına ve veritabanı sistemi ile olan etkileşimine, veritabanı sistemi seviyesindeki son kullanıcı hesabı	Seçilen iş uygulamasının çalışma mantığına ve veritabanı sistemi ile olan etkileşimine, veritabanı sistemi seviyesindeki son kullanıcı hesabı	Seçilen iş uygulamasının çalışma mantığına ve veritabanı sistemi ile olan etkileşimine, veritabanı sistemi seviyesindeki son kullanıcı hesabı

Uygulama Seviyesi Değerlendirme	Risk	Düşük Risk (URP < 40)	Orta Risk (40 < URP < 70)	Yüksek Risk (70 < URP)
		sayısına, veritabanı seviyesine erişim yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınması önerilir.	sayısına, veritabanı seviyesine erişim yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınması önerilir.	sayısına, veritabanı seviyesine erişim yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınır.
Ağ Bileşenleri		Seçilen iş uygulaması ve buna bağlı sunucu ve veritabanı sistemlerinin ağ üzerinden etkileşimine, veri alışveriş yöntemlerine, ağ seviyesi üzerinden ilgili sistemlere doğrudan son kullanıcı erişimi erişim olup olmamasına bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınabilir.	Seçilen iş uygulaması ve buna bağlı sunucu ve veritabanı sistemlerinin ağ üzerinden etkileşimine, veri alışveriş yöntemlerine, ağ seviyesi üzerinden ilgili sistemlere doğrudan son kullanıcı erişimi erişim olup olmamasına bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınması önerilir.	Seçilen iş uygulaması ve buna bağlı sunucu ve veritabanı sistemlerinin ağ üzerinden etkileşimine, veri alışveriş yöntemlerine, ağ seviyesi üzerinden ilgili sistemlere doğrudan son kullanıcı erişimi erişim olup olmamasına bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınır.

Sistem Denetim Kapsamında Yürütülecek BT Denetimi Kapsamı

Sistem denetimi kapsamında Kurum Seviyesi Risk Değerlendirme ve Uygulama Risk Değerlendirme sonuçlarına yürütülebilecek denetim çalışmaları için göre belirlenebilecek kapsama ilişkin yönlendirme aşağıda belirtilmiştir.

Kurum Seviyesi Risk Değerlendirme	Düşük Risk (KRP < 40)	Orta Risk (40 < KRP < 70)	Yüksek Risk (70 < KRP)
BT Kurum Seviyesi Kontrolleri	Kapsamda	Kapsamda	Kapsamda
BT Yönetişim Kontrolleri	Kapsamda değil	Kapsamda	Kapsamda
BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup	Zorunlu denetim adımları kapsamda	<ul style="list-style-type: none"> Zorunlu denetim adımları kapsamda Seçime bağlı denetim adımlarının kapsama alınması önerilir 	Zorunlu ve Seçime Bağlı denetim adımlarının tamamı kapsamda
BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 2. Grup	Denetlenen kurumun faaliyetlerine ya da denetim dönemi içinde sistem değişikliği olup olmadığına bağlı olarak seçilecek süreçler (ör: DS2, AI2) dışında kapsamda değil	<ul style="list-style-type: none"> Zorunlu denetim adımları kapsamda Denetlenen kurumun faaliyetlerine ya da denetim dönemi içinde sistem değişikliği olup olmadığına bağlı olarak seçilecek süreçler (ör: DS2, AI2) için Seçime Bağlı denetim adımları kapsamda 	Zorunlu ve Seçime Bağlı denetim adımlarının tamamı kapsamda

Uygulama Seviyesi Değerlendirme	Risk	Düşük Risk (URP < 40)	Orta Risk (40 < URP < 70)	Yüksek Risk (70 < URP)
İş Uygulamaları		BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen Zorunlu denetim adımlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim adımlarının tümü ve 2. Grup içinde belirtilen denetim adımlarından Zorunlu olanlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim adımlarının tümü ve 2. Grup içinde belirtilen denetim adımlarından Zorunlu olanlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır. Buna ilave olarak 2. Grup içinde belirtilen Seçime Bağlı denetim adımlarının ilgili iş uygulaması üzerinde yürütülebilecek olanların kapsama alınması da önerilir.
İşletim/Sunucu Sistemleri		Seçilen iş uygulamasının çalışma mantığına ve sunucu sistemi ile olan etkileşimine, sunucu sistemi seviyesindeki son kullanıcı hesabı sayısına ve sunucu sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınabilir.	Seçilen iş uygulamasının çalışma mantığına ve sunucu sistemi ile olan etkileşimine, sunucu sistemi seviyesindeki son kullanıcı hesabı sayısına ve sunucu sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımlarının kapsama alınması önerilir.	Seçilen iş uygulamasının çalışma mantığına ve sunucu sistemi ile olan etkileşimine, sunucu sistemi seviyesindeki son kullanıcı hesabı sayısına ve sunucu sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınır.
Veritabanı Sistemleri		Seçilen iş uygulamasının çalışma mantığına ve veritabanı sistemi ile olan etkileşimine, veritabanı sistemi seviyesindeki son kullanıcı hesabı	Seçilen iş uygulamasının çalışma mantığına ve veritabanı sistemi ile olan etkileşimine, veritabanı sistemi seviyesindeki son kullanıcı hesabı	Seçilen iş uygulamasının çalışma mantığına ve veritabanı sistemi ile olan etkileşimine, veritabanı sistemi seviyesindeki son kullanıcı hesabı

Uygulama Seviyesi Değerlendirme	Risk	Düşük Risk (URP < 40)	Orta Risk (40 < URP < 70)	Yüksek Risk (70 < URP)
		sayısına, veritabanı seviyesine erişim yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınması önerilir.	sayısına, veritabanı seviyesine erişim yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınması önerilir.	sayısına, veritabanı seviyesine erişim yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınır.
Ağ Bileşenleri		Seçilen iş uygulaması ve buna bağlı sunucu ve veritabanı sistemlerinin ağ üzerinden etkileşimine, veri alışveriş yöntemlerine, ağ seviyesi üzerinden ilgili sistemlere doğrudan son kullanıcı erişimi erişim olup olmamasına bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınabilir.	Seçilen iş uygulaması ve buna bağlı sunucu ve veritabanı sistemlerinin ağ üzerinden etkileşimine, veri alışveriş yöntemlerine, ağ seviyesi üzerinden ilgili sistemlere doğrudan son kullanıcı erişimi erişim olup olmamasına bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınması önerilir.	Seçilen iş uygulaması ve buna bağlı sunucu ve veritabanı sistemlerinin ağ üzerinden etkileşimine, veri alışveriş yöntemlerine, ağ seviyesi üzerinden ilgili sistemlere doğrudan son kullanıcı erişimi erişim olup olmamasına bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınır.

Performans Denetim Kapsamında Yürütülecek BT Denetimi Kapsamı

Performans denetimi kapsamında Kurum Seviyesi Risk Değerlendirme ve Uygulama Risk Değerlendirme sonuçlarına yürütülebilecek denetim çalışmaları için göre belirlenebilecek kapsama ilişkin yönlendirme aşağıda belirtilmiştir.

Kurum Seviyesi Değerlendirme	Risk	Düşük Risk (KRP < 40)	Orta Risk (40 < KRP < 70)	Yüksek Risk (70 < KRP)
BT Kurum Seviyesi Kontrolleri		Kapsamda	Kapsamda	Kapsamda
BT Yönetişim Kontrolleri		Kapsamda	Kapsamda	Kapsamda
BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup		Denetlenen kurumun faaliyetlerine ve denetlenen kurumda performans yönetimine etki edebileceği düşünülen süreçler kapsama alınabilir		
BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 2. Grup		Denetlenen kurumun faaliyetlerine ve denetlenen kurumda performans yönetimine etki edebileceği düşünülen süreçler kapsama alınabilir		

Performans denetimi sırasında yürütülebilecek BT denetiminin amacı kurumun kaynaklarının etkin, verimli ve tutumlu bir şekilde kullanıldığının değerlendirilmesi olduğundan, BT altyapı bileşenleri üzerinde gerçekleştirilecek bir genel kontrol denetim çalışmasının ana hedefi, söz konusu iş uygulamaları ve diğer bileşenlerin doğru ve güvenilir veri üretip üretmediği ve ilgili uygulamaların ve altyapı bileşenlerinin ilgili iş hedeflerini ne derece karşılayıp karşılamadığının tespit edilmesi olacaktır. Bu anlamda BT altyapı genel kontrollerine ilişkin kapsam çalışması bu yaklaşım göz önünde bulundurularak yürütülür.

Uygulama Seviyesi Risk Değerlendirme	Düşük Risk (URP < 40)	Orta Risk (40 < URP < 70)	Yüksek Risk (70 < URP)
İş Uygulamaları	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen Zorunlu denetim adımlarından veri üretimine ve iş ihtiyaçlarının karşılanmasına doğrudan etki edebilecek olanlar kapsama alınabilir.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. ve 2. Grup içinde belirtilen Zorunlu denetim adımlarından veri üretimine ve iş ihtiyaçlarının karşılanmasına doğrudan etki edebilecek olanların kapsama alınması önerilir.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. ve 2. Grup içinde belirtilen Zorunlu denetim adımlarından veri üretimine ve iş ihtiyaçlarının karşılanmasına doğrudan etki edebilecek olanlar kapsama alınır. Buna ilave olarak 1. ve 2. Grup içinde Seçime Bağlı olarak belirtilenlerin de kapsama alınması değerlendirilmelidir.
İşletim/Sunucu Sistemleri	Seçilen iş uygulamasının çalışma mantığına ve sunucu sistemi ile olan etkileşimine, sunucu sistemi seviyesindeki son kullanıcı hesabı sayısına ve sunucu sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımlarından özellikle veri üretimine doğrudan etki edebilecek olanlar kapsama alınabilir.	Seçilen iş uygulamasının çalışma mantığına ve sunucu sistemi ile olan etkileşimine, sunucu sistemi seviyesindeki son kullanıcı hesabı sayısına ve sunucu sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımlarından özellikle veri üretimine doğrudan etki edebilecek olanların kapsama alınması önerilir.	Seçilen iş uygulamasının çalışma mantığına ve sunucu sistemi ile olan etkileşimine, sunucu sistemi seviyesindeki son kullanıcı hesabı sayısına ve sunucu sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımlarından özellikle veri üretimine doğrudan etki edebilecek olanlar kapsama alınır.

Uygulama Seviyesi Risk Değerlendirme	Düşük Risk (URP < 40)	Orta Risk (40 < URP < 70)	Yüksek Risk (70 < URP)
Veritabanı Sistemleri	Seçilen iş uygulamasının çalışma mantığına ve veritabanı sistemi ile olan etkileşimine, veritabanı sistemi seviyesindeki son kullanıcı hesabı sayısına, veritabanı seviyesine erişim yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımlarından özellikle veri üretimine doğrudan etki edebilecek olanlar kapsama alınabilir.	Seçilen iş uygulamasının çalışma mantığına ve veritabanı sistemi ile olan etkileşimine, veritabanı sistemi seviyesindeki son kullanıcı hesabı sayısına, veritabanı seviyesine erişim yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımlarından özellikle veri üretimine doğrudan etki edebilecek olanların kapsama alınması önerilir.	Seçilen iş uygulamasının çalışma mantığına ve veritabanı sistemi ile olan etkileşimine, veritabanı sistemi seviyesindeki son kullanıcı hesabı sayısına, veritabanı seviyesine erişim yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımlarından özellikle veri üretimine doğrudan etki edebilecek olanlar kapsama alınır.
Ağ Bileşenleri	Seçilen iş uygulaması ve buna bağlı sunucu ve veritabanı sistemlerinin ağ üzerinden etkileşimine, veri alışveriş yöntemlerine, ağ seviyesi üzerinden ilgili sistemlere doğrudan son kullanıcı erişimi erişim olup olmamasına bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları özellikle veri üretimine doğrudan etki edebilecek olanlar kapsama alınabilir.	Seçilen iş uygulaması ve buna bağlı sunucu ve veritabanı sistemlerinin ağ üzerinden etkileşimine, veri alışveriş yöntemlerine, ağ seviyesi üzerinden ilgili sistemlere doğrudan son kullanıcı erişimi erişim olup olmamasına bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları özellikle veri üretimine doğrudan etki edebilecek olanların kapsama alınması önerilir.	Seçilen iş uygulaması ve buna bağlı sunucu ve veritabanı sistemlerinin ağ üzerinden etkileşimine, veri alışveriş yöntemlerine, ağ seviyesi üzerinden ilgili sistemlere doğrudan son kullanıcı erişimi erişim olup olmamasına bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları özellikle veri üretimine doğrudan etki edebilecek olanlar kapsama alınır.

Uyum Denetimi Kapsamında Yürütülecek BT Denetimi Kapsamı

Uyum denetimi kapsamında Kurum Seviyesi Risk Değerlendirme ve Uygulama Risk Değerlendirme sonuçlarına yürütülebilecek denetim çalışmaları için göre belirlenebilecek kapsama ilişkin yönlendirme aşağıda belirtilmiştir.

Kurum Seviyesi Risk Değerlendirme	Düşük Risk (KRP < 40)	Orta Risk (40 < KRP < 70)	Yüksek Risk (70 < KRP)
BT Kurum Seviyesi Kontrolleri	Kapsamda	Kapsamda	Kapsamda
BT Yönetişim Kontrolleri	Uyum gerektiren mevzuat ya da diğer kriterler uyarınca kapsama alınabilir	Uyum gerektiren mevzuat ya da diğer kriterler uyarınca kapsama alınabilir	Uyum gerektiren mevzuat ya da diğer kriterler uyarınca kapsama alınabilir
BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup	<ul style="list-style-type: none"> Zorunlu denetim adımları kapsamda Seçime Bağlı denetim adımlarından seçilecekler ilgili mevzuat ya da kritere göre kapsama alınabilir 	<ul style="list-style-type: none"> Zorunlu denetim adımları kapsamda Seçime Bağlı denetim adımlarından seçilecekler ilgili mevzuat ya da kritere göre kapsama alınması önerilir 	
BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 2. Grup	Denetlenen kurumun faaliyetlerine, denetim dönemi içinde sistem değişikliği olup olmadığına ve denetlenen kurumda uyum gösterilmesi gereken kriterler uyarınca seçilecek süreçler kapsama alınabilir	Denetlenen kurumun faaliyetlerine, denetim dönemi içinde sistem değişikliği olup olmadığına ve denetlenen kurumda uyum gösterilmesi gereken kriterler uyarınca seçilecek süreçlerin kapsama alınması önerilir	

Uygulama Seviyesi Risk Değerlendirme	Düşük Risk (URP < 40)	Orta Risk (40 < URP < 70)	Yüksek Risk (70 < URP)
İş Uygulamaları	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen Zorunlu denetim	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim adımlarının	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim adımlarının

Uygulama Seviyesi Değerlendirme	Risk	Düşük Risk (URP < 40)	Orta Risk (40 < URP < 70)	Yüksek Risk (70 < URP)
		adımlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır.	tümü ve 2. Grup içinde belirtilen denetim adımlarından Zorunlu olanlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır.	tümü ve 2. Grup içinde belirtilen denetim adımlarından Zorunlu olanlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır. Buna ilave olarak 2. Grup içinde belirtilen Seçime Bağlı denetim adımlarının ilgili iş uygulaması üzerinde yürütülebilecek olanların kapsama alınması da önerilir.
İşletim/Sunucu Sistemleri		Seçilen iş uygulamasının çalışma mantığına ve sunucu sistemi ile olan etkileşimine, sunucu sistemi seviyesindeki son kullanıcı hesabı sayısına ve sunucu sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınabilir.	Seçilen iş uygulamasının çalışma mantığına ve sunucu sistemi ile olan etkileşimine, sunucu sistemi seviyesindeki son kullanıcı hesabı sayısına ve sunucu sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımlarının kapsama alınması önerilir.	Seçilen iş uygulamasının çalışma mantığına ve sunucu sistemi ile olan etkileşimine, sunucu sistemi seviyesindeki son kullanıcı hesabı sayısına ve sunucu sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınır.
Veritabanı Sistemleri		Seçilen iş uygulamasının çalışma mantığına ve veritabanı sistemi ile olan etkileşimine, veritabanı sistemi seviyesindeki son kullanıcı hesabı sayısına, veritabanı seviyesine erişim yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınması önerilir.		Seçilen iş uygulamasının çalışma mantığına ve veritabanı sistemi ile olan etkileşimine, veritabanı sistemi seviyesindeki son kullanıcı hesabı sayısına, veritabanı seviyesine erişim yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen

Uygulama Seviyesi Değerlendirme	Risk	Düşük Risk (URP < 40)	Orta Risk (40 < URP < 70)	Yüksek Risk (70 < URP)
				programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınır.
Ağ Bileşenleri		Seçilen iş uygulaması ve buna bağlı sunucu ve veritabanı sistemlerinin ağ üzerinden etkileşimine, veri alışveriş yöntemlerine, ağ seviyesi üzerinden ilgili sistemlere doğrudan son kullanıcı erişimi erişim olup olmamasına bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınabilir.	Seçilen iş uygulaması ve buna bağlı sunucu ve veritabanı sistemlerinin ağ üzerinden etkileşimine, veri alışveriş yöntemlerine, ağ seviyesi üzerinden ilgili sistemlere doğrudan son kullanıcı erişimi erişim olup olmamasına bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınması önerilir.	Seçilen iş uygulaması ve buna bağlı sunucu ve veritabanı sistemlerinin ağ üzerinden etkileşimine, veri alışveriş yöntemlerine, ağ seviyesi üzerinden ilgili sistemlere doğrudan son kullanıcı erişimi erişim olup olmamasına bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımları kapsama alınır.

Güvenlik Denetimi Kapsamında Yürütülecek BT Denetimi Kapsamı

Güvenlik denetimi kapsamında Kurum Seviyesi Risk Değerlendirme ve Uygulama Risk Değerlendirme sonuçlarına yürütülebilecek denetim çalışmaları için göre belirlenebilecek kapsama ilişkin yönlendirme aşağıda belirtilmiştir.

Kurum Seviyesi Risk Değerlendirme	Düşük Risk (KRP < 40)	Orta Risk (40 < KRP < 70)	Yüksek Risk (70 < KRP)
BT Kurum Seviyesi Kontrolleri	Kapsamda	Kapsamda	Kapsamda
BT Yönetişim Kontrolleri	Güvenlik ile ilgili denetim adımları kapsama alınır	Güvenlik ile ilgili denetim adımları kapsama alınır	Güvenlik ile ilgili denetim adımları kapsama alınır
BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup	<ul style="list-style-type: none"> Güvenlik Hizmetleri Yönetimi sürecinin tüm denetim adımları kapsama alınır Diğer süreçlerde bulunan denetim adımları arasında kurum güvenlik süreçleri ile ilgili düşünülenler kapsama alınabilir 	<ul style="list-style-type: none"> Güvenlik Hizmetleri Yönetimi sürecinin tüm denetim adımları kapsama alınır Diğer süreçlerde bulunan denetim adımları arasında kurum güvenlik süreçleri ile ilgili düşünülenlerin kapsama alınması önerilir 	
BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 2. Grup	Denetlenen kurumun faaliyetleri ile denetim dönemi içinde sistem değişikliği olup olmadığına bağlı olarak ve denetlenen kurumdaki güvenlik faaliyetleri uyarınca süreçlerdeki ilgili denetim adımları seçilebilir	Denetlenen kurumun faaliyetleri ile denetim dönemi içinde sistem değişikliği olup olmadığına bağlı olarak ve denetlenen kurumdaki güvenlik faaliyetleri uyarınca süreçlerdeki ilgili denetim adımlarının seçilmesi önerilir	

Uygulama Seviyesi Değerlendirme	Risk	Düşük Risk (URP < 40)	Orta Risk (40 < URP < 70)	Yüksek Risk (70 < URP)
İş Uygulamaları		BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen Zorunlu denetim adımlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır. Buna ilave olarak 1. Grup içinde Seçime Bağlı olarak belirtilen denetim adımları da kapsama alınabilir.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim adımlarının tümü ve 2. Grup içinde belirtilen denetim adımlarından Zorunlu olanlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır. Buna ilave olarak 2. Grup içinde Seçime Bağlı olarak belirtilen denetim adımlarının da kapsama alınması önerilir.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim adımlarının tümü ve 2. Grup içinde belirtilen tüm denetim adımlarının ilgili iş uygulaması üzerinde yürütülebilecek olanları kapsama alınır.
İşletim/Sunucu Sistemleri		Seçilen iş uygulamasının çalışma mantığına ve sunucu sistemi ile olan etkileşimine, sunucu sistemi seviyesindeki son kullanıcı hesabı sayısına ve sunucu sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin tüm denetim adımları kapsama alınır.		
Veritabanı Sistemleri		Seçilen iş uygulamasının çalışma mantığına ve veritabanı sistemi ile olan etkileşimine, veritabanı sistemi seviyesindeki son kullanıcı hesabı sayısına, veritabanı seviyesine erişim yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin tüm denetim adımları kapsama alınır.		
Ağ Bileşenleri		Seçilen iş uygulaması ve buna bağlı sunucu ve veritabanı sistemlerinin ağ üzerinden etkileşimine, veri alışveriş yöntemlerine, ağ seviyesi üzerinden ilgili sistemlere doğrudan son kullanıcı erişimi erişim olup olmamasına bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim adımlarının tümü kapsama alınabilir.		

2.2.5. Denetim Planının Hazırlanması

Denetim Planının Hazırlanmasına İlişkin Esaslar

Bilgi sistemleri denetimi öncesinde denetimin amaçlarını karşılayacak, denetim stratejisine uygun, denetim boyunca kişi ve kurumların yükleneceği sorumlulukları dikkate alan, bağımsızlık ilkesi, yasal yükümlülük ve uluslar arası denetim standartları ile uyumlu, denetlenen kurum ve denetçinin üzerinde mutabık kaldığı bir denetim planı oluşturulmalıdır. Denetim planı oluşturulmadan önce denetlenecek alanlar, denetim stratejisi, denetim alanları ve kısıtlar gibi konuların belirlenmiş olması gerekmektedir.

Ön araştırma bölümünde detaylı şekilde anlatıldığı üzere denetim planının hazırlanması amacıyla Kurum bünyesinde var olan BT süreçleri, BT tarafından üretilen bilgi, BT uygulamaları, BT altyapısı ve çalışanları detaylı bir şekilde irdelenmelidir. Bunun yanı sıra, denetçinin yaklaşımına katkı sağlaması açısından kurum bünyesindeki mevcut iç kontrol faaliyetleri üst seviyede de olsa analiz edilmelidir.

Denetim planı oluşturulurken, denetlenecek kurumun kullandığı teknolojik altyapı ve içerisinde bulunduğu ortamın yanı sıra denetime ve diğer dış etkenlere bağlı oluşabilecek ek sorumluluk ve görevler de göz önünde bulundurulmalıdır. Bununla birlikte denetim planı; denetim sırasında ortaya çıkabilecek riskleri, hatalı varsayımları ya da o ana kadar tamamlanan denetim adımlarındaki hatalı tespitler sonucu doğan düzeltme gereksinimlerini de karşılayabilecek esneklikte oluşturulmalıdır. Diğer bir deyişle, önemlilik değerlendirmesi profesyonel bir bakış açısı ve tecrübe gerektirir.

Denetim süresince denetim çalışmalarına girdi sağlayacak doküman ve veriler analiz edilip, denetim süresince beklenen çıktılar bu aşamada belirlenmelidir. Değerlendirme sonucu bu girdi ve çıktılarından önemli olanlar denetim kapsamına alınır. Bu adımlar sonucunda bilgi sistemleri uygulamaları ve süreçleri; bu uygulama ve süreçlere dayanan hizmetler, veri akışı ve bilgilerin önemliliği kurum ve BT hedefleri çerçevesinde değerlendirilerek kapsama alınır.

Oluşturulacak denetim planı genel itibariyle Kamu İç Denetim Rehberi'nde belirtilen prensipler göz önünde tutularak hazırlanır. Denetim planı kurum bünyesinde devam eden faaliyetler, risk değerlendirme sonuçları ve önceki denetim sonuçlarına göre en azından yıllık olarak güncellenmelidir.

Denetim Stratejisinin Oluşturulması

Denetim kapsamının belirlenmesini takiben kurum içinde gerçekleştirilecek denetim çalışması için bir Denetim Stratejisi oluşturulur. Denetim stratejisi genel olarak denetimin hedefi ve amacı, buna ilişkin olarak seçilen denetim alanı, denetim zaman planı ve kapsamını içerir. Bunların yanında Denetim Stratejisi içinde aşağıda belirtilen konular tartışılır ve gerekli olduğu ölçüde değerlendirilir:

- Kurum bünyesinde bir önceki denetimden bu yana gerçekleşen değişiklikler, ilgili faaliyet alanını etkileyen düzenlemeler ve olaylar
- Bilgi toplama ve BT ortamının anlaşılması aşamasında gözlemlenen önemli hususlar
- Kurumun mali ve iş faaliyetleri ile ilgili bilinmesi gereken konular
- Önceki dönemlerden devam eden açık bulguların ya da risklerin yaratacağı etkiler
- Denetim stratejisine etki edebileceği düşünülen diğer konular

Denetim stratejisi hazırlandıktan sonra kurum İç Denetim Başkanlığı tarafından onaylanır ve tüm denetim ekibi ile paylaşılır.

Denetim Programının Oluşturulması

Denetim stratejisinin de belli olması ile birlikte yürütülecek denetim çalışmalarına ilişkin bir program hazırlanır. Denetim programı denetimi yürütecek olan iç denetçilerin denetim sırasında kendilerine atanmış olan çalışma alanları, bunlara ilişkin çalışma zamanları, çalışmalar sonucunda üretmeleri gereken sonuçlara ilişkin beklentiler gibi hususları düzenler.

Denetim programı temel olarak şu konuları içermelidir:

- Denetlenecek konuların denetim ekibindeki personelin yetkinlik, bilgi ve tecrübe seviyelerine göre ilgili personele dağıtımı
- Denetim sırasında yürütülecek her bir denetim çalışması için öngörülen süre (ör: adam-gün ya da adam-saat birimleri üzerinden)
- Denetim çalışmaları sonucunda denetçilerden beklenen çıktılar
- Denetim çalışmaları sırasında denetlenen birimden denetçilere yardımcı olacak personelin (mümkünse) isim, soyisim ve iletişim bilgileri
- Denetim raporlarının ve ilgili takip çalışmalarına ilişkin zaman planı

Denetim programının hazırlanması, onaylanması ve paylaşılması, Kamu İç Denetim Rehberi'nde belirtilen usul ve esaslar çerçevesinde gerçekleştirilir.

2.3. Yürütme

2.3.1. Kontrollerin Değerlendirilmesi

Ön Bilgi

Denetim çalışmalarının kapsamının belirlenmesi sırasında denetim tipine göre zorunlu ve zorunlu olmayan alanların seçimi ve uygulamasıyla ilgili yönlendirmelere yukarıda, Kapsam Belirleme bölümü içerisinde yer verilmiştir.

BT denetim çalışmaları;

- BT Kurum Seviyesi Kontrolleri ve BT Yönetişim Kontrolleri Denetimi
- BT Yönetim Süreçlerinin Denetimi
- Uygulama Kontrolleri Denetimi
- Bilgi Güvenliği Teknik Kontrolleri Denetimi

olmak üzere temelde dört katmanda değerlendirilmektedir.

Yukarıda belirtilen katmanların detaylı açıklamaları ve bunlara ilişkin detaylı denetim adımları, rehberin sonraki bölümlerinde aktarılmıştır. Bu bölümlerin nasıl ele alınabileceği ve kullanılabilirliği aşağıda belirtilmiştir.

Anahtar Kontrollerin Tespit Edilmesi

Anahtar kontroller, Kamu İç Denetim Rehberi'nde de belirtildiği üzere, süreç içinde tasarlandığı şekilde çalışmayan ya da etkin bir şekilde işletilmediği durumlarda ilgili faaliyetin ya da sürecin sekteye uğraması ya da mali kayıpların oluşması gibi sonuçlara yol açabilecek kontrollerdir. Anahtar kontroller etkin bir şekilde işletildiğinde sürece ait risklerin önemli bir bölümünü giderecek özelliklere sahiptir. Bu nedenle, rehber içinde verilmiş kontrollerden hangilerinin denetlenen kurum bünyesinde diğerlerinden daha kritik işleve ve daha fazla risk azaltıcı etkiye sahip olduğunun tespit edilmesi, denetim çalışmaları sırasında gerekli eforun verimli ve etkin bir şekilde planlanmasına ve harcanmasına yardımcı olacaktır.

Denetçi, kurum faaliyet, süreç ve BT ortamını anladıktan ve rehber içinde belirtilen kontrolden hangilerinin kurum içinde uygulandığını tespit ettikten sonra bu kontroller içinden anahtar kontrolleri ayırıştırıp önceliği bu kontrollerin denetlenmesine vermelidir. Bu anlamda rehber içinde ilerleyen bölümlerde denetim adımları içinde Zorunlu olarak belirtilmiş denetim adımlarına sahip kontrollerin öncelikle ele alınması ve değerlendirilmesi denetçiye yardımcı olacaktır.

Tasarım Etkinliğinin Değerlendirilmesi

Denetim yürütülmesi sırasında kullanılan denetim tekniklerinden olan tasarımın değerlendirilmesi ya da "Üzerinden Gitme veya İz Süre, örneklem seçimi ve uygulamanın değerlendirilmesi adımları genel itibarıyla Kamu İç Denetim Rehberi'nde belirtildiği şekliyle kullanılacaktır.

Tasarımın Değerlendirilmesi / Üzerinden Gitme / İz Sürme: Herhangi bir kontrolün, tasarım etkinliği ve yeterliliği açısından ilgili olduğu riskleri karşılayıp karşılamadığı değerlendirilir ve rasgele seçilecek tek bir örnek işlem üzerinden kontrolün denetime tabi tutulmasıdır. Bu değerlendirme sırasında ayrıca Kamu İç Denetim Rehberi'nde de bulunan ve aşağıda verilmiş olan sorulardan da faydalanılabilir:

- Kontrol, hata veya usulsüzlüklerin ortaya çıkma olasılığını yeterli düzeyde azaltmakta mıdır?
- Kontrol, ilgili olduğu riskin gerçekleşmesi halinde etkilerini en aza indirmekte midir?
- Kontrol, hata veya usulsüzlüklerin ortaya çıkması halinde bunları tespit edebilmekte midir?
- Kontrol, süreç içerisinde doğru aşamada mı yer almaktadır?
- Kontrolün uygulanma sıklığı doğru belirlenmiş midir?

Rehber içinde verilmiş olan denetim prosedürleri içerisinde verilmiş olan kontrollere ilişkin denetim adımlarının bir kısmı ilgili kontrolün tasarım etkinliğinin değerlendirilmesine yönelik hazırlanmış olup (T) harfiyle belirtilerek ayırıştırılmıştır.

Kontrol tasarımının etkinliği ve yeterliliği üzerinde olumlu bir sonuca varıldığında, ilgili kontrolün denetim dönemi boyunca tasarlandığı haliyle işletilip işletilmediğinin belirlenmesi, bir başka deyişle "test" edilmesi gerekir.

Örnekleme Seçimi

Denetim çalışmaları sırasında denetçinin kurum BT ortamında ilgili süreçlerde, uygulamalarda ya sistemlerde oluşan tüm işlem ya da kayıtları incelemesine gerek yoktur. Uygun yöntemlerle seçilecek yeterli sayıda kaydın ya da işlemin incelenmesi makul bir güvence oluşturmak açısından yeterli olacaktır.

Örnekleme seçimi, kontrol tasarımının etkin ve yeterli görüldüğü durumda söz konusu kontrolün tüm denetim dönemi boyunca tasarlandığı haliyle işletildiği ile ilgili makul bir güvence almak üzere test çalışmasına tabi tutulacak örnek işlem ve kayıtların seçimini ifade eder.

Örnekleme seçimi, Kamu İç Denetim Rehberi'nde de belirtildiği gibi istatistiki ya da istatistiki olmayan yöntemler kullanılarak, ilgili kontrole ilişkin denetim dönemi boyunca oluşmuş kayıt, belge ve diğer çıktılarının tamamı üzerinden (denetçinin hakkında kanata varmayı istediği veri topluluğu, ana kütle) belirli bir sayıda rasgele örnek seçimi ile gerçekleştirilir. İstatistiki ve istatistiki olmayan örnekleme yöntemlerine ilişkin detay bilgi Kamu İç Denetim Rehberi'nden alınabilir.

Seçilecek örnek sayısı aşağıdaki hususlara bağlıdır:

- Kontrolün gerçekleştirilme sıklığı (frekans) – Örnek: Aylık, haftalık, vb.
- Ana kütle boyutu / Örneklem popülasyonu (uzayı) – İçinden örnek seçilecek kayıt, belge ve diğer çıktılarının toplam sayısını ve hacmini belirtir.

Örnekleme sayısının belirlenmesi amacıyla Kamu İç Denetim Rehberi'nde de verilmiş olan aşağıdaki tablo kullanılabilir.

Tablo 2.1 – Örnekleme Belirleme		
Kontrol Sıklığı	Asgari Örnek Büyüklüğü	
	Risk Düzeyi	
	Düşük	Yüksek
Yılda bir	1	1
Aylık	2	3
Haftalık	5	8
Günlük	15	25
İşlem bazında	25	40

Tablodan da görüldüğü üzere denetçi, riskli gördüğü alanlara ilişkin kontrollerin denetimi sırasında örnek sayısında artış yapabilir. Seçilen örnekler içinde hatalara ya da istisnalara rastlanması durumunda da denetçi benzer bir yaklaşımla daha fazla örnek seçerek ilgili kontrole dair güvence seviyesini artırma yoluna gidebilir.

Örnekleme seçimi ile ilgili alternatif yöntemlere Kamu İç Denetim Rehberi'nde yer verilmiştir. Kısaca bahsetmek gerekirse bu yöntemlerden en çok kullanılanı ve istatistiki olarak makul güvence vermeye aday yöntem, bir rasgele sayı üretici vasıtasıyla yapılacak “rassal” seçimdir. Bu yöntemde, ana kütle içinde her

bir kayıta bir numara verilir. Bilgisayar üzerinde çalıştırılabilecek bir rasgele sayı üretici aracı vasıtasıyla ana kütle sayısı ile sınırlı olmak koşulu ile örneklem büyüklüğü (ör: günlük kontrol sıklığı için 15) kadar rassal sayı üretilir. Üretilen rassal sayılara karşılık gelen örneklem birimi ayrıştırılarak denetime tabi tutulur.

İşletim Etkinliğinin Değerlendirilmesi

Tasarımının etkin ve yeterli olduğu değerlendirilen kontrollerin, kontrole ilişkin tüm denetim boyunca oluşmuş kayıt, belge ve diğer çıktılar üzerinden örneklem yoluyla seçilenleri üzerinde, kontrolün unsurlarının aranması ve teyit edilmesi aşamasıdır. Buna ek olarak Test çalışmalarının diğer amaçları Kamu İç Denetim Rehberi'nde belirtildiği üzere şu şekilde özetlenebilir:

- Bir taşınır malın var olup olmadığının belirlenmesi (veya bir işin yapılıp yapılmadığının belirlenmesi) ise, uygulanacak test, taşınır malın var olup olmadığının (veya işin yapılıp yapılmadığının) gözlemlenmesidir.
- Bir rapordaki bilgilerin doğruluğunun araştırılması ise, uygulanacak test, bu bilgilerin dayandığı kaynakların belirlenerek doğrulanmasıdır.

Test sonucunda incelenen örnekler üzerinde olumlu bir sonuca varılması, ilgili kontrolün denetim dönemi boyunca tasarlandığı şekliyle işletildiğine dair makul bir güvence sunmaktadır.

Bu kapsamda, kanıt ve bilgi toplanmasında kullanılan yöntemlerden (yeniden hesaplama, gözlem, doğrulama, görüşme, evrak inceleme, yerinde gözlem, analitik inceleme ve araştırma gibi) en uygun olanları kullanılır ve uygulanır.

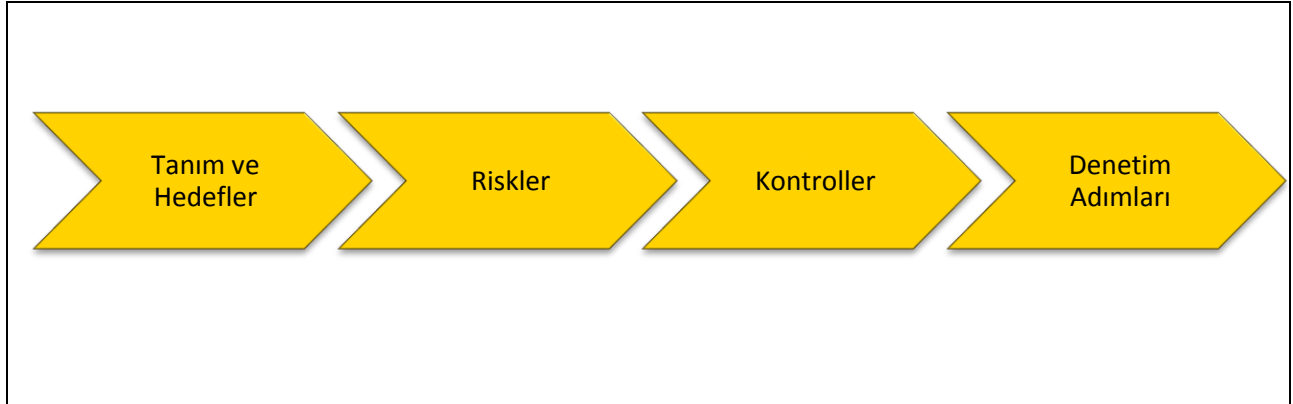
Rehber içinde verilmiş olan denetim prosedürleri içerisinde verilmiş olan kontrollere ilişkin denetim adımlarının bir kısmı ilgili kontrolün işletim etkinliğinin değerlendirilmesine yönelik hazırlanmış olup (İ) harfiyle belirtilerek ayrıştırılmıştır.

Standart Denetim Prosedürlerinin Kullanılması

BT Kurum Seviyesi Kontrolleri ve BT Yönetişim Kontrolleri Denetimi

Denetim tipine bağlı olarak risk değerlendirme ve kapsam belirleme sonuçlarına göre seçilecek olan BT Kurum Seviyesi Kontrolleri ve/veya BT Yönetişim Kontrolleri'ne ilişkin denetim adımları, rehberin üçüncü bölümünde verilmiş olup, belirtilen kontrollere ilişkin detay denetim adımlarının hepsi zorunlu kılınmıştır. Bu bölümde gerek BT Kurum Seviyesi Kontrolleri gerekse de BT Yönetişim Kontrolleri için verilmiş olan denetim adımlarına ilişkin akış şu şekildedir:

Şekil 2.5 – BT Kurum Seviyesi Kontrolleri ve BT Yönetişim Kontrolleri Denetimi İçin Denetim Prosedürlerinin Akışı



BT Genel Kontrollerinin (Yönetim Süreçlerinin) Denetimi

BT Yönetim Süreçleri denetimine ilişkin bilgiler rehber içinde dördüncü bölümde iki gruba ayrılarak verilmiştir. Birinci ve ikinci grupta verilmiş olan BT yönetim süreçleri ve bunların içinde verilmiş olan detay denetim adımlarından hangilerinin denetim sırasında ele alınacağı, kurum bünyesinde seçilecek olan denetim tipi uyarınca ve risk değerlendirme sonuçlarına göre karar verilecektir. Rehber içinde birinci grup süreçler denetim tipinden bağımsız, her BT denetimi sırasında kapsama alınmasında fayda görülen süreçler olarak değerlendirilmiş olup, ikinci grup süreçler denetim tipi ve risk değerlendirme sonuçlarına ilave olarak denetlenen kurumun BT ortamının karmaşıklığına, kontrol ortamının genel olgunluk seviyesine ve denetçinin yargısına bağlı olarak denetime tabi tutulabilir.

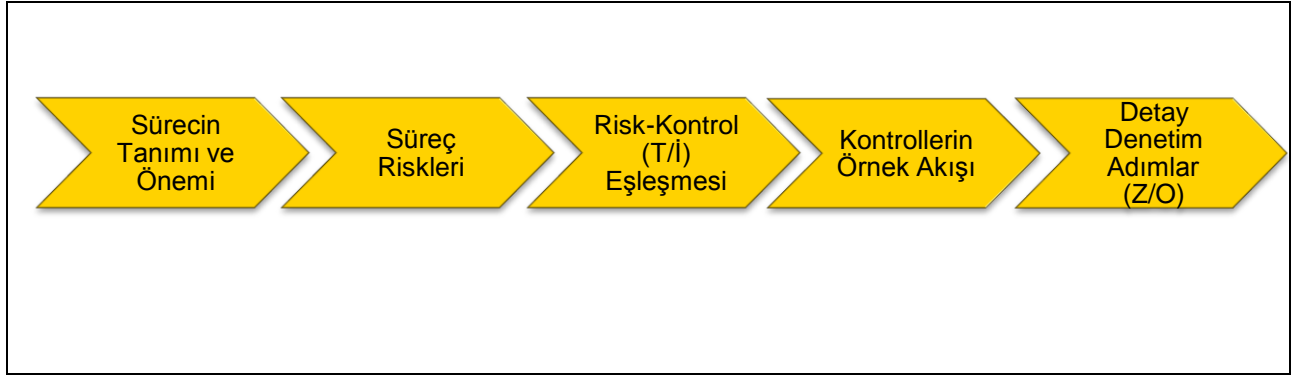
Seçilecek süreçlerde Zorunlu olarak ifade edilen denetim adımlarının uygulanması zorunludur. Seçime Bağlı olarak belirtilen denetim adımlarının uygulanması ise, denetlenen kurumun yapısına, denetçinin profesyonel yargısına ve kurum ile ilgili risk algısına göre ele alınabilecektir.

BT Yönetim Süreçleri denetimine ilişkin akışa rehberin dördüncü bölümünde yer verilmiştir. Buna göre her bir süreç için:

- Sürecin tanımı ve BT denetimi açısından önemi
- Sürecin riskleri
- Süreç risklerine karşılık gelecek şekilde hazırlanmış Tasarım (T) ve İşletim'e (İ) yönelik kontroller
- Her bir kontrol için Zorunlu ve Seçime Bağlı detay denetim adımları
- Sürecin ve kontrollerin gösterildiği örnek bir akış şeması

verilmiştir. Söz konusu akış aşağıdaki şekilde de gösterilebilir.

Şekil 2.6 – BT Yönetim Süreçleri Denetimi İçin Denetim Prosedürlerinin Akışı



Uygulama Kontrolleri Denetimi

Uygulama kontrollerinin denetiminde gündeme gelebilecek uygulama kontrolleri tipleri ve bunlara ilişkin örnek kontrollere rehberin beşinci bölümünde yer verilmiştir. Bununla birlikte gerek faaliyet alanı ve iş süreçlerindeki gerekse de BT uygulama altyapısının karmaşıklık seviyelerinde farklılıklar sebebiyle uygulama kontrolleri kurumdan kuruma farklılaşabilir ve her kurum için ortak denetim adımlarının oluşturulmasının mümkün olamayabilir. Bu nedenle kurum içindeki uygulama kontrollerinin denetçi tarafından tespit edilebilmesi amacıyla aşağıdaki konuların anlaşılması önem arz etmektedir:

- Denetim hedefi ve denetim alanı göz önünde bulundurularak kurumun faaliyet alanı ve iş süreçlerinde oluşabilecek risklerin ya da yaşanması muhtemelen aksaklıkların ortaya konması
- Belirlenen riskler ve yaşanması muhtemel hataların önlenmesi ya da tespit edilebilmesi adına ilgili faaliyet alanı ve iş sürecini destekleyen iş uygulamaları üzerinde bulunması öngörülen otomatik ya da yarı-otomatik kontrollerin listesinin çıkarılması
- Söz konusu otomatik ya da yarı-otomatik kontrollerinin hangilerinin mevcut durumda ilgili iş uygulaması üzerinde bulunduğu anlaşılması

Yukarıda belirtilen hususların tamamlanmasını takiben denetçi her bir uygulama kontrolü için rehberin beşinci bölümünde belirtilen yönlendirmeler ışığında denetim çalışmalarını gerçekleştirir ve sonuçlarını değerlendirir.

BT Altyapı Genel Kontrolleri Denetimi

Uygulama risk değerlendirmesi sonucu kapsama alınan uygulamalar ve teknoloji envanterinde belirtildiği üzere bu uygulamaların üzerinde çalıştığı ve kullandığı altyapı bileşenleri üzerinde yürütülebilecek denetim adımları rehberin altıncı bölümünde belirtilmiştir.

BT Altyapı Genel Kontrolleri denetimin uygulama alanı ve gerçekleştirilecek risk değerlendirme sonuçlarına bağlı olarak kapsama alınan uygulamalar üzerinde gerçekleştirilen denetim çalışmalarının altyapı seviyesine de uygulanması gereken durumlarda ele alınabilecek ve özellikle güvenlik odaklı bakış açısına sahip nitelikte kontrollerdir. Kapsama alınan uygulamalar üzerinde gerçekleştirilen çalışmaları

destekleyecek ve bu uygulamalar üzerine verilecek güvence seviyesine destek olunması amacıyla kullanılabilir.

BT Altyapı Genel Kontrolleri sunucu/işletim sistemleri, veritabanı sistemleri ve/veya ağ bileşenleri üzerinde uygulanacak şekilde sınıflandırılmış olup denetim uygulama alanı, uygulama risk değerlendirme sonuçları, kapsama alınan uygulamaların kurum içi önem ve kritikliği ve karmaşıklığına bağlı olarak tüm seviyeleri (işletim sistemi, veritabanı, ağ) ele alınabileceği gibi, denetçinin yargısına ve risk algısına bağlı olarak belirli seviyeler ya da seçilen seviyelerden belirli kontroller denetim kapsamına alınabilir.

Rehberin altıncı bölümünde verilmiş olan BT Altyapı Genel Kontrolleri'nin bir kısmı, kurumlarda en çok karşılaşılabilecek platformlar (ör: Windows, UNIX, Oracle, MS SQL) bazında verilmiş olup, kurum bünyesinde bunlar haricinde farklı bir üretici tarafından geliştirilmiş olan bir platform varsa, ilgili üreticinin konfigürasyon, güvenlik ve/veya denetim kılavuzlarından bilgi alınabilir.

Denetim prosedürlerini gerçekleştirecek olan denetçi, öncelikle rehberde açıklanmış olan ilgili sürecin tanımını ve kontrol hedeflerini anlamalıdır. Buna ek olarak örnek kontrol akışını incelenmesi, kontrol akışının bir kurumda nasıl işleyebileceğinin anlamak açısından yardımcı olacaktır. Akışın ardından süreçle ilgili riskler ve bu risklerin etkin bir şekilde yanıtladığının kontrolünü sağlayan kontroller tablo halinde riskler kısmında listelenmektedir. Bu tabloda, seçilen belirli risklere karşı gelecek kontroller bulunabilir. Devam kısmında ise bu kontroller incelenir ve etkinliğini değerlendirmek üzere tasarlanmış olan detay denetim adımları uygulanır.

Denetim adımlarının uygulama zorunluluğu “Zorunlu” ve “Seçime bağlı” olarak ikiye ayrılmaktadır. İlgili kontrolün etkinliği hakkında bir kanaate ulaşılabilmesi için zorunlu adımların uygulanması gerekmektedir. Risk değerlendirme sonuçlarına bağlı olarak kontrolün etkinliği hakkında daha geniş bilgi sahibi olmak ya da denetim hedefleri doğrultusunda daha derinlemesine bir BT denetiminin yürütülmesi için “Seçime bağlı” olarak işaretlenmiş denetim adımları da uygulanabilir.

Çalışma Kağıtlarının Kullanımı

Denetim çalışmalarının belgelendirdiği en önemli araç çalışma kağıtlarıdır (bkz: **Ek 5 - Çalışma Kağıdı**). Çalışma kağıtları, form şeklinde ve denetçi tarafından doldurulmak üzere hazırlanmıştır.

Çalışma kağıdının ilk sütunu denetlenen süreci (değişiklik yönetimi, operasyon yönetimi v.b) belirtir. İkinci sütunda denetlenen süreçle ilgili olarak test edilecek kontrol yazılır. Burada belirtilen kontroller, “Bölüm 4: Bilgi Teknolojileri Yönetim Süreçleri Denetimi” bölümünde belirtilen kontrollerdir. Devam eden sütunlarda denetim adımının numarası ve kontrolün gerçekleştirme frekansı/sıklığı belirtilir.

Üzerinden gitme (ÜG) çalışmaları ilgili sütunda gerçekleştiren kişinin ismi, gerçekleştirilen tarih, örneklem popülasyonu, seçilen örnek sayısı, açıklama ve kanıt numarası/referansı belirtilecek şekilde belgelenir. Gerçekleştirilen test çalışması yine aynı ÜG için yapıldığı şekilde belgelenir.

Denetlenen kontrolün ardından belirlenen sonuç “ÜG Etkin / Test Etkin”, “ÜG Etkin / Test Etkin Değil” veya “ÜG Etkin Değil” şeklinde işaretlenir ve çalışma sonucunda eğer bir bulgu tespiti söz konusu ise, “Bulgu” sütununa açık şekilde yazılır.

Çalışma kağıtlarında belirtilen kontroller ve yürütülen çalışmalar ilgili yöneticiler tarafından gözden geçirilir ve yöneticinin ismi ve gözden geçirme tarihi “Gözden Geçirme” sütununa yazılır.

2.3.2. Bulguların Değerlendirilmesi

Denetim çalışmaları kapsamına alınan süreçler, uygulamalar ve diğer unsurlar üzerinde yürütülen çalışmalar sonucunda kontrollerin tasarımı ya da işletimine dair tespit edilen aksaklık, istisna ya da uyumsuzluklar, bulgu olarak nitelendirilebilir. Kamu İç Denetim Rehberi’nde belirtildiği üzere, herhangi bir aksaklığın ya da uyumsuzluğun bulgu olarak nitelendirilebilmesi için konu ile ilgili alınan bilgi, belge ve kanıtların denetçi tarafından değerlendirilmesi ve analiz edilmesi ve olumsuz bir kanata varılması gerekmektedir.

Denetçi, değerlendirme ve analizler sonucunda olumlu ve olumsuz bir sonuca ulaşamıyorsa ya daha fazla örnek sayısı inceleyerek ya da gerekli tüm bilgi ve belgelerin eksiksiz elde edilip incelendiğinden emin olarak söz konusu durumu bertaraf etmeye çalışmalıdır.

Bulguların hazırlanması sırasında aynı kontrol hedefine ait hususlar ya da birbirleriyle benzerlik ve bütünlük arzeden konular mümkün mertebe birleştirilmeye çalışılır.

Hazırlanmış olan bulgu, denetlenen birim tarafından okunduğunda bulgunun içeriği, nedeni, bulgunun yaratabileceği riskleri net ve bir şekilde anlaşılacak şekilde basit bir dile sahip olmalı ve ek bir bilgiye ya da belgeye ihtiyaç duyulmadan bulgu hakkında fikir sahibi olunacak şekilde gerekli tüm detayları içermeli ve tarafsız (objektif) bir şekilde ifade edilmelidir.

Bulguların sunumu sırasında tespit edilen hususların önem derecesine göre hazırlanmış olması, denetlenen birim tarafından yürütülecek düzeltici ve önleyici faaliyetlerin hangi alanlarda önceliklendirilmesi gerektiği konusunda yardımcı olacaktır. Bu anlamda bulguların değerlendirilmesi sırasında belirli bir ölçeklendirme yöntemine göre sınıflandırılması gerekebilir. Söz konusu sınıflandırma için Kamu İç Denetim Rehberi’nde verilmiş olan bulgu önem düzey tablosu kullanılabilir.

Bulgu Önem Düzeyi	Açıklama
--------------------------	-----------------

Kritik	Faaliyetin yürütülmesini veya istenilen çıktı, ürün ya da hizmetin sunulmasını engelleyecek tüm bulgular bu grupta değerlendirilir. Risk ve etkileri değerlendirildiğinde, can kayıplarına veya bedensel bütünlüğe zarar vermesi ya da kurumun faaliyetlerini durdurması veya büyük mali kayıplara neden olacak bulgulardır.
Yüksek	Faaliyetin yürütülmesinde uzun süreli gecikmelere ve ciddi sorunlara neden olabilecek bulgular bu grupta değerlendirilir. Risk ve etkileri değerlendirildiğinde, kurum faaliyetlerini sekteye uğratabilecek veya kurumun önemli mali kayıplarla karşılaşmasına neden olacak bulgulardır.
Orta	Faaliyetin çıktılarının kalitesini etkileyen, yürütülmesinde gecikmelere ve sorunlara neden olabilecek bulgular bu grupta değerlendirilir.
Düşük	Faaliyetin genel işleyişini etkilemeyen ancak daha iyi bir hizmet sunulmasını sağlamaya yönelik bulgular bu grupta değerlendirilir.

Bulguların hazırlanması sırasında Kamu İç Denetim Rehberi'nde belirtildiği üzere, bulgulara ait aşağıdaki hususlar kayıt altına alınmalıdır:

- Bulguya ilişkin mevcut durum,
- Bulgunun sebebi / kök nedeni,
- Bulguya ilişkin risk ve etkiler,
- Kriter (ör: mevzuat, kurum içi düzenlemeler, Kamu İç Kontrol Standartları, Stratejik Plan, Uluslar arası genel kabul görmüş standartlar ve Ulusal ya da uluslar arası iyi uygulamalar)

Bulguların kayıt altına alınması ve takip edilmesi amacıyla hazırlanmış olan bulgu takip formu Ek 6 – Bulgu Takip Formu olarak sunulmuştur.

2.4. Raporlama ve izleme

2.4.1. Taslak Raporun hazırlanması ve sunumu

Gerçekleştirilen denetim çalışmaları neticesinde denetçi tarafından yapılan tespitler ve denetçi görüşü, tam, nesnel (objektif) ve anlaşılır olarak raporlanmalıdır.

Denetim sonuçlarının denetlenen birim ile paylaşılması öncelikle düzenlenecek olan kapanış toplantısı aracılığıyla taslak rapor üzerinden gerçekleşir. Kapanış toplantısı denetlenen birim yöneticileri ve sorumluları ile gerçekleştirilir. Bu toplantıda taslak bulgular denetlenen birimle paylaşılır, bulgulara dair öneriler sunulur ve denetlenen birimin bulgular için ne gibi düzeltici ya da önleyici aksiyonlar alacağı hakkında görüşleri alınır.

Raporun öncelikle taslak olarak sunulmasının sebebi gerek denetçi tarafından gözden kaçırılan bilgi, belge ve kanıtlar sebebiyle gerekse de denetlenen birim tarafından zamanında denetçiye iletilmemiş ek bilgiler ya da belgeler sebenu ile bulgu olarak nitelendirilmemesi gerekirken bulgu olarak belirtilen hususların tespit edilmesi ve buna istinaden yapılabilecek güncellemeler sonrasında denetçi ve denetlenenin bulgular üzerinde mutabakata varmasına izin vermesidir.

Kapanış toplantısında denetçi, tespitlerin tamlığı ve doğruluğunu denetlenen ile teyit eder ve bulgu önerileri için düzeltici faaliyetlerin tamamlanma tarihlerinin belirlenmesine destek olur.

Bu aşamada denetim sonuçlarıyla ilgili hata ya da eksikler tespit edilirse, denetçi tarafından ek prosedürler uygulanarak tespitlerde düzeltme ve güncelleme yapılabilir.

Bulgular üzerinde denetçi ile denetlenen arasında bir uyumsuzluk olduğunda Kamu İ Denetim Rehberi'nde verilmiş olan karar mekanizması kullanılabilir.

TASLAK

Tablo 2.3 Bulgu İçeriği

Denetlenen Birim	İç Denetim Birimi	Üst Yönetici		Bulgunun Durumu
Bulguya katılıyor.	----->			Raporda yer verilir.
Bulguya katılmıyor. (Düzeltilemez husus)	Denetlenen birimin görüşüne katılıyor.	----->		Raporda yer verilmez.
Bulguya katılmıyor. (Düzeltilbilir husus)	Denetlenen birimin görüşüne katılıyor.	----->		Düzeltilme yapılarak raporda yer verilir.
Bulguya katılmıyor	Denetlenen birimin görüşüne katılmıyor.	Uzlaşılmayan husus olarak üst yöneticiye aktarılır.	Denetlenen birimin görüşüne katılıyor.	Raporda yer verilmez.
Bulguya katılmıyor	Denetlenen birimin görüşüne katılmıyor.		İDB'nin görüşüne katılıyor.	Eylem planı alınarak raporda yer verilir.

2.4.2. Nihai denetim raporunun hazırlanması ve iletilmesi

Taslak raporda belirtilmiş olan bulgular üzerinde denetlenen birim ile varılan mutabakat sonrasında denetime ilişkin nihai rapor hazır hale getirilir. Denetim raporu içinde bulunması gereken en temel unsurlar, Kamu İç Denetim Rehberi'nde belirtildiği üzere şu şekildedir:

- Denetimin amacı,
- Denetimin kapsamı,
- Denetim yöntemi,
- Tespitler (mevcut durum),
- Uygulanabilir öneriler,
- Eylem planı,
- Bulgunun önem düzeyi, ve
- İyi uygulamalar ve başarılı performans.

Denetim raporu, aşağıda belirtilmiş olan konuların ele alınmasıyla tamamlanmış olur:

- Amaç olarak yazılan ifadenin, denetim sonucunda ulaşılan durumun ne olduğunu anlatmada yeterli olduğundan emin olunur. Gerektiğinde neden böyle bir denetime ihtiyaç duyulduğu bilgisine de yer verilebilir.
- Kapsam olarak yazılan ifadenin denetlenen birim, faaliyet ve dönemi net bir şekilde ortaya koyduğundan emin olunur. Denetim alanı içinde yer alan ancak kapsam dışı bırakılan birim ya da faaliyetler de belirtilir.

- Yöntem ile ilgili ifadelerin, denetim sırasında kullanılan metodolojiyi tam olarak tanımladığından emin olunur.
- Üzerinde uzlaşma sağlanan bulgulara raporda yer verilir.

Yine Kamu İç Denetim Rehberi'nde belirtildiği üzere, denetim raporu aşağıdaki içerikte sunulmalıdır:

a) Rapor kapağı: Rapor kapağında, İDB'nin adına, denetim adına, denetim alanına, denetimi gerçekleştiren iç denetçilere, DGS'ye, raporun tarih ve numarasına yer verilir.

b) Yönetici özeti: Üst yöneticiye ve denetlenen birim yöneticisine yönelik olarak iki sayfayı geçmeyecek şekilde yönetici özeti hazırlanır. Yönetici özeti bölümünde aşağıdaki hususlara yer verilir;

- Kısaca denetimin amacı ve kapsamı,
- Özet olarak kritik tespit ve öneriler,
- Özet olarak denetlenen süreçle ilgili başarılı performans ve iyi uygulama örnekleri.
- Denetim görüşü.

c) Rapor metni: Rapor metni asgari olarak aşağıdaki hususları içerir;

- Görevin dayanağı denetim plan ve programı ile denetlenen birim ya da süreç hakkında kısa bilgilerin açıklandığı "Giriş" bölümü,
- Denetimin hedefleri ile denetime tabi tutulan dönem, faaliyet ve işlemler ile denetlenen birimleri vb. bilgileri içeren "Amaç ve Kapsam" bölümü
- Denetimde uygulanan teknik ve yöntemlerin açıklandığı "Denetim Yöntemi" bölümü
- Rapora alınmasına lüzum görülen her bir tespit ve öneriyi içeren "Mevcut Durum ve Öneriler" bölümü ile bölüm altında aşağıdaki alt bölümler;
 - Önem derecesine göre sınıflandırılmış şekilde denetim amacı karşısında mevcut durumun ortaya konulduğu "Mevcut Durum" bölümü,
 - Mevcut durumu olması gereken duruma getirmek için alınması gereken tedbir ve eylemleri içeren "Öneriler" bölümü,
 - Denetlenen birimin verdiği cevaplar ile eylem planını içeren "Eylem Planı" bölümü,
- İç denetçinin denetlenen süreçle ilgili iç kontrollerin yeterlilik ve etkinliğine ilişkin değerlendirmesini içeren "Denetim Görüşü" bölümü,
- Denetlenen faaliyet ve süreçle ilgili yaygınlaştırılmasında fayda görülen hususların yer aldığı "Başarılı performans ve iyi uygulama örnekleri" bölümü.

Denetim raporunun gözden geçirilmesi, onaylanması, dağıtım listesinin hazırlanması ve resmi bir şekilde iletilmesi için gerekli yönergeler, Kamu İç Denetim Rehberi'nde belirtilmiştir.

Denetim raporu için kullanılacak şablon Kamu İç Denetim Rehberi'nde verilmiştir.

2.4.3. Kalite-kontrol

Denetim çalışmalarının denetim planına ve hedefine uygun yürütülüp yürütülmediği, buna ilave olarak gerçekleştirilen denetim adımlarının bu rehberde belirtilen hususlar, genel itibariyle Kamu İç Denetim Rehberi'ne ve ilgili olabilecek diğer mevzuat hükümlerine paralel olarak ele alınıp alınmadığının kalite kontrol açısından değerlendirilmesi gerekir. Kalite-kontrol çalışmasının temel amacı denetim sırasında karşılaşılan zorluklar, denetçilerin yaptıkları hatalar ya da denetim sırasında temel alınan rehber ve kılavuzlarda karşılaşılabilecek eksikliklerin zamanında tespit edilebilmesi ve bunlara ilişkin düzeltici önlemlerin alınabilmesine olanak sağlamaktır.

Kalite-kontrol çalışmaları gerçek zamanlı ve tamamlanan her denetim adımından sonra ele alınabileceği gibi, nihai raporun verilmesinden sonra gerçekleştirilebilir.

Kalite kontrol çalışmaları temel olarak aşağıdaki konulara odaklanır:

- Denetim gerçekleştirilecek birim üzerinde gerek BT ortamı, gerekse de BT organizasyonu ile ilgili gerekli bilgi toplama ve anlayış geliştirme faaliyetlerinin uygun bir şekilde yerine getirilip getirilmediği
-
- Gerçekleştirilen denetim alanı uyarınca gerekli risk değerlendirmelerinin doğru bir şekilde tamamlanıp tamamlanmadığı
- Risk değerlendirme sonucu uyarınca denetlenecek denetim kapsamının doğru bir şekilde seçilip seçilmediği
- Önceki dönemlerden devam eden açık bulgu ya da risk alanlarının risk değerlendirmesinde ve kapsam belirlenmesinde göz önünde bulundurulup bulundurulmadığı
- Denetim stratejisinin hazırlanıp hazırlanmadığı
- Denetlenecek birim yönetimi ve ilgili diğer sorumlular ile birlikte bir açılış toplantısının gerçekleştirilip gerçekleştirilmediği
- Risk değerlendirme ve kapsam belirleme sonuçları uyarınca denetlenecek birim bünyesinde gerçekleştirilecek kontrol değerlendirme çalışmaları için anahtar kontrollerin seçiminin yapılıp yapılmadığı
- Denetim çalışmaları sırasında yürütülen çalışmalara ilişkin çalışma kağıtlarının ve ilgili kanıtlara ilişkin belgelerin uygun şekilde hazırlanıp hazırlanmadığı
- Denetim sırasında tespit edilen taslak bulguların bir listesinin oluşturulup oluşturulmadığı
- Tespit edilen taslak bulguların denetlenen birim ile bir kapanış toplantısı vasıtası ile paylaşıp paylaşılmadığı
- Belirtilen tüm bu çalışmalara ilişkin uygun kayıtların ve belgelerin hazırlanıp hazırlanmadığı
- Bu rehber, Kamu İç Denetim Rehberi, ilgili diğer kılavuz ve yönergeler ile denetim stratejisi uyarınca denetim sırasında yerine getirilmesi gereken bir faaliyetin tamamlanamadığı durumlar için ilgili durumun gerekçesi ile birlikte kayıt altına alınıp alınmadığı
-

2.4.4. Denetim sonuçlarının izlenmesi

Denetim çalışması sonucunda denetlenen birim ile mutabık kalınan ve hazırlanmış olan Nihai Rapor eşliğinde belirtilmiş olan bulgulara ilişkin denetlenen birim tarafından verilmiş olan iyileştirici, düzeltici ya da önleyici aksiyon planlarının yine bu aksiyon planlarının tamamlanması için ön görülen tarihler öncesinde tamamlandığı ya da bu tarihe uygun şekilde aksiyonların alındığından emin olunabilmesi adına ilgili bulguların düzenli aralıklarla izlenmesi gerekir.

Söz konusu izleme çalışmaları gerek denetlenen birim ile görüşmeler ve/veya ilgili bulgular için yerinde tekrar denetim çalışmalarının yürütülmesi vasıtası ile yerine getiriliriz. Bu çalışmalar sonrasında gerekli aksiyonların alındığına kanaat getirildiği durumlarda ilgili bulgunun durumu “TAMAMLANDI” olarak güncellenir. Bulgulara ilişkin aksiyon planlarının öngörülen tarih itibarıyla tamamlanmadığı ya da tamamlanamayacağına anlaşıldığı durumlarda, Kamu İç Denetim Rehberi’nde de belirtildiği üzere bir defaya mahsus olmak üzere süre uzatımı verilir ve izleme faaliyeti bir sonraki döneme aktarılır. Verilen ek süre, bulgunun önem düzeyi ve mahiyetine bağlı olarak belirlenir, ancak bu süre hiçbir surette 24 ayı geçemez.

İkinci izleme periyodunda da herhangi bir ilerleme kaydedilmemesi halinde, riskin üstlenildiği kabul edilerek bulgu, “RİSK ÜSTLENİLDİ” olarak kapatılır. Ancak İDB Başkanı, kurum için kabul edilemeyecek bir riskin üstlenildiğini düşünüyorsa bu durumu denetlenen birim yöneticisiyle müzakere eder. Müzakere sonucunda mutabakat sağlanamaması durumunda konu çözüme kavuşturulması amacıyla üst yöneticiye bildirilir.

İzleme sonuçları birleştirilerek dönemsel raporlama kapsamında üst yöneticiye sunulur. Bu raporlamada üst yönetici özellikle, “RİSK ÜSTLENİLDİ” olarak kapatılan bulgular konusunda bilgilendirilir.

3. BT KURUM SEVİYESİ KONTROLLERİ VE YÖNETİŞİM SÜREÇLERİ DENETİMİ

Bu bölümde aşağıdaki BT kurum seviyesi kontrolleri ve yönetişim süreçleri denetimine yönelik olarak hazırlanmış olan denetim prosedürleri yer almaktadır:

- 3.1. Kurum Seviyesi Kontroller
- 3.2. BT Yönetişim Süreci Denetimi

3.1. KURUM SEVİYESİ KONTROLLER

Sürecin Genel Tanımı

Bu bölüm kurum seviyesi kontrollerin değerlendirilmesi amacı ile uygulanması önerilen denetim adımlarını içermektedir. Kurum seviyesi kontroller, kurum yönetiminin yönergelerinin ve talimatlarının eksiksiz uygulandığına dair bir güvence sağlanması için tüm kuruma ve personele yaygın şekilde tasarlanmış olan ve uygulanan iç kontrollerdir.

Kurum seviyesi kontroller, bir hata ya da dolandırıcılık sonucu olarak mali tablolarda herhangi bir yanıltıcı bilgi bulunma riskinin değerlendirilmesi ve gerçekleştirilecek denetim süreçlerinin yapısının tasarlanması ve bütçe ve kapsamının belirlenmesi amacı ile denetçi tarafından iyi anlaşılmalıdır (AICPA, 2006). Bu sebeple, mali raporlamaların BT sistemleri üzerinde ilerlediği kurumlarda BT kurum seviyesi kontrollerinin de kapsamlı olarak değerlendirilmesi gereklidir.

Kurumsal risk yönetiminin amacı paydaşlar için değer üretmektir. Bu değer azami seviyede olması büyüme, getiriler ve bunlarla ilgili risklerin etkin ve verimli yönetimi arasında bir denge kurmaktadır. Kurumsal risk yönetimi aşağıdaki unsurları kapsar (Committee of Sponsoring Organizations of the Treadway Commission, 2004).

- Kurumsal risk iştahının (kurumun risk alma eğiliminin) ve stratejinin uyumu: Yönetim stratejik seçenekler arasında değerlendirme yaparken, hedeflerini belirlerken ve riski yönetirken kurumsal risk iştahını da dikkate alır.
- Risk yanıt karar mekanizmasının iyileştirilmesi: Kurumsal risk yönetimi risk yanıtları (riskten kaçınma, riski azaltma, riski paylaşma, risk kabulü gibi) arasından seçim yapmada net bir bakış açısı sağlar.
- Beklenmeyen operasyonel olayların ve kayıpların azaltılması: Kurumlar olası olayları tanımlar ve bunlara verilecek yanıtları belirler ve ilgili kayıpları ve maliyetleri azaltır.
- Kurumlar arası ve çoklu risklerin tanımlanması ve azaltılması: Kurumların karşı karşıya kaldığı farklı birimleri etkileyen sayısız risk ve bunların ortak etkileri karşısında etkin yanıtlar geliştirilir.
- Fırsatların değerlendirilmesi: Tüm olası olayların değerlendirilmesiyle kurumlar fırsatları önceden tanımlar ve değerlendirir.
- Sermaye dağıtımının geliştirilmesi: Risk yönetimi konusunda iyi bir bilgi akışına sahip olmak kurum yönetimlerine genel sermaye ihtiyaçlarının belirlenmesi konusunda yardımcı olur.

Kurumsal risk yönetiminin önerdiği ana bileşenlerden biri olan kontrol ortamının anlaşılması ve değerlendirilmesi sırasında yukarıda bahsi geçen kurum seviyesi kontrollerin ve bir BT denetimi sırasında da bunun bir alt kümesi olan BT kurum seviyesi kontrollerinin anlaşılması önem arz etmektedir.

Kurum Seviyesi Riskler

Riskler
R1. Kurum yönetim felsefesinin BT tarafından doğru anlaşılabilmesi
R2. Kurum stratejisinin ve hedeflerinin BT tarafından desteklenmemesi
R3. Kurum hedefleri doğrultusunda çalışmayan BT yapısı sebebiyle sonucu olarak kurum kaynaklarının etkin ve verimli kullanılmaması
R4. Yatırım yapılacak alanların doğru bir şekilde belirlenmemesi ve/veya yönetim onayı alınmaması sebebiyle yanlış BT yatırımlarının gerçekleştirilmesi
R5. Kurum bünyesinde kullanılan teknolojik ekipman, yazılım ve donanımlar arasında uyumsuzlukların oluşması
R6. BT süreçlerinin iş hedefleri doğrultusunda oluşturulmaması
R7. BT yapısının yürürlükteki mevzuat ve yönetmeliklerle uyumsuzluk göstermesi
R8. İş birimleri için kritik olan bilgi kaynaklarının güvenliğinin sağlanamaması
R9. BT'nin kaynak yetersizliği sonucu kurum iş hedeflerini ve faaliyetlerini destekleyememesi
R10. İş ve BT risklerinin birbirinden bağımsız olarak değerlendirilmesi
R11. BT risklerinin iş üzerindeki etkisinin değerlendirilememesi
R12. BT projelerinin önceliklendirilmesinin doğru yapılamaması

Denetim Prosedürleri

K1 - BT'nin kurum hedefleri doğrultusunda faaliyet göstermesi için gerekli mekanizmalar ve iletişim kanalları kurulur ve işletilir. Bu doğrultuda hedefler, ilkeler ve faaliyetler göz önünde bulundurularak gerekli politika ve prosedür yapısı oluşturulur.			
#	Denetim prosedürleri	T/İ	Z/O
K1.1	BT'nin kurum içerisindeki önemi değerlendirilerek organizasyonel yapı içerisinde hangi seviyede konumlandırıldığı gözlemlenir.	T	Z
K1.2	Kurum bünyesindeki BT organizasyon yapısı incelenir ve iş hedeflerine ve BT önceliklerine en uygun şekilde yapılandırıldığı kontrol edilir	İ	Z
K1.3	Kurum bünyesinde tüm BT personelinin rol ve sorumluluklarının tanımlanmış olduğu ve bunların kurum BT hedeflerini gerçekleştirmesi için en uygun şekilde belirlendiği gözlemlenir.	T	Z
K1.4	Kurum bünyesinde BT yönetimi ile ilgili politika ve prosedürlerinin oluşturulduğu gözlemlenir. Bunların kurum ihtiyaçlarına uygun şekilde yapılandırıldığı gözlemlenir..	T	Z
K1.5	Kurum verilerinin ve uygulamaları için sahiplik kavramının tanımlandığı ve ilgili kişilere/birimlere atama yapıldığı kontrol edilir. Veri sahiplerinin, ilgili verilerin güvenlik açısından sınıflandırılmasında ve belirlenen sınıflara göre gerekli güvenlik önlemlerinin seçiminde karar sahibi olduğu teyit edilir.	İ	Z
K1.6	Kurum bünyesindeki prosedürlerin ve süreçlerin sürekli geliştirilmeye açık olduğu ve bu doğrultuda gerekli çalışmalar yapıldığı kontrol edilir. Bu çalışmaların izlemeyi, kalite yönetimini, otomasyonu ve eğitim aşamalarını içerdiği değerlendirilir.	İ	Z
K1.7	Oluşturulmuş olan politika ve prosedürlere kurum bünyesinde uyum sağlanması için çalışmaların (eğitimler, duyurular, yaptırımlar) gerçekleştirildiği kontrol edilir	İ	Z
K1.8	Kurum bünyesinde kişilere atanan rol ve sorumlulukların görevler ayrılığı ilkesi dikkate alınarak gerçekleştirildiği teyit edilir. Mevcut olması halinde görevler ayrılığı ile ilgili yapılmış çalışmalar (görev tanımları, görevler ayrılığı matrisi vb.) incelenir. Herhangi bir sürecin uçtan uca tek bir kişi tarafından gerçekleştirilemediği teyit edilir.	İ	Z

K2 - Kurum bünyesinde var olan iş süreçlerinin, bilginin, verinin, uygulamaların ve teknolojik altyapının tüm katmanlarının ele alındığı kurumsal bir mimari yapı oluşturulur. Kurumsal mimari yapısı ile ilgili standartlar ve prosedürler oluşturulur, kurum BT mimari bileşenleri (ör: uygulamalar, veri yapıları, vb.) arasındaki ilişkiler tanımlanır.			
#	Denetim prosedürleri	T/i	Z/O
K2.1	Kurum bünyesinde hedeflerin etkin bir biçimde gerçekleştirilmesi için bir kurumsal mimari yapısının tanımlandığı kontrol edilir. Bu yapının içerisinde iş süreçlerinin, veri ve uygulamalar ile teknolojik altyapının göz önünde bulundurulduğu teyit edilir.	T	Z
K2.2	Hedeflenen mimari yapıya ulaşılması için yapılması gerekenlerin belirlendiği ve hayata geçirildiği gözlemlenir. Mevcut durumda uygulanan ya da uygulanacak çözümlere ilişkin değerlendirmelerin gerçekleştirildiği ve kurum yapısına en uygun ve en verimli çözümün seçilmesi için azami gayret gösterildiği kontrol edilir	T	Z
K2.3	Kurumsal mimari bileşenleri arasındaki etkileşimlerin ve ilişkilerin tanımlanmış ve kayıt altına alınmış olduğu kontrol edilir.	T	Z
K2.4	Mimari yapının kurum bünyesinde yerleştirilmesi için bir uygulama planının oluşturulduğu ve düzenli olarak gözden geçirilerek gerektiği durumlarda güncellendiği gözlemlenir	İ	Z

K3 - Kurum bünyesinde bir proje ve portföy yönetim çerçevesi oluşturulur. Bu çerçevede BT yatırımları kurum hedeflerine, kurumsal mimari yapısına ve kaynak ihtiyacına göre belirlenir ve önceliklendirilir. Bu çerçeveye ayrıca master plan, kaynak planlaması, çıktıların tanımlanması, kullanıcı onayları, kalite güvence, test planlama, kabul ve gözden geçirme süreçleri dâhil edilir.			
#	Denetim prosedürleri	T/İ	Z/O
K3.1	Kurum hedeflerine ulaşılması için gerekli olan ve ortak ve/veya paralel şekilde yürütülen birden çok projenin bir arada yönetilmesi anlamına gelen BT programı ile, ortak özellikleri bulunan birçok projeyi ifade eden portföy ve projelerin yönetimi amacıyla bir çerçevenin ya da politikanın tanımlandığı kontrol edilir. Kurum ve BT stratejisine uygunluk, maliyet, getiri ve risk gibi etmenlerin değerlendirilmeye alınarak projelerin önceliklendirildiği gözlemlenir	T, İ	Z
K3.2	BT program, portföy ve projelerinin yürütülmesi için gereken bütçenin belirlendiği ve farklı finansman yöntemlerinin göz önünde bulundurulduğu örneklem bazında gözlemlenir.	İ	Z
K3.3	Yüksek öncelikte olan programların ve projelerin fizibilite çalışmaları ve maliyet-fayda analizleri dikkate alınarak seçildiği ve buna uygun şekilde yürütüldüğü gözlemlenir.	İ	Z
K3.4	Kurum bünyesinde yürütülmekte olan program ve projeler için düzenli olarak bir master plan hazırlandığı, program ve proje yönetimi için ilgili yöntemlerin geliştirilmiş olduğu ve bu yöntemlerin kaynak planlaması, çıktı tanımlaması, proje kabul kriter ve şartları ve kalite güvence süreçleri ile izleme ve değerlendirme aşamalarını içerdiği örneklem bazında değerlendirilir.	İ	Z
K3.5	Kurum bünyesinde programların ve bunların dahil olduğu BT yatırım portföylerinin düzenli olarak takip edildiği ve güncellendiği gözlemlenir.	İ	Z
K3.6	Gerçekleştirilen projelerin ve programların ardından faydaların gözlemlendiği ve öğrenilen derslerin saptanarak kaydedildiği gözlemlenir.	İ	Z

K4 - Kurum BT fonksiyonu ve süreçleri ile ilgili tüm hedeflere dair performans ölçütleri tanımlanır, bunlara ilişkin veriler düzenli olarak toplanır, doğrulanır, değerlendirilir ve uygun yönetim kademelerine raporlanır.

#	Denetim prosedürleri	T/İ	Z/O
K4.1	Kurum bünyesinde BT performansı göstergelerinin ve ölçütlerinin tanımlanması, değerlendirilmesi, izlenmesi ve uygun birimlere raporlanması için bir yaklaşım ya da yöntem oluşturulduğu gözlemlenir. Bu yaklaşım için tüm hedeflerin ve bu hedefler doğrultusunda oluşacak performans ihtiyaçlarının belirlendiği gözlemlenir.	T	Z
K4.2	Oluşturulan performans ölçüm ve değerlendirme sistemi için hedef performans değerlerinin belirlendiği ve ilgili yönetim birimlerince onaylandığı gözlemlenir	T	Z
K4.3	Performans değerlerinin belirlenen ölçütler çerçevesinde düzenli olarak ölçüldüğü ve kayıt altına alındığı kontrol edilir.	İ	Z
K4.4	Toplanan performans değerlerinin analiz edildiği ve raporlandığı gözlemlenir. Raporların ilgili paydaşlarla ve yönetim kademeleriyle paylaşıldığı kontrol edilir..	İ	Z
K4.5	Performans incelemelerinin sonucu olarak düzeltici ya da önleyici faaliyetlerin gerçekleştirildiği teyit edilir	İ	Z

K5 - Kurum BT iç kontrol ortamı düzenli olarak izlenir ve değerlendirilir. Bu değerlendirmelere öz değerlendirmeler ve bağımsız denetimler dâhildir. Kurum yönetimi, bu değerlendirmeler ışığında, mevcut kontrol eksikliklerini ve verimsizlikleri tespit eder, düzeltici ya da önleyici önlemler alır, kurum bünyesindeki kontrol değerlendirme yöntemlerini planlar ve tesis eder

#	Denetim prosedürleri	T/i	Z/O
K5.1	Kurum bünyesindeki kontrollerin etkinliğinin düzenli olarak değerlendirmelerden geçtiği kontrol edilir. Kontrol değerlendirmelerinin sonucu olarak kontrol eksikliklerinin saptandığı ve raporlandığı gözlemlenir. Bu eksikliklere karşılık olarak düzeltici ya da önleyici faaliyetlerin gerçekleştirildiği kontrol edilir.	İ	Z
K5.2	Süreç sahiplerinin, süreçler üzerindeki kontrollerin etkinliğini ve geçerliliğini ölçmek için öz değerlendirmeler gerçekleştirdiği gözlemlenir	İ	Z
K5.3	Kurum hedeflerine ulaşılabilmesi için BT iç kontrol ortamının sürekli olarak izlendiği ve en iyi uygulamalar incelenerek geliştirildiği gözlemlenir..	İ	Z
K5.4	Kurum bünyesinde güvence ve denetim faaliyeti gerçekleştiren bölüm ve kişilerin bağımsız olduğu ve bu faaliyetleri gerçekleştirmek için yeterli yetkinliğe sahip oldukları değerlendirilir..	İ	Z

TASLAK

3.2. BT YÖNETİŞİM SÜRECİ DENETİMİ

Sürecin Genel Tanımı

Bilgi Teknolojileri yönetişimi, bir işletmenin tüm teknoloji kaynaklarının, kurumun ihtiyaçlarına ve önceliklerine göre yönetilmesini ifade etmektedir. Bu kaynaklar; bilgisayar donanımı, yazılım, veri, ağ ve sunucu gibi unsurların yanı sıra, bu kaynakların yönetimini ve bakımını yapacak görevli personeli de içermektedir. Kurum içindeki bu sorumluluğu yönetmek için bütçeleme, personel alımı, tanzim ve kontrol gibi temel yönetim fonksiyonlarına ek olarak, değişim yönetimi, yazılım tasarımı, ağ ve iletişim altyapısı planlaması ve teknik destek gibi konuların da kurumda etkin bir şekilde uygulanması gerekmektedir. Bilgi teknolojilerinin ana odak noktası, teknolojiyi kullanarak işletme için değer yaratmaktır. İşleyen iç fonksiyonlar ve dış çevre arasındaki ilişki ağı güçlü olduğu sürece, teknoloji bir organizasyonun değer zincirinin geliştirilmesinde önemli bir rol oynamaktadır.

Bu çerçevede, bilgi teknolojileri yönetişim denetimleri kurum ve bilgi teknolojileri stratejilerinin eşgüdümlü olarak yürütüldüğünün değerlendirilmesi açısından önem arz etmektedir. Kurum faaliyetleri, süreçleri, riskleri, iç kontrolleri, performans hedef ve ölçütlerinin oluşturulması, ölçümlerin gerçekleştirilmesi ve sürekli iyileştirme döngüsünün kurulması yönetişim denetiminin ana konularını oluşturmaktadır

Kurum Seviyesi Riskler

Riskler
R1. İş ve bilgi teknolojileri stratejilerinin eşgüdümlü olmaması
R2. Performans ölçütlerinin iş, yönetim ve yönetim ihtiyaçlarını karşılamayacak şekilde tanımlanması
R3. İş birimlerinin beklenti ve ihtiyaçlarının yeterli şekilde tanımlanamaması ya da anlaşılabilmesi
R4. Gelişim fırsatlarının belirlenememesi
R5. Üst yönetimde ve iş birimlerinde bilgi teknolojileri hizmetleri ile ilgili memnuniyetsizliklerin oluşması
R6. Bilgi teknolojileri yatırımlarının iş ihtiyaçlarına uygun yönetilmemesi
R7. Risklerin etkin şekilde tespit edilememesi veya yönetilememesi
R8. Kritik bilgi teknolojileri hizmet ve uygulamalarının kullanım dışı kalması
R9. Kaynak planlamasındaki eksiklikler sebebiyle etkin ve verimli bir kaynak yönetimi ve önceliklendirmesi yapılamaması
R10. Kurum ve bilgi teknolojileri kaynak yönetim stratejilerinin uyumsuz olması

Denetim Prosedürleri

K1 - Kurum bilgi teknolojileri yönetim süreci standart ve prosedürlerle tanımlanır ve sorumluluk atamaları gerçekleştirilir. Yönetişim ölçüm metrikleri, iletişim ve raporlama yöntemleri kurum standartlarına uygun şekilde tasarlanır. Yönetişimin devamı olarak iş birimi ve bilgi teknolojileri stratejileri düzenli olarak gözden geçirilir ve ilgili paydaşlarla paylaşılır.

#	Denetim prosedürleri	T/İ	Z/O
K1.1	Kurum hedeflerinin gerçekleşmesi açısından BT'nin önemini anlaşıldığı, ve BT'nin bu yöndeki rolünün belirlendiği gözlemlenir. Bu doğrultuda kurum BT stratejisi ve yönetim ile ilgili politika, yönerge ve diğer dokümanlar incelenir. Bu dokümanlar tasarlanırken kamu ve kurum ihtiyaçlarının gözetildiği teyit edilir.	T	Z
K1.2	Yönetişim rol ve sorumluluklarının tanımlandığı, kurum ve BT fonksiyonlarının iletişim kanallarının tesis edildiği ve iletişim yöntemlerinin önceden belirlenmiş olduğu teyit edilir	T	Z
K1.4	Kurum yönetim performans ölçütlerinin tanımlı olduğu ve bilgi teknolojileri yönetişiminin söz konusu ölçütler kullanılarak düzenli olarak değerlendirildiği teyit edilir.	İ	Z
K1.5	Üst yönetim ve iş birimi beklentilerinin düzenli gözden geçirmeler aracılığıyla bilgi teknolojileri faaliyetleri içerisinde değerlendirildiği ve uygulamaya alındığı teyit edilir.	İ	Z

K2 - Kurum stratejik hedeflerine ulaşılması amacıyla BT fonksiyonunda yapılması gerekenler belirlenir ve bu doğrultuda girişimlerde bulunulur. BT stratejik planı iş hedefleri ile örtüşecek şekilde oluşturulur.			
#	Denetim prosedürleri	T/İ	Z/O
K2.1	BT stratejisi ile ilgili tüm planlarda ve diğer belgelerde kurum hedeflerinin temel alındığı incelenir. Bu dokümanların kurum hedeflerinin dikkate alınarak oluşturulduğu gözlemlenir.	T	Z
K2.2	Mevcut BT yeteneklerinin ve dışarıdan sağlanan BT hizmetlerinin kurum hedeflerinin gerçekleştirilmesi konusunda yeterlilik açısından değerlendirildiği gözlemlenir	T	Z
K2.3	Ulaşılmak istenen BT yapısı için bir stratejik plan oluşturulduğu ve izlenecek yolun tanımlandığı gözlemlenir.	T	Z
K2.4	Tanımlanan BT stratejisi ve yönünün kurum bünyesinde paylaşıldığı kontrol edilir.	İ	Z
K2.5	Kurum BT stratejisinin düzenli olarak gözden geçirildiği ve yenilendiği gözlemlenir. Bu sayede, kısa, orta ve uzun vadede yapılacakların belirlendiği gözlemlenir	İ	Z
K2.6	Kanun, yönetmelik ve yasalardaki değişikliklerin düzenli olarak izlenerek kurum stratejilerinin güncellendiği teyit edilir.	İ	Z
K2.7	Üst yönetim strateji toplantı tutanakları incelenir ve bu toplantılarda alınan kararların alt birimlerce uygulandığı değerlendirilir.	İ	Z

K3 - Yatırımlar sonucu iş süreçlerinden, BT hizmetlerinden ve BT varlıklarından sağlanan fayda uygun maliyetlerle en iyi seviyeye çekilir.

#	Denetim prosedürleri	T/i	Z/O
K3.1	Bilgi teknolojileri yatırım planı ve kurum iş stratejilerinin uyumu değerlendirilir	T	Z
K3.2	Bilgi teknolojileri yatırım planının ve proje gereksinimlerinin birbiriyle örtüştüğü gözlemlenir	T	Z
K3.3	Projelerde fayda maliyet analizlerinin gerçekleştirildiği ve üst yönetimle paylaşıldığı teyit edilir.	İ	Z
K3.4	Bilgi teknolojileri yatırımlarının düzenli gerçekleşen komitelerde ya da çalışma gruplarında paydaşlar tarafından değerlendirildiği kontrol edilir.	İ	Z
K3.5	Bilgi teknolojileri fonksiyonu ve hizmetleri bazında proje ve yatırımların değerlendirilebilmesini sağlayacak izlemenin gerçekleştirildiği teyit edilir..	İ	Z

TASLAK

K4 - Kurum risk yönetimi çerçevesi ile uyumlu bir BT risk yönetimi çerçevesi oluşturulur. Kurum risk iştah ve toleransı anlaşılır, kurum bünyesinde açıkça ifade edilir ve paylaşılır. Bununla beraber bilgi sistemlerinin kullanımı ile ilgili riskler de belirlenir ve yönetilir.

#	Denetim prosedürleri	T/İ	Z/O
K4.1	Kurum risk yönetimi çerçevesine uygun şekilde hazırlanmış bir BT risk yönetimi çerçevesinin varlığı incelenir. BT risk yönetimi çerçevesinin iş odaklı olarak strateji, program, proje ve operasyon bileşenlerini içerdiği kontrol edilir.	T	Z
K4.2	Bilgi teknolojileri risk iştahı ve toleransına istinaden hazırlanmış risk dokümanları incelenir, yeterlilikleri değerlendirilir	İ	Z
K4.3	Risk yönetim süreci ana kontrol hedeflerini sağlaması açısından değerlendirilir	T	Z
K4.4	Düzenli hazırlanan risk değerlendirme raporları ve/veya risk komite toplantı tutanakları incelenir süreç etkinliği bakımından değerlendirilir	İ	Z
K4.5	Risk envanterinde bulunmayan risklerin tespiti amacıyla düzenli gözlem yapıldığı değerlendirilir	İ	Z

TASLAK

K5 - BT çalışanları, süreçleri ve altyapısı, kurum hedeflerini desteklemek için yeterli seviyede yetkinliğe ve kabiliyete sahiptir. Kurumdaki çalışanların mesleki yeterlilikleri Mesleki Yeterlilik Kurumu tarafından yayınlanan 5544 nolu 21.09.2006 tarihli Mesleki Yeterlilik Kanununa ve ilgili diğer mevzuata uygun şekildedir			
#	Denetim prosedürleri	T/i	Z/O
K5.1	İnsan kaynakları yönetim dokümanlarının ve standartlarının kurum stratejisine uygun şekilde oluşturulduğu teyit edilir.	T	Z
K5.2	Proje kaynak atamaları ve genel kurum stratejisi birbiriyle uyum açısından değerlendirilir.	T	Z
K5.3	Kurum bünyesinde BT çalışanlarının işe alım sırasında ilgili mesleki yeterlilik kriterlerine göre değerlendirildiği ve kurum içinde mesleki yetkinlik ve yeterlilikleri uyarınca görevlendirildikleri örneklem üzerinden incelenir.	İ	Z
K5.4	Kamuya ilişkin bağlayıcı kanun ve yönetmeliklere uyum için yeterli prosedürlerin oluşturulmuş olduğu teyit edilir. BT personelinin yetkinlik ve yeterliliklerinin değerlendirilmesinde ilgili mevzuatın temel alındığı gözlemlenir.	T	Z

TASLAK

4. BİLGİ TEKNOLOJİLERİ YÖNETİM SÜREÇLERİ DENETİMİ

Bu bölümde aşağıdaki BT yönetim süreçlerinin denetimine yönelik olarak hazırlanmış olan denetim prosedürleri yer almaktadır:

- 4.1. Deęişiklik Yönetimi
- 4.2. Güvenlik Hizmetleri Yönetimi
- 4.3. Yardım Masası Olay ve Problem Yönetimi
- 4.4. BT Operasyon ve Yedekleme Yönetimi
- 4.5. Süreklilik Yönetimi
- 4.6. BT Altyapı ve Yazılım Edinim, Kurulum ve Bakımı
- 4.7. BT Hizmet Yönetimi
- 4.8. BT Risk Yönetimi

4.1. DEĞİŞİKLİK YÖNETİMİ

Sürecin Genel Tanımı

Değişiklik yönetimi süreci, kurum kritik iş faaliyetlerini ve süreçlerini destekleyen BT uygulamaları ve altyapısı üzerindeki tüm değişikliklerin kontrollü bir biçimde gerçekleştirilmesi ve üretim ortamlarının güvenilirlik ve bütünlüklerinin korunması amacını taşımaktadır. Bu değişiklikler, uygulama kodlarında yapılacak bir değişiklik olabileceği gibi, veritabanları, işletim sistemleri, uygulamaya ait kritik konfigürasyon dosyaları gibi bir dizi diğer değişiklik tiplerini de içerebilir. Ayrıca BT uygulamaları ve altyapısı ile ilgili acil durum değişiklikleri, bakım faaliyeti kapsamındaki değişiklikler (bug-fix) ve yama yönetimi unsurları da bu süreç kapsamında ele alınmaktadır.

Değişiklik yönetimi sürecinin etkin bir biçimde uygulanması ile değişikliğin getirilerinden azami ölçüde fayda sağlama şansı yakalanırken, değişikliklerden kaynaklanan riskler asgari düzeye indirilir, zaman ve kaynak tasarrufu elde edilir. Değişiklik yönetimi sürecinin etkin bir şekilde yürütülmesi sayesinde kurumun yasal zorunluluklar, yönetmelikler ve sözleşmeler gibi gerekliliklere uyumlu olması ve kurumun faaliyetleri ve süreçlerinin yüksek performanslı ve güvenilir bir şekilde gerçekleştirilmesi sağlanır.

Sürecin BT Denetimi Açısından Önemi

Değişiklik yönetimi, kurumun faaliyetlerini ve süreçlerini işletebilmesi için gerekli olan ve bilgi sistemleri tarafından sağlanan “kritik BT işlevselliği” üzerindeki değişikliklerle doğrudan ilgili olduğundan, BT denetimlerinde en çok öne çıkan konulardan biridir. Değişiklik yönetiminin değerlendirilmesi sayesinde, BT uygulamalarından beklenen işlevselliğin değişikliklerden kaynaklanabilecek hata ve suistimallerden olumsuz etkilenmediğine ve değişikliklerin iş hedeflerine uygun bir biçimde gerçekleştirildiğine ilişkin bir makul güvence sağlanabilir. Bu sayede, BT uygulamalarının hesaplama, raporlama vb. gibi denetim açısından kritiklik taşıyan işlevselliklerine ilişkin değişikliklerin, denetim dönemi içerisinde kontrollü bir biçimde gerçekleştirilip gerçekleştirilmediğine ilişkin bir kanaat oluşturulabilir. Değişiklik yönetimi, uygulama kontrollerinin etkinliğini destekleyen en önemli BT genel kontrol gruplarından biridir. Bu çerçevede değişiklik yönetimi sürecinin denetimi, özellikle mali ve sistem odaklı denetimlerde sıklıkla ele alınan konulardan biri olmaktadır.

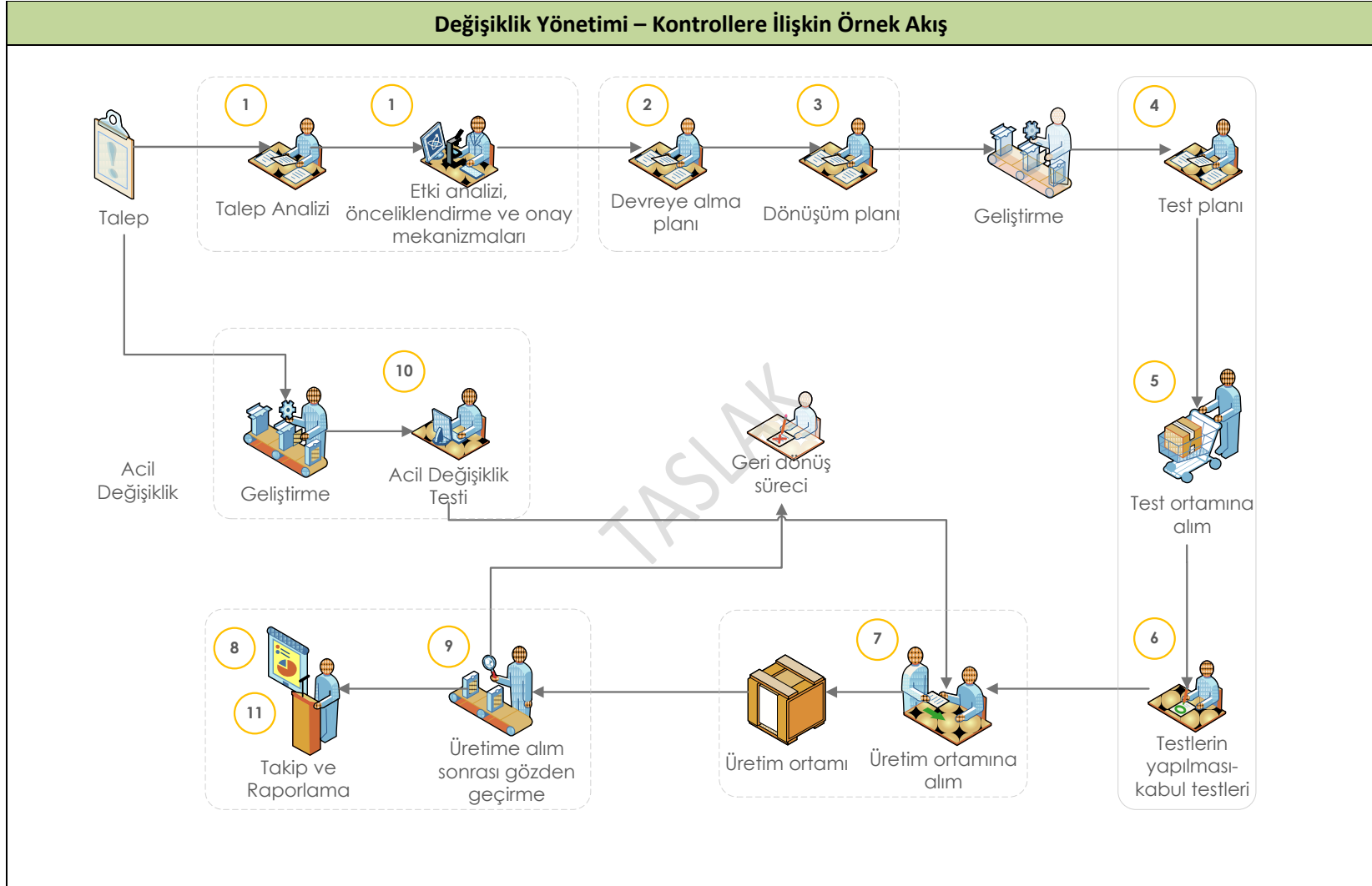
Değişiklik yönetimi, BT denetimi açısından aşağıdaki süreç ve kontroller üzerinden takip edilebilir. Söz konusu akış her kurum için farklı olabileceği gibi, süreç içerisinde ele alınan değişiklik tipleri, kullanılan değişiklik yönetimi araçları, değişiklikler için aktive edilen denetim izi mekanizmaları, takip ve raporlama mekanizmaları da kurumdan kuruma değişebilmektedir.

Kontrollere İlişkin Örnek Akış

Süreçte yer alan tipik kontrollere aşağıdaki tabloda yer verilmiştir:

Değişiklik Yönetimi – Kontroller	
K1	İlgili birimler tarafından değişiklik yönetimi sürecinde gerçekleştirilecek etki analizi, önceliklendirme ve onay mekanizmaları vasıtasıyla, değişiklik yapılan uygulama ve/veya altyapı bileşenlerinin veri bütünlüğü ve güvenilirliğini olumsuz etkileyecek riskler azaltılır.
K2	Uygulama ve altyapı sistemleri üzerinde tüm değişiklik tiplerini kapsayan ve sistem ve/veya veri dönüşümü, kabul kriterleri, devreye alma duyurusu ve eğitim gibi unsurları içeren bir değişiklik "devreye alma planı" oluşturulur.
K3	Değişiklikler, iş süreçleri, uygulama, altyapı bileşenleri ve/veya veri seviyesinde bir dönüşümü gerekli kılıyorsa (ör: bir uygulamanın veri tabanı sisteminin değiştirilmesi), buna uygun bir dönüşüm planı hazırlanır.
K4	Kurum çapında değişikliklerin testine yönelik rolleri, sorumlulukları, testlere ilişkin kriterleri ve test sonuçlarına ilişkin beklentileri tanımlayan bir değişiklik test planı oluşturulur.
K5	Değişiklikler sonrasındaki durumu iş süreçleri ile BT uygulama ve altyapı bileşenleri açısından yansıtacak güvenli bir test ortamı oluşturulur.
K6	Değişikliğin devreye alınması öncesinde "değişiklik kabul testleri" önceden belirlenmiş test planına ve/veya kriterlere göre gerçekleştirilir.
K7	Test sonuçları başarılı olarak değerlendirilen değişikliklerin üretim ortamına aktarımı ve devreye alınması yazılım sürecinde görev almayan birim ya da kişiler tarafından gerçekleştirilir.
K8	Gerçekleştirilen değişiklikler ile ilgili olarak belirli bir süre destek sağlanır.
K9	Değişikliklerin devreye alınmasını müteakip çıktıları ve sonuçları gözlemlemek için bir "devreye alma sonrası gözden geçirme" çalışması gerçekleştirilir.
K10	Acil değişiklikler sonrası oluşabilecek ek sorunlar ya da güvenlik hususları en aza indirgenir.
K11	Reddedilen ve gerçekleştirilen tüm değişikliklerin raporlamaya uygun şekilde kayıt altına alınması amacıyla bir takip ve raporlama sistemi oluşturulur.

Bahsi geçen kontrollere ilişkin örnek akış şeması aşağıda yer almaktadır:



 Kontrol numaraları

Risk – Kontrol Eşleşmeleri

Değişiklik Yönetimi Risk – Kontrol Eşleşmeleri											
Riskler	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11
R1. Yetkisiz, onaysız ya da kontrolsüz değişikliklerin gerçekleşmesi ve sonucunda uygulama ve/veya altyapı bileşenleri üzerinde veri ve işlem bütünlüğünün bozulması	+	+	+	+	+	+	+	+	+	+	+
R2. Değişikliklerin öncelik derecesine göre sıralanmaması sonucu önemli değişikliklerin gözden kaçırılması ya da kurum için önem/öncelik arz etmeyen taleplere gereğinden fazla kaynak ayrılması	+										
R3. Değişikliklerin ön kabul ya da son kabul gibi aşamalar uygulanmadan ya da test edilmeden gerçekleştirilmesinin sonucu olarak sistemlerin güvenilirliğinin bozulması		+	+	+	+	+	+				
R4. Üretim ortamından bağımsız bir test ortamının bulunmamasına bağlı olarak yapılan değişikliklerin üretim ortamının performansını ve erişilebilirliğini olumsuz etkilemesi ve hizmet kesintilerine yol açması					+						
R5. Değişikliklerin gerçekleştirilmesinden önceki sistem verilerinin yedeklenmeden yeni sisteme geçilmesi sonucunda ihtiyaç duyulduğunda eski verilere ulaşılamaması	+	+	+				+				
R6. Değişikliklerin kayıt altına alınmaması ya da izlenememesi	+									+	+
R7. Acil değişikliklerin kontrolsüz olarak ve kayıt altına alınmadan gerçekleştirilmesi										+	

Değişiklik Yönetimi Risk – Kontrol Eşleşmeleri											
Riskler	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11
R8. Gerçekleştirilen değişiklikler sonucunda faaliyet, süreç ya da BT kaynaklarında öngörülmeyen sorun ve aksaklıkların yaşanması		+		+		+		+			
R9. BT yatırımlarının beklentileri karşılayamaması ya da yatırım beklentilerinin ne derece karşılandığının tespit edilememesi	+								+		+
R10. Değişiklikler için kaynakların doğru olarak atanamaması ya da belirli personele bağımlılıkların oluşması	+	+		+							
R11. Değişikliklerin zamanında ve doğru olarak yapılamaması sonucunda yasal zorunluluklardan, yönetmeliklerden ve sözleşmelerden kaynaklanabilecek ve kurumun faaliyetlerini ilgilendiren gereksinimlere uyumun sağlanmaması	+	+	+				+				
R12. BT altyapısının performans ve kapasitesinin verimli bir şekilde kullanılamaması		+	+		+						
R13. Değişiklikler sonrası ön görülemeyen güvenlik açıkları sebebi ile uygulama ve/veya altyapı sistemlerinin saldırılara karşı savunmasız kalınması								+			

Denetim Prosedürleri

K1 - İlgili birimler tarafından değişiklik yönetimi sürecinde gerçekleştirilecek etki analizi, önceliklendirme ve onay mekanizmaları vasıtasıyla, değişiklik yapılan uygulama ve/veya altyapı bileşenlerinin veri bütünlüğü ve güvenilirliğini olumsuz etkileyecek riskler azaltılır.				
#	Denetim prosedürleri	T/İ	Z/O	
K1.1	Kurum içerisinde kullanılmakta olan uygulama ve altyapı bileşenlerine yönelik tüm değişiklik taleplerinin standart bir yöntemle ele alındığını kontrol etmek amacıyla değişiklik yönetim politika, prosedür ve/veya iş akış şemaları temin edilir.	T	Z	
K1.2	Değişiklik yönetimi ile ilgili dokümanların (ör: politika, prosedür, akış, vb.) aşağıdakileri içerip içermediği kontrol edilir. <ul style="list-style-type: none"> • Süreçte rol alan personelin görev ve sorumlulukların tanımı • Değişiklik kavramının ve tiplerinin tanımı (değişik tiplerine örnekler aşağıdadır): <ul style="list-style-type: none"> • Sürüm/versiyon yükseltmeleri • Yama yüklemeleri, • Hata ve problem düzeltmeleri, • Süreci ya da mali verileri etkileyen parametre değişiklikleri • Değişikliklerin altyapı ve uygulama bazında değerlendirilmesi ve daha önceden belirlenmiş kriterler uyarınca önceliklendirilmesi • Değişikliğin kurumun faaliyetlerine, süreçlerine ya da veri bütünlüğüne olan etkisinin değerlendirilmesine ilişkin yönlendirmeler • İç/dış kaynak kullanımına ilişkin değerlendirmeyi de içeren kaynak planlamasına ilişkin yönlendirmeler • Değişiklerin yapılmasına ilişkin süreç içindeki karar ve gerekli onay seviyeleri • Değişikliklerin talep ve takip/kayıt mekanizması • Acil değişiklik süreci ve takip/kayıt mekanizması • Bir problem ya da aksaklık ile karşılaşılması durumunda değişikliğin geri alınması için uygulanması gereken adımlar • Değişikliklerin iş ve/veya BT sürekliliğine olan etkilerinin değerlendirilmesi • Değişiklik süreci içinde birbirinden ayrılması gereken sorumluluklara (değişikliklerin geliştirilmesi, test edilmesi, devreye/kullanıma alınması, izlenmesi/değerlendirilmesi) ilişkin görevler ayrılığı ilkesi 	T	Z	
K1.3	<ul style="list-style-type: none"> • Kapsama alınan uygulama ve sistemler üzerinde denetim dönemi içerisinde gerçekleşmiş olan değişikliklerin listesi (tercihen değişikliğin yapıldığı sistemin kendisi üzerinden ve değişikliklere ilişkin detayları içeren denetim izleri / log ile desteklenecek şekilde) temin edilir. Canlı sistemden doğrudan temin edilen değişiklik listesi içerisinden, uygun görülen örneklem yöntemi kullanılarak gerekli sayıda örnek değişiklik seçilir. 	İ	Z	

	<ul style="list-style-type: none"> Değişikliklerin listesine doğrudan canlı sistemden ulaşamaması durumunda uygulamanın çalıştırılabilir program ya da kütüphane dosyalarının (örnek olarak.exe, .dll, .cab, vb. uzantısına sahip olan dosyalar sayılabilir) işletim sistemi üzerinde gözlemlenebilen son dosya değişiklik tarihleri alınır. Daha sonra bu tarihlerden denetim dönemi içine isabet edenler arasından örneklem usulü seçilen tarihler, manüel tutulan bir değişiklik listesi varsa bu listedeki kayıtlar ve ilgili tarihleri ile karşılaştırılarak söz konusu manüel listenin bütünlüğünden emin olunur ve değişiklik yönetimi sürecinin değerlendirilmesi için gerekli örnekler bu manüel liste üzerinden seçilebilir. 		
K1.4	<p>Seçilen örnek değişiklikler üzerinden:</p> <ul style="list-style-type: none"> Faaliyet ya da süreç sahiplerinin, kendi alanları, faaliyetleri ya da süreçleri ile ilgili talep ettikleri değişiklikleri onayladığı teyit edilir. Talep edilen değişikliklerin uygun şekilde sınıflandırıldığı (ör: altyapılar, işletim sistemleri, ağ sistemleri, uygulamalar, satın alınan uygulamalar) görülür. Talep edilen değişikliklere belirlenen kriterlere göre öncelik verildiği doğrulanır. Değişiklikler değerlendirilirken (varsa) yasal zorunluluklardan, sözleşmeler ve hizmet seviyesi anlaşmalarından kaynaklanan gereksinimlerle uyumun sağlanıp sağlanmadığı kontrol edilir. Değişikliklerin gerçekleştirilmesi sırasında gerekli olacak kaynakların planlandığı ve iç ya da dış personel kullanımı ile ilgili değerlendirmelerin yapıldığı gözlemlenir. Yukarıda belirtilen tüm aşamaların gerekli ve uygun olduğu şekliyle kayıt altına alınmış olduğu kontrol edilir. Değişikliklerin devreye alınması ile ilgili bir zaman planı oluşturulduğu ve söz konusu planın ilgili tüm birim ve kişilere duyurulduğu incelenir. 	İ	Z

K2 - Uygulama ve altyapı sistemleri üzerinde tüm değişiklik tiplerini kapsayan ve sistem ve/veya veri dönüşümü, kabul kriterleri, devreye alma duyurusu ve eğitim gibi unsurları içeren bir değişiklik "devreye alma planı" oluşturulur.

#	Denetim prosedürleri	T/İ	Z/O
K2.1	<p>Bir önceki adımda seçilen örnek değişiklikler üzerinden:</p> <ul style="list-style-type: none">• Devreye alma planlarının bulunduğu gözlemlenir.• Devreye alma planlarının gözden geçirildiği, onaylandığı ve kurum değişiklik yönetim süreciyle uyumlu olduğu kontrol edilir.• Devreye alma planlarında değişikliklerden kaynaklanan sorunlara yanıt verebilmek adına bir önceki duruma geri dönüş ve kurtarma adımlarının tanımlanıp tanımlanmadığı incelenir.• Devreye alma planlarının donanım, ağ, işletim sistemleri, yazılım, veri, kritik dosyalar, yedekler, uyum gereksinimleri, kontrol prosedürleri ve iş prosedürleri gibi bileşenleri kapsadığı gözlemlenir.• Devreye alma planlarında iş risklerinin ve teknik risklerin dikkate alındığı gözlemlenir.	İ	O

TASLAK

K3 - Değişiklikler, iş süreçleri, uygulama, altyapı bileşenleri ve/veya veri seviyesinde bir dönüşümü gerekli kılıyorsa (ör: bir uygulamanın veri tabanı sisteminin değiştirilmesi), buna uygun bir dönüşüm planı hazırlanır.

#	Denetim prosedürleri	T/İ	Z/O
K3.1	İş süreçleri, uygulama, altyapı ve/veya veri dönüşüm planlarının hazırlanmış olduğu kontrol edilir. Bu planların oluşturulmasında donanım, ağ, işletim sistemleri, yazılım, işlem verileri, ana dosyalar, yedekler ve arşivleme, diğer sistemlerle olan veri alış verişini sağlayan ara birimler, uyum ihtiyaçları, iş prosedürleri ve dokümantasyon konularının dikkate alındığı kontrol edilir.	T	Z*
K3.2	Dönüşüm planlarında iş ve BT sürekliliği ile başarısız bir durumda ilgili sistemin ya da uygulamanın çalışır durumda bulunan bir önceki haline mevcut bulunan yedeklerden geri dönüş unsurlarına yer verildiği gözlemlenir.	T	O

* Kurum bünyesinde denetim dönemi içerisinde bir sistem ve/veya altyapı dönüşümü olduğunda Zorunlu olarak ele alınacaktır.

TASLAK

K4 - Değişikliklerin testine yönelik rolleri, sorumlulukları, testlere ilişkin kriterleri ve test sonuçlarına ilişkin beklentileri tanımlayan bir değişiklik test planı oluşturulur.

#	Denetim prosedürleri	T/İ	Z/O
K4.1	İş ve BT süreç/sistem sahipleri ile iletişime geçilerek kurum standartlarıyla uyumlu bir test planının varlığı araştırılır.	T	O
K4.2	Test planının, risk değerlendirmelerini, gerekli fonksiyonel ve teknik gereksinimleri, testi gerçekleştirmeye olanak sağlayacak kaynakları ve kabul kriterlerini içerdiği incelenir.	T	O
K4.3	Test planının uygulanacak detaylı test aşamalarını içerdiği kontrol edilir. <i>Test aşamalarına örnek olarak: sistem testleri, entegrasyon testleri, kullanıcı kabul testleri, performans testleri, stres testleri, veri dönüşüm testleri, güvenlik testleri, yedekleme ve kurtarma testleri sayılabilir. Her bir değişiklik için farklı test gereklilikleri olabileceği gibi hangi testlerin uygulanacağı ile ilgili kararda değişikliğin olası etkileri, büyüklüğü ve kapsamı gibi unsurlar dikkate alınır.</i>	T	O
K4.4	Test planının test gereksinimleri, test ortamının kurulması veya güncellenmesi, testlerin gerçekleştirilmesi, test sonuçlarının belgelenmesi ve saklanması, hata ve problemlerin çözülmesi ve bunlara ilişkin ilgili/gerekli onayların kayıt edilmesi gibi adımları içerdiği kontrol edilir.	T	O
K4.5	Örnek olarak seçilecek değişikliklerinde test adımlarının ilgili iş süreç sahipleri ve BT personeli tarafından ve belirlenen başarı kriterlerine göre değerlendirildiği kontrol edilir.	İ	O

K5 - Değişiklikler sonrasındaki durumu iş süreçleri ile BT uygulama ve altyapı bileşenleri açısından yansıtacak güvenli bir test ortamı oluşturulur.

#	Denetim prosedürleri	T/İ	Z/O
K5.1	Test ortamının üretim ortamından (canlı ortam) bağımsız olduğu ve fiziksel ya da mantıksal olarak üretim ortamından ayrıştırıldığı gözlemlenir.	T, İ	Z
K5.2	Test ortamı içinde bulunan verilerin yetkisiz erişim açısından güvenliğinin sağlandığı ve test ortamında bulundurulanan verilere erişimlerin kontrollü olduğu gözlemlenir.	İ	Z
K5.3	Test ortamında kullanılacak test verileri üretim ortamından kopyalama suretiyle oluşturuluyorsa, bu verilerin bilgi gizliliği açısından üretim ortamından test ortamına aktarılması sırasında kullanılmakta olan asıl/orijinal verilerin anlaşılamayacak bir şekilde karmaşık hale getirildiği incelenir. <i>Örnek olarak üretim ortamında bulunan ve vatandaşlara ait gerçek TC kimlik numaralarının test ortamına aynen değil, karıştırılarak aktarılması verilebilir.</i>	İ	Z
K5.4	Test ortamının üretim ortamı ile benzer (ya da mümkünse aynı) özelliklere sahip olduğu kontrol edilir. Buna örnek olarak test ortamının, iş yükü, veri, işletim sistemi, uygulama yazılımları, veritabanı yönetim sistemleri, ağ ve altyapı bakımından üretim ortamına yakın bir şekilde yapılandırıldığı değerlendirilir.	İ	O

K6 - Değişikliğin devreye alınması öncesinde “değişiklik kabul testleri” önceden belirlenmiş test planına ve/veya kriterlere göre gerçekleştirilir.

#	Denetim prosedürleri	T/i	Z/O
K6.1	Değişikliklerin üretim ortamına taşınmalarından önce gerçekleştirilen son kabul test sonuçlarının, iş süreç sahipleri ile gerekiyorsa ilgili BT personeli ve üçüncü taraflarca, ilgili test planlarına uygun olarak onaylandığı kontrol edilir.	İ	Z
K6.2	Test sürecinde ortaya çıkan hataların kaydedildiği, düzeltildiği ve düzeltilmiş değişikliğin tekrar test edildiği gözlemlenir.	İ	O

TASLAK

K7 - Test sonuçları başarılı olarak değerlendirilen değişikliklerin üretim ortamına aktarımı ve devreye alınması yazılım sürecinde görev almayan birim ya da kişiler tarafından gerçekleştirilir.

#	Denetim prosedürleri	T/i	Z/O
K7.1	Değişikliklerin devreye alınmasının devreye alma planına uygun olarak gerçekleştirildiği gözlemlenir.	İ	Z
K7.2	Değişikliklerin devreye alınması ve canlı/üretim ortamına aktarımı otomatik olarak gerçekleşiyorsa, otomatik aktarım mekanizması incelenir; aktarımın sadece doğru hedeflere yapıldığı gözlemlenir. Eğer değişikliklere ilişkin dağıtım el yordamıyla (manüel) yapılıyorsa doğru hedeflere dağıtımdan nasıl emin olunduğu sorgulanır.	İ	Z
K7.3	Değişikliklerin, değişiklik yönetimi sürecinde talep, onay, geliştirme ve test kabulü gibi aşamalarda görev almayan bir kişi ya da grup tarafından canlı ortama ve kullanıma alındığı incelenir. Söz konusu inceleme örneklem bazında gerçekleştirilebileceği gibi, mümkün olan durumlarda tüm değişiklikler için de yürütülebilir.	İ	O
K7.4	Değişikliklerin devreye alınması sırasında buna engel olacak bir sorun yaşanmış ise buna yönelik olarak daha önceden hazırlanmış olan geri dönüş planlarının işletildiği gözlemlenir.	İ	O
K7.5	Değişikler sonrasında ilgili değişikliğin niteliğine bağlı olarak gerekli durumlarda ilgili iş süreçlerinin, sistem ve kullanıcı dokümantasyonunun ve varsa konfigürasyon yönetiminin taikp edildiği sistemlerdeki konfigürasyon bilgilerinin güncellendiği gözlemlenir.	İ	

K8 - Gerçekleştirilen değişiklikler ile ilgili olarak son kullanıcılara değişikliğin niteliğine ve etkisine bağlı olarak belirlenecek bir süre zarfında destek sağlanır.

#	Denetim prosedürleri	T/i	Z/O
K8.1	Devreye alınan değişiklikler beklendiği bir şekilde çalışmaya başlayana kadar oluşabilecek problemleri tespit etmek adına son kullanıcılara destek verecek bir kişi ya da gurubun görevlendirildiği gözlemlenir.	T	O
K8.2	Devreye alınan değişiklikler ile ilgili açılan olay kayıtları incelenir ve bu olayların çözümlendiği teyit edilir.	İ	O

TASLAK

K9 - Değişikliklerin devreye alınmasını takiben çıktıları ve sonuçları gözlemek için bir “devreye alma sonrası gözden geçirme” çalışması gerçekleştirilir.

#	Denetim prosedürleri	T/İ	Z/O
K9.1	Uygulama sonrası gözden geçirme yöntemlerinin belirlendiği ve/veya prosedürlerinin oluşturulduğu gözlemlenir.	T	O
K9.2	Devreye alma sonrası gözden geçirme adımlarının/prosedürlerinin aşağıdaki unsurları içerdiği gözlemlenir. <ul style="list-style-type: none"> • Hangi iş ihtiyaçları karşılanmıştır? • Projeden beklenen hangi faydalar sağlanmıştır? • Sistem ne kadar kullanılabilir? • Paydaşların beklentileri ne oranda karşılanmıştır? • Beklenmeyen hangi etkiler oluşmuştur? • Hangi kontrol eksiklikleri giderilmiştir? • Değişiklik yönetimi, kurulum ve onay süreçleri ne derecede etkin ve verimli olarak yerine getirilmiştir? 	T	O
K9.3	Devreye alma sonrası gözden geçirmelerde kullanılacak başarı kriterlerinin belirlenmesinde ilgili iş süreci ve/veya talep sahiplerinin de yer aldığı teyit edilir. <i>Talep sahibi iş birimi ya da değişikliklerden etkilenen birimler olabilir.</i>	T	O
K9.4	Devreye alma sonrası gözden geçirmelerde iç denetim, risk yönetimi ve uyuma dair ek ihtiyaçlar tespit edilmiş ise bunların da yerine getirildiği ya da eylem planlarına dahil edildiği gözlemlenir.	İ	O

K10 - Acil değişiklikler sonrası oluşabilecek ek sorunlar ya da güvenlik hususları en aza indirgenir.

#	Denetim prosedürleri	T/İ	Z/O
K10.1	Acil değişiklik prosedürleri temin edilir ve acil değişiklik tanımının, acil değişikliklerde uygulanacak aşamaların ve gerekli olabilecek ek erişim / yetkilendirme mekanizmasının söz konusu prosedür içinde belirtildiğinden emin olunur.	T	Z
K10.2	Denetim dönemi içerisinde gerçekleşmiş acil değişikliklerin içinden örneklem seçilerek: <ul style="list-style-type: none">• Acil değişikliğin prosedürlere uygun olarak gerçekleştirildiği,• Ek bir sistemsel erişim hakkı sağlanmış olması durumunda bu erişim hakkının temini ve kullanımına ilişkin kayıtların (log) saklandığı ve ilgili erişimin ihtiyaç kalmadığı belirli bir süre sonunda geri alındığı,• Acil değişikliklerin uygulanması sonrasında ilgili değişikliğin sisteme beklenmedik bir hasar vermediğinden emin olmak için gerekli gözden geçirmelerin gerçekleştirildiği ve değişikliğe ilişkin beklenen adımlardan ve oluşturulması gereken belgelerden atlanmış olanlar (ör: onay, test kabul, vb.) varsa, bunların geriye dönük olarak kayıt altına alınmış olduğu incelenir.	İ	Z

K11 - Gerçekleştirilen ve reddedilen tüm değişikliklerin raporlamaya uygun şekilde kayıt altına alınması amacıyla bir takip ve raporlama sistemi oluşturulur.

#	Denetim prosedürleri	T/i	Z/O
K11.1	Değişiklik raporlama ve takip sisteminin tüm birimlerce talep edilen ve sonrasında tamamlanan, reddedilen, onaylanan fakat başlatılmayan ve işlem gören tüm değişiklik taleplerini içerip içermediği kontrol edilir.	İ	Z
K11.2	Değişikliklerin değişiklik yönetimi akışına uygun olarak gerçekleştirildiği ve denetim dönemi boyunca kurum yönetiminin bilgisi dışında bir değişiklik gerçekleştirilip gerçekleştirilmediğinin tespiti amacıyla, uygulama ve altyapı bileşenleri üzerindeki değişikliklerin belirli aralıklarla değişiklik yönetimi sürecinde görev almayan bağımsız bir personel ya da ekip tarafından, mümkünse sistemsel denetim izleriyle desteklenecek şekilde gözden geçirildiği sorgulanır.	İ	Z

TASLAK

Ek Kaynaklar

- ISACA. (2007). COBIT 4.1 Framework – AI6 & AI7. Rolling Meadows, Illionis, United States of America.
- ISACA. (2012). COBIT 5 Enabling Processes – BAI6 & BAI7. Rolling Meadows, Illinois, United States of America.
- ISO/IEC 20000 9.2 Change Management (International Organization for Standardization(ISO)- International Electrotechnical Commission(IEC), 2005)
- ITIL V3 2011 ServiceTransition, 4.2 Change Management (UK Cabinet Office, 2011)
- ITIL V3 2011 ServiceTransition, 4.3 Service Asset and Configuration Management (UK Cabinet Office, 2011)
- ISO/IEC 27001, 10.1.2, 10.1.3, 10.1.4 (International Organization for Standardization(ISO)- International Electrotechnical Commission(IEC), 2005)
- GTAG Change and Patch Management Controls: Critical for Organizational Success (The Institute of Internal Auditors, 2012)

TASLAK

4.2. GÜVENLİK HİZMETLERİ YÖNETİMİ

Sürecin Genel Tanımı

Bir kurumun iş süreçlerini yürütebilmesi için ihtiyaç duyduğu en önemli varlıklardan biri de bilgidir ve gün geçtikçe bilginin ulusal, kurumsal ve kişisel anlamda ifade ettiği önem artmaktadır. Artan önemi ile beraber, kurumların bilgi varlıklarının maruz kaldığı tehditler de çeşitlenmekte ve yeni zafiyet noktaları (zayıflıkları) ortaya çıkmaktadır. Bu noktada kuruma ait bu değerli varlıkların güvenliğinin sağlanması ihtiyacı ortaya çıkmaktadır.

Bilgi güvenliği, kuruma ait bilgilerin, iş sürekliliğini sağlamak, iş risklerinin etkilerini azaltmak ve BT yatırımlarından ve fırsatlarından azami faydayı sağlamak adına korunmasını amaçlar. Bilgi güvenliğinin temel unsurları gizlilik, bütünlük ve erişilebilirliktir.

Sürecin BT Denetimi Açısından Önemi

Güvenlik hizmetleri yönetimi sürecini etkin şekilde uygulayan kurumlar, kurum bilgilerinin ve bu bilgileri işleyen altyapının güvenilirliğini sağlarken güvenlik zafiyetlerinin etkisini de en aza indirirler. Güvenlik hizmetleri bu doğrultuda bilgi sistemlerini hem fiziksel hem de mantıksal olarak tüm iç ve dış tehditlerden korumayı amaçlamaktadır. Bu tehditler yetkisiz işlemler, zararlı yazılımlar, ağ (siber) saldırıları ve fiziksel saldırılar gibi hem dış hem de iç etkenleri/tehditleri kapsamaktadır. Güvenlik hizmetleri yönetimi süreci bir kurumun bilgi varlıklarının maruz kaldığı riskleri kurumca kabul edilen en alt seviyeye indirmeyi hedefler. Güvenlik hizmetleri yönetimi sürecinin etkin yönetildiği kurumlarda bilginin gizliliği, bütünlüğü ve erişilebilirliği sağlanır. Böylece, kurum bilgi varlıklarını hedefleyen tehditlerden doğacak ekonomik ve itibar kaybından korunmuş olur.

Güvenlik hizmetleri yönetimi kurum faaliyetlerinin ve süreçlerinin işleyebilmesi için gerekli olan ve bilgi sistemleri tarafından sağlanan “kritik BT işlevselliği”nin gizliliği, bütünlüğü ve erişilebilirliği ile doğrudan ilgili olduğundan, tipik bir BT denetiminde kapsama alınması olmazsa olmaz bir konudur. Güvenlik hizmetleri yönetimi sürecinin değerlendirilmesi ile kurum BT yazılım, altyapı ve süreçlerinin işlevselliğinin fiziksel ve mantıksal zafiyetlerden veya tehditlerden kaynaklanabilecek olumsuz etkilere karşı kontrollü bir biçimde korunduğuna dair makul bir güvence sağlanabilir. Bu sayede, BT uygulamalarının hesaplama, raporlama vb. gibi denetim açısından kritiklik taşıyan işlevselliklerinin kontrollü bir biçimde korunduğuna ve güvenlik açıklıklarından faydalanılarak yetkisiz değişikliklerin gerçekleştirilip gerçekleştirilmediğine ilişkin bir kanaat oluşturulabilir. Güvenlik hizmetleri yönetimi, uygulama kontrollerinin etkinliğini destekleyen en önemli BT genel kontrol gruplarından biridir. Bu

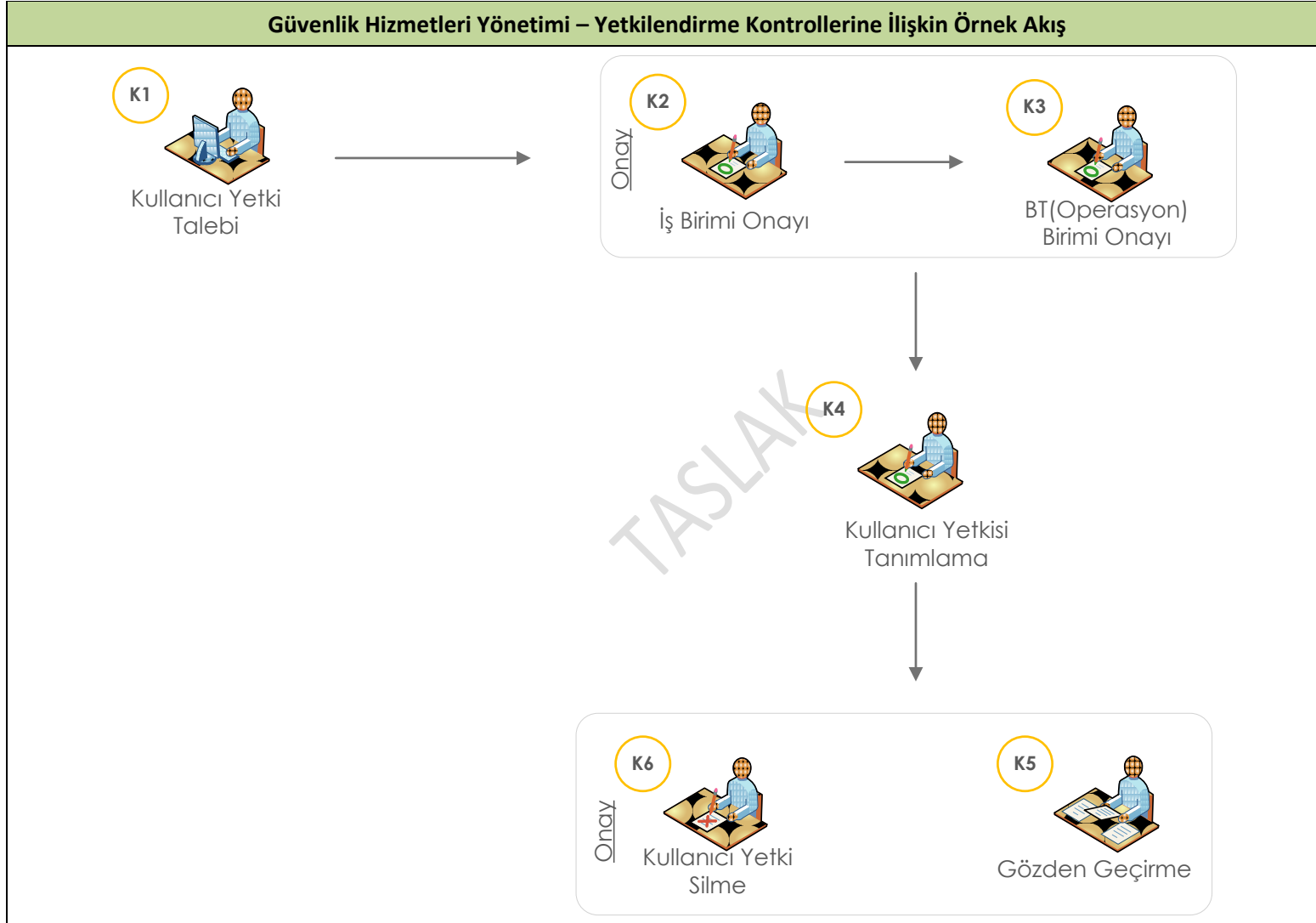
çerçevede güvenlik hizmetleri yönetimi sürecinin denetimi, özellikle mali ve sistem odaklı denetimlerde sıklıkla ele alınan konulardan biri olmaktadır.

Kontrollere İlişkin Örnek Akış

Süreçte yer alan tipik kontrollere aşağıdaki tabloda yer verilmiştir:

Güvenlik Hizmetleri Yönetimi - Kontroller	
K1	Kurum bünyesinde güvenliğe dair standart, resmi ve sürekli bir bakış açısıyla bir bilgi güvenliği yönetim sistemi (BGYS) oluşturulur.
K2	Bilgi güvenliğinden kaynaklanabilecek risklerin nasıl yönetileceğinin belirlendiği, kurumsal strateji ve kurumsal mimariye uygun bir bilgi güvenliği planı hazırlanır.
K3	Kurum bünyesinde bilgi güvenliği uygulamalarının sürekli olarak gelişmesi için BGYS izlenir ve gözden geçirilir.
K4	Kurum bilgi sistemleri üzerinde önleyici, tespit edici ve düzeltici uyarlamaların yapılması ve kurum bünyesinde bu uyarlamalara paralel olarak güvenlik yamalarının ve anti-virüs uygulamalarının kullanılması gibi önlemlerin alınması ile bilgi sistemleri ve teknolojisinin kötü amaçlı yazılımlardan etkilenme riski azaltılır.
K5	İletişim ortamındaki bilgilerin korunması için kurum bünyesindeki bilgi sistemleri ağının güvenliği sağlanmalıdır.
K6	Kurum ağı erişim noktaları (dizüstü bilgisayarlar, masaüstü bilgisayarlar, sunucular ve diğer mobil ve ağ aygıtları ve yazılımlar), kurum ağı üzerinden iletilen veri için tanımlanan gerekli minimum güvenlik seviyelerini karşılamalıdır.
K7	Tüm kullanıcılar, bilgi sistemleri üzerinde iş tanımları ile paralel, ihtiyaç duyacakları en az seviyede erişim yetkilerine sahip olmalıdır.
K8	İş gereksinimlerini ve acil durumları göz önünde bulundurarak; binalara, tesislere ve kritik alanlara fiziksel erişimler için yetki verme, yetki kısıtlama ve bu yetkileri iptal etmeye yönelik prosedürler tanımlanmalıdır. Bu alanlara erişimlerin kontrollü olmasının yanında yetkilerin tümü onaya istinaden verilmeli, denetim izleri tutulmalı ve gözden geçirilmelidir. Bu kontroller ilgili alanlara fiziksel erişimi olan daimi ve geçici çalışanlara, ziyaretçilere, müşterilere tedarikçilere veya tüm üçüncü şahıslar dahil olmak üzere herkese uygulanmalıdır.
K9	Kurum bünyesinde kullanılan hassas ve bilgi güvenliği açısından kritik bilgi teknolojileri cihazları, özel formlar, kıymetli evrak, özel ihtiyaca yönelik yazıcı ve güvenli anahtar (şifre) üreticiler üzerinde uygun fiziksel güvenlik önlemleri ve envanter (döküm) yönetimi teknikleri uygulanmalıdır.
K10	Kurum bilgi sistemleri altyapısı yetkisiz erişimlere karşı izlenir ve bilgi sistemleri altyapısı üzerindeki tüm faaliyetlerin olay izleme ve vaka yönetimi süreci içerisinde kapsandığı teyit edilir.

Bahsi geçen kontrollere ilişkin örnek akış şeması aşağıda yer almaktadır:



 Kontrol numaraları

Risk – Kontrol Eşleşmeleri

Güvenlik Hizmetleri Yönetimi Risk – Kontrol Eşleşmeleri										
Riskler	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10
R1. Bilgi güvenliği olaylarının takip edilmemesi ve zamanında çözülmemesinin sonucu olarak kurum bilgi sistemlerine sızılması, kurum bilgilerinin çalınması	+	+	+	+	+	+		+		+
R2. Bilgi güvenliği stratejisinin BT stratejisi ile uyumsuzluk göstermesi	+	+	+							
R3. Bilgi sistemleri üzerinde meydana gelen güvenlik olaylarının zamanında çözülememesi ve bu sebeple iş kesintilerinin oluşması				+	+					+
R4. Kurum veri bütünlüğünün bozulması ve veri işleyen sistemlerin iş gerekliliklerine uygun çalışmaması	+	+	+	+	+	+	+	+	+	+
R5. Zararlı yazılımların bilgi sistemleri ağına sirayet etmesi ve bu şekilde performans ve veri kayıplarının oluşması				+	+					
R6. Kritik dosya ve diğer bilgi kaynaklarının bilinçli ya da farkında olmadan değiştirilmesi					+	+	+			
R7. BT ekipmanlarına yetkisiz erişimlerin sağlanabilmesi								+		
R8. BT cihaz, ekipman ve donanımlarına yönelik fiziksel güvenliğe olan tehditlerin fark edilememesi								+		
R9. Kritik iş süreçlerinin üzerinde çalıştığı sistemlerin fiziksel olarak korunamaması								+		
R10. Kritik veriler içeren sabit disklerin ve diğer veri saklama ortamlarının çalınması ve bu şekilde verilerin ifşa olması								+		

Güvenlik Hizmetleri Yönetimi Risk – Kontrol Eşleşmeleri										
Riskler	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10
R11. Cihazlarda izinsiz konfigürasyon değişikliklerinin gerçekleştirilmesi								+		
R12. Bilgi güvenliği konusundaki yasal yükümlülüklerin yerine getirilememesi; kanun ve yükümlülüklerle uyumsuzlukların ortaya çıkması. Örn: 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun	+	+	+	+	+	+	+	+	+	+
R13. Bilgi sistemleri üzerinde otomatik olarak tanımlanan varsayılan kullanıcılar üzerinden diğer kullanıcıların yetkilerinin artırılması							+			
R14. Bilgi sistemleri uygulamaları üzerinde kritik veri, bilgi, donanım ve cihazlara yetkisiz erişimlerin gerçekleştirilmesi							+	+		
R15. Bilgi sistemleri uygulamaları üzerinde gerçekleşen erişimlerin izlenmemesi sonucu yetkisiz erişimlerin ya da erişim girişimlerinin yönetim tarafından fark edilememesi										+
R16. Kurum bünyesinde gerekli anlayışın ya da farkındalığın oluşmaması sebebiyle bilgi güvenliği sürecinin etkin bir şekilde yönetilememesi	+	+								
R17. Bilgi sistemleri ve ilgili ağ yapısı üzerinden şifrelenmeden (kriptolanmadan) iletilen kullanıcı adı ve kullanıcı şifrelerinin yetkisiz kişiler tarafından ele geçirilmesi					+	+	+			

Güvenlik Hizmetleri Yönetimi Risk – Kontrol Eşleşmeleri										
Riskler	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10
R18. Kullanıcılar tarafından bilinçli ya da farkında olmadan bilgi sistemleri üzerinde erişim yetkisi artırma işlemlerinin gerçekleştirilmesi							+			
R19. Kısıtlanmayan medya yüklemeleri (download) (dosya paylaşımı, video, ses vb.) sonucunda bilgi sistemleri sürekliliği, performans ve kapasitesini etkileyecek hususların oluşması.								+	+	
R20. Kontrolsüz dosya paylaşımlarının (ör: dosya paylaşım ağları üzerinden yapılan paylaşımlar) gerçekleşmesi sonucu olarak fikri mülkiyet haklarının ihlal edilmesi	+									
R21. Bilgi sistemleri üzerindeki güvenlik ve şifre parametrelerinin, yetkisiz erişimleri önleyecek şekilde tanımlanmaması		+					+			
R22. Güvenlik denetim izlerinin tutulmaması sebebiyle, kurum bünyesinde gerçekleşen güvenlik ihlallerinin sorumlularının ve nedenlerinin belirlenememesi	+					+				

Denetim Prosedürleri

K1 - Kurum bünyesinde güvenliğe dair standart, resmi ve sürekli gelişim bakış açısıyla bir bilgi güvenliği yönetim sistemi (BGYS) oluşturulur.				
#	Denetim prosedürleri	T/i	Z/O	
K1.1	Kurumun stratejisi, genel güvenlik yapısı, risk iştahı, konumu, varlıkları ve teknolojik yapısına göre tasarlanmış bir BGYS'nin varlığı sorgulanır.	T	Z	
K1.2	BGYS'nin kurum genelindeki güvenlik anlayışı ile uyumlu olduğu kontrol edilir. BGYS'nin oluşturulmasında kurum bünyesindeki diğer güvenlik (bina güvenliği, iş güvenliği vb.) birimlerinde bulunan paydaşların da sürece dâhil olduğu gözlemlenir.	T	O	
K1.3	Kurum bünyesinde uygulanan BGYS'nin üst yönetim tarafından (genel müdür veya genel müdür yardımcısı) onaylı olduğu gözlemlenir.	İ	Z	
K1.4	Kurum bünyesinde bir güvenlik yürütme/yönlendirme kurulunun varlığı sorgulanır. Kurul üyeleri arasında iç denetim, insan kaynakları, idari işler, bina güvenliği, BT güvenlik ve hukuk birimlerinden temsilcilerin ve kritik faaliyetlere ilişkin yöneticilerin bulunması beklenir.	İ	O	
K1.5	Güvenlik yönetimi fonksiyonunun kapsamını, hedeflerini, rol ve sorumluluklarının yanında ilgili mevzuat uyarınca gerekli uyum ve risk etmenlerini de içeren bir bilgi güvenliği tüzüğüne ya da benzeri bir dokümanın varlığı araştırılır.	T	O	
K1.6	Kurum bünyesinde güncel ve üst yönetim tarafından onaylanmış bir bilgi güvenliği politikasının varlığı incelenir. Bilgi güvenliği politikasının aşağıdaki unsurları içermesi beklenir <ul style="list-style-type: none"> • Bilgi güvenliğinin tanımı, amaçları, kapsamı ve önemi • İş stratejisi ve hedefleri ile uyumlu olacak şekilde yönetimin güvenlik ilkelerine ve prensiplerine ilişkin beyanı • Güvenlik kontrolleri tasarım yöntemi çerçevesi • Güvenlik ile ilgili politikaların kısa açıklamaları • Kurumun güvenlik ile ilgili yasal uyum ihtiyaçları • Güvenlik farkındalığı ve eğitim süreçleri • Bilgi güvenliği politikalarına uyulmaması sonucunda uygulanacak yaptırımlar • Bilgi güvenliği yönetiminin rol ve sorumlulukları 	T	Z	
K1.7	Bilgi güvenliği politikasının, bilgi güvenliği konusunda yönetim kurulunun, üst yönetimin, diğer yönetim kademelerinin ve çalışanların sorumluluğunu içerdiği, bilgi sistemlerine ilişkin kabul edilebilir kullanım şartlarını tanımladığı ve detay güvenlik standartlarına ve prosedürlerine referans verdiği gözlemlenir.	T	Z	
K1.8	Kurum bünyesinde hazırlanmış, güncel ve kullanılan detay güvenlik standartları ve prosedürleri incelenir. Bu dokümanların aşağıdaki konuları içerdiği	T	Z	

	<p>gözlemlenir.</p> <ul style="list-style-type: none">• Güvenlik uyum politikası• Yönetimin risk kabulü• İletişim güvenliği• Erişim ve yetkilendirme• Güvenlik duvarı yönetimi• E-posta güvenliği• BT güvenlik prosedürleri ile uyum• Güvenlik olayları ve ihlal yönetimi• Dizüstü/masaüstü bilgisayar güvenliği• İnterne kullanımı güvenliği• Ağ güvenliği• Denetim izleri güvenliği• Fiziksel ve çevresel güvenlik• Lisans yönetimi• Temiz masa politikası		
K1.9	Bilgi güvenliği yönetiminin altında bulunduğu hiyerarşik yapı incelenir. Bilgi güvenliği ile ilgilenen birimlerin karar verme yetkilerine sahip olduğu gözlemlenir.	T	O

TASLAK

K2 - Bilgi güvenliğinden kaynaklanabilecek risklerin nasıl yönetileceğinin belirlendiği, kurumsal strateji ve kurumsal mimariye uygun bir bilgi güvenliği planı hazırlanır.

#	Denetim prosedürleri	T/İ	Z/O
K2.1	Kurum stratejik hedefleri ve kurumsal mimarisi ile uyumlu, yönetim tarafından onaylı ve güncel bir bilgi güvenliği planının varlığı gözlemlenir. Planın kurumda güvenlik riskinin yönetimi ile ilgili olarak en uygun güvenlik yönetimi uygulamalarını, güvenlik çözümlerini, kaynakları, sorumlulukları ve öncelikleri içerdiği kontrol edilir.	T	Z
K2.2	Bilgi güvenliği planının oluşturulmasında veri yönetişiminin, teknoloji standartlarının, güvenlik ve kontrol politikalarının, risk yönetiminin ve ilgili mevzuat yükümlülüklerinin dikkate alındığı gözlemlenir.	T	Z
K2.3	Bilgi güvenliği planının aşağıdaki unsurları içerdiği gözlemlenir. <ul style="list-style-type: none"> • Kurum çapında geçerli olacak güvenlik standartları • Politikaların kurum genelinde uygulanması amacıyla oluşturulmuş politikalar • Bilgi güvenliği yeni personel ihtiyacı ve planlaması • Bilgi güvenliği yatırımları 	İ	Z
K2.4	Kurumsal mimarinin bir parçası olarak güvenlik yönetimi için kullanılan çözümlerin (ör: sistem, araç, vb.) bir envanterinin tutulduğu kontrol edilir.	İ	O
K2.5	Kurum bünyesinde kullanıcıların bilgi güvenliği farkındalığını artırmak amacı ile bilgi güvenliği eğitimlerinin düzenlendiği ve bunlara katılımın sağlandığı kontrol edilir.	İ	Z

K3 - Kurum bünyesinde bilgi güvenliği uygulamalarının sürekli olarak gelişmesi için BGYS izlenir ve gözden geçirilir.

#	Denetim prosedürleri	T/i	Z/O
K3.1	Kurum bünyesindeki BGYS'nin etkinliğinin sürekli olarak değerlendirildiği, BGYS politikalarının ve güvenlik uygulamalarının sürekli izleme ve değerlendirme yolu ile BGYS'nin gelişimi için gereksinimlerin tespit edildiği gözlemlenir. Bu doğrultuda güvenlik denetimlerinden, güvenlik olaylarından, önerilerden, kullanıcı geri bildirimlerinden (ör: anketler yolu ile) ve güncel güvenlik eğilimlerinden yararlanıldığı gözlemlenir.	İ	O
K3.2	Kurum bünyesinde uygulanmakta olan BGYS ile ilgili düzenli olarak iç denetim faaliyetlerinin yürütüldüğü gözlemlenir.	İ	O
K3.3	BGYS'nin yönetim tarafından düzenli olarak değerlendirmeye tabi tutulduğu ve gerektiğinde kapsam değişikliklerine ve geliştirmelere gidildiği gözlemlenir.	İ	O
K3.4	BT güvenlik planının izleme ve gözden geçirme çalışmaları neticesinde ihtiyaç ve gereksinimler uyarınca güncellendiği gözlemlenir.	İ	Z

TASLAK

K4 - Kurum bilgi sistemleri üzerinde önleyici, tespit edici ve düzeltici uyarlamaların yapılması ve kurum bünyesinde bu uyarlamalara paralel olarak güvenlik yamalarının ve anti-virüs uygulamalarının kullanılması gibi önlemlerin alınması ile bilgi sistemleri ve teknolojisinin kötü amaçlı yazılımlardan etkilenme riski azaltılır.

#	Denetim prosedürleri	T/İ	Z/O
K4.1	Kurum bünyesinde zararlı yazılımların önlenmesine ilişkin bir politikanın ya da prosedürün oluşturulduğu, belgelendiği ve tüm kurum çapında farkındalığın yaratıldığı teyit edilir.	T, İ	Z
K4.2	Zararlı yazılımlardan korunmak amacıyla tüm bilgisayar ve sunucularda zararlı yazılım tespit edici ve bunların etkilerini giderici otomatik kontrollerin uygulandığı ve saptanan ihlallerin düzgün bir şekilde raporlandığı teyit edilir.	İ	Z
K4.3	Zararlı yazılımları saptayan uygulamaların (ör: anti-virüs, kişisel güvenlik duvarı tanımları gibi) düzenli olarak güncellendiği gözlemlenir.	İ	Z
K4.4	Örnek personel bilgisayarları ve sunucular seçilerek, bunlar üzerinde anti-virüs programının kurulu olduğunun, virüs tanımlarını içeren dosyaların son güncellenme tarihleri gözlemlenir.	İ	Z
K4.5	Kurum içerisindeki BT güvenliği ile sorumlu çalışanlar ile görüşülerek, zararlı yazılımların önlenmesine ilişkin politika ve politikaya uyum amacıyla kendilerine atanan sorumluluklar ile ilgili farkındalıklarının mevcut olduğu teyit edilir.	İ	Z
K4.6	Tüm güvenlik yazılımlarının ve güncellemelerinin merkezi bir konfigürasyon ve değişiklik yönetimi kullanılarak yönetildiği, dağıtıldığı ve izlendiği gözlemlenir.	İ	Z
K4.7	Kurum bünyesinde BT güvenliğini sağlamakla sorumlu personelin kullanılan mevcut yazılımlar ile ilgili güvenlik tehditlerini düzenli olarak takip ettiği teyit edilir.	İ	Z
K4.8	Kurum e-posta servisine gelen e-postaların, personelce indirilen dosyaların ve diğer dışarıdan veri girişlerinin (taşınabilir diskler vs.) filtrelendiği ve tehdit oluşturabilecek e-posta ve dosyaların engellendiği kontrol edilir.	İ	Z

K5 - Bilgi sistemleri bileşenleri ve iletişim ortamındaki bilgilerin korunması için kurum bünyesindeki bilgi sistemleri ağının güvenliği sağlanmalıdır.

#	Denetim prosedürleri	T/İ	Z/O
K5.1	Kurum bünyesinde bir ağ güvenlik politikasının (verilen hizmetler, izinli trafik ve bağlantı türleri v.b. içerecek şekilde) oluşturulduğu ve uygulandığı teyit edilir. Politikanın iş ihtiyaçları ve risk değerlendirmeleri baz alınarak oluşturulduğu kontrol edilir.	T	Z
K5.2	Sadece kurum tarafından yetkilendirilmiş cihazların kurum ağına ve bilgi sistemlerine erişebileceği ve bu cihazların sadece en azından bir şifre/parola erişimi ile kullanılabildiği kontrol edilir.	T	Z
K5.3	Güvenlik duvarları (firewall), saldırı tespit ve engelleme (IDS/IPS) sistemleri, web içerik filtreleme gibi ağ filtreleme mekanizmalarının ağ trafiğini kontrol etmek amacıyla mevcut olduğu ve aktif şekilde kullanıldığı gözlemlenir.	İ	Z
K5.4	Tüm kritik ağ bileşenlerinin (ana routerlar, DMZ, VPN switchleri) yönetimi için oluşturulmuş prosedürlerin ve talimatların bulunduğu, bu dokümanların yetkili personel tarafından düzenli olarak güncellendiği, yönetimce onaylandığı ve belgeler üzerinde yapılan değişikliklerin belge geçmişi kısmında tutularak izlenilebilirliğinin sağlandığı doğrulanır.	İ	Z
K5.5	Kurum ağ bileşenlerinin standart konfigürasyonlarının tanımlanıp tanımlanmadığı kontrol edilir. Her ağ bileşeninden bir örnek seçilerek, kurum ağ güvenliğini sağlayacak şekilde standart olarak kabul edilen konfigürasyonlara uygun şekilde ayarlanmış olduğu kontrol edilir.	İ	Z
K5.6	Kurum ağ bileşenlerinde yapılacak konfigürasyon değişikliklerinin değişiklik yönetimi sürecine uygun olarak gerçekleştirildiği kontrol edilir.	İ	Z
K5.7	Ağ korumasının yeterli düzeyde olduğunun kontrolü için yılda en az bir kez olmak üzere hem kurum dışından hem de kurum içinden sızma testlerinin ve zafiyet taramalarının düzenlendiği gözlemlenir. Bu test ve taramaların sonuçlarının raporlandığı ve bulguların takibinin yapıldığı gözlemlenir.	İ	Z
K5.8	Kurum bünyesindeki verilerin belirlenen kriterlere göre (dışarıya açıklık seviyeleri, içerdiği bilgi vs.) göre gizlilik ve hassaslık konusunda sınıflandırıldıkları kontrol edilir.	İ	O
K5.9	Kurum dışına iletilen verilerin, sınıfına göre güncel yöntemler ile kriptolandığı gözlemlenir.	İ	O
K5.10	Kurum bünyesinde kriptolama (şifreleme) süreçleri uygulanıyorsa, bu süreçle ilgili politika ve prosedürler incelenir. Güçlü anahtar üretimi için gerekli minimum anahtar boyutlarını, anahtar üretim algoritmaları kullanımını, anahtarların üretimi için gerekli standartların tanımını, anahtar kullanım amaç ve sınırlamalarını, anahtarlar için izin verilen kullanım süreleri veya aktif yaşam sürelerini, anahtar yedekleme, arşiv ve imha süreçleri ile kabul edilebilir anahtar dağıtım yöntemlerini tanımlayan bir anahtar yaşam döngüsü yönetim sürecinin mevcudiyeti gözlemlenir.	T	O

K5.11	Özel anahtarların gizlilik ve bütünlüğünü korumak için bulunan kontrolleri deęerlendirilerek, özel imzalama anahtarlarının güvenli kriptolama aracılığıyla (FIPS 140-1, ISO 15782-1, ANSI X9.66 gibi) depolandığı, özel anahtarların güvenli kriptolama modülünden üretildiğı, özel anahtarların yedeklendiğı ve sadece yetkili personel tarafından saklandığı ve güvenli fiziksel ortamdan geri alınabileceğı teyit edilir.	İ	O
-------	--	---	---

TASLAK

K6 - Kurum ağı erişim noktaları (dizüstü bilgisayarlar, masaüstü bilgisayarlar, sunucular ve diğer mobil ve ağ aygıtları ve yazılımlar), kurum ağı üzerinden iletilen veri için tanımlanan gerekli minimum güvenlik seviyelerini karşılamalıdır.

#	Denetim prosedürleri	T/İ	Z/O
K6.1	Kurum bünyesindeki sunucular için belirlenmiş standart güvenlik konfigürasyonlarının bulunup bulunmadığı kontrol edilir. Denetim kapsamına alınan uygulamaların kurulu olduğu kritik sunucularda yer alan ve kullanıcı yönetiminin sağlandığı işletim sistemlerinin güvenlik ayarlarının standart güvenlik konfigürasyonlarına uygun olduğu kontrol edilir.	T	Z
K6.2	Kurum bünyesindeki tüm uygulamalara, işletim sistemlerine, veri tabanlarına, cihazlara, sistemlere ve diğer teknolojik cihazlara erişim sağlanması için kullanılan şifrelerin kurum bünyesinde tanımlanmış olan şifre parametrelerine uygun olarak belirlendiği gözlemlenir.	İ	Z
K6.3	Örnek kullanıcı bilgisayarları seçilerek, bu bilgisayarların kurum güvenlik politikalarına uygun şekilde, belirli bir süre kullanılmadıklarında otomatik olarak kilitlendiği kontrol edilir.	İ	O
K6.4	Kurum bünyesinde belirlenmiş olan veri sınıflarına göre kritik verilerin kriptolanarak ya da ilgili diğer önlemler alınarak saklandığı gözlemlenir.	İ	O
K6.5	Kurum bilgi kaynaklarına kurum dışından erişim gerçekleştirilmesi süreci ile ilgili politika dokümanlarının mevcut olduğu gözlemlenir.	T	Z
K6.6	Kurum bilgi kaynaklarına erişimin uygun bir kimlik doğrulama yöntemi ile (örn: kullanıcı adı/parola, iki faktörlü vb.) gerçekleştirildiği gözlemlenir.	İ	Z
K6.7	Kurum bünyesinde kullanıcıların bilgi kaynaklarına erişimleri ile ilgili denetim izlerinin tutulmasına dair bir politika ya da prosedürün varlığı gözlemlenir. Prosedürde denetim izi olarak hangi parametrelerin (ör: başarılı ya da başarısız giriş denemeleri, bilgi sistemleri üzerinde yapılan faaliyetler, vb.) tutulacağını belirlendiği kontrol edilir.	T	Z
K6.8	Kurum bilgi kaynaklarına erişimlerin denetim izlerinin prosedürlerde belirtilen sistemler için, prosedürlerde belirtildiği şekilde tutulduğu ve düzenli olarak gözden geçirme ve izlemeye tabi tutulduğu incelenir.	İ	Z
K6.9	Örnek ağ cihazları seçilerek (Güvenlik duvarı, IDS gibi) bunların kurum güvenlik politikalarına ve genel kabul görmüş güvenlik prensiplerine uygun şekilde yapılandırıldıkları gözlemlenir.	İ	Z
K6.10	Örnek ağ cihazları seçilir ve bunlara ilişkin yama ve güncellemelerin takip edildiği, düzenli olarak kontrol edildiği ve gerekli görülen yama ve güncellemelerin uygulandığı teyit edilir.	İ	Z
K6.11	Son kullanıcı bilgisayarlarının ağ trafiklerini filtreleyen kişisel güvenlik duvarı, web içerik filtrelemesi gibi mekanizmaların kurulu olduğu gözlemlenir.	İ	Z

K6.12	Son kullanıcı cihazlarının imhası ile ilgili kurum politikalarının mevcut olduęu gözlemlenir. Örnek seçilecek imha kayıtları incelenir ve seçilen cihazların bu politikalara göre kurum bilgilerinden arındırıldıęı ve imha edildięine dair kayıtlar incelenir.	İ	O
-------	---	---	---

TASLAK

K7 - Tüm kullanıcılar, bilgi sistemleri üzerinde iş tanımları ile paralel, ihtiyaç duyacakları en az seviyede erişim yetkilere sahip olmalıdır.

#	Denetim prosedürleri	T/İ	Z/O
K7.1	<p>Kurum bünyesindeki bilgi kaynaklarına erişim sağlanması ile ilgili kontrolleri belirleyen bir erişim ve yetkilendirme politikası ya da prosedürünün mevcut olduğu gözlemlenir.</p> <p>Erişim yetkilendirme prosedürleri görevler ayrılığı ilkesine uygun olarak tasarlanmalıdır. Görevler ayrılığı bir görevi tek bir kişinin başından sonuna kadar tamamlamasını engelleme ve dolayısıyla bu sebeple ortaya çıkacak riskleri azaltma amacını taşır. Görevler ayrılığının sağlandığı durumlarda kişilerin uygulamalara, verilere, sistemlere ve ilgili diğer fonksiyonlara erişimi kontrollü ve belirli bir kritik işlemi aynı kişinin başlatıp sonlandıramadığı bir şekilde olur.</p> <p>Bu doğrultuda, erişim ve yetkilendirme politikalarının ya da prosedürlerinin en azından aşağıdaki unsurları içermesi beklenir.</p> <ul style="list-style-type: none"> • Kurum bünyesinde farklı sistem ve platformlar için uygulanan yetkilendirme yöntem ve akışları • Yetkilendirme ile ilgili rol ve sorumluluklar • Yeni işe başlayan personel için takip edilecek yetkilendirme süreci • Görev değiştiren personel için takip edilecek yetkilendirme süreci • İşten ayrılan personelin kullanıcı haklarının silinmesi ya da askıya alınması ile ilgili süreç • Uygulama kullanıcı ve yetki listelerinin düzenli olarak izlenmesi, değerlendirilmesi ve doğrulanması süreci • Görevler ayrılığı ilkesinin sağlanması 	T	Z
K7.2	Kurum bünyesindeki uygulamalarda ve sistemlerde kullanıcı adlarının belli standartlara göre oluşturulduğu teyit edilir.	İ	Z
K7.3	Tüm kullanıcıların birbirinden ayrı eşsiz kullanıcı isimlerine veya tanımlayıcılara sahip olduğu gözlemlenir.	İ	Z
K7.4	Uygulama kullanıcılarının yetkilendirmelerinin görevlerine ve unvanlarına göre tanımlandığı kontrol edilir. Yetkilendirme için kullanıcının birim ve pozisyonuna karşılık olarak uygulama üzerinde sahip olacağı yetkilerin belirlenmiş olduğu gözlemlenir. Buradaki yetkilerin ise kullanıcının sahip olması gereken en düşük seviyede yetki prensibine göre atandığı kontrol edilir.	İ	Z

K7.5	Kapsamdaki uygulamalar, işletim sistemleri, veri tabanları ve ağ cihazları için erişim ve yetki kontrol listelerinden bir örneklem seçilir ve yetkilerin aşağıdaki hususlar dikkate alınarak verildiği kontrol edilir. <ul style="list-style-type: none"> • Bilgi güvenliği politikaları • Bilginin ve uygulamanın kritikliği • Kişinin pozisyonuna göre ilgili yetkinin gerekliliği • Genel iş tanımları için hazırlanmış standart kullanıcı profilleri • Verilen yetkilerin görevler ayrılığı ilkesi ile uyumu • Veri sahibinin ve yönetimin yetki için onayı • Kullanıcı kimlikleri ve yetkileri ile ilgili dokümanların merkezi olarak saklanması • Şifrelerin oluşturulması, kullanıcıya iletilmesi ve değiştirilmesi 	İ	Z
K7.6	İnsan Kaynakları biriminden denetim döneminde unvan veya bölüm değiştirmiş ve işten ayrılmış kullanıcıların listesi temin edilir. İlgili yetki değişikliklerinin ve iptallerinin ilgili personel hareketleriyle uygun bir zamanda gerçekleştiği kontrol edilir.	İ	Z
K7.7	Gerek BT bünyesinde gerekse de iş uygulamaları seviyesinde görevler ayrılığı ilkesinin oluşturulması ve bu ilkeye aykırılık oluşturabilecek konuları belirlemek için bir risk değerlendirilmesinin yapıldığı araştırılır.	İ	Z
K7.8	Erişim yetki taleplerinin, bunlara ilişkin onayların, ilgili erişimlerin uygulama ve sistemlerde tanımlanması ve bunlara ilişkin izleme ve değerlendirme çalışmalarının farklı kişiler ya da gruplar tarafından yürütüldüğü örneklem bazında incelenir.	İ	Z
K7.9	Kullanıcı yetkilerinin, ilgili uygulamanın, veritabanının veya işletim sisteminin izleme sorumluları tarafından (iş birimi yöneticileri, iç kontrol birimleri vs.) düzenli olarak gözden geçirildiği ve saptanan uygunsuz yetkilerin değiştirilmesi için ilgili önlemlerin alındığı gözlemlenir.	İ	Z
K7.10	Yüksek seviyede yetkilere sahip olan yönetici hesaplarının yetkilendirmeleri için üst düzey yönetici onayının bulunduğu, bu yetkilere sahip kullanıcıların listesinin düzenli olarak gözden geçirildiği kontrol edilir.	İ	Z
K7.11	Kritik verilerin bulunduğu uygulamalara, veritabanlarına veya işletim sistemlerine girişlerde ek güvenlik mekanizmalarının kullanıldığı teyit edilir (örnek olarak şifre, token (yetkili kullanıcılara BT servislerine erişim için otomatik anahtar üreten fiziksel cihazlara verilen isim), dijital imza).	İ	Z
K7.12	Denetim döneminde açılmış hesaplar listesi temin edilir. Örnek olarak seçilen hesapların yetkilendirme süreçleri aşağıdaki hususlar doğrultusunda kontrol edilir. <ul style="list-style-type: none"> • Açılan talebin istenilen rolü ve yetkileri açıkça belirttiği • Yetki için iş gereksinimleri • Veri sahibinin ve yöneticinin onayı • Standart dışı talepler için iş gerekçesi ve yönetim onayı • İstenilen yetkinin kişinin rolüyle ve görevler ayrılığı ilkesiyle uyumu • Yetki sağlama sürecinin tamamlandığına dair belgelerin varlığı ve saklanması. 	İ	Z

K7.13	Tüm kritik verilere kullanıcı erişimlerinin denetim izlerinin tutulduğu ve bu denetim izlerine, ilgili veriler üzerinde yetkileri bulunan kullanıcılarının hiçbir şekilde erişemediği kontrol edilir.	İ	Z
-------	---	---	---

TASLAK

K8 - İş gereksinimlerini ve acil durumları göz önünde bulundurarak; binalara, tesislere ve kritik alanlara fiziksel erişimler için yetki verme, yetki kısıtlama ve bu yetkileri iptal etmeye yönelik prosedürler tanımlanmalıdır. Bu alanlara erişimlerin kontrollü olmasının yanında yetkilerin tümü onaya istinaden verilmeli, denetim izleri tutulmalı ve gözden geçirilmelidir. Bu kontroller ilgili alanlara fiziksel erişimi olan daimi ve geçici çalışanlara, ziyaretçilere, müşterilere tedarikçilere veya tüm üçüncü şahıslar dahil olmak üzere herkese uygulanmalıdır.

#	Denetim prosedürleri	T/İ	Z/O
K8.1	Bilgi sistemleri ekipmanlarının, donanımlarının ve cihazlarının bulunduğu sistem odalarına girişlerin, giriş yapan kişilerin tanımlanabileceği ve kayıt altına alınabileceği şekilde gerçekleştirilmesi için mekanizmaların mevcut olduğu gözlemlenir (ör: kartlı giriş, parmak izi, retina kontrolü vs.)	T	Z
K8.2	Sistem odalarına giriş yetkilendirmelerinin nasıl yapılması gerektiğine dair güvenlik adımlarını içeren politika ve prosedürlerin varlığı gözlemlenir.	T	Z
K8.3	Sistem odalarına yapılan tüm giriş denemelerinin (başarılı ya da başarısız) kaydedildiği teyit edilir.	İ	Z
K8.4	Sistem odaları için talep edilen giriş yetkilerinin ilgili kişinin yöneticisi ve ilgili BT yöneticisi tarafından onaylanarak verildiği, sistem odasına giriş yetkisine sahip kişilere sistem odasında uymaları gereken kurallara dair bir bilgilendirmenin yapıldığı ve imzalarının alındığı gözlemlenir.	İ	Z
K8.5	Sistem odasında bulunan tüm kişilerin kimliklerini dışarıdan görülebilecek şekilde taktıkları ya da taşıdıkları gözlemlenir.	İ	Z
K8.6	Sistem odasına giriş yetkisi bulunmayan ziyaretçilere her an yetkili bir çalışanın eşlik ettiği gözlemlenir.	İ	Z
K8.7	Düzenli olarak fiziksel güvenlik ve bunlara ilişkin hususların ele alındığı eğitimlerin düzenlendiği teyit edilir.	İ	O
K8.8	Kurumdaki BT donanımlarının bulunduğu alanların güvenliğini sağlamak adına Fiziksel güvenlik yönetimi politika ve prosedürlerinin oluşturulduğu görülür. Bu prosedürlerde belirtilen kurallara kurum bünyesinde uyulduğu gözlemlenir.	İ	Z
K8.9	Sistem odası giriş yetkilendirme süreci incelenir. Giriş yetkilerinin yönetim tarafından onaylandığı ve sadece görev tanımı gereği sistem odasında girmesi gerekebilecek kişilerin yetkilerinin bulunduğu gözlemlenir.	İ	Z
K8.10	Sistem odasının kameralar ile izlenildiğinden ve bu kameraların sistem odasının her noktasını göreceği şekilde konumlandırıldığı gözlemlenir.	İ	Z

K8.11	<p>Kurum bünyesinde temiz masa politikasının uygulandığı gözlemlenir. Bu kapsamda örnek çalışanlar seçilir ve aşağıdaki kurallara uydukları gözlemlenir.</p> <ul style="list-style-type: none">• Masada o sırada ihtiyaç duyulan belgelerin haricinde belge bulunmaması• Şifre ve kullanıcı adı bilgilerini içeren kağıtlar açıkta bulunmaz• Kurum bilgileri içeren kağıtların çöpe atılmaması, kağıt imha makinelerinde kırılması• Masalarda cep telefonu, PDA, USB bellek, harici disk, CD, DVD gibi elektronik veri içeren cihazların başıboş bırakılmaması• Masalarda hesap cüzdanı, kredi kartı, çek defteri ve benzeri kritik veriler içeren dokümanların başıboş bırakılmaması• Proje dosyaları gibi önemli dokümanların kilitli dolaplarda tutulması• Kullanıcılar bilgisayarın başında değilken şifre korumasının aktif olması	İ	Z
-------	---	---	---

TASLAK

K9 - Kurum bünyesinde kullanılan hassas ve bilgi güvenliği açısından kritik bilgi teknolojileri cihazları, özel formlar, kıymetli evrak, özel ihtiyaca yönelik yazıcı ve güvenli anahtar (şifre) üreticiler üzerinde uygun fiziksel güvenlik önlemleri ve envanter yönetimi teknikleri uygulanmalıdır.

#	Denetim prosedürleri	T/İ	Z/O
K9.1	Kurum bünyesindeki hassas belgelerin, dokümanların ve bunların çıktı olarak alındığı cihazların (ör: yazıcı, faks makinası, vb.) alınması, kullanılması, kullanımdan kaldırılması ve imhası ile ilgili olarak süreçlerin tanımlandığı ve prosedürlerin oluşturulduğu gözlemlenir.	T	O
K9.2	Hassas dokümanlara ve çıktı cihazlarına erişim yetkilerinin, “ihtiyaç duyulacak en düşük seviyede yetki” prensibine göre verildiği kontrol edilir.	+İ	O
K9.3	Hassas dokümanların ve çıktı cihazlarının envanterinin tutulduğu ve düzenli olarak sayımların yapılarak bu envanter ile karşılaştırmaların yapıldığı gözlemlenir.	İ	O
K9.4	Hassas dokümanlar ve çıktı cihazları için fiziksel koruma önlemlerinin alındığı gözlemlenir.	İ	O
K9.5	Hassas dokümanların ve çıktı cihazlarının, içerdikleri veya içerebilecekleri bilgilerin sonradan bir daha kullanılmayacağı şekilde imha edildiği gözlemlenir.	İ	O

K10 - Kurum bilgi sistemleri altyapısı yetkisiz erişimlere karşı izlenir ve bilgi sistemleri altyapısı üzerindeki kritik görülen faaliyetlerin olay izleme ve vaka yönetimi süreci içerisinde kapsandığı teyit edilir.

#	Denetim prosedürleri	T/İ	Z/O
K10.1	Altyapı güvenliği izleme araçları tarafından üretilen güvenlik ile ilgili kayıtların risk seviyelerine göre kayıt altına alındığı gözlemlenir.	T, İ	Z
K10.2	Güvenlik olaylarının belirlenip kurum bünyesinde paylaşıldığı kontrol edilir.	İ	Z
K10.3	Güvenlik olay kayıtlarının düzenli olarak izlendiği ve önemli olarak görülen olaylar için gerekli eylemlerin alındığı (disiplin sürecinin başlatılması, yaptırımlar, işten çıkarma vb.) gözlemlenir. Bu doğrultuda denetim dönemi boyunca gerçekleşmiş olaylar arasından bir örneklem seçilir ve alınan eylemler incelenir.	İ	Z

TASLAK

2.4.5. Ek Kaynaklar

- ISACA. (2007). COBIT 4.1 Framework – DS5. Rolling Meadows, Illinois, United States of America.
- ISACA. (2012). COBIT 5 Enabling Processes – APO13, DSS05. Rolling Meadows, Illinois, United States of America.
- ITIL V3 2011 Service Operation, 4.5 Access Management (UK Cabinet Office, 2011)
- ISO/IEC 27002, Code of Practice for Information Security Management (International Organization for Standardization(ISO)-International Electrotechnical Commission(IEC), 2005)
- Global Technology Audit Guide (GTAG), Identity and Access Management (The Institute of Internal Auditors, 2007)

TASLAK

4.3. YARDIM MASASI, OLAY VE PROBLEM YÖNETİMİ

Sürecin Genel Tanımı

Yardım masası bir kurumda, ürün ve hizmetler ile ilgili son kullanıcılara ve iç müşterilere destek sağlamak adına BT hizmetleri ile ilgili sorunları gidermek veya bu sorunları çözüm için ilgili uzmanlara yönlendirme görevini üstlenmektedir. BT hizmetleri ile ilgili herhangi bir ihtiyaç ya da sorun ortaya çıktığında BT yardım masası kullanıcı ile ilk temas kuran birimdir. Yardım masası bazı kurum ya da kuruluşlarda hizmet masası olarak da isimlendirilebilir.

BT hizmetlerinde oluşan beklenmedik kesintilere ya da BT hizmet kalitesinin düşmesine sebep verecek durumlar “olay” olarak değerlendirilmektedir. Olay yönetimi sürecinin hedefi olay tanımına uyan durumlar ile karşılaştığı andan itibaren hizmetlerin (BT ve diğer iş birimleri ile üzerinde mutabakata varılmış olan anlaşmalarca belirtilen şekilde bkz: BT Hizmet Yönetimi) en kısa sürede normal haline dönmelerinin sağlanmasıdır. Olay yönetimi, BT hizmetlerinde veya iş süreçlerinde aksamaya sebep olabilecek BT kaynaklı tüm olayları kapsamaktadır.

Kullanıcılar, BT hizmetleri ile ilgili herhangi bir desteğe ihtiyaç duyduklarında yardım masasına başvururlar. Bu başvurular örnek olarak BT ortamında çalışan bir araç üzerinde kayıt açma şeklinde gerçekleşebilir. Yardım masası, olay tanımına uyan başvuruları otomatik veya sürece uygun şekilde olay yönetimi sürecine aktarılır ve ilgili uzmanlara yönlendirilir.

Çözümlemeyen, tekrarlayan veya kurum tarafından kritik olarak değerlendirilen olaylar, “problem” olarak değerlendirilir. Problemler, problem yönetimi ekipleri tarafından ele alınır ve takip edilir.

Problem yönetimi süreci, kurumdaki tüm problemlerin oluştuğu andan çözümlenmesi ve çözüm sonrası raporlanmasına kadar olan tüm yaşam döngüsünün yönetilmesidir. Problem yönetim süreci problem tanımına uyan olayları ardındaki kök nedenleri saptayarak çözümlenmeyi, çözümlenemeyen problemlerin iş süreçleri üzerindeki etkileri azaltmak için engellemeyi hedefler. Bilgi sistemleri değişiklik yönetimi ve olay yönetimi süreçleri ile beraber problem yönetimi süreci, BT hizmetlerinin güvenilirliğinin ve kalitesinin artırılmasına, kesintilerin azaltılmasına ve hizmet erişilebilirliğinin artırılmasına yardımcı olur.

Olay veya problemlerin çözümünün bilgi sistemleri üzerinde bir değişiklik gerektirdiği durumlarda çözüm, kurumun değişiklik yönetimi sürecine uygun bir şekilde gerçekleştirilir. Son kullanıcı tarafından açılan talep kaydından, çözüm için açılan değişiklik kaydı ve uygulanan değişikliğe kadar durum, takip edilebilir durumda bulunur.

Yardım masası, olay ve problem yönetimi sürecinin etkin bir şekilde uygulanması ile olaylar en erken şekilde fark edilir ve çözüme kavuşturulur. Bu durum BT hizmetlerinin sürekliliğini sağlanmasına ve işlevselliğinin artırılması konusunda fayda sağlar.

Sürecin BT Denetimi Açısından Önemi

Yardım masası, olay ve problem yönetimi BT ve BT'ye bağımlı iş süreçlerinin sürdürülebilirliği ve kritik BT işlevselliği açısından önemli olması sebebiyle, BT denetimlerinde sıkça incelenen süreçlerden biridir. Bu sürecin değerlendirilmesi ile iş sürekliliğini olumsuz olarak etkileyebilecek durumların saptandığına ve çözümlendiğine dair makul bir güvence sağlanabilir. Bu sayede, BT uygulamalarının hesaplama, raporlama vb. gibi denetim açısından kritiklik taşıyan işlevlerini etkileyen durumların, hataların ve olumsuzlukların denetim dönemi içerisinde kontrollü bir biçimde tespit edilip, değerlendirilip çözümlendiğine ve tekrarlanmasının önlenmesine dair gerekli önlemlerin alındığına ilişkin bir kanaat oluşturulabilir. Bu çerçevede yardım masası, olay ve problem yönetimi sürecinin denetimi, özellikle mali ve sistem odaklı denetimlerde sıklıkla ele alınan konulardan biri olmaktadır.

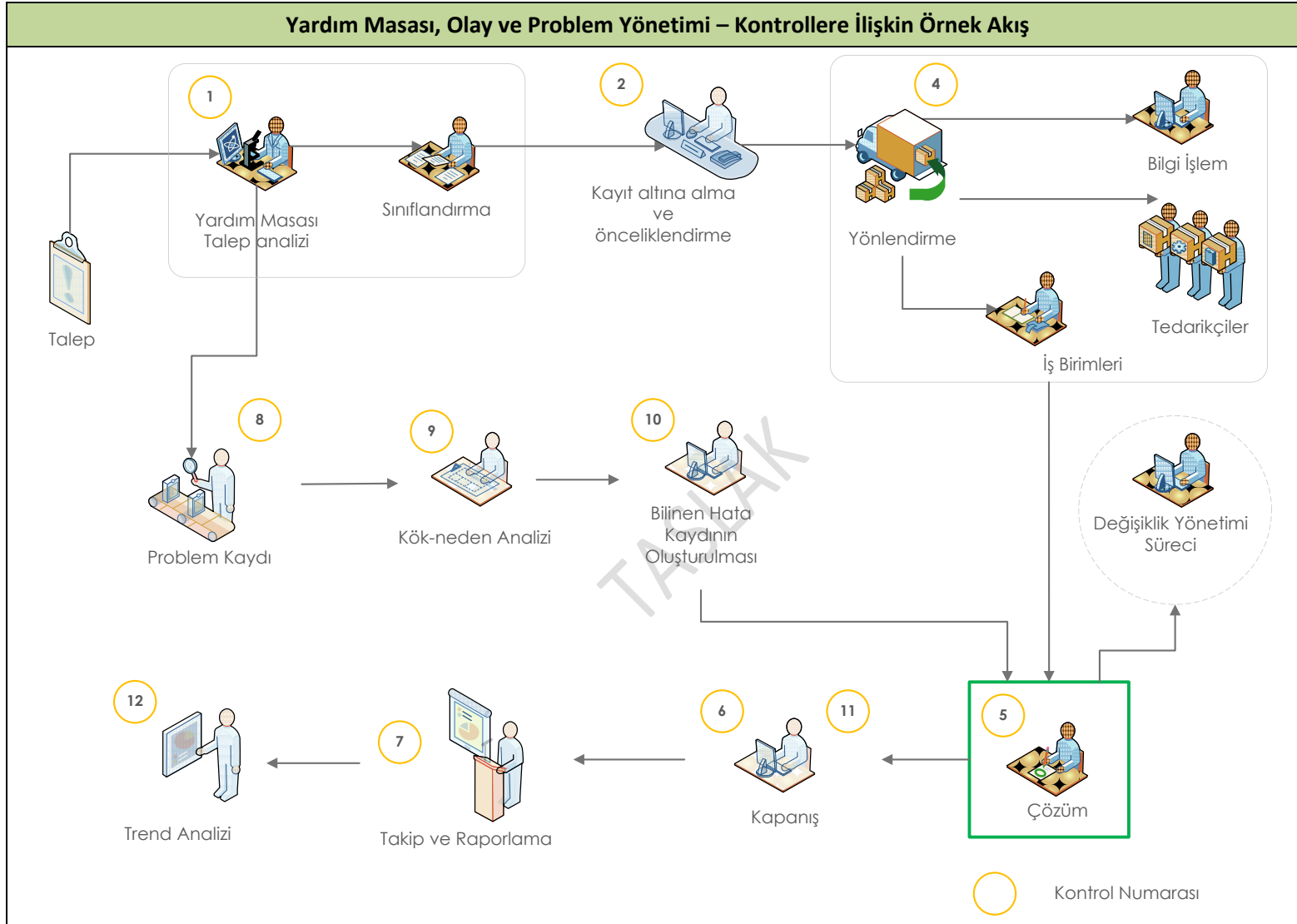
Yardım masası, olay ve problem yönetimi, BT denetimi açısından aşağıdaki süreç ve kontroller üzerinden takip edilebilir. Söz konusu akış her kurum için farklı olabileceği gibi, süreç içerisinde ele alınan olay ve problem tipleri, kullanılan olay ve problem yönetimi araçları ve takip ve raporlama mekanizmaları da kurumdan kuruma değişebilmektedir.

TASLAK

Kontrollere İlişkin Örnek Akış

Süreçte yer alan tipik kontrollere aşağıdaki tabloda yer verilmiştir:

Yardım Masası, Olay ve Yönetimi - Kontroller	
K1	İlgili BT birimi tarafından olay ve yardım masası yönetim süreci belirlenir, talep sınıflandırma yöntemleri ve modelleri tanımlanır.
K2	Yardım talepleri ve olaylar, ilgili BT birimi tarafından iş kritikliğine ve yürürlükteki hizmet seviyesi sözleşmesine göre tanımlanır, kayıt altına alınır ve sınıflandırılır.
K3	Olay belirtileri tanımlanır ve kaydedilir, olası nedenler belirlenir ve çözüm planı hazırlanır.
K4	Olaylarla ilgili tanımlanmış çözüm ya da geçici çözümler belgelendirilir, uygulanır ve kayıt altına alınır. İlgili BT hizmetinin tekrar devreye alınması için gerekli işlemler yapılır.
K5	Olay çözümünün yeterli olduğu ve talebin karşılandığı doğrulanır ve olay kaydı sonlandırılır.
K6	Problemlerin sınıflandırması ve raporlanması için gerekli kriter ve prosedürler tanımlanır ve uygulanır.
K7	Gerçekleşen problemlere ilişkin kök nedenleri değerlendirmek ve analiz etmek için ilgili konuda uzmanlar görevlendirilerek problemler araştırılır ve teşhis edilir.
K8	Problemin kök analizi tanımlandıktan sonra, ilgili çözüm yöntemlerinin ileride referans olarak kullanılabilmesi için “bilinen hatalar” kayıtları oluşturulur ve uygun bir geçici çözüm hazırlanarak potansiyel çözümler belirlenir.
K9	Bir problemin ortadan kaldırılması için tasarlanan çözümler değişiklik yönetimi sürecinden geçerek uygulanır. Çözümler kök nedenlere yönelik olarak kalıcı olacak şekilde tasarlanır. Problemden etkilenen çalışanların, yapılanların ve çözüm için hazırlanan planların farkında olması sağlanır.
K10	Yeni problemlere neden olabilecek eğilimleri gözlemleyebilmek ve tespit edebilmek için özellikle olay ve değişiklik kayıtları verileri toplanır ve analiz edilir.



Risk – Kontrol Eşleşmeleri

Yardım Masası, Olay ve Problem Yönetimi Risk – Kontrol Eşleşmeleri											
Riskler	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11
R1. Çözilemeyen ya da saptanamayan olaylar sebebiyle iş faaliyetlerinde ve iş süreçlerinde kesintilerin oluşması	+	+	+	+	+	+	+	+	+	+	+
R2. BT hizmetlerinin kesintiye uğraması	+	+	+	+	+	+	+	+	+	+	+
R3. Bilgi kaybı	+	+	+	+	+	+	+	+	+	+	+
R4. Yardım masasının etkin bir şekilde çalışmaması sonucu önemli olayların zamanında çözümlenmemesi	+							+			
R5. Kök nedeni saptanmayan ve sadece geçici çözümler bulunan problemlerin ve olayların tekrarlaması							+	+			
R6. Problemlerin zamanında çözülmemesi								+	+	+	
R7. Kaynakların verimli kullanılamaması								+			+
R8. Tüm olayların ve problemlerin takip edilememesi	+	+				+					+
R9. Olaylar ve problemler arasında önceliklendirmenin doğru yapılamaması sonucu önemli sorunların geç çözülmesi		+							+		

Yardım Masası, Olay ve Problem Yönetimi Risk – Kontrol Eşleşmeleri											
Riskler	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11
R10. BT hizmetlerinde kalite eksikliği	+	+	+	+	+	+	+	+	+	+	+
R11. Olay yönetimi ile ilgili geri dönüşlerde BT hizmetlerinden memnuniyetsizlik	+	+	+	+	+	+	+	+	+	+	+

TASLAK

Denetim Prosedürleri

K1 - İlgili BT birimi tarafından olay ve yardım masası yönetim süreci belirlenir, talep sınıflandırma yöntemleri ve modelleri tanımlanır.			
#	Denetim prosedürleri	T/İ	Z/O
K1.1	Kurum bünyesinde bir BT yardım masasının varlığı tespit edilir.	T	Z
K1.2	Yardım masasının işleyişinin tanımlandığı politika ve prosedürlerin varlığı araştırılır.	T	Z
K1.3	Mevcut politika ve/veya prosedürlerde olay ve hizmet taleplerinin sınıflandırıldığı olay önceliklendirme yöntemlerinin ve/veya kriterlerinin tanımlandığı gözlemlenir.	T	Z
K1.4	Verimli ve etkin çözümler sağlamak amacıyla, daha önceden yaşanan ve çözümü bilinen olaylar için çözüm yöntemlerinin tanımlanmış olduğu kontrol edilir.	T	O
K1.5	Standart hizmetlerde kişinin kendi kendine ve etkili bir şekilde çözüm üretmesinde, yardım talebi çeşidine göre yardım türü modellerinin tanımlanmış olduğu kontrol edilir.	T	O
K1.6	Teknik hususlar içeren ya da yüksek seviyede uzmanlık gerektiren özellikle önceliği yüksek olay ve güvenlik ihlallerinde, olay eskalasyon (seviye yükseltme) kuralları ve sorumluluklarının tanımlanmış olduğu gözlemlenir.	T	Z
K1.7	Olay yönetimi için kullanılan araçlar incelenir. Olay yönetimi için sadece bu tanımlanmış araçların kullanıldığı doğrulanır.	İ	Z

K2 - Yardım talepleri ve olaylar, ilgili BT birimi tarafından iş kritikliğine ve yürürlükteki hizmet seviyesi sözleşmesine göre tanımlanır, kayıt altına alınır ve sınıflandırılır.

#	Denetim prosedürleri	T/İ	Z/O
K2.1	Yardım masası ve olay yönetimi sürecinde kullanılan araç(lar) incelenir. Bu araç(lar) üzerinden denetim dönemi boyunca açılmış kayıtlar temin edilir ve içerisinden uygun örnekleme ile örnek kayıtlar seçilir. Seçilen yardım (hizmet) taleplerinin ve olayların ilgili politika ve prosedürlerde belirtildiği şekliyle kayıt altına alınmış olduğu ve durumlarının takip edilebildiği kontrol edilir.	İ	Z
K2.2	Olaylar ile ilgili eğilim (trend) analizlerinin gerçekleştirilmesi için, yardım talepleri ve olayların tanımlanan tür ve kategoride sınıflandırılmış olduğu seçilen örnekler üzerinden kontrol edilir.	İ	Z
K2.3	Bir üst adımda seçilen örnek yardım talepleri ve olayların, tanımlanan hizmet seviyesi anlaşmalarındaki iş etkisi ve aciliyetine göre önceliklendirilmiş olduğu gözlemlenir.	İ	Z

TASLAK

K3 - Geçmiş olaylara ilişkin belirtiler tanımlanır ve kaydedilir, olası nedenler belirlenir ve çözüm planı hazırlanır.

#	Denetim prosedürleri	T/İ	Z/O
K3.1	Geçmişte karşılaşılmış olaylara yol açan belirtilerin tanımlandığı ve gelecekte oluşabilecek olaylar için bu belirtilerin izlendiği gözlemlenir.	İ	O
K3.2	Olayların saptanması için belirtilerin kayıt altına alınmış olduğu bir bilgi kaynağının (ör: veri tabanının) varlığı gözlemlenir.	T	O
K3.3	Tespit edilen olay bir problem olarak tanımlandığında ilgili problemin, daha önce karşılaşılan bir durumu işaret etmiyorsa ve bu durum, “tanımlanmış olan problem kaydı” olma kriterlerini barındırıyorsa, yeni bir problem olarak kaydedildiği kontrol edilir.	İ	O
K3.4	Kurum bünyesindeki uzman birimlere, uzmanlıkları ile ilgili olay tiplerinin atanmış olduğu denetlenir. Uzmanlık gerektiren durumlarda, ilgili birimin uygun seviyede katılım göstermiş olduğu kontrol edilir.	İ	O

TASLAK

K4 - Olaylarla ilgili tanımlanmış çözüm ya da geçici çözümler belgelendirilir, uygulanır ve kayıt altına alınır. İlgili BT hizmetinin tekrar devreye alınması için gerekli işlemler yapılır.

#	Denetim prosedürleri	T/İ	Z/O
K4.1	Denetim dönemi içerisinde açılmış olay kayıtları arasından bir örneklem seçilir ve seçilen örnekler için gerekli görülen olay çözümlerinin (geçici ve/veya kalıcı çözümler) seçilip uygulandığı kontrol edilir.	İ	Z
K4.2	Seçilen örnek olayların çözümlenmesinde kullanılan geçici çözümlerin kayıt altına alındığı ve takip edildiği gözlemlenir.	İ	Z
K4.3	Gerekli durumlarda bilgi sistemleri üzerinde bilgi ya da veri kurtarma eylemlerinin gerçekleştirilip gerçekleştirilmediği sorgulanır.	İ	O
K4.4	Olay çözümlerinin belgelendiği ve çözümün daha sonra benzer olaylar oluştuğunda bilgi kaynağı olarak kullanılıp kullanılmayacağını değerlendirildiği kontrol edilir.	İ	O
K4.5	Çözümlenen olayların çözüm yöntemlerinin kaydedildiği gözlemlenir	İ	Z

K5 - Olay çözümünün yeterli olduğu ve talebin karşılandığı doğrulanır ve olay kaydı sonlandırılır.			
#	Denetim prosedürleri	T/İ	Z/O
K5.1	Denetim dönemi içinde yardım masasına iletilen ve kapatılmış olan kayıtlar arasından örnek seçilerek olayın çözümü ile ilgili hizmet seviyesinin yeterli olduğu, olayın tatmin edici bir şekilde çözümlendiği ve çözümün etkilenen kullanıcılar ile birlikte doğrulandığı gözlemlenir.	İ	Z
K5.2	Örnek olarak seçilen olay kayıtlarının, olayı bildiren personelin onayı alınarak kapatıldığı teyit edilir.	İ	Z

TASLAK

K6 - Problemlerin sınıflandırması ve raporlanması için gerekli kriter ve prosedürler tanımlanır ve uygulanır.			
#	Denetim prosedürleri	T/İ	Z/O
K6.1	Problemlerin tespit edilmesi ve sınıflandırılması için gerekli sürecin kurulmuş olduğu çalışanlar ile görüşmeler yapılarak ve mevcut politika ya da prosedürler incelenerek teyit edilir.	T	Z
K6.2	Durum ya da olayların, problem olarak tanımlanması için gerekli kriterlerin belirlenmiş olduğu gözlemlenir.	T	Z
K6.3	Problem önceliklendirme kriterlerinin ilgili iş süreçlerinin niteliği dikkate alınarak belirlendiği gözlemlenir.	İ	Z
K6.4	Problem kategorizasyonu/sınıflandırmasına ilişkin yöntemlerin tanımlanmış olduğu gözlemlenir.	T	Z
K6.5	Denetim dönemi boyunca gerçekleşen tüm problemlerin kayıt altına alındığı ve belgelerinin prosedürlere uygun olarak oluşturulduğu sorgulanır.	İ	Z
K6.6	Değişiklik yönetimi sisteminden gelen girdiler de dahil olacak şekilde örnek seçilecek problemlerin politika ve/veya prosedürlere uygun şekilde ele alınmış olduğu incelenir.	İ	O
K6.7	Problem tanımlaması ve kök neden analizlerinin zamanında ve daha önceden tanımlanan hizmet seviyesi anlaşmalarına göre ele alınmasını sağlayacak şekilde, öncelik seviyelerinin iş birimlerine danışılarak tanımlandığı gözlemlenir. Öncelik seviyelerinin iş etkisi ve aciliyete dayandırıldığı gözlemlenir.	İ	O

K7 - Gerçekleşen problemlere ilişkin kök nedenleri değerlendirmek ve analiz etmek için ilgili konuda uzmanlar görevlendirilerek problemler araştırılır ve teşhis edilir.

#	Denetim prosedürleri	T/i	Z/O
K7.1	Farklı tipte problemlerin çözümü için gerekli olduğu düşünülen durumlarda farklı yetkinliklere sahip uzman kişilerin görevlendirildiği gözlemlenir.	İ	O
K7.2	Kök neden analizi sırasında bilinen hataların tutulduğu bilgi kaynaklarının ve veri tabanlarının araştırılmış olduğu gözlemlenir.	İ	O
K7.3	Problemlerin çözümünde raporların oluşturularak çözüme ilişkin ilerleyişin bildirildiği kontrol edilir. Çözümeyen problemlerin süregelen etkilerinin izlendiği gözlemlenir.	İ	O

TASLAK

K8 - Problemin kök neden analizi tanımlandıktan sonra, ilgili çözüm yöntemlerinin ileride referans olarak kullanılabilmesi için “bilinen hatalar” kayıtları oluşturulur ve uygun bir geçici çözüm hazırlanarak potansiyel çözümler belirlenir.

#	Denetim prosedürleri	T/İ	Z/O
K8.1	Problemin kök analizi tanımlandıktan sonra bilinen hata kayıtları ve uygun geçici çözümlerin geliştirildiği gözlemlenir.	İ	O
K8.2	Problemlerin kök nedenlerinin bulunmasının ardından fayda-maliyet, iş etkisi ve aciliyetine göre çözümlerin tanımlandığı, değerlendirildiği, önceliklendirildiği ve değişiklik yönetimi sürecine uygun şekilde işletildiği kontrol edilir.	İ	O

TASLAK

K9 - Bir problemin ortadan kaldırılması için tasarlanan çözümler ilgili prosedür uyarınca ya da değişiklik yönetimi sürecinden geçerek uygulanır. Çözümler kök nedenlere yönelik olarak kalıcı olacak şekilde tasarlanır. Problemden etkilenen çalışanların, yapılanların ve çözüm için hazırlanan planların farkında olması sağlanır.

#	Denetim prosedürleri	T/i	Z/O
K9.1	Örnek olarak seçilen problemlerin sadece ilgili hatanın başarılı bir şekilde çözümlenmesi ve onaylanmasından sonra ya da iş birimleri ile problemin nasıl çözümleneceği ile ilgili anlaşmaya varıldıktan sonra kapatılmış olduğu kontrol edilir.	İ	Z
K9.2	Örnek olarak seçilen problemlerin ancak ilgili paydaşların onayı ile “çözümlendi/tamamlandı/giderildi, vb.” durumuna alındığı gözlemlenir.	İ	Z
K9.3	Örnek olarak seçilen problemler için problemin kapatılma planı ya da konu ile ilgili uygulanacak değişikliğe kadar problemin açık kalacağı ile ilgili bilginin yardım masasına iletildiği gözlemlenir. Etkilenen kullanıcı ve müşterilerin bu durum ile ilgili haberdar edildiği kontrol edilir.	İ	O
K9.4	Açık durumdaki problemlerin listesi temin edilir. Bu problemlerin durumlarının BT yönetiminin ve kullanıcıların haberdar olması için yardım masasına raporlandığı gözlemlenir.	İ	Z
K9.5	Problemin çözülmesi ile ilgili kayıtların hazırlanmış olduğu gözlemlenir.	İ	O
K9.6	Problemlerin ve bilinen hataların hizmetler üzerindeki etkisinin izlendiği kontrol edilir.	İ	Z
K9.7	Problemlerin çözümlerinin gözden geçirildiği ve onaylandığı gözlemlenir.	İ	Z

K10 - Yeni problemlere neden olabilecek eğilimleri gözlemleyebilmek ve tespit edebilmek için özellikle olay ve değişiklik kayıtları verileri toplanır ve analiz edilir.

#	Denetim prosedürleri	T/İ	Z/O
K10.1	Problem yönetimi sürecinin değişiklik yönetimi ve olay yönetimi süreçleri ile entegre olacak şekilde ele alındığı değerlendirilir.	İ	Z
K10.2	Olay, problem, değişiklik yönetimi süreç sahipleri ve yöneticilerinin bilinen problemler ile ilgili düzenli olarak görüştükleri sorgulanır.	İ	O
K10.3	Problemler sonucu oluşan toplam maliyetin belirlendiği, kurumsal olarak izlendiği ve harcanan iş gücünün takip edildiği kontrol edilir.	İ	O
K10.4	İş gereksinimleri ve hizmet seviyesi anlaşmalarına göre problem çözümlerinin izlediği raporların hazırlanmış olduğu gözlemlenir. Daha önceden belirlenen kriterlere göre problemin daha üst bir seviyeye aktarılması, dış tedarikçilerle iletişime geçilmesi gibi problem seviye yükseltme sürecinin işletildiği kontrol edilir.	İ	O
K10.5	Kaynakların kullanılmasını optimize etmek ve geçici çözümleri azaltmak adına problem eğilimlerinin izlendiği gözlemlenir.	İ	O
K10.6	Kök nedene yönelik kalıcı çözümlerin belirlenerek uygulandığı ve değişiklik yönetimi sürecine uygun şekilde değişikliklerin gerçekleştirildiği kontrol edilir.	İ	O

K11 - Olay yönetimi sürecinin sürekli iyileştirilmesini sağlamak için, olay ve taleplerin çözülme yöntemleri, süreleri ve eğilimleri düzenli olarak izlenir, analiz edilir ve raporlanır.

#	Denetim prosedürleri	T/İ	Z/O
K11.1	Kritik veya çözilemeyen olayların eskalasyon (bir üst seviyeye aktarma) süreçleri incelenir. Problem yönetimi sürecinin varlığı ve bu tip olaylar için sürecin nasıl tetiklendiği araştırılır.	T, İ	Z
K11.2	Çözülmemiş durumda olan problemlere ilişkin durumların düzenli olarak takibinin yapıldığı ve ilgili yönetim birimine raporlandığı kontrol edilir.	İ	Z
K11.3	Olay yönetimi raporlama ihtiyaçlarının tanımlanmış olduğu gözlemlenir. Raporlama zamanlamaları ve dönemleri ile varsa ilgili aracın belirlendiği gözlemlenir.	T	Z
K11.4	Eğilim göstergelerini oluşturmak, tekrarlanan sorunların modelleri tanımlamak ve hizmet seviyesi anlaşmalarındaki ihlalleri ve verimsizlikleri belirlemek için, olay ve yardım taleplerinin kategori ve tür bazında analiz edildiği kontrol edilir. Buradaki bilgilerin iyileştirme planlarında girdi olarak kullanıldığı gözlemlenir.	İ	O
K11.5	Gerçekleşen olaylar ile ilgili olarak düzenli olarak eğilim analizlerinin yapıldığı ve bu analizlerin sonuçlarının yorumlanıp, bu yorumlara göre eylem planlarının yapılıp yapılmadığı incelenir.	İ	O
K11.6	Sıkça karşılaşılan olaylar için bir bilgi kaynağının ya da veritabanının (sıkça sorulan sorular gibi) varlığı gözlemlenir.	İ	O
K11.7	Prosedürler incelenerek olay yönetimine ilişkin raporların yönetim ile paylaşılma sıklığı öğrenilir. Bu sıklıklara göre örnek dönemler için (örnek günler, haftalar veya yıllar) ilgili raporların oluşturulmuş ve paylaşılmış olduğu denetlenir.	İ	O
K11.8	Yardım masası performansının artırılması için düzenli olarak iç müşteri memnuniyeti anketlerinin yapıldığı gözlemlenir. Bu anketlerinin sonuçlarına göre eylem planlarının oluşturulduğu kontrol edilir.	İ	Z

Ek Kaynaklar

- ISACA. (2007). COBIT 4.1 Framework – DS5. Rolling Meadows, Illinois, United States of America.
- ISACA. (2012). COBIT 5 Enabling Processes – APO13, DSS05. Rolling Meadows, Illinois, United States of America.
- ITIL V3 2011 Service Operation, 4.5 Access Management (UK Cabinet Office, 2011)
- ISO/IEC 27002, Code of Practice for Information Security Management (International Organization for Standardization(ISO)-International Electrotechnical Commission(IEC), 2005)
- Global Technology Audit Guide (GTAG), Identity and Access Management (The Institute of Internal Auditors, 2007)

TASLAK

4.4. BT OPERASYON VE YEDEKLEME YÖNETİMİ

Sürecin Genel Tanımı

BT operasyon ve yedekleme yönetimi süreci temel olarak, BT altyapısı ile ilgili günlük faaliyetlerin etkin bir şekilde gerçekleştirilmesi, izlenmesi, kontrol edilmesi ve bakımının sağlanması ile uygulamalar, hizmetler ve faaliyetler aracılığı ile üretilen ve işlenen veriler ile ilgili yedekleme ihtiyaçlarının karşılanması amacını taşımaktadır. Kurum bünyesinde veri işleyen mekanizmaların doğru şekilde çalışması, veri yönetimi prosedürlerinin oluşturulması, verilerin gizlilik, bütünlük ve erişilebilirlik açısından korunacak şekilde saklanması, etkin bir operasyon ve yedekleme yönetimi sürecinin tesis edilmesi ile mümkündür. Operasyon yönetiminin etkin bir şekilde yürütülmesi ile BT hizmetlerinin istenilen şekilde çalışması, BT kaynaklarının verimli şekilde kullanılması, veri yönetiminin kurum iş ihtiyaçları ile uyumlu şekilde gerçekleştirilmesi sağlanır.

Sürecin BT Denetimi Açısından Önemi

BT operasyon ve yedekleme yönetimi, kurumun faaliyetlerini ve süreçlerini işletebilmesi için gerekli olan ve bilgi sistemleri tarafından sağlanan “kritik BT işlevselliği”nin sürekliliği, performansı ve fiziksel güvenliği ile doğrudan ilgili olduğundan, BT denetimlerinde öne çıkan konulardan biridir. Operasyon ve yedekleme yönetiminin değerlendirilmesi ile BT faaliyetlerinin iş hedeflerine uygun olarak ve planlandığı şekilde gerçekleştiği ve herhangi bir felaket ya da kesinti sonrasında kurumun kritik faaliyetlerinin kesilmemesi için uygulamalara ait yedeklerin farklı ortamlarda bulunduğu konusunda makul bir güvence sağlanabilir. Bu sayede, BT uygulamalarının hesaplama, raporlama vb. gibi denetim açısından kritiklik taşıyan işlevlerini destekleyen altyapının bakımı ve izlenmesi ile operasyonel faaliyetlerin ve yedeklemelerin denetim dönemi içerisinde kontrollü bir biçimde gerçekleştirilip gerçekleştirilmediğine ilişkin bir kanaat oluşturulabilir.

Kontrollere İlişkin Örnek Akış

Süreçte yer alan tipik kontrollere aşağıdaki tabloda yer verilmiştir:

BT Operasyon ve Yedekleme Yönetimi - Kontroller	
K1	Kurum bünyesinde gerçekleştirilen BT faaliyetleri ve işlemleri tutarlı ve güvenilir bir biçimde tanımlanır ve yönetilir.
K2	Kurum bünyesinde iş ihtiyaçlarına uygun olarak veri oluşturma, işleme, saklama, yedekleme ve imha mekanizmaları ve bunlara ilişkin süreçler tesis edilir.
K3	Kurum BT altyapısı izlenir ve ilgili olaylar kayıt altında tutulur ve raporlanır.
K4	Kurum bilgi sistemlerini oluşturan tüm parçaların çevresel etkenlere karşı uygun şekilde korunmasını sağlayacak önlemler alınır.

TASLAK

Risk – Kontrol Eşleşmeleri

BT Operasyon ve Yedekleme Yönetimi Risk – Kontrol Eşleşmeleri				
Riskler	K1	K2	K3	K4
R1. Hassas verilerin doğru şekilde işlenmemesi ve bundan dolayı mali kayıpların oluşması	+	+		
R2. BT hizmetlerinin iş hedeflerine uygun bir şekilde yürütülememesi	+	+		
R3. Veri saklama süreleri ile ilgili olarak yasal zorunluluklara uyum sağlanamaması		+		
R4. İş sağlığı ve güvenliği ile ilgili kanunlara uyumun sağlanamaması				+
R5. BT kaynaklarının etkin bir şekilde kullanılamaması	+		+	
R6. Veri yönetiminin iş ihtiyaçlarını karşılayamaması		+		
R7. BT altyapısı ile ilgili problemlerin iş süreçlerini kabul edilebilir seviyelerden fazla etkilemesi	+		+	+
R8. BT operasyonlarına ilişkin prosedürler ya da kılavuzların mevcut olmaması veya yanlış anlaşılması sonucu faaliyetlerin istenilen şekilde ve verimlilikte gerçekleştirilmemesi	+			
R9. Güç kesintilerine karşı yeterli korumanın sağlanmaması sonucunda sistem hatalarının yaşanması				+
R10. BT faaliyetlerinde ortaya çıkacak problemler ile baş edilememesi	+		+	
R11. BT altyapısının çevresel etkenlere karşı savunmasız kalması				+
R12. Zamanlanmış, yığın, gün sonu vs. işlerinin takip edilememesi ve bu sebeple ortaya çıkan sıkıntıların zamanında çözülememesi ve raporlanamaması	+			

2.4.6. Denetim Prosedürleri

K1 - Kurum bünyesinde gerçekleştirilen BT faaliyetleri ve işlemleri tutarlı ve güvenilir bir biçimde tanımlanır ve yönetilir.			
#	Denetim prosedürleri	T/İ	Z/O
K1.1	Kurum bünyesinde gerçekleşmekte olan operasyonel BT faaliyetlerine dair prosedürlerin ve kılavuzların varlığı gözlemlenir ve incelenir. Prosedürlerin ve kılavuzların, BT operasyonlarına ilişkin tanımlama, izleme ve değerlendirme ile ilgili süreçleri içerdiği gözlemlenir.	T	Z
K1.2	İncelenen BT faaliyetlerine dair prosedürlerde ve kılavuzlarda personele ilişkin rol ve sorumlulukların tanımlanmış olduğu gözlemlenir.	T	Z
K1.3	Yığın iş (batch) ve zamanlanmış (otomatik olarak önceden belirlenmiş zamanlarda gerçekleşen işler) iş gerçekleştirme prosedürleri incelenir. Bu prosedürlerin onaylı olduğu ve izleme faaliyetlerini de içerdiği gözlemlenir.	T	Z
K1.4	Kurum bünyesinde gerçekleştirilen yığın ve zamanlanmış işlerin listesi temin edilir. Bu listeden örneklem yöntemine uygun olarak örnekler seçilir. Örnek olarak seçilen yığın ve zamanlanmış işlerin taleplerinin ilgili iş birimi yöneticisi ve BT yöneticisi tarafından onaylandığı gözlemlenir	İ	Z
K1.5	Örnek olarak seçilen yığın ve zamanlanmış işleri gerçekleştirmiş olan operatörlerin kim olduğu öğrenilir, ilgili kişinin görev tanımı incelenir ve bu kişilerin aynı zamanda söz konusu işlere ait denetim izlerinin değerlendirilmesinden sorumlu olmadıkları gözlemlenir.	İ	Z
K1.6	BT faaliyetlerini gerçekleştiren ve izleyen ekipler için vardiya takviminin oluşturulduğu ve yönetim ile paylaşıldığı gözlemlenir.	İ	O
K1.7	Yığın işlerin gerçekleştirilmesi için, vardiya günlükleri incelenerek vardiyaların her an en az bir operatörün çalışacağı şekilde ayarlandığı gözlemlenir.	İ	O
K1.8	Vardiyalar sırasında tespit edilen sorunlar incelenir. Bu sorunlar için olay yönetimi sürecine uygun şekilde kayıt açıldığı gözlemlenir.	İ	O

K2 - Kurum bünyesinde iş ihtiyaçlarına uygun olarak veri oluşturma, işleme, saklama, yedekleme ve imha mekanizmaları ve bunlara ilişkin süreçler tesis edilir.

#	Denetim prosedürleri	T/İ	Z/O
K2.1	Kurum bünyesinde sistemlerin, uygulamaların ve verilerin yedekleme politika ve prosedürlerinin oluşturulmuş olduğu ve aşağıda belirtilen örnek konuları içerdiği gözlemlenir. <ul style="list-style-type: none"> • Yedekleme sıklığı • Yedekleme tipi (tüm, artalan vb.) • Yedekleme ortamı tipi • Yedekleme tipi (otomatik, manuel) • Veri tiplerine göre farklı yedekleme seçenekleri • Yedeklemelere ilişkin denetim izlerinin (log) oluşturulması • Önemli son kullanıcı verileri (belgeler vb.) • Veri kaynaklarının fiziksel ve mantıksal yerleri • Güvenlik ve yetkiler • Şifreleme (kriptolama) ihtiyaçları 	T	Z
K2.2	Kurum BT bünyesinde saklanan ve işlenen veri tiplerinin tanımlandığı ve gizlilik, bütünlük ve erişilebilirlik seviyelerine göre değerlendirildiği incelenir.	İ	O
K2.3	Kapsama alınan uygulamalara/sistemlere ait verilerin iş ihtiyaçlarına ve süreklilik planlarına göre kategorize edildiği gözlemlenir.	T	O
K2.4	Kapsama alınan uygulamalara ait verilerin yedeklenmesinin ve bu yedeklerin saklanmasının verilerin kategorilerine, yasal zorunluluklara ve prosedürlere uygun şekilde gerçekleştirildiği gözlemlenir.	İ	O
K2.5	Yedekleme sürecinin izlenmesi ile ilgili rol ve sorumlulukların atanmış olduğu gözlemlenir.	T	Z
K2.6	Yedeklerin sorunsuz olarak alındığına ya da yedeklerin alınması ile ilgili olarak sorunların çıktığı durumlara dair bilgilendirmelerin ilgili personele yapıldığı gözlemlenir. Otomatik yedekleme yapan cihazların durum raporlarının oluşturulduğu ve izlemeden sorumlu personel tarafından görüntülenebilir olduğu gözlemlenir.	İ	Z
K2.7	Yedekleme sürecinde çıkan sorunlar için olay yönetimi sürecine uygun şekilde kayıt açıldığı gözlemlenir.	İ	Z
K2.8	Yedeklerin envanter listesi incelenir ve örnek olarak seçilen yedeklerin fiziksel varlığı gözlemlenir, varsa yedeklerin üzerindeki etiketlerin doğruluğu araştırılır.	İ	O
K2.9	Yedekleme ortamlarının çalıştığından ve geri dönülebilir olduğundan emin olmak adına, kapsamdaki sistemlerin, uygulamaların ve verilerin yedeklerinin düzenli olarak geri dönüş testlerinin yapıldığı kontrol edilir. Bu doğrultuda örnek yedekler seçilerek bunların geri dönüş testlerine dair belgeler incelenir. İlgili iş birimlerinin geri dönüşün sorunsuz olarak gerçekleştirildiği konusunda onay verdiği gözlemlenir.	İ	Z

K2.10	Kurum bünyesinde kullanılmayan ya da saklama süresi dolan verilerin ve ilgili saklama medyalarının (disk, DVD, vb.) imhasına ilişkin bir sürecin mevcut olduğu gözlemlenir.	İ	O
K2.11	Veri imhası ile ilgili rol ve sorumlulukların açık bir şekilde belirlendiği gözlemlenir.	T	O
K2.12	Tekrar kullanılacak ortamlarda bulunan verilerin kesin bir şekilde yok edildiğinden (üzerine yazma vb. yöntemler ile) emin olunduğu gözlemlenir.	İ	Z
K2.13	İmha sürecine sokulan verilerin ve saklama ortamlarının tüm imha sürecinin bir kurum görevlisi tarafından izlenip raporlandığı kontrol edilir.	İ	Z
K2.14	İmha sürecinde yer alan (varsa) taşıyon firmaların fiziksel güvenlik gereksinimlerini sağladığı kontrol edilir.	İ	O

TASLAK

K3 - Kurum BT altyapısı izlenir ve ilgili olaylar kayıt altında tutulur ve raporlanır.

#	Denetim prosedürleri	T/i	Z/O
K3.1	BT altyapısının iş ihtiyaçları, risk ve performans göstergeleri dikkate alınarak düzenli olarak izlendiği ve altyapı ile ilgili olarak oluşan olayların ve çözümlerinin kaydedildiği ve takip edildiği gözlemlenir.	İ	Z
K3.2	İzlenecek altyapı elemanlarının iş ihtiyaçlarına bağlı olarak kritikliklerine göre önceliklendirildikleri kontrol edilir.	İ	O
K3.3	İzlenen altyapı elemanları için eşik değerlerinin belirlendiği ve bu eşik değerlerini aşan göstergeler için ilgili birimin harekete geçtiği ve gerekli önlemlerin alındığı gözlemlenir.	İ	O
K3.4	İzlenen altyapı elemanlarının izlenen özelliklerindeki değişimlerin ve eğilimlerinin düzenli olarak kontrol edildiği, probleme yol açabilecek eğilimler için gerekli önlemlerin alındığı gözlemlenir.	İ	O
K3.5	Denetim dönemi boyunca gerçekleşmiş BT altyapısını ilgilendiren olaylar arasından örneklem seçilir ve bu örnek olaylar için olay kaydı açılıp açılmamış olduğu kontrol edilir.	İ	Z

K4 - Kurum bilgi sistemlerini oluşturan tüm parçaların çevresel etkenlere karşı uygun şekilde korunmasını sağlayacak önlemler alınır.			
#	Denetim prosedürleri	T/İ	Z/O
K4.1	Kurum bünyesinde kullanılan kritik uygulamaların sunucularının bulunduğu sistem odası gezilir ve sistem odası girişlerinde güvenliğin sağlandığı kontrol edilir. Sistem odası giriş kapısının sadece kimlik kartı veya benzeri kişiye özel tanımlayıcılar ile açılabilirdiği ve turnike vb. yöntemlerle tek seferde sadece bir kişinin kapıdan girişine izin verildiği gözlemlenir.	İ	Z
K4.2	Sistem odasının bulunduğu yerin seçiminde şirketin iş ve güvenlik ihtiyaçlarının değerlendirildiği çevresel etmenlerin ve risklerin (hırsızlık, ısı, yangın, duman, sel, deprem, terör, kimyasallar, paylayıcılar vs.) dikkate alındığı gözlemlenir.	İ	Z
K4.3	Sistem odasının maruz kaldığı risklerin değerlendirildiği ve bu risklerin gerçekleşmesi durumunda bunların işe olan etkisinin ölçüldüğü gözlemlenir.	İ	O
K4.4	Sistem odasında önceden belirlenmiş eşik değerlerin aşılması halinde alarm veren ısı, nem, duman ve yangın dedektörleri gibi izleme ve alarm sistemlerinin bulunduğu gözlemlenir.	İ	Z
K4.5	Sistem odası yangın söndürme sistemi incelenir. Sistem odasında yangın söndürme sistemi olarak FM200 gazlı ya da benzeri sistemlerin olduğu kontrol edilir.	İ	Z
K4.6	Sistem odasının düzenli ve temiz tutulduğu gözlemlenir. Odada yanıcı ve tutuşucu (kağıt, karton, yanıcı kimyasallar vb.) maddelerin bulunmadığı kontrol edilir. Sistem odasında insan sağlığını tehlikeye atacak unsurların bulunmadığı, kabloların çalışanların ayaklarına takılmayacak şekilde derli toplu bir biçimde tutulduğu gözlemlenir.	İ	Z
K4.7	BT teçhizatının elektrik altyapısının korunması ve çalışırılığının sağlanması için voltaj regülatörlerinin ve kesintisiz güç kaynaklarının (UPS) varlığı araştırılır.	İ	Z
K4.8	Kesintisiz güç kaynaklarının, yangın söndürme sistemlerinin, sistem odasında bulunan soğutma sistemlerinin ve çevresel etkilere karşı tesis edilmiş diğer cihaz ve ekipmanların bakımlarının düzenli olarak gerçekleştirildiği gözlemlenir. Bunun için denetim döneminde gerçekleşmiş bakımlar arasından bir örneklem seçilir ve bakım belgeleri incelenerek, bakımın gerçekleştiği teyit edilir.	İ	Z
K4.9	Sistem odasında alternatif güç, iletişim, su ve gaz hatlarının varlığı kontrol edilir.	İ	O
K4.10	Sistem odasına giriş yetkisi olan personelin sistem odasında uyulması gereken iş sağlığı ve güvenliği kuralları hakkında bilgilendirildiği gözlemlenir.	İ	Z
K4.11	Sistem odası ile ilgili gerçekleşen olayların yönetiminin olay yönetimi sürecine uygun şekilde takip edildiği ve kayıt altına alındığı kontrol edilir.	İ	O

Ek Kaynaklar

- ISACA. (2012). COBIT 5 Enabling Processes DSS01 Manage Operations. Rolling Meadows, Illinois, United States of America.
- ITIL V3 2011 Service Operation, 4.1 Event Management (UK Cabinet Office, 2011)

TASLAK

4.5. SÜREKLİLİK YÖNETİMİ

Sürecin Genel Tanımı

Süreklilik yönetimi kaza, arıza ya da doğal felaket gibi, sonucunda kurumun faaliyetlerinde kesintilere yol açabilecek olayların gerçekleşmesi sonrasında, iş ve BT birimlerinin zamanında ve doğru aksiyonları alarak, bilgi ve verileri korumayı ve kritik iş süreçlerinin ve faaliyetlerinin devamlılığını sağlamayı amaçlayan planlama faaliyetleri, politika, prosedür, süreçler ve bunlara istinaden yürütülen aksiyonlar bütünüdür. Süreklilik yönetimi çerçevesi, operasyonel kesintilerin etkileri sonucunda ortaya çıkabilecek potansiyel kayıpları asgariye indirmeyi etmeyi hedefler. Kurumların yüksek önemlilik arz eden süreçlerini yürüttükleri BT uygulamaları da bu süreçlerin önemi ölçüsünde kritiktir. Bir başka deyişle, bu süreçlerin üzerinde çalıştığı BT uygulamalarının sürekliliği de, bu süreçlerin sürekliliği kadar önemlidir. Süreklilik kontrollerinin yetersiz olduğu durumlarda en küçük kesintiler bile faaliyetlerin aksamasına, kurumun hizmet verebilme kapasitesini kullanamamasına, veri kayıplarına ve verilerin yanlış işlenmesine sebep olabilir.

Kritik BT bileşenlerinin bir felaket anında erişilebilirliğinin ve sürekliliğinin sağlanması için kurumlarda felaket kurtarma planları oluşturulur. Felaket kurtarma planının asıl hedefi insanları ve kurumun ana faaliyetlerini sürdürebilmesini etkileyecek durumlara karşılık verebilmek ve yasal gerekliliklerle uyum sağlamaktır. Süreklilik yönetimi kapsamında gerçekleştirilen iş etki analizi ve risk değerlendirmesi çalışmalarının ardından felaket kurtarma planı oluşturulur. Felaket kurtarma planı kapsamında, bir felaket olduğu anda devreye girecek ve bilgi sistemlerinin sürekliliğini sağlayacak olağanüstü durum merkezleri kurulur. Olağanüstü durum merkezlerinde çevresel kontroller, kurum sistemlerinin bulunduğu sistem odasında olduğu şekilde ve güvenlik seviyesinde oluşturulur. Olağanüstü durum merkezleri mevcut sistem odasında kesintiye yol açabilecek riskleri taşımaz.

Süreklilik yönetiminin etkin bir şekilde uygulanması ile kurumun etkilenebileceği ve faaliyet kesintilerine neden olabilecek mevcut iç ve dış tehditler ve ileride oluşabilecek yeni tehditler tespit edilmeye çalışılır ve bu tehditlere bağlı olarak ortaya çıkabilecek olayların etkisi azaltılmaya çalışılır. Süreklilik yönetimi ile kurumlar, felaket ya da kriz anlarında kritik iş süreçlerinin ve faaliyetlerinin acil durum müdahale yönetimi ile ayakta kalmasını veya öngörülecek azami sürelerde bu süreçlerin ve faaliyetlerin tekrar sürdürülmeye başlamasını sağlar.

Sürecin BT Denetimi Açısından Önemi

Süreklilik yönetimi, kurumun faaliyetlerini ve süreçlerini kesintisiz bir şekilde sürdürebilmesi ile bilgi sistemleri tarafından sağlanan “kritik BT işlevselliği”nin sürekliliği ile doğrudan ilgili olduğundan BT denetimlerinde en çok öne çıkan konulardan biridir. Bu sürecin değerlendirilmesi ve gerekli iyileştirmelerin yapılması ile herhangi bir felaket veya kriz anında süreç ve faaliyetlerin asgari düzeyde etkileneceğine ve en kısa sürede yeniden devreye alınmaya (ayağa kaldırılmaya) hazır durumda olduklarına dair makul bir güvence sağlanabilir. Bu şekilde, BT uygulamalarının hesaplama, raporlama vb. gibi denetim açısından kritik işlevselliklerinin herhangi bir felaket, kriz veya benzeri bir durumda güvenilirliğinin, tutarlılığının ve sürdürülebilirliğinin sağlanabileceğine dair bir kanaat oluşturulabilir.

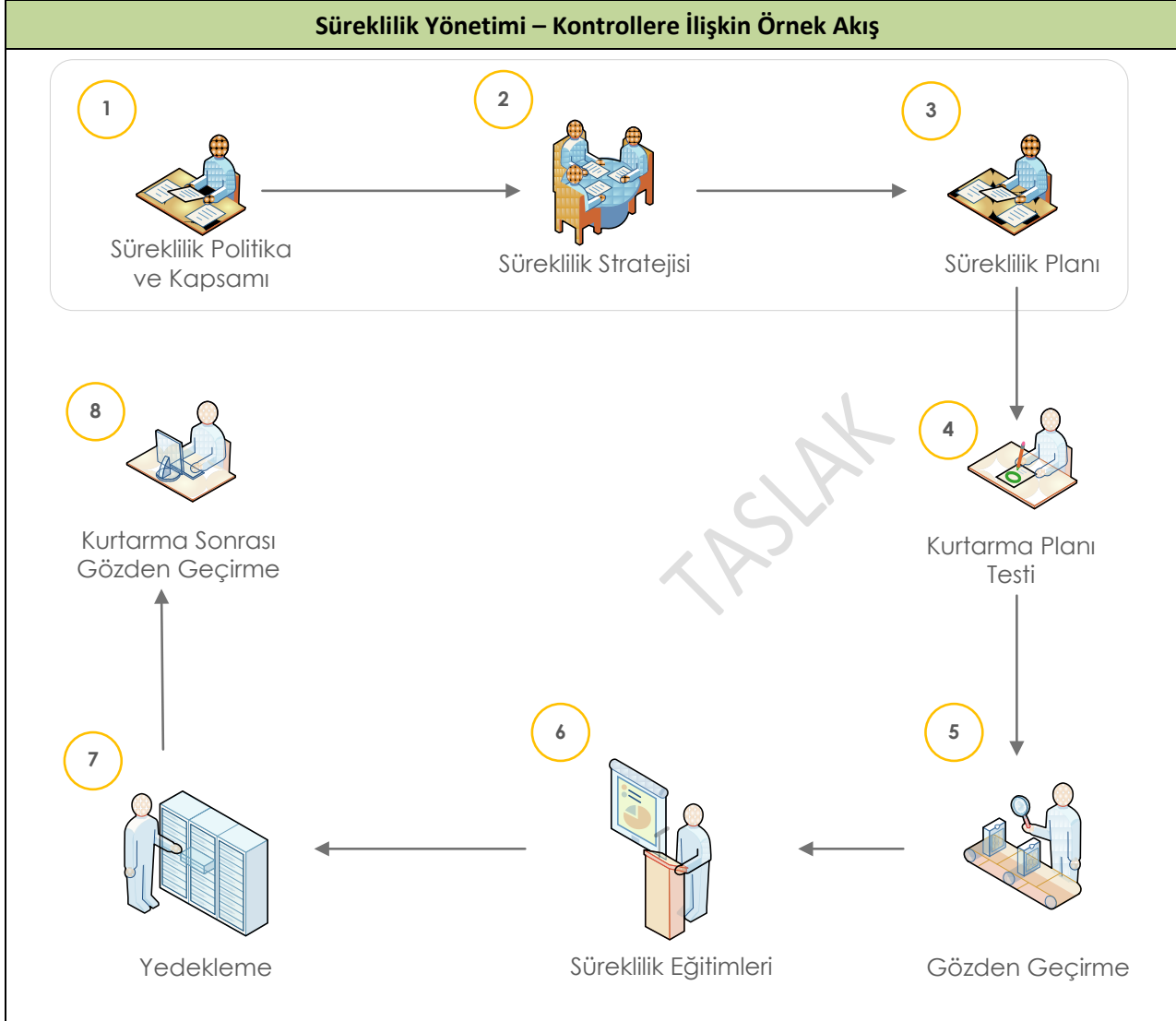
Süreklilik yönetimi, BT denetimi açısından aşağıda belirtilen süreç akışı üzerinden takip edilebilir. Söz konusu akış her kurum için farklı olabileceği gibi, süreç içerisinde ele alınan planlama şekilleri, etki değerlendirme yöntemleri, yedekleme araçları ve raporlama mekanizmaları kurumdan kuruma farklılık gösterebilir.

TASLAK

Kontrollere İlişkin Örnek Akış

Süreçte yer alan tipik kontrollere aşağıdaki tabloda yer verilmiştir:

Süreklilik Yönetimi – Kontroller	
K1	Kurum ve paydaş hedefleri ile uyumlu bir süreklilik politikası ve kapsamı belirlenir.
K2	Süreklilik yönetimi seçenekleri değerlendirilir ve felaket anında kurum iş süreçlerinin kurtarılmasını sağlayacak düşük maliyetli, sürdürülebilir bir süreklilik stratejisi ortaya koyulur.
K3	Bir kesinti ya da felaket olduğu durumlarda yapılması gerekenleri belgeleyen, kurumun kritik faaliyetlerine süreklilik stratejisine dayalı bir iş sürekliliği planı hazırlanır.
K4	Kritik iş süreçlerinin ve faaliyetlerinin başarı ile ayağa kaldırılmasından emin olunması amacı ile kurtarma planı düzenli olarak test edilir.
K5	Kurumdaki süreklilik yapısı, çerçevesi ve ilgili plan ve prosedürler, süreklilik yönetimi sürecinin yeterliliğinin, uygunluğunun ve etkinliğinin sağlanması amacıyla yönetim tarafından düzenli olarak gözden geçirilir.
K6	Tüm iç ve dış taraflar ve paydaşlar için iş sürekliliği konusunda eğitimler düzenlenir.
K7	Süreklilik ile ilgili yedekleme faaliyetlerine yönelik olarak felaket anında ve sonrasında iş için kritik olan verilerin erişebilirliği sağlanır. Bu doğrultuda kritik uygulamaların yedekleri düzenli olarak alınır ve güvenli olarak saklanır. (Bu kontrol BT Operasyon ve Yedekleme Yönetimi başlığı altındaki süreç içerisinde de değerlendirilse de Süreklilik Yönetimi için kritiklik arz ettiğinden, bu süreç altında da incelenmektedir. BT Operasyon ve Yedekleme Yönetimi sürecinin denetlendiği durumlarda, bu kontrolün denetimi seçime bağlıdır).
K8	İş süreçlerinin ve faaliyetlerin başarılı şekilde devreye alınması (ayağa kaldırılması) ardından süreklilik planının süreçteki yeterliliği değerlendirilir.



Risk – Kontrol Eşleşmeleri

Değişiklik Yönetimi Risk – Kontrol Eşleşmeleri								
Riskler	K1	K2	K3	K4	K5	K6	K7	K8
R1. Bir felaket ya da kesinti anında ve sonrasında kritik süreçlerin ve faaliyetlerin yürütülememesi ve sürdürülememesi	+	+	+	+	+	+	+	+
R2. Süreklilik planının yetersiz kalması ve bu doğrultuda iş sürekliliği konusunda güvencenin sağlanamaması	+	+	+	+	+	+	+	+
R3. Bir felaket ya da kesinti sonrasında bilgi sistemlerinin öngörülen zamanda çalışabilir duruma getirilememesi / ayağa kaldırılamaması	+	+	+	+	+	+	+	+
R4. Bir felaket ya da kesinti anında ve sonrasında kritik verilerin doğru işlenememesi, kaybedilmesi, bütünlüğünün korunamaması ve ifşa edilmesi	+	+	+	+	+	+	+	+
R5. Süreklilik planlarının iş ve teknolojik ihtiyaçları karşılamaması	+	+	+	+	+	+	+	+
R6. Kritik BT kaynaklarının kullanılamaz hale gelmesi	+	+	+	+	+	+	+	+
R7. Faaliyet, süreç ve BT sistemlerinin yeniden devreye alınmaları için yeterli kaynağın bulunmaması	+	+	+		+			
R8. Süreklilik planında kurum açısından önemi az olan iş süreçlerine ve faaliyetlerine öncelik verilmesi	+	+	+		+			
R9. İş ve BT süreçlerinde gerçekleşen değişimlerin süreklilik planına yansıtılmaması		+			+			+
R10. Süreklilik yönetiminde belirli personele bağımlılığın bulunması	+	+	+			+		

Deęişiklik Yönetimi Risk – Kontrol Eşleşmeleri								
Riskler	K1	K2	K3	K4	K5	K6	K7	K8
R11. Süreklilik yönetimi uyarınca alınması gereken eğitimlerin yetersiz olması sonucu kritik iş ve BT sistemlerinde kurtarmanın ya da yeniden devreye almanın beklenen şekilde gerçekleşmemesi						+		
R12. Süreklilik ve ilgili acil durum müdahale ve kurtarma planlarının istenildiğinde ya da gerekli olduğu durumda kolay ulaşılabilecek bir şekilde bulunmaması							+	
R13. Süreklilik yönetimine ilişkin maliyetlerin artması	+	+	+	+	+			+
R14. Kritik faaliyetlerin ve süreçlerin yeniden devreye alınması sırasında iç ve dış paydaşlarla iletişim eksiklięinin olması	+		+	+		+	+	

Denetim Prosedürleri

K1 - Kurum ve paydaş hedefleri ile uyumlu bir süreklilik politikası ve kapsamı belirlenir			
#	Denetim prosedürleri	T/i	Z/O
K1.1	Kurum bünyesinde oluşturulmuş ve tüm kurum faaliyet ve süreçlerini kapsayan Süreklilik Yönetimi (SY) ile ilgili plan, politika ve prosedürler temin edilerek incelenir, kurum politikaları ve ilgili mevzuata uygun şekilde üst yönetim tarafından onaylandığı teyit edilir.	T	Z
K1.2	SY dahilinde hedef ve kapsama ilişkin tanımların net bir şekilde yapılmış olduğu gözlemlenir.	İ	Z
K1.3	Kurumun işleyişi için kritik olan ve yasal ya da sözleşmelerden doğan yükümlülüklerini karşılamak için gerekli iş süreçleri ve hizmet faaliyetlerinin net bir şekilde tanımlanmış olduğu gözlemlenir.	İ	Z
K1.4	SY dâhilinde, kritik iç ve dış süreçler ile bu süreçleri destekleyen temel süreçler ve ilgili bilgi teknolojileri hizmetlerinin ve sistemlerin tanımlanmış olduğu tespit edilir.	İ	Z
K1.5	Süreklilik politikası ve kapsamı üzerinde anlaşma yapılmış olan tüm paydaşların ve süreç içinde yer alacak personelin görev ve sorumluluklarının tanımlanmış olduğu kontrol edilir.	İ	Z
K1.6	SY dahilinde herhangi bir kesintinin gerçekleşmesi durumunda, bu durumdan etkilenecek olan paydaşların süreklilik ile ilgili ihtiyaçlarının belirlendiği gözlemlenir.	İ	Z
K1.7	Kurum bünyesinde bilgi sistemlerini kullanan iş süreçlerinin kesilmesinin ve kritik verilerin kaybının yaratacağı etki (iş-etki analizi) göz önüne alınarak bir risk değerlendirmesinin gerçekleştirildiği, iş süreçlerinin ve ilgili BT sistemlerinin bu analize göre önceliklendirilmiş olduğu gözlemlenir.	İ	Z
K1.8	SY dâhilinde hazırlanmış olan planların, sorumlu kişileri, rol ve sorumlulukları ve felaket anında uygulanacak iletişim mekanizmasını, izlenecek kurtarma adımlarını, planın düzenli olarak test edilmesi için gerekli adımları ve yasal zorunlulukları ele alıp almadığı sorgulanır.	İ	Z

K2 - Süreklilik yönetimi seçenekleri değerlendirilir ve felaket anında kurum iş süreçlerinin kurtarılmasını sağlayacak düşük maliyetli, sürdürülebilir bir süreklilik stratejisi ortaya koyulur.

#	Denetim prosedürleri	T/i	Z/O
K2.1	Süreklilik planları ve prosedürleri incelenerek potansiyel felaket senaryolarının belirlendiği ve bunlarla karşılaşıldığında yol açacağı zararlar ile ilgili olarak iş etki analizlerinin yapılmış olduğu teyit edilir.	İ	Z
K2.2	Kritik süreç ve faaliyetler ve bunları destekleyen BT hizmetleri ile ilgili olarak kurtarma zamanı (kurumun hangi faaliyette ne kadar iş görememeye tahammülü olduğu) ve kurtarma noktalarının (kurumun ne kadar veri kaybına tahammülü olduğu) belirlenmiş olduğu teyit edilir.	İ	Z
K2.3	Kesinti sonrasında kritik ve faaliyetlerin tekrar devreye alınması ve ayağa kaldırılması işlemleri için, iş ve teknik gereksinimlerin belirlenmiş olduğu teyit edilir.	İ	Z
K2.4	Süreklilik yönetimine ilişkin gereksinimler göz önünde bulundurularak maliyet analizlerinin yapılmış olduğu teyit edilir.	İ	O
K2.5	İş sürekliliği stratejisinin ve ilgili diğer plan, politika ve prosedür gibi dokümanların iş ve teknolojik ihtiyaçlara göre düzenli olarak gözden geçirildiği ve gerekli durumlarda güncellendiği gözlemlenir.	İ	Z

K3 - Bir kesinti ya da felaket olduğu durumlarda yapılması gerekenleri belgeleyen, kurumun kritik faaliyetlerine süreklilik stratejisine dayalı bir iş sürekliliği planı hazırlanır.

#	Denetim prosedürleri	T/İ	Z/O
K3.1	Tüm kritik iş birimleri ve süreçleri için süreklilik planlarının oluşturulduğu ya da mevcut planın tüm ilgili birimleri ve kritik süreçleri kapsadığı gözlemlenir.	İ	Z
K3.2	İnsan kaynakları, tesis(ler)in fiziki durumu ve BT altyapısı göz önünde bulundurularak, süreklilik ve iş kurtarma prosedürlerinin desteklenmesi için gerekli kaynak ihtiyacının belirlendiği ve belgelendirildiği gözlemlenir.	İ	Z
K3.3	Faaliyetleri açısından kritik olarak değerlendirilen tedarikçilerin süreklilik planında yer aldığı ve tedarik edilen hizmetlerin de sürekliliğinin dikkate alındığı gözlemlenir.	İ	Z
K3.4	Süreklilik planlarını destekleyecek şekilde ilgili BT sistemlerinin yedekleme ihtiyaçlarının belirlendiği gözlemlenir.	İ	Z
K3.5	Süreklilik yönetimi dahilindeki planların, acil durum müdahale prosedürlerinin ve gerekli diğer dokümanların güncel versiyonlarının kurumun yerleşkesi/tesisi içinde ve mümkünse kurum dışında belirlenecek bir yerde tutulduğu ve her türlü felaket senaryosu sırasında erişilebilir durumda olduğu teyit edilir.	İ	Z
K3.6	Süreklilik yönetimi sürecinde görev alan personelin hangi becerilere ve yeteneklere sahip olması gerektiğinin tanımlandığı kontrol edilir.	İ	O
K3.7	Herhangi bir kesinti anında BT işlevlerinin sürdürülebilmesi için bir olağanüstü durum merkezinin bulunduğu ve felaket anında bu merkezden yürütülmeye başlanacak olan süreçlerin ve çalışma şeklinin plan dahilinde belirtildiği gözlemlenir.	İ	Z

K4 - Kritik iş süreçlerinin ve faaliyetlerinin başarı ile ayağa kaldırılmasından emin olunması amacı ile kurtarma planı düzenli olarak test edilir.

#	Denetim prosedürleri	T/İ	Z/O
K4.1	İş ve faaliyetlere ilişkin risklerin doğru şekilde karşılanması ve etkilerinin azaltılması için Süreklilik Planının ve ilgili diğer politika ve prosedürlerin bütünlüğünün sağlanması doğrultusunda süreklilik planlarının test edilmesine ilişkin hedeflerin tanımlandığı gözlemlenir	T	Z
K4.2	Süreklilik Planı üzerinde gerçekleştirecek test çalışmalarının, herhangi bir felaketin kritik iş süreçleri ve faaliyetleri üzerindeki oluşturacağı etkiyi asgari düzeye çekebilmek için tanımlandığı gözlemlenir. Test çalışmalarının gerçekçi, süreklilik planını doğrulayıcı, rol ve sorumluluk tanımlarını ve veri saklama düzenlemelerini içerecek şekilde tanımlandığı ve bu doğrultuda paydaşlar ile üzerinde uzlaşıldığı gözlemlenir.	İ	Z
K4.3	Süreklilik Planı'nda tanımlandığı şekilde test faaliyetleri takviminin hazırlandığı kontrol edilir.	İ	Z
K4.4	Süreklilik ve felaket kurtarma testlerinin düzenli olarak gerçekleştirildiği incelenir. Bu testler kapsamında olağanüstü durum merkezinin de çalışırılığının test edildiği gözlemlenir.	İ	Z
K4.5	Testlerin, en güncel süreklilik planının dikkate alınarak gerçekleştirildiği gözlemlenir.	İ	Z
K4.6	Gerçekleştirilen test sonrası sonuçların ve sonuç analizlerinin belgelendirildiği gözlemlenir.	İ	Z
K4.7	Gerçekleştirilen testler sonucunda süreklilik planının iyileştirilmesi amacıyla önerilerin geliştirildiği ve raporlandığı gözlemlenir.	İ	Z

K5 - Kurumdaki süreklilik yapısı, çerçevesi ve ilgili plan ve prosedürler, süreklilik yönetimi sürecinin yeterliliğinin, uygunluğunun ve etkinliğinin sağlanması amacıyla yönetim tarafından düzenli olarak gözden geçirilir.

#	Denetim prosedürleri	T/İ	Z/O
K5.1	Mevcut operasyonel ve stratejik hedeflere uygun olarak iş sürekliliği ve felaket kurtarma planlarına yönelik düzenli olarak gözden geçirme çalışmalarının yapılıp yapılmadığı sorgulanır.	İ	Z
K5.2	Planın gözden geçirilmesinin ardından değişikliği tetikleyen herhangi bir durum oluştuğunda, plan üzerinde yapılması gereken değişiklikler için takip edilecek süreç adımlarının belirlendiği gözlemlenir.	İ	Z
K5.3	İş sürekliliği planı üzerinde yapılacak değişiklikler ile ilgili yönetim kademesinin onayının alındığının teyidi yapılır.	İ	Z
K5.4	Güncellenen planlarda sürüm değişikliklerinin açıkça belirtildiği gözlemlenir.	İ	O

TASLAK

K6 - Tüm iç ve dış taraflar ve paydaşlar için iş sürekliliği konusunda eğitimler düzenlenir.

#	Denetim prosedürleri	T/İ	Z/O
K6.1	SY dahilinde ilgili personel ve paydaşlar tarafından alınması gereken eğitimlerin sıklığına ve eğitim yöntemlerine (ör: sınıf eğitimi, e-eğitim) plan içerisinde yer verildiği gözlemlenir.	İ	Z
K6.2	Süreklilik yönetimi sürecinde planlama, etki değerlendirme, risk analizi, iletişim ve acil müdahale konularında gerekli eğitimlerin, verildiği katılımcı listeleri incelenerek teyit edilir.	İ	Z
K6.3	Süreklilik yönetimi sürecinde görev alan personelin bilgi birikimi ve yeteneklerinin testler düzenlenerek ölçüldüğü gözlemlenir.	İ	O

TASLAK

K7 - Süreklilik ile ilgili yedekleme faaliyetlerine yönelik olarak felaket anında ve sonrasında iş için kritik olan verilerin erişebilirliği sağlanır. Bu doğrultuda kritik uygulamaların yedekleri düzenli olarak alınır ve güvenli olarak saklanır. (Bu kontrol BT Operasyon ve Yedekleme Yönetimi başlığı altındaki süreç içerisinde de değerlendirilse de Süreklilik Yönetimi için kritiklik arz ettiğinden, bu süreç altında da incelenmektedir. BT Operasyon ve Yedekleme Yönetimi sürecinin denetlendiği durumlarda, bu kontrolün denetimi seçime bağlıdır).

#	Denetim prosedürleri	T/İ	Z/O
K7.1	Yedekleme politika ve prosedürleri incelenir.	T	Z
K7.2	Kritik uygulamalar, veriler, dökümanlar ve sistemlerin belirtildiği bir envanterin mevcudiyeti sorgulanır.	İ	Z
K7.3	Envanterde belirtilen uygulama, veri ve sistemlerin (ör: işletim sistemi, veritabanı, vb.) prosedürde belirtilen şekilde stratejilere (yedekleme sıklığı, yedekleme metotları, yedekleme tipi, yedekleme ortamı, yedeklenen veri tipleri, yedeklerin saklanma alanları ve koşulları, yedekler üzerinde erişim hakları ve yedeklerin şifrelenmesi-kriptolanması gibi) uygun şekilde yedeklendiği, örnek yedeklere ait denetim izi (log), tutanak v.b. gibi belgeler incelenerek teyit edilir.	İ	Z
K7.4	Yedeklenen verilerin kurumun tesis/yerleşkesi dışında, ana sistemlerin bulunduğu ortamla benzer riskleri içermeyen başka bir ortamda saklandığı teyit edilir.	İ	Z
K7.5	Yedeklenen verilerin tesis/yerleşke dışına taşınırken güvenliğinin sağlandığı ve bulunduğu ortamın fiziksel ve mantıksal güvenliğinin sağlanmış olduğu teyit edilir.	İ	Z
K7.6	Yedek saklama ortamlarının çalışır durumda olduğunun ve yedeklerin sağlıklı olarak alındığının kontrol edilebilmesi amacıyla düzenli olarak yedeklerden geri dönüş testlerinin yapıldığı örneklem üzerinden teyit edilir.	İ	Z
K7.7	Yedekleme hizmeti için üçüncü bir taraf (hizmet sağlayıcı) ile çalışılıyorsa, bu hizmete ilişkin anlaşma ve sözleşmeler incelenir ve yukarıda bahsi geçen kontrolleri içerip içermediği kontrol edilir.	İ	Z

K8 - İş süreçlerinin ve faaliyetlerin başarılı şekilde devreye alınması (ayağa kaldırılması) ardından süreklilik planının süreçteki yeterliliği değerlendirilir.

#	Denetim prosedürleri	T/i	Z/O
K8.1	Bir felakete veya operasyonel kesintiye neden olan bir olayı takiben süreç boyunca süreklilik planına ne kadar uyulduğunun değerlendirildiği gözlemlenir.	İ	O
K8.2	Bir felakete veya operasyonel kesintiye neden olan bir olayı takiben, uygulanan süreklilik planının eksikliklerinin ve yapılabilecek iyileştirme çalışmalarının değerlendirilerek raporlandığına dair belgeler temin edilerek incelenir ve takip çalışmalarının gerçekleştirildiği gözlemlenir.	İ	O

TASLAK

Ek Kaynaklar

- ISACA. (2007). COBIT 4.1 Framework – DS4. Rolling Meadows, Illinois, United States of America.
- ISACA. (2012). COBIT 5 Enabling Processes – DSS04. Rolling Meadows, Illinois, United States of America.
- ISO/IEC 20000 6.3 Service Continuity and Availability Management (International Organization for Standardization(ISO)-International Electrotechnical Commission(IEC), 2005)
- ITIL V3 2011 Service Design, 4.6 IT Service Continuity Management (UK Cabinet Office, 2011)
- ISO/IEC 27002, 14 Business Continuity Management (International Organization for Standardization(ISO)-International Electrotechnical Commission(IEC), 2005)
- ISO 22301 Societal Security – Business Continuity Management Systems, (International Standards Organization, 2012)
- Global Technology Audit Guide (GTAG), Business Continuity Management (The Institute of Internal Auditors, 2008)

TASLAK

4.6. BT ALTYAPI VE YAZILIM EDİNİM, KURULUM VE BAKIMI

Sürecin Genel Tanımı

BT altyapı ve yazılım edinim, kurulum ve bakımı süreci, kurumun stratejik ve operasyonel hedeflerini yerinde getirebilmesi için zamanlı ve uygun maliyetli BT çözümlerinin uygulamaya konması amacıyla taşımaktadır. Bu çözümler, yazılımı kurum tarafından gerçekleştirilecek veya dışarıdan tedarik edilecek uygulamalar, altyapı bileşenlerini ve BT hizmetlerini içerebilir.

Bu sürecin etkin bir biçimde uygulanması ile temin edilecek çözümün kurumun faaliyetlerine ilişkin ihtiyaçlarını azami ölçüde karşılaması sağlanırken, yeni çözümün uygulanmasına dair kesinti riskleri asgari düzeye indirilir ve kullanıcı memnuniyeti sağlanır. Yeni çözümlerin edinilmesi sırasında kurum kaynaklarının en verimli şekilde kullanılması da BT altyapı ve yazılım edinim, kurulum ve bakımı sürecinin hedeflerinden biridir.

Sürecin BT Denetimi Açısından Önemi

BT altyapı ve yazılım edinim, kurulum ve bakımı süreci kurum faaliyetlerinin gerçekleştirilmesi için gerekli olan ve bilgi sistemleri tarafından sağlanan “kritik BT işlevselliği”ni sağlayan süreçler, uygulamalar ve altyapı ile doğrudan ilgili olduğundan, BT denetimlerinde mutlaka ele alınması gereken konulardan biridir. Bu sürecin değerlendirilmesi ile kurum bünyesinde temin edilen BT çözümlerinin iş hedeflerine uygun olarak tasarlandığı ve uygulamaya konduğu konusunda makul bir güvence sağlanabilir. Bu sayede, BT uygulamalarının hesaplama, raporlama vb. gibi denetim açısından kritiklik taşıyan işlevselliklerine ilişkin unsurların, denetim dönemi içerisinde kontrollü bir biçimde ele alındığına, tasarlandığına ve uygulamaya konduğuna ilişkin bir kanaat oluşturulabilir.

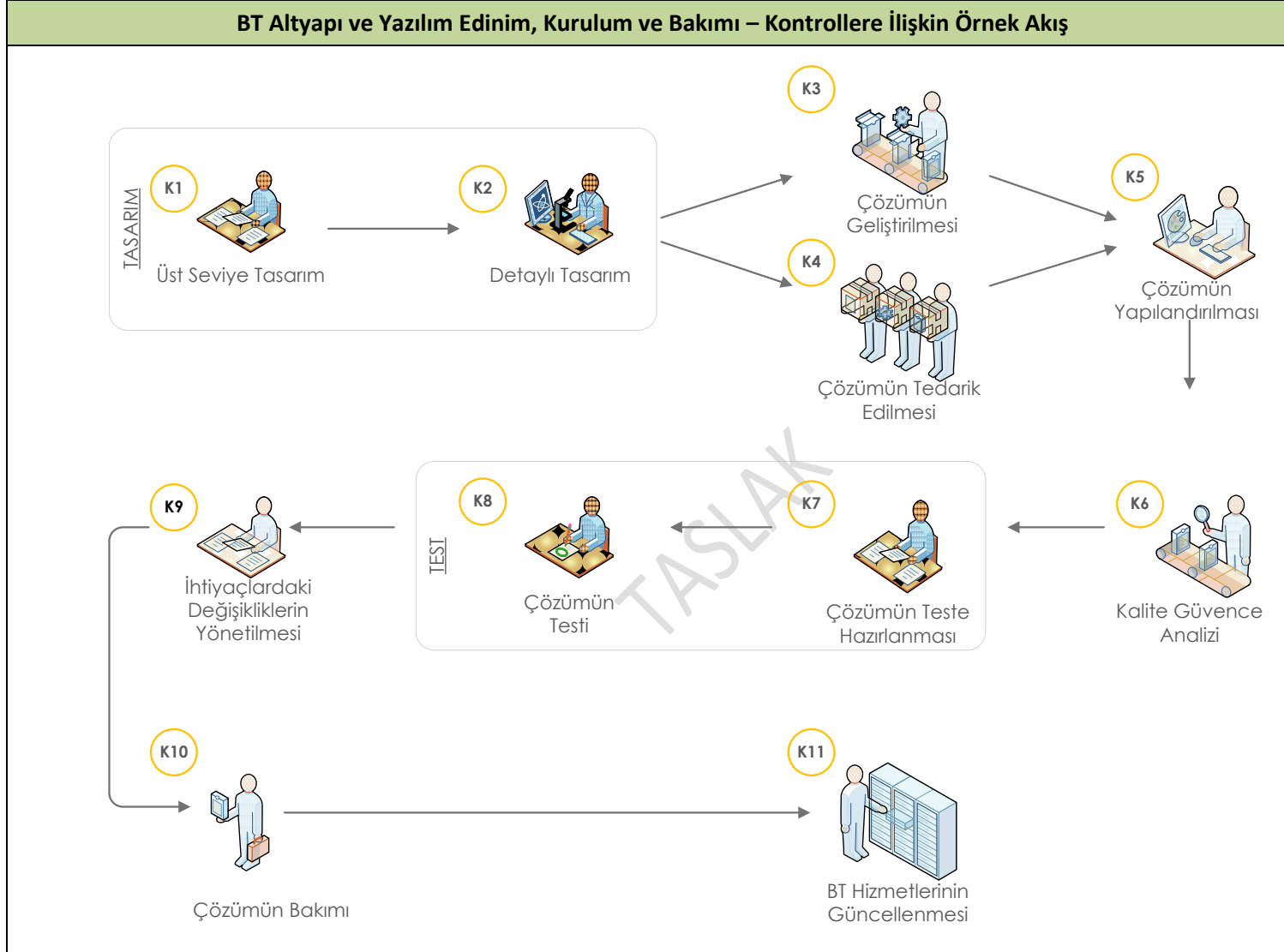
BT altyapı ve yazılım edinim, kurulum ve bakımı süreci, BT denetimi açısından aşağıdaki örnek süreç akışı üzerinden takip edilebilir. Söz konusu akış her kurum için farklı olabileceği gibi, süreç içerisinde ele alınan altyapı, yazılım veya hizmet tipleri, kullanılan yazılım ve tasarım araçları ile takip ve raporlama mekanizmaları da kurumdan kuruma değişebilmektedir.


Kontrollere İlişkin Örnek Akış

Süreçte yer alan tipik kontrollere aşağıdaki tabloda yer verilmiştir:

BT Altyapı ve Yazılım Edinim, Kurulum ve Bakımı - Kontroller	
K1	Üzerinde önceden anlaşılmış yazılım geliştirme tekniklerine ve kurum BT stratejisine uygun, üst seviye tasarım dokümanları oluşturulur..
K2	Detaylı tasarım ve teknik yazılım geliştirme ihtiyaçları belirlenir.
K3	Oluşturulmuş detaylı tasarımlara bağlı olarak ilgili çözümün bileşenleri, mevcut durumunda bulunan yazılım geliştirme, kalite ve dokümantasyon standartlarına uygun olarak geliştirilmeye başlanır.
K4	İlgili çözümün kurum dışından tedarik edildiği durumlarda yazılım tedarik planına, ihtiyaçlara, detay tasarımlara, mimari yapıya ve kurumun genel tedarik süreçlerine uygun şekilde ilgili çözüm bileşenleri tedarik edilir
K5	Tedarik edilen ya da iç kaynaklarla geliştirilen çözümler, mevcut iş süreçleri ile entegre olacak şekilde yapılandırılır. Yapılandırma sırasında kontrol, güvenlik ve denetlenebilirlik unsurları dikkate alınır.
K6	Kurum kalite yönetim sistemine uygun bir şekilde bir kalite planı oluşturulur ve ihtiyaç duyulan çözümün temini sürecinde bu kalite planı uygulanır.
K7	Çözüm bileşenleri için bir test planı ve bu doğrultuda iş süreçleri, uygulamalar ve altyapıyı dahil edecek şekilde bir test ortamı oluşturulur
K8	Edinilen çözümler ile ilgili testler, test planına ya da senaryolara uygun şekilde gerçekleştirilir
K9	Proje yaşam döngüsü boyunca gerçekleşmiş olan tüm yeni ihtiyaçlar ve değişiklikler ilgili birimler tarafından onaylanır ve takip edilir.
K10	Çözümün ve ilgili altyapı bileşenlerinin bakımı için bir bakım planı geliştirilir ve uygulanır.
K11	Temin edilen çözümlere bağlı olarak değişecek veya yeni oluşacak BT hizmetleri için yeni hizmet seviyeleri tanımlanır (Bkz: BT Hizmet Yönetimi). Hizmet seviyesi yönetimi bir servisin hizmet kalitesinin belli performans göstergeleri ışığında değerlendirilmesidir. Bu performans göstergeleri hizmet seviyesi olarak adlandırılır

BT Altyapı ve Yazılım Edinim, Kurulum ve Bakımı – Kontrollere İlişkin Örnek Akış



 Kontrol numaraları

Risk – Kontrol Eşleşmeleri

BT Altyapı ve Yazılım Edinim, Kurulum ve Bakımı Risk – Kontrol Eşleşmeleri											
Riskler	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11
R1. Temin edilen ya da geliştirilen BT çözümlerinin kurum iş hedeflerini karşılayamaması	+										
R2. Altyapı ve yazılım edinimi, kurulumu ve bakımı sırasında kurum kaynaklarının verimsiz kullanılması	+	+	+	+	+	+	+	+	+	+	+
R3. Çözümlerin BT stratejisi doğrultusunda belirlenen gereksinimleri sağlayamaması	+										
R4. Kanun ve yönetmeliklere uyum problemi yaratacak çözümlerin devreye alınması ya da kullanılması	+		+	+		+					
R5. Sistem erişilebilirliğinin / kullanılabilirliğinin olumsuz etkilenmesi	+	+	+	+	+	+	+	+	+	+	+
R6. Verilerin doğru şekilde işlenememesi ve bunun neticesinde veri güvenliğinin, bütünlüğünün ve erişilebilirliğinin bozulması	+	+	+	+	+	+	+	+	+	+	+
R7. Kurum BT sistemlerinde zafiyetlerin ve tehditlerin ortaya çıkması	+	+	+	+	+						
R8. Yeni çözümlerin güncellemelerinin yapılamaması									+	+	
R9. Kurum kalite standartlarına uymayan çözümlerin uygulamaya alınması						+					

BT Altyapı ve Yazılım Edinim, Kurulum ve Bakımı Risk – Kontrol Eşleşmeleri											
Riskler	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11
R10. Yeni çözümler için gerçekleştirilen testlerin gerçek faaliyet ortamını yansıtmaması							+				
R11. Üzerinde yetersiz test gerçekleştirilen çözümlerin devreye/kullanıma alınması								+			
R12. Yeni çözümlerin altyapı ile uyumsuzluk göstermesi, entegrasyon için ek kaynak harcanması		+	+	+							

TASLAK

Denetim Prosedürleri

K1 - Üzerinde önceden anlaşılmış yazılım geliştirme tekniklerine ve kurum BT stratejisine uygun, üst seviye tasarım dokümanları oluşturulur			
#	Denetim prosedürleri	T/i	Z/O
K1.1	Kurum bünyesinde BT altyapı ve yazılım edinimi, kurulumu ve bakımı ile ilgili olarak hazırlanmış politika, prosedür ve iş akışlarının varlığı kontrol edilir.	T	Z
K1.2	Kurum bünyesinde gerçekleştirilen BT altyapı ve yazılım edinim, kurulum ya da bakım ile ilgili çalışmalar ya da projeler (BT projeleri) için iş ihtiyaçlarının en doğru şekilde karşılanması amacıyla üst seviye tasarım dokümanlarının hazırlanmasının zorunlu tutulduğu kontrol edilir. Üst seviye tasarım dokümanlarında temin edilecek çözümün tüm unsurların, genel bir bakış açısıyla incelendiği gözlemlenir.	İ	Z
K1.3	Kurum bünyesinde denetim dönemi içerisinde gerçekleştirilmiş çalışmalar ya da BT projeleri arasından bir örneklem seçilir. Bu örneklemdeki projelere ait üst seviye tasarım tanımlarının bulunduğu, bu tanımların iş planları, stratejisi ve hedefleri ile uyumlu olduğu gözlemlenir.	İ	Z
K1.4	Örnek olarak seçilen projelerin tasarım yaklaşımının kurum tasarım standartlarına uygun şekilde gerçekleştirildiği hazırlanmış dokümanlar incelenerek ve BT ekipleri ile görüşülerek değerlendirilir.	İ	O
K1.5	Örnek projeler için hazırlanmış proje belgeleri incelenir. Bu belgelerde kullanıcıların, BT uzmanlarının, paydaşların ve ilgili yönetim birimlerinin tasarım sürecindeki rol ve sorumluluklarına yer verildiği gözlemlenir.	İ	Z
K1.6	Örnek projelerin üst seviye tasarımlarının kalite gözden geçirmesine tabi tutulduğu ve paydaşların onayından geçtiği gözlemlenir.	İ	O

K2 - Detaylı tasarım ve teknik yazılım geliştirme ihtiyaçları belirlenir.

#	Denetim prosedürleri	T/İ	Z/O
K2.1	Örnek projeler için yazılım kodu üzerinden geçme ve belge inceleme yöntemleri ile veri sözlüğü (veritabanlarındaki tüm veri öğelerinin isimlerinin, cinslerinin, değer aralıklarının, kaynaklarının ve varsa erişim yetkilerinin tutulduğu veritabanı) standartlarına uyulduğu gözlemlenir	İ	Z
K2.2	Örnek projeler için detay dokümanlar incelenerek uygun hata kurtarma ve yedekleme ihtiyaçlarının belirlendiği ve düzenlemelerinin yapıldığı gözlemlenir. Bu doğrultuda aynı zamanda çözüm ile ilgili yedekleme planı ve prosedürleri gözden geçirilir ve erişilebilirlik açısından yeterliliği denetlenir	İ	O
K2.3	Örnek projeler için detay tasarım dokümanlarında veri saklama (verinin saklanma şekli), konumlandırma (verinin saklanacağı yer), veri çekme (veriye ulaşılması ve elde edilmesi için yapılması gerekenler) kurallarının tanımlandığı gözlenir	T	O
K2.4	Örnek projeler için detay tasarım dokümanları incelenerek veri güvenliği, bütünlüğü ve erişilebilirliği ile ilgili ihtiyaçların ve yapılacakların tanımlandığı gözlemlenir.	İ	Z
K2.5	Örnek projelerin tasarım dokümanlarında denetlenebilirlik ve ağ ihtiyaçları konularına değinildiği ve en iyi uygulamaların dikkate alındığı gözlemlenir.	İ	O
K2.6	Örnek projeler için detay tasarım dokümanları incelenerek var olan sistemler ile entegrasyonun nasıl sağlanacağını dokümanlarda belirtildiği gözlemlenir	İ	O
K2.7	Örnek projeler için detay tasarım dokümanları incelenir ve kullanıcıların çalışacakları önyüzlerin tasarımları hakkında detaylara yer verildiği gözlemlenir.	İ	O
K2.8	Yazılım süreci başlamadan önce detaylı tasarım standartlarının üzerinden gidilerek kontrolünün yapıldığı teyit edilir.	İ	O

K3 - Oluşturulmuş detaylı tasarımlara bağlı olarak ilgili çözümün bileşenleri, mevcut yazılım geliştirme, kalite ve dokümantasyon standartlarına uygun olarak geliştirilmeye başlanır.

#	Denetim prosedürleri	T/i	Z/O
K3.1	Örnek olarak seçilen projeler için iş süreçlerinin, bunları destekleyen hizmetlerin, uygulamaların, altyapının ve bilgi kaynaklarının üzerinde önceden mutabık kalınmış tasarım standartlarına ve ihtiyaçlarına uygun olarak geliştirildiği gözlemlenir.	İ	Z
K3.2	Çözümün geliştirmesi ile ilgili olarak dış firmaların dahil olduğu durumlarda, bu firmalarla yapılan sözleşmelerde bakım, destek, geliştirme standartları ile uyum ve lisans konularına yer verildiği gözlemlenir.	İ	Z
K3.3	Proje sonunda ilgili paydaşlarla beraber değişiklik taleplerine uygun olarak tasarım, kalite ve performans değerlendirmelerinin yapıldığı kontrol edilir.	İ	O
K3.4	Uygulanacak çözüm ile ilgili tüm bileşenlerin belirlenmiş standartlara uygun şekilde belgelendirildiği ve yenilik ve değişiklikler üzerinde sürüm kontrolünün sağlandığı kontrol edilir.	İ	Z
K3.5	Temin edilen çözümler üzerinde yapılan tüm özelleştirme veya kişiselleştirme çalışmalarının etkinliğe, performansa ve diğer sistemlerle entegrasyona olan etkisinin değerlendirildiği gözlemlenir.	İ	Z

K4 - İlgili çözümün kurum dışından tedarik edildiği durumlarda yazılım tedarik planına, ihtiyaçlara, detay tasarımlara, mimari yapıya ve kurumun genel tedarik süreçlerine uygun şekilde ilgili çözüm bileşenleri tedarik edilir.

#	Denetim prosedürleri	T/İ	Z/O
K4.1	Kurum bünyesinde BT çözümlerinin teminine dair bir planın bulunduğu gözlemlenir. Planın içerisinde proje boyunca değişebilecek ihtiyaçlarla ilgili olarak yapılması gerekenlerin belirtildiği gözlemlenir.	T	Z
K4.2	Kamu İhale Kanunu kapsamına girmeyen fakat yine dışarıdan tedarik yolu ile gerçekleşen projeler arasından bir örneklem seçilir. Bu projeler için tüm tedarik planlarının, risk, maliyet, getiriler ve teknik uygunluk unsurlarına dikkate alınarak onaylandığı gözlemlenir. Kamu İhale Kanunu kapsamına giren çözümler için ilgili kanunda belirtilen tüm adımların uygulandığı incelenir.	İ	Z
K4.3	Tedarik edilen çözümlerle ilgili kurum ihtiyaçlarına yönelik olarak, çözümün özelleştirilme ihtiyaçlarının belgelendiği gözlemlenir.	İ	O
K4.4	Tedarik edilen tüm yazılım ve altyapı bileşenlerinin BT varlık envanterine kaydedildiği gözlemlenir	İ	Z

K5 - Tedarik edilen ya da iç kaynaklarla geliştirilen çözümler, mevcut iş süreçleri ile entegre olacak şekilde yapılandırılır. Yapılandırma sırasında kontrol, güvenlik ve denetlenebilirlik unsurları dikkate alınır.

#	Denetim prosedürleri	T/İ	Z/O
K5.1	Seçilen örnek çözümler için uygulanacak çözüme dair iş süreçlerinin ve BT ile ilgili tüm bileşenlerin, detay tasarımlara ve kalite ihtiyaçlarına uygun şekilde yapılandırıldığı teyit edilir.	T	Z
K5.2	Örnek çözümler için, çözümün kurum süreçlerine göre özelleştirilmesinin söz konusu olduğu durumlarda, süreçlerin ve operasyonel kılavuzların bu özelleştirmelere göre güncellendiği gözlemlenir	İ	Z
K5.3	Örnek olarak seçilen projeler için iş süreçleri kontrol gereksinimlerine dayalı olarak, otomatik uygulama kontrollerinin tanımlandığı kontrol edilir.	İ	O
K5.4	Örnek olarak seçilen çözümlerin dokümanları incelenerek güvenlik, veri bütünlüğü, denetim izleri, erişim kontrolü ve veritabanı bütünlüğü gibi kontrollerin dikkate alındığı gözlemlenir.	İ	O

TASLAK

K6 - Kurum kalite yönetim sistemine uygun bir şekilde bir BT kalite planı oluşturulur ve ihtiyaç duyulan çözümün temini sürecinde bu kalite planı uygulanır.

#	Denetim prosedürleri	T/i	Z/O
K6.1	Çözümün temini ile ilgili olarak kalite güvence planı ve uygulamalarının aşağıdaki maddeleri içerecek şekilde tanımlandığı kontrol edilir. <ul style="list-style-type: none">• Kalite kriterlerinin tanımlanması• Doğrulama ve onay süreçleri• Gözden geçirme süreçleri• Kalite sorumlularının sahip olması gereken nitelikler• Kalitenin sağlanması için gerekli olan rol ve sorumluluklar	İ	Z
K6.2	Kalite gözden geçirmelerinin yazılım sürecinden bağımsız kişilerce gerçekleştirildiği kontrol edilir..	İ	Z
K6.3	Geliştirme sürecinde hazırlanan kalite dokümanları ve hata kayıtları örneklem üzerinden incelenir ve kalite standartlarına uymayan tüm durumların saptandığı ve düzeltici faaliyetlerin gerçekleştirildiği teyit edilir.	İ	O

TASLAK

K7 - Çözüm bileşenleri için bir test planı ve bu doğrultuda iş süreçleri, uygulamalar ve altyapıyı dahil edecek şekilde bir test ortamı oluşturulur.

#	Denetim prosedürleri	T/İ	Z/O
K7.1	Çözümlerin temininde test planlarının oluşturulduğu ve düzenli testlerin gerçekleştirildiği gözlemlenir. Test planı, yeni uygulamanın ya da ilgili BT bileşeninin mevcut uygulamalar ve altyapı ile entegre çalışabilirliği, sistem performans verimliliği, kapasitesi ve veri bütünlüğü gibi konuları kapsamalıdır	T, İ	Z
K7.2	Çözümlere uygun test prosedürlerinin ve var olan şartlar altında çözümü en iyi şekilde değerlendirme imkanını sunacak test senaryolarının hazırlanmış olduğu gözlemlenir.	İ	Z
K7.3	Test ortamının, ilgili çözümün tam kapsamlı olarak test edilmesini mümkün kılacak şekilde hazırlandığı kontrol edilir. Test ortamı mevcut teknolojik koşulları, kullanıcı tiplerini, işlem tiplerini, dağıtım koşullarını ve iş süreçlerini mümkün olduğu kadar gerçekçi bir biçimde yansıtmalıdır.	İ	Z
K7.4	Test prosedürlerinin çözüm üzerindeki kontrollerin yeterliliğini değerlendirmeye imkan verecek şekilde tasarlandığı ve test sonuçlarının proje paydaşları tarafından onaylandığı gözlemlenir.	İ	O

K8 - Edinilen çözümler ile ilgili testler, test planına ya da senaryolara uygun şekilde gerçekleştirilir

#	Denetim prosedürleri	T/İ	Z/O
K8.1	Örnek olarak seçilen projelerde testlerin test planına ve senaryolarına uygun şekilde gerçekleştirildiği gözlemlenir	İ	Z
K8.2	Son kullanıcı kabul testlerinin yazılım ekibinden bağımsız son kullanıcılar veya iş süreç sahipleri tarafından gerçekleştirildiği gözlemlenir.	İ	Z
K8.3	Testlerin sadece test ortamında gerçekleştirildiği, canlı ortamda test yapılmasının engellendiği teyit edilir.	İ	Z
K8.4	Temin edilen çözümler için hem otomatik gerçekleştirilen testlerin hem de kullanıcı testlerinin gerçekleştirildiği gözlemlenir.	İ	O
K8.5	Test sırasında ortaya çıkan hataların belirlendiği ve kaydedildiği gözlemlenir	İ	O
K8.6	Testlerin kullanıcılar tarafından nihai onaylar verilene kadar devam ettiği, kullanıcı onayı olmayan çözümlerin uygulamaya konmadığı gözlemlenir.	İ	Z
K8.7	Test sonuçlarının kayıt altına alınarak muhafaza edildiği ve ilgili paydaşlarla paylaşıldığı gözlemlenir.	İ	Z

K9 - Proje yaşam döngüsü boyunca gerçekleşmiş olan tüm yeni ihtiyaçlar ve değişiklikler ilgili birimler tarafından onaylanır ve takip edilir.

#	Denetim prosedürleri	T/i	Z/O
K9.1	Örnek olarak seçilen projeler için proje geliştirme süreci boyunca ortaya çıkmış olan tüm ihtiyaçlar ve değişiklik taleplerinin takip edildiği gözlemlenir. Bu değişiklik taleplerinin değerlendirildiği ve BT bütçesine olan etkisinin gözden geçirildiği gözlemlenir.	İ	O
K9.3	Değişiklik taleplerinin önceliklendirildiği kontrol edilir.	İ	O
K9.4	Tüm paydaşların gerçekleşen değişikliklerden haberdar olmasını sağlayacak mekanizmaların kurulmuş olduğu ve bu değişikliklerin paydaşları temsil eden birimler tarafından da onaylandığı gözlemlenir.	İ	O

TASLAK

K10 - Çözümün ve ilgili altyapı bileşenlerinin bakımı için bir bakım planı geliştirilir ve uygulanır.

#	Denetim prosedürleri	T/İ	Z/O
K10.1	Yama yönetimi, risk analizi, zafiyet analizi ve güvenlik gereklilikleri gibi iş ihtiyaçları ve operasyonel gerekliliklere dair, çözüm bileşenlerini kapsayan bir bakım planı oluşturulur.	T	Z
K10.2	Örnek olarak seçilen çözümlere (tedarik edilmiş ya da kurum bünyesinde geliştirilmiş) ait kayıtlar ve belgeler incelenir ve aşağıdaki unsurları içerip içermediği kontrol edilir. <ul style="list-style-type: none"> • Devreye alma planı • Kaynak planı • Hata düzeltme • Küçük geliştirmeler • Dokümanların bakımı • Acil değişiklikler • Diğer uygulamalar ve altyapı ile ilişkiler • İyileştirme stratejisi • Destek konuları • İş riskine ve güvenlik gerekliliklerine dair gözden geçirmeler 	T	Z
K10.3	Çözümlerin bakımı sürecinde ihtiyaç duyulan tüm değişikliklerin, değişiklik yönetimi sürecine uygun şekilde gerçekleştiği teyit edilir.	İ	Z
K10.4	Önerilen bakım faaliyetlerinin var olan çözüm faaliyetleri üzerindeki etkisinin analiz edildiği gözlemlenir. Bu analiz kapsamında risk, kullanıcılara olan etkisi ve bakıma ayrılacak kaynakların değerlendirildiği kontrol edilir.	İ	O
K10.5	İş süreç sahiplerinin bakım süreçleri ile ilgili bilgilendirildiği ve yapılacaklardan haberdar olduğu teyit edilir.	İ	O
K10.6	Bakım faaliyetlerinin yoğunluğunun ve eğilimlerinin incelendiği ve anormal yoğunluk olan durumların saptandığı ve önlemlerin alındığı kontrol edilir	İ	O

K11 - Temin edilen çözümlere bağlı olarak değişecek veya yeni oluşacak BT hizmetleri için yeni hizmet seviyeleri tanımlanır (Bkz: BT Hizmet Yönetimi). Hizmet seviyesi yönetimi bir servisin hizmet kalitesinin belli performans göstergeleri ışığında değerlendirilmesidir. Bu performans göstergeleri hizmet seviyesi olarak adlandırılır

#	Denetim prosedürleri	T/i	Z/O
K11.1	Yeni uygulamaya alınan çözümlerin hizmet seviyeleri üzerine getirebileceği değişikliklerin yönetim tarafından değerlendirildiği kontrol edilir.	İ	Z
K11.2	Yeni hizmet seviyelerinin aşağıdaki örnek unsurları barındıracak biçimde şekillendirildiği kontrol edilir. <ul style="list-style-type: none">• Hizmet süreleri• Kullanıcı memnuniyeti• Erişebilirlik• Performans• Kapasite• Güvenlik• Süreklilik• Uyum• Kullanışlılık	İ	O

Ek Kaynaklar

- ISACA. (2007). COBIT 4.1 Framework – AI02. Rolling Meadows, Illionis, United States of America.
- ISACA. (2012). COBIT 5 Enabling Processes – BAI03. Rolling Meadows, Illinois, United States of America.

TASLAK

4.7. BT HİZMET YÖNETİMİ

Sürecin Genel Tanımı

BT hizmet yönetimi BT'nin iş birimlerine etkin ve verimli bir hizmet sağlayabilmesi için kullanılan süreç ve prosedürleri içerir. BT hizmet yönetimi iş birimlerinin hedeflerini gerçekleştirmesi yolunda BT'nin hizmet sunmasına olanak sağlayan BT altyapısının yönetimini kapsar. Bu doğrultuda BT hizmetleri iş birimlerinin değişen hedeflerini karşılamak için sürekli bir gelişme halindedir. Uzun dönemde ise BT hizmet yönetimi artan hizmet kalitesi ve düşen maliyet ile kurumdaki BT yapısını daha verimli ve işe yarar hale getirmeyi hedefler.

BT birimi kurumlarda son kullanıcılara olabilecek en iyi hizmeti sağlamaktan sorumludur. Bundan dolayı BT bölümünün başarısı kullanıcıları memnun ederek ve hizmet seviyesi anlaşmasınca (HSA) ortaya konulan hedeflere uyarak mümkün olur. BT hizmeti, iç BT biriminden ya da dışarıdaki BT servis sağlayıcılarından temin edilebilir. Buna ek olarak kurumlar bir bölüm BT hizmetlerini kurum içerisinden, geri kalanlarını ise dışarıdan da temin edebilir.

HSA, BT birimi ile hizmet ettiği müşteriler (iş birimleri) arasındaki bir anlaşmadır. HSA'lar, BT tarafından sağlanacak hizmetleri teknik olmayan bir dille, müşterinin bakış açısından açıklar. Anlaşma süresince hizmetlerin ölçümü ve düzenlenmesi HSA'lar ile mümkündür

Sürecin BT Denetimi Açısından Önemi

BT hizmet yönetimi süreci kurum faaliyetlerinin gerçekleştirilmesi için gerekli olan ve bilgi sistemleri tarafından sağlanan "kritik BT işlevselliği"nin iş birimlerinin ihtiyaçları ve hedefleri doğrultusunda sağlanması ile doğrudan ilgili olduğundan, BT denetimlerinde ele alınması gereken konulardan biridir. Bu sürecin değerlendirilmesi ile, kurum bünyesinde temin edilen BT hizmetlerinin iş hedeflerinin gerçekleştirilebilmesi hedefiyle tasarlandığı, takip edildiği, ölçüldüğü, değerlendirildiği ve düzenlendiği konusunda makul bir güvence sağlanabilir.

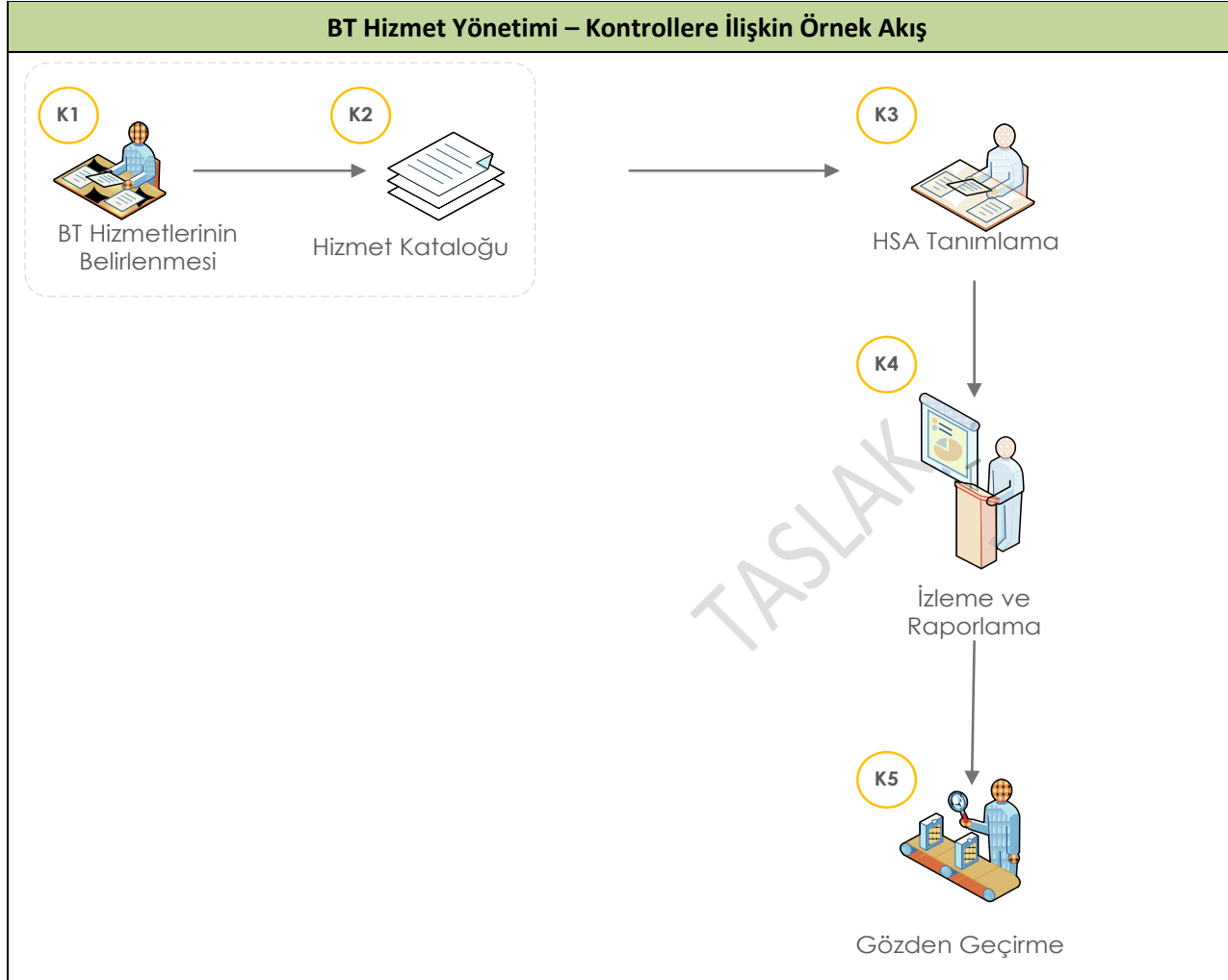
BT hizmet yönetimi süreci, BT denetimi açısından aşağıdaki örnek süreç akışı üzerinden takip edilebilir. Söz konusu akış her kurum için farklı olabileceği gibi, süreç içerisinde ele alınan HSA'ların yapısı, hizmet tipleri, takip ve raporlama mekanizmaları da kurumdan kuruma değişebilmektedir.


Kontrollere İlişkin Örnek Akış

Süreçte yer alan tipik kontrollere aşağıdaki tabloda yer verilmiştir:

BT Hizmet Yönetimi - Kontroller	
K1	İş ihtiyaçları ve BT tarafından sağlanan hizmetlerin ve hizmet seviyelerinin iş süreçlerini nasıl desteklediği incelenir. Hizmet seviyeleri üzerinde iş birimleri ile değerlendirilir ve bu seviyeler üzerinde anlaşılır.
K2	İlgili hedef gruplar için hizmet katalogları tanımlanır. BT tarafından sağlanan hizmetler bu kataloglarda yayınlanır.
K3	Tüm kritik BT hizmetleri için HSA'lar düzenlenir. Bu anlaşmalar taahhütleri, destek ihtiyaçlarını, nitel ve nicel metrikleri, eğer mevcutsa ticari anlaşmaları ve rol ve sorumlulukları içerir.
K4	Hizmet seviyesi performans kriterleri sürekli olarak izlenir. Saptanan başarılar ve eğilimler yönetimi performans yönetimi açısından bilgilendirmek amacı ile raporlanır.
K5	HSA'lar ve eğer varsa bağlı oldukları sözleşmeler güncellikleri, ihtiyaçları yansıttıkları ve etkinliklerini kontrol amacı ile düzenli olarak gözden geçirilir.

Bahsi geçen kontrollere ilişkin örnek akış şeması aşağıda yer almaktadır:



 Kontrol numaraları

Risk – Kontrol Eşleşmeleri

BT Hizmet Yönetimi Risk – Kontrol Eşleşmeleri					
Riskler	K1	K2	K3	K4	K5
R1. İş birimlerinin beklentileri ile BT'nin yapabilecekleri arasında farklılık olması sebebiyle anlaşmazlıkların ortaya çıkması, iş birimlerinin hedefledikleri başarıya ulaşamaması	+	+	+	+	+
R2. izmet seviyelerinin doğru belirlenmemesi neticesinde BT tarafından verimsiz ve yüksek maliyetli hizmetlerin sağlanması	+	+	+		
R3. Hizmetlerin değişen iş ihtiyaçlarına cevap verememesi			+	+	+
R4. Hizmetler ile ilgili kritik olaylara zamanında cevap verilememesi			+		
R5. Güncel olmayan sözleşmelerin yasal ve ticari zorunluluklardan kaynaklanan gereksinimlere uyum konusunda problem yaratması			+		+
R6. Hizmetlerin yanlış önceliklendirilmesi neticesinde önemli hizmetlerin göz ardı edilmesi.	+	+	+		+
R7. BT'nin kalitesiz hizmet üretmesi sonucu paydaşların memnuniyetinin sağlanmaması	+	+	+	+	+
R8. İş birimlerinin ve BT'nin sorumluluklarını kavrayamaması	+	+	+		

2.4.7. Denetim Prosedürleri

K1 - İş ihtiyaçları ve BT tarafından sağlanan hizmetlerin ve hizmet seviyelerinin iş süreçlerini nasıl destekleyeceği kararlaştırılır. Hizmet seviyeleri iş birimleri ile birlikte değerlendirilir ve bu seviyeler üzerinde anlaşılır.

#	Denetim prosedürleri	T/İ	Z/O
K1.1	Hizmet seviyesi anlaşmaları (HSA) politika ve prosedürleri incelenir. HSA hedefleri ve performans göstergelerinin, iş hedefleri ve BT stratejisi ile uyumu değerlendirilir.	T	Z
K1.2	Kurum bünyesinde BT tarafından iş birimlerine sağlanan hizmetler, hizmet katalogu incelenerek ve BT ve iş birimleri ile görüşerek belirlenir. Bu hizmetler için, iş ihtiyaçlarına ve BT stratejisine uygun şekilde HSA'ların oluşturulmuş olduğu gözlemlenir.	İ	Z
K1.3	İş birimlerine sağlanan BT hizmetlerinin düzenli olarak incelendiği ve hizmet yapısında ve hizmet seviyelerinde gerekebilecek değişikliklerin saptandığı gözlemlenir. Buna ek olarak bu incelemeler sonrasında geçerliliğini yitirmiş hizmetlerin de saptandığı ve kaldırıldığı gözlemlenir.	İ	O

K2 - İlgili hedef gruplar için hizmet katalogları tanımlanır. BT tarafından sağlanan hizmetler bu kataloglarda yayınlanır.

#	Denetim prosedürleri	T/i	Z/O
K2.1	İş birimlerine sağlanan ilgili BT hizmetlerinin ve hizmet seviyelerinin bulunduğu katalogların hazırlandığı kontrol edilir.	İ	Z
K2.2	Hizmet kataloglarının güncel olduğu ve düzenli olarak güncelliğinin kontrol edildiği gözlemlenir.	İ	Z
K2.3	Hizmet kataloglarında denetim dönemi içerisinde gerçekleşmiş olan güncellemeler temin edilir, bu güncellemeler ile ilgili olarak iş birimlerinin bilgilendirildiği kontrol edilir.	İ	Z

TASLAK

K3 - Tüm kritik BT hizmetleri için HSA'lar düzenlenir. Bu anlaşmalar taahhütleri, destek ihtiyaçlarını, nitel ve nicel metrikleri, eğer mevcutsa ticari anlaşmaları ve rol ve sorumlulukları içerir.

#	Denetim prosedürleri	T/İ	Z/O
K3.1	Sağlanan BT hizmetleri ile ilgili tüm paydaşların HSA'lar ile ilgili bilgilendirilmiş oldukları ve şartları kabul ettikleri gözlemlenir.	İ	Z
K3.2	Örnek olarak seçilen HSA'ların istisnaları, ticari anlaşmaları ve işletim seviyesi anlaşmalarını (İSA) içerdiği kontrol edilir.	İ	Z
K3.3	Kurumdaki HSA yönetimi süreci incelenir ve HSA anlaşmalarında belirlenmiş hedeflerin takip edildiği gözlemlenir	İ	Z
K3.4	Örnek olarak seçilen HSA'ların uygun BT ve iş birimi temsilcileri tarafından onaylandığı ve imzalandığı kontrol edilir.	İ	Z
K3.5	HSA'ların düzenli olarak gözden geçirildiği ve değişikliğin gerektiği durumlarda uygun ihtiyaç duyulan değişikliğin gerçekleştirildiği kontrol edilir	İ	Z
K3.6	Hizmetlerin teknik olarak nasıl sağlanacağını açıklayan İSA'ların oluşturulması, yönetilmesi, gözden geçirilmesi ve düzeltilmesi süreçlerinin kurum bünyesinde mevcut olduğu gözlemlenir.	T	Z
K3.7	Örnek olarak seçilen HSA'lara ait İSA'ların ilgili hizmete dair hizmet ihtiyaçlarını içerdiği kontrol edilir.	İ	Z
K3.8	Örnek olarak seçilen İSA'ların hizmetin sağlanması ile ilgili uygulanabilir ve uygun tanımları içerdiği kontrol edilir.	İ	Z
K3.9	Örnek olarak seçilen HSA'ların aşağıdaki unsurları içerdiği gözlemlenir. <ul style="list-style-type: none"> Hizmetin tanımı Hizmetin maliyeti Asgari hizmet seviyeleri BT fonksiyonundan sağlanacak hizmetin seviyesi Erişilebilirlik, güvenilirlik ve büyüme kapasitesi Anlaşmadaki herhangi bir değişiklik için izlenmesi gereken değişiklik prosedürü Süreklilik planı Güvenlik ihtiyaçları Hizmeti sağlayan ve hizmeti temin eden arasındaki resmi onaylı anlaşma Geçerli olduğu dönem ve yeni dönem gözden geçirme tarihi Performans raporlama içeriği ve sıklığı Hizmet iyileştirme taahhütü 	İ	Z

K4 - Hizmet seviyesi performans kriterleri sürekli olarak izlenir. Saptanan başarılar ve eğilimler performans yönetimi açısından üst yönetimi ve ilgili iş birimlerini bilgilendirmek amacı ile raporlanır.

#	Denetim prosedürleri	T/İ	Z/O
K4.1	HSA'ların izlenmesi ve izleme sonuçlarının raporlanması ile ilgili sürecin kurum bünyesinde tanımlı olduğu gözlemlenir.	T	Z
K4.2	Sağlanan hizmetlerin performansının değerlendirildiği ve düzenli ve resmi olarak iş birimlerine raporlandığı kontrol edilir. Raporlananlar arasında önceden üzerinde mutabık kalınmış değerlerden sapmaların bulunduğu dikkat edilir.	İ	Z
K4.3	Hizmet seviyesi performansı ile ilgili olarak tahminlerin yapıldığı ve eğilimlerin izlendiği kontrol edilir.	İ	O
K4.4	Performans ile ilgili problemlerin olduğu hizmetler öğrenilir. Bu problemlerin çözümü için aksiyon planlarının hazırlandığı gözlemlenir.	İ	Z

TASLAK

K5 - HSA'lar ve eğer varsa bağlı oldukları sözleşmeler güncellikleri, ihtiyaçları yansıttıkları ve etkinliklerini kontrol amacı ile düzenli olarak gözden geçirilir.

#	Denetim prosedürleri	T/i	Z/O
K5.1	Örnek olarak seçilen HSA'lar ve varsa bağlı oldukları sözleşmeler incelenir, güncel oldukları ve gerektiğinde değişiklik gördükleri gözlemlenir.	İ	Z
K5.2	HSA'ların ve eğer varsa bağlı oldukları sözleşmelerin düzenli olarak iş ihtiyaçlarına uygunluk açısından değerlendirildikleri gözlemlenir	İ	Z

TASLAK

Ek Kaynaklar

- ISACA. (2007). COBIT 4.1 Framework – DS1. Rolling Meadows, Illinois, United States of America.
- ISACA. (2012). COBIT 5 Enabling Processes – APO09, Rolling Meadows, Illinois, United States of America.
- ITIL V3 2011 Service Strategy, 4.4 Demand Management (UK Cabinet Office, 2011)
- ITIL V3 2011 Service Strategy, 4.2 Service Portfolio Management (UK Cabinet Office, 2011)
- ITIL V3 2011 Service Design, 4.2 Service Catalogue Management (UK Cabinet Office, 2011)
- ITIL V3 2011 Service Design, 4.3 Service Level Management (UK Cabinet Office, 2011)

TASLAK

4.8. RİSK YÖNETİMİ

Sürecin Genel Tanımı

Risk yönetimi, bir kurumda iş hedeflerinin gerçekleşmesi doğrultusunda kullanılan BT kaynaklarını etkileyen zafiyetlerin ve tehditlerin tanımlanması ve bu kaynakların kurum için değeri doğrultusunda riskleri kabul edilebilir seviyeye indirecek önlemlerin alınması sürecidir. BT risk yönetimi sayesinde BT risklerinin sebep olabileceği olumsuzluklar belirlenir ve önlemler alınır. BT risk yönetim metodolojisi, kurumsal risk yönetim metodolojisi, kurumun bilgi güvenliği sistemi ve yasal zorunluluklar ile uyumlu olmalıdır.

BT risk yönetimi, BT süreçleri ile ilgili riskleri belirlemeyi, analiz etmeyi, değerlendirmeyi, BT risklerine müdahale etmeyi, izlemeyi ve bunlarla ilgili iletişim faaliyetlerini kapsar. Maruz kalınan risklerin etkisi ve bu etkiye karşı olan risk toleransının tanımlanması ile kurum risk yönetimi stratejisi belirlenir. Bilgi sistemleri üzerinde tesis edilen yönetimin etkinliği; risk yönetimi, iç kontrol ve iç denetim kapsamında yürütülecek çalışmaların ortak katkısıyla sağlanır. Kurumlar kendi risk profillerine, operasyonel yapılarına, kurumsal yönetim kültürlerine ve ilgili diğer mevzuat ile çizilen çerçeveye uygun olarak bilgi sistemlerine ilişkin risk yönetim süreçlerini geliştirirler.

Sürecin BT Denetimi Açısından Önemi

Risk yönetimi süreci kurum faaliyetlerinin gerçekleştirilmesi için gerekli olan ve bilgi sistemleri tarafından sağlanan “kritik BT işlevselliği”nin karşı karşıya olduğu risklerin kabul edilebilir seviyeye indirilmesi ile doğrudan ilgili olduğundan, BT denetimlerinde ele alınması gereken konulardan biridir. Risk yönetiminin değerlendirilmesi sayesinde, BT hizmetlerinin karşı karşıya olduğu risklerin kurumca kabul edilmiş düzeylere indirildiğine dair makul güvence sağlanabilir. Bu sayede, BT uygulamalarının hesaplama, raporlama vb. gibi denetim açısından kritiklik taşıyan işlevselliklerine ilişkin risklerin, denetim dönemi içerisinde kontrollü bir biçimde takip edildiğine, gerçekleşen risklerle ilgili eyleme geçildiğine ilişkin bir kanaat oluşturulabilir.

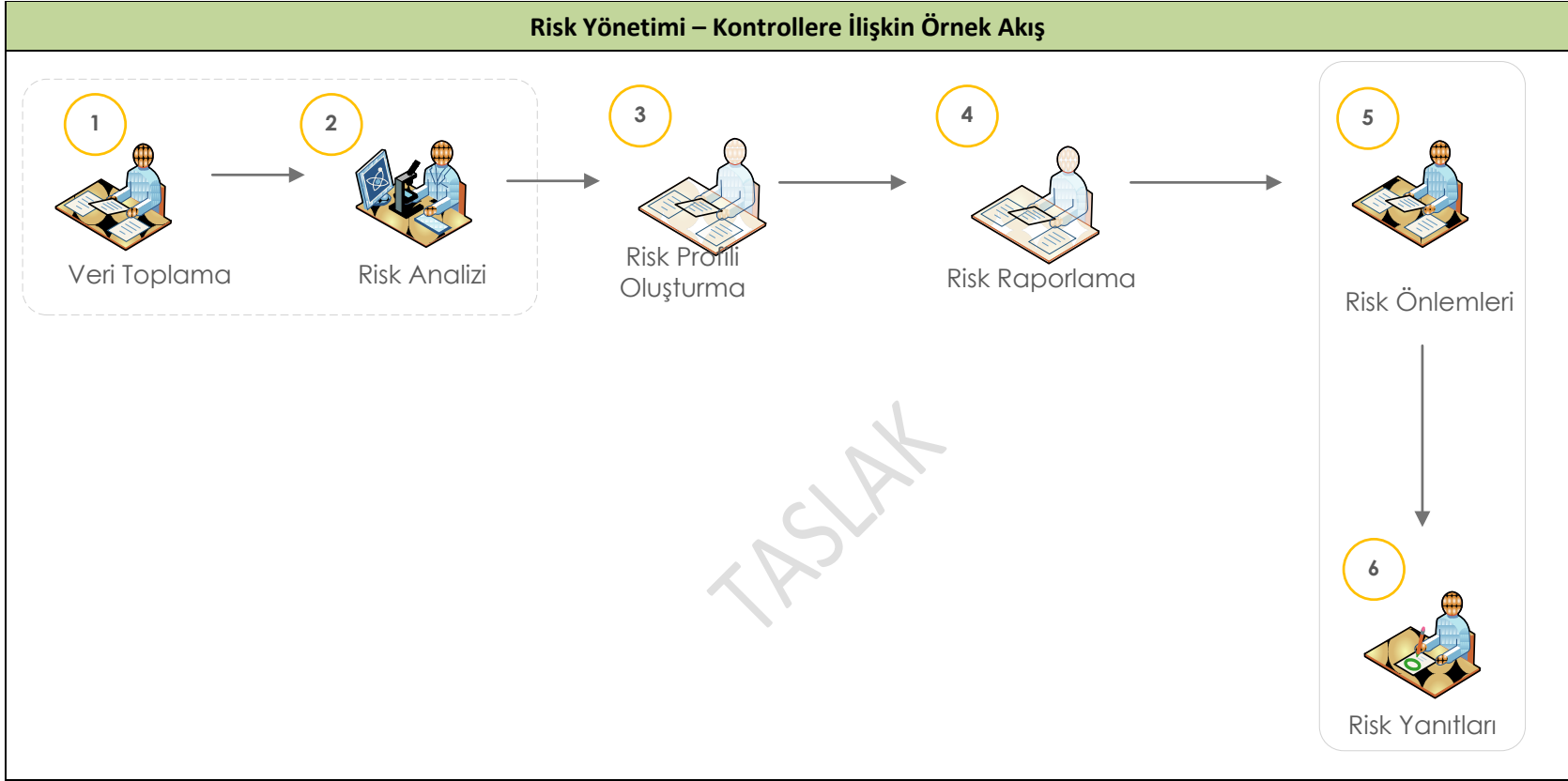
Risk yönetimi, BT denetimi açısından aşağıdaki süreç ve kontroller üzerinden takip edilebilir. Söz konusu akış her kurum için farklı olabileceği gibi, süreç içerisinde ele alınan risk değerlendirme yöntemleri, oluşturulan risk envanterleri, risk yönetimi için kullanılan uygulamalar, takip ve raporlama mekanizmaları da kurumdan kuruma değişebilmektedir.


Kontrollere İlişkin Örnek Akış

Süreçte yer alan tipik kontrollere aşağıdaki tabloda yer verilmiştir:

Risk Yönetimi - Kontroller	
K1	Etkin bir BT risk tanımlama, analiz ve raporlama mekanizmasının kurulması için risk verileri tanımlanır ve toplanır.
K2	İş hedeflerine olan etkileri göz önüne alınarak riskler üzerinde verilecek kararları destekleyecek bilgiler toplanır. Bu doğrultuda tanımlanan tüm risklerin etkisi nicel ve nitel yöntemler kullanılarak belirlenir.
K3	Potansiyel etki, risk nitelikleri, risk yanıtları ve öngörülen gerçekleşme sıklığı gibi bilgileri içeren bir envanter oluşturularak kaynaklar, yetkinlikler ve mevcut kontrol aktiviteleri kayıt altına alınır.
K4	Maruz kalınan BT risklerinin mevcut durumu ve fırsatlar ile ilgili bilgiler, paydaşlar ile zamanında paylaşılır.
K5	Kurum tarafından riskleri kabul edilebilir bir seviyeye indirebilmek için olanaklar etkin bir şekilde yönetilir.
K6	Uygun maliyetli kontroller ile risklerin etkilerini azaltmak üzere tasarlanmış bir risk yanıt sürecinin geliştirilir.

Bahsi geçen kontrollere ilişkin örnek akış şeması aşağıda yer almaktadır:



 Kontrol numaraları

Risk – Kontrol Eşleşmeleri

Risk Yönetimi Risk – Kontrol Eşleşmeleri						
Riskler	K1	K2	K3	K4	K5	K6
R1. Önlem alınmamış risklerin gerçekleşmesi sonucu kurum isminin zarar görmesi ve mali kayıpların oluşması	+	+	+	+	+	+
R2. BT'nın iş süreçleri üzerindeki etkisinin değerlendirilememesi		+	+	+		
R3. Risk azaltıcı kontrollerin beklenen etkiyi sağlamaması		+				
R4. Risklerin yanlış nitelik ve nicelik analizlerine göre değerlendirilmesi						+
R5. Risklerin nitelik ve niceliksel olarak yanlış analiz edilmesi		+				

Denetim Prosedürleri

K1 - Etkin bir BT risk tanımlama, analiz ve raporlama mekanizmasının kurulması için risk verileri tanımlanır ve toplanır.				
#	Denetim prosedürleri	T/İ	Z/O	
K1.1	Farklı BT risk kategorileri ve risk faktörleri de dâhil olmak üzere BT riskleri ile ilgili verilerin toplanması, sınıflandırılması ve analiz edilmesi için bir metodun geliştirilmiş ve verilerin işleme yönteminin belirlenmiş olduğu kontrol edilir.	T	Z	
K1.2	Kurumun iç ve dış çalışma ortamı ile ilgili BT risk yönetimi verilerinin kayıt altına alınarak analiz edilmesi ve geçmişe yönelik olarak saklanması için tanımlı bir sürecin varlığı gözlemlenir.	T	Z	
K1.3	Kurum tarafından incelenen risk verileri ve tespit edilen eğilimler değerlendirilirken benzer kurum ve kuruluşlardaki en iyi örneklerden faydalandığı gözlemlenir.	İ	O	
K1.4	BT hizmetlerine, projelerine ve operasyonlarına etkisi olabilecek risk olaylarının kayıt altına alındığı ve incelendiği kontrol edilir.	İ	Z	
K1.5	Benzer tip olaylar sonucunda toplanan risk verilerinin organize bir şekilde tutulduğu ve olaya sebebiyet veren etmenlerin saptandığı gözlemlenir. Farklı olaylara sebep olan ortak etmenlerin de Kurum tarafından belirlendiği teyit edilir.	İ	O	
K1.6	Risk olayları oluştuğunda, hangi koşulların mevcut olduğunun ya da hangilerinin bulunmadığının Kurum tarafından kayıt altına alınmış olduğu ve olayın gerçekleşme sıklığı ile zarar büyüklüğünün saptandığı ve belirlendiği kontrol edilir.	İ	O	
K1.7	Yeni veya ortaya çıkmak üzere olan risk konularının tespit edilmesi için, olay ve risk etmenlerinin periyodik olarak Kurum tarafından analiz edildiği denetlenir.	İ	O	

K2 - İş hedeflerine olan etkileri göz önüne alınarak riskler üzerinde verilecek kararları destekleyecek bilgiler toplanır. Bu doğrultuda tanımlanan tüm risklerin etkisi nicel ve nitel yöntemler kullanılarak belirlenir.

#	Denetim prosedürleri	T/İ	Z/O
K2.1	Tüm risk faktörleri ve varlıkların iş süreçleri açısından kritikliği değerlendirilerek risk analizi için harcanacak eforun kapsamının ve derinliğinin tanımlanmış olduğu kontrol edilir. Risk değerlendirmesi kapsamının maliyet-fayda analizine dayandırılmış olduğu değerlendirilir.	T	Z
K2.2	BT risk senaryolarının geliştirilip düzenli aralıklarla güncellendiği denetlenir. Bunun için senaryolar talep edilir ve incelenir, kurumun içinde bulunduğu mevcut koşullara ve şartlara uygun senaryolar olduğu değerlendirilir.	İ	Z
K2.3	Risk senaryolarının gerçekleşme olasılıklarının hesaplandığı, risklerin sebep olacağı etkilerin istatistiksel olarak değerlendirildiği ve artık risk seviyelerinin tahminlendiği gözlemlenir.	İ	Z
K2.4	Artık risklerin kurumun risk toleransı ile karşılaştırıldığı ve aksiyon alınması gereken risklerin belirlendiği gözlemlenir.	İ	Z
K2.5	BT risk senaryoları ile ilgili olası kayıp ya da kazançların ve tahmin edilen gerçekleşme olasılığının tanımlandığı kontrol edilir.	İ	O
K2.6	Riskten korunma, risk azaltma ve hafifletme, riski transfer etme veya riski paylaşma gibi potansiyel risk yanıt seçenekleri için fayda maliyet analizlerinin gerçekleştirilmiş olduğu kontrol edilir. Bu analizlere uygun olarak (en uygun fayda maliyet oranına sahip) bir risk yanıtının belirlenmiş olduğu gözlemlenir.	İ	Z
K2.7	Tanımlanan risklere yanıt vermek için uygulanacak olan proje ve programlar için üst seviye gereksinimlerin tanımlanmış olduğu kontrol edilir. Risk azaltma amacıyla uygulanacak anahtar kontroller için gereksinim ve beklentilerin tanımlandığı gözlemlenir.	İ	O
K2.8	Risk analizi sonuçlarının kurumsal gereksinimler ile uyumlu olduğu ve kararlar alınmadan önce onaylandığı kontrol edilir.	İ	Z

K3 - Potansiyel etki, risk nitelikleri, risk yanıtları ve öngörülen gerçekleşme sıklığı gibi bilgileri içeren bir envanter oluşturularak kaynaklar, yetkinlikler ve mevcut kontrol aktiviteleri kayıt altına alınır

#	Denetim prosedürleri	T/İ	Z/O
K3.1	Kurum bünyesinde personel, uygulamalar, altyapın, tesisler, kritik manüel kayıtlar, dış firmalar ve tedarikçilerin dahil olduğu bir iş süreçleri envanterinin hazırlanmış olduğu ve bu iş süreçlerinin BT hizmetlerine ve BT altyapı kaynakları ile olan ilişkilerinin ve bunlara olan bağımlılıklarının belgelendirildiği gözlemlenir	İ	Z
K3.2	BT hizmetlerinin ve BT altyapı kaynaklarının hangi iş süreçleri operasyonların sürdürülmesi için kritik olduğunun tanımlanmış olduğu kontrol edilir. Bu bağımlılıkların analiz edildiği ve risklerin belirlendiği gözlemlenir.	İ	Z
K3.3	Risk profil bilgilerinin düzenli olarak tutulduğu ve risk profili kapsamında kurum risklerine entegre bir şekilde ele alındığı kontrol edilir.	İ	O
K3.4	Risk profillerine göre, risk göstergelerinin tanımlandığı ve mevcut risk ve risk trendlerinin belirlendiği ve izlendiği kontrol edilir	İ	Z
K3.5	Gerçekleşen riskler ile ilgili bilgilerin tutulduğu ve kurumun BT risk profiline dahil edildiği kontrol edilir.	İ	Z
K3.6	Risk aksiyon planının belgelendiği ve kurum BT risk profiline dahil edildiği kontrol edilir.	İ	Z

K4 - Maruz kalınan BT risklerinin mevcut durumu ve fırsatlar ile ilgili bilgiler, paydaşlar ile zamanında paylaşılır.			
#	Denetim prosedürleri	T/i	Z/O
K4.1	Risk analizi sonuçlarının etkilenen tüm paydaşlara raporlanmış olduğu gözlemlenir. Bu raporlamaların risklerin gerçekleşme ihtimalleri, oluşabilecek olası kayıp ya da kazanç aralıklarını ve güven seviyelerini içerdiği gözlemlenir.	İ	Z
K4.2	Yasal ve düzenleyici hususlar, zorunluluklar, itibar, durum tespitleri ve en kötü ve en olası senaryolar da göz önünde bulundurularak karar alındığı gözlemlenir.	İ	O
K4.3	Risk yönetim sürecinin etkinliği, kontrollerin etkinliği, eksikler, uyumsuzluklar, fazlalıklar, iyileştirme durumu ve bunların risk profiline etkisi de dâhil olmak üzere mevcut risk profiline tüm paydaşlara iletilmiş olduğu kontrol edilir.	İ	Z
K4.4	Üçüncü taraf değerlendirmeleri, iç denetim ve kalite güvence gözden geçirmelerinin incelenmiş olduğu ve risk profili ile eşleştirilmiş olduğu kontrol edilir. Ek bir risk analizi ihtiyacını belirlemek için tanımlanan eksiklerin ve maruz kalınan risklerin gözden geçirildiği denetlenir.	İ	Z
K4.5	Risk içeren alanlar için düzenli olarak, daha büyük risk kabulünü sağlayacak ve daha çok getiri getirecek BT ile ilgili fırsatların belirlendiği gözlemlenir.	İ	Z

K5 - Kurum tarafından riskleri kabul edilebilir bir seviyeye indirebilmek için olanaklar etkin bir şekilde yönetilir.

#	Denetim prosedürleri	T/i	Z/O
K5.1	Risklere karşı belirlenmiş kontrol aktivitelerinin ve bu riskler karşısındaki risk toleransının belirtildiği bir envanterin kurum bünyesinde tutulduğu kontrol edilir.	İ	Z
K5.2	Riskleri yönetmek için uygulanan kontrol aktivitelerinin sınıflandırıldığı ve BT risk bileşenlerine eşlendiği gözlemlenir.	İ	Z
K5.3	Her bir birimin risklerini izlediği ve bu risklerin ve olası etkilerinin farkında olarak faaliyetlerini sürdürme sorumluluğunu kabul etmiş oldukları gözlemlenir.	İ	O

TASLAK

K6 - Uygun maliyetli kontroller ile risklerin etkilerini azaltmak üzere tasarlanmış bir risk tedavi süreci oluşturulur.

#	Denetim prosedürleri	T/İ	Z/O
K6.1	Bir riskin, ciddi bir iş etkisi ile birlikte önemli bir operasyonel olaya neden olduğunda atılması gereken belirli adımların dokümanite edildiği ve test planlarının hazırlanmış olduğu kontrol edilir.	T	Z
K6.2	Gerçekleşen risklerin ardından hazırlanan belgeler incelenir ve gerçekleşen risklerin kategorize edildiği ve riskin etkisi ile risk toleransı eşiklerinin karşılaştırıldığı kontrol edilir. Gerçekleşen risklerin iş süreçlerine olan etkilerinin karar verici mercilere bildirildiği ve risk profilinin düzenli olarak güncellendiği kontrol edilir.	T	Z
K6.3	Denetim döneminde gerçekleşmiş olan tanımlı riskler remin edilir. Olaylar meydana geldiğinde, etkiyi en aza indirmek için uygun müdahale planının uygulandığı denetlenir.	İ	Z
K6.4	Geçmiş dönemlerde gerçekleşen risklerin, kayıpların ve kaçırılan fırsatların incelendiği ve kök nedenlerin belirlendiği kontrol edilir. Risklere verilecek ek yanıt ihtiyaçları ve süreç iyileştirmelerine ek olarak riskin gerçekleşmesine sebep olan kök nedenlerin ilgili karar vericilere bildirildiği gözlemlenir ve bunların risk yönetim süreçlerine dahil edildiği kontrol edilir.	T	Z

Ek Kaynaklar

- ISACA. (2007). COBIT 4.1 Framework – PO9. Rolling Meadows, Illinois, United States of America.
- ISACA. (2012). COBIT 5 Enabling Processes – APO12, Rolling Meadows, Illinois, United States of America.
- ISO/IEC 27001, Information Security Management Systems – Requirements, Section 4 (International Organization for Standardization(ISO)-International Electrotechnical Commission(IEC), 2005)
- ISO/IEC 27002, 4 Risk Assessment and Treatment (International Organization for Standardization(ISO)-International Electrotechnical Commission(IEC), 2005)

5. UYGULAMA KONTROLLERİNİN DENETİMİ

5.1. Uygulama kontrolleri

Uygulama kontrollerine ilişkin tanım, diğer kontrol türleriyle olan ilişkisi ve diğer hususlar, rehberin ikinci bölümünde verilmiştir. Temel itibarıyla süreçler üzerinde bilgi sistemleri tarafından desteklenen otomatik ve yarı otomatik bir şekilde tasarlanabilecek uygulama kontrollerinin belirlenen kapsam ve gerçekleştirilen risk değerlendirmelerine istinaden denetlenmesi gerekebilecektir. Uygulama kontrolleri iş faaliyetleri sırasında işlenen verilerin ilgili bilgi sistemine girişinden çıkışına kadar olan süre içinde tam ve doğru bir şekilde işlenmesi için tasarlanmış ve kurgulanmış kontrollerdir.

Uygulama kontrolleri aşağıdaki ana kategoriler kapsamında incelenmektedir:

Tablo 5.1 Uygulama Kontrolleri	
Uygulama kontrolü kategorileri	Örnek uygulama kontrolleri
1. Kaynak veri hazırlığı ve yetkilendirme	
	Kaynak belgelerin tasarımı, verilerin doğru bir şekilde kaydedilmesi, akışın kontrol edilebilmesi ve referans kontrollerine izin verecek şekilde yapılır.
	Kaynak veri hazırlığı için prosedürler hazırlanır ve ilgili personele duyurulur. Söz konusu prosedürler kaynak belgelerin girilmesi, düzeltilmesi, yetkilendirilmesi ile kabul ya da reddedilmesi konularını içerirler. Buna ilave olarak kaynak verilerin hangi medya ortamında kabul edilebileceği belirtilir.
	Uygulamalara kaynak veri girişinden sorumlu personelin güncel bir listesi tutulur, gerekli yönetim kademeleri tarafından onaylanır ve personel değişiklikleri oldukça güncellenir.
	Tüm kaynak belge tipleri standart bir içerikte ve formatta hazırlanır, onaylanır ve değişiklik gerektiğinde güncellenir.
	Uygulama üzerinde gerçekleşen tüm işlemlere otomatik olarak eşsiz ve ardışık işlem numaraları

Tablo 5.1 Uygulama Kontrolleri	
	atanır.
	Eksik, hatalı ya da onaylanmamış kaynak belgelerin sisteme girişi yapılmaz ve düzeltme için iade edilir.
2. Kaynak Verilerin Toplanması ve Girilmesi	
	Kaynak belgelerin zamanlılığı (ör: doğru döneme ait olmaları), tamlığı ve doğruluğunun tespit edilebilmesi adına kriterler belirlenir ve veri girişleri bu doğrultuda yapılır.
	Uygulamalara kaynak veri girişinden sorumlu personelin güncel bir listesi tutulur, gerekli yönetim kademeleri tarafından onaylanır ve personel değişiklikleri oldukça güncellenir.
	Kaynak veri girişleri sırasında karşılaşılan hataların tespit edilebilmesi, göz ardı edilmesi, çözülmesi, onaylanması ve giderilen hata sonrasında girişinin yapılması için gerekli prosedürler hazırlanır. Karşılaşılan tüm hatalar kayıt altına alınır, gözden geçirilir ve gerekli yönetim kademelerine raporlanır. Hata alınan bir kaynak veri girişinin alınan hataya rağmen uygulamaya girişi engellenir.
	Kaynak verileri içeren belgeler gerekli yasal gereksinimler de göz önünde bulundurularak ve uygun güvenlik önlemleriyle korunarak saklanır.
3. Doğruluk, Tamlık ve Orijinallik Kontrolleri	
•	Kaynak veri girişi sırasında verinin doğruluğu, tamlığı (ilgili tüm kayıtları içerdiği) ve orijinalligi kontrol edilir. Uygulamanın tespit edilen hatalar için anlamlı mesajlar üretmesi sağlanır. Veri girişi sırasında bunlara ek olarak varsa mevzuat gereği yapılması gereken kontroller de göz önünde bulundurulur.
•	Uygulamalara kaynak veri girişinden sorumlu personelin güncel bir listesi tutulur, gerekli yönetim kademeleri tarafından onaylanır ve

Tablo 5.1 Uygulama Kontrolleri	
	personel değişiklikleri oldukça güncellenir.
•	Kaynak veri girişi, düzeltme ve onaylama aşamalarının tek bir kişi tarafından yapılmasının sakıncalı olarak değerlendirildiği durumlar için gerekli görevler ayrılığı kontrolleri uygulamalar içine eklenir, söz konusu görevler ayrılığının sistemsal olarak sağlanamadığı durumlarda risk azaltıcı ek izleme ve gözden geçirme çalışmaları
•	Kaynak veri doğrulamalarına ilişkin hata üreten veri giriş işlemleri ayrı bir şekilde takip edilir, çözülür ve raporlanır. Uygulamalar üzerinde bu tür hataların tüm kaynak veri giriş işlemlerini durdurmasını engelleyecek önlemler alınır.
4. Veri İşleme Bütünlüğü ve Doğrulaması	
•	Veri işlemenin yalnız onaylanmış uygulama ve araçlar üzerinde yapılabildiğinden emin olunması için gerekli önlemler tesis edilir ve uygulanır.
•	Veri işleme sürecinde gerekli noktalarda otomatik kontroller vasıtası ile işlenen verinin tam ve doğru olarak işlendiği kontrol edilir. Söz konusu kontroller işlem numaralarının ardışıklığının, mükerrer kayıtların oluşup oluşmadığının kontrol edilmesi gibi hususları içerir.
•	Veri işleme sırasında karşılaşılan hatalara ilişkin uygulama tarafından anlamlı mesajlar üretilmesi için gerekli önlemler alınır, hatalar zamanında takip edilir, çözülür ve raporlanır.
•	Kurum tarafından özellikle kritik olarak belirlenmiş tüm işlemlerin başlangıç saati, kim tarafından başlatıldığı, ne kadar sürdüğü vb. gibi detayları kayıt altına alınır ve güvenli bir şekilde saklanır.
•	İşlemlerin doğruluğu ve tamlığının kontrol edilebilmesi adına işlemin başlangıcı ve tamamlanması ile ilgili kayıtlar ya da işlemin

Tablo 5.1 Uygulama Kontrolleri	
	başladığı ve tamamlandığı sistemler arasında mutabakat kontrolleri tasarlanır ve uygulanır. Mutabakat kontrollerinin otomatik olmadığı durumlarda yürütülen manuel çalışmalar incelenir.
•	İşlemlerin elektronik olarak farklı ortamlar arasında gerçekleştirildiği durumlarda, ilgili iletişimin ve karşılıklı doğrulamaların standart bir şekilde yapılabilmesi için üzerinde önceden belirlenmiş kurallar tesis edilir, bu farklı ortamları yöneten birimlere iletilir ve ilgili uygulamalar üzerinde uygulanır.
5. Çıktı Kontrolü, Mutabakatı ve Hata Yönetimi	
•	Uygun olduğu durumlarda düzenli olarak alınan çıktı verilerin, belgelerin ya da sonuçların ilgili envanterle mutabakatı yapılır. Bununla ilgili tüm hata ve istisnalar ile bunlara ilişkin çözümler kayıt altına alınır ve çözülür.
•	Uygulamalar tarafından üretilen çıktılara ilişkin dip toplam, veri boyutu, veri içeriği vb. bileşenler kullanılarak kaynak verilerle karşılaştırması yapılır. Karşılaştırma sonucunda istisna ve hataların tespit edildiği durumlarda çözüme yönelik aksiyonlar yürütülür ve kayıt altına alınır. Bu tür karşılaştırma ve hata çözme çalışmaları, çıktı veriyi ya da belgeyi girdi olarak kullanacak başka bir sürecin ya da işlemin başlamasından önce tamamlanır.
•	Uygulamalar vasıtası ile üretilen çıktıların gizli, kritik ve/veya hassas bilgiler içerdiği durumlarda söz konusu çıktılara erişebilecek personel önceden belirlenir, uygun yönetim kademeleri tarafından onaylanır.

5.2

Uygulama kontrolleri doğası gereği her kurum ve kuruluşta ilgili faaliyet alanına ve bilgi sistemlerinin karmaşıklık yapısına göre farklılık göstermektedir. Uygulama kontrollerinin denetimi ancak, söz konusu faaliyetlerin, bilgi sistemleri üzerinde nasıl ve hangi koşullarda desteklediğinin net bir şekilde anlaşılması

ve ilgili faaliyet ve süreçler üzerinde tasarlanmış olan kontrollerin tespit edilmesi sonrasında mümkün olabilecektir.

Kontrollerin tasarımı, işletimi ve üretilen çıktılar her kurumda ciddi şekilde farklılaşabildiğinden, bunlara ilişkin standart bir liste ya da denetim adımı oluşturmak mümkün olmayabilir. Uygulanacak en doğru yaklaşım, bu tür bir denetim faaliyeti gereken durumlarda, daha önce bu tür çalışmalarda bulunmuş tecrübeli bir denetçi eşliğinde bu çalışmaların yürütülmesi olacaktır.

Uygulama kontrollerinin denetiminin kullanım alanlarından en yaygın olanlardan biri de veri analizi olarak ortaya çıkmaktadır. Özellikle mali denetimler başta olmak üzere belirli bir hacmin üzerinde bir veri yığını ile çalışılmak durumunda kalındığında, bazı araçlar ve teknikler de kullanarak (ör: MS Excel, MS Access, ACL, SQL) ilgili veri yığınları içinde aranan sonuca ulaşmak üzere analizler tasarlanabilir, söz konusu analizler rutin bir şekilde belirli aralıklarla yürütülecekse bunlara ilişkin sorgular hazır hale getirilebilir ve hatta bu veri yığınları içinde usulsüzlük ya da sahtekarlık vakalarına dair izler aranabilir. Uygulama kontrolü olarak yürütülebilecek veri analizlerine bazı örnekler şu şekilde sıralanabilir:

- Muhasebe bilgi sistemi üzerinde kesilmiş olan muhasebe fişlerinin ardışık numara alıp almadığının analizi
- Yine muhasebe fişleri üzerinde belirli kriterlere sahip fişlerin analiz edilmesi (ör: birbiri ile karşılıklı çalışmaması gereken hesapların tespit edilmesi, fiş kesmeye yetkili olmayan personel tarafından kesilen fişlerin ortaya çıkarılması, ayın ya da yılın belirli dönemlerinde rutin olarak kesilen ve belirli bir tutarın üzerinde kesilen fişler, açıklama girilmeden kesilmiş fişler, geriye dönük kesilen fişler, vb.)
- Kurum ya da kuruluşun ticari borç ya da alacaklarına ilişkin yaşlandırma analizleri
- Kurum ya da kuruluşun envanteri üzerindeki hareketlerin değerlendirilmesi
- Belirli bir fonksiyona ve işleme erişim yetkisine sahip olan kişi ve grupların ortaya çıkarılması
- Bilsisistemleri üzerinde gerçekleştirilen işlemlere ait denetim izleri (log) üzerinden bu işlemlerin doğruluğu ve geçerliliklerinin analiz edilmesi

5.2. Uygulama kontrolleri – BT genel kontrolleri ilişkisi

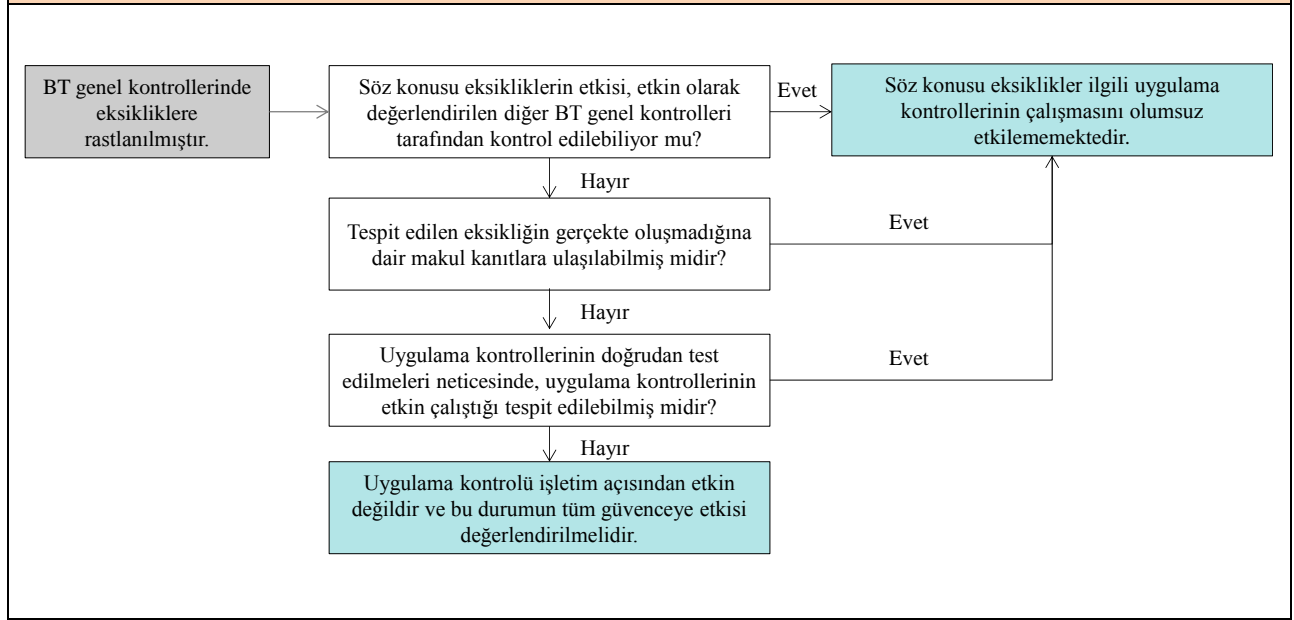
Rehberin ikinci bölümünde kontrol tiplerinin birbirleriyle olan ilişkisi verilmiştir. Buna ilave olarak uygulama kontrollerinin denetimi sırasında ele alınması gereken konulardan biri, söz konusu uygulamalar üzerinde BT genel kontrollerinin etkinlik durumudur.

BT genel kontrolleri ilgili uygulamalar üzerinde tanımlı ve ayarlanmış olan uygulama kontrollerinin tasarlandığı şekilde ve etkin bir biçimde çalışması için kritik bir rol oynamaktadır. Buna örnek olarak BT genel kontrollerinin değerlendirilmesi sırasında bir iş uygulaması üzerinde etkin olmayan yetkilendirme kontrollerinin bulunmasının, söz konusu uygulama üzerinde veri işlemeye doğrudan etki edebilecek parametrelerin kimler ve hangi koşullar altında değiştirilebileceğine dair alınacak güvenceyi olumsuz olarak etkilemesi verilebilir.

Yukarıda belirtilen örnekte olduğu gibi özellikle etkin olmayan BT genel kontrollerinin uygulama kontrolleri üzerine etkisinin değerlendirilmesi kalan denetim çalışmalarının seyri, içeriği ve detay seviyesi hakkında planların değiştirilip değiştirilmemesi açısından önem arz etmektedir. Şöyle ki, etkin bir genel BT kontrol ortamı sunmayan kurumlarda yürütülen uygulama kontrolleri denetim çalışmalarından makul bir güvence alabilmek adına bir takım ek çalışmaların yürütülmesi gerekebilecektir. Söz konusu çalışmalar sınırlı olmamak adına şunları içerebilir:

- BT genel kontrol ortamının etkinliğinin olumsuz olarak değerlendirilmesine yol açan hususların etkilerin azaltılması için kurum çapında yürütülmesi gereken ek detay analizler (ör: tüm mali işlemlerin analizi, BT bileşenleri üzerindeki işlemlerin analizi, vb.)
- Etkin bir BT genel kontrol ortamı olması durumunda uygulama kontrollerinin denetim döneminden tek bir örneklem üzerinden denetlenebilmesinin aksine, uygulama kontrolünün denetimi için seçilecek örneklemin, örneklem yöntemine uygun olacak şekilde hacminin artırılması, ilgili otomatik kontroller sanki manuel birer kontrolmüş gibi denetim testlerine tabi tutulması (uygulama kontrolünün doğrudan test edilmesi)
- Uygulama kontrolü denetim sonuçlarına makul bir güvence verilememesi sebebiyle denetimin diğer alanlarına (ör: mali kayıtların denetimi) ağırlık verilmesi, kaynak ve çıktı verilerinin ve belgelerinin ek doğrulama çalışmalarına tabi tutulması

Bu anlamda etkin olmayan bir genel BT kontrol ortamının mevcut olduğu bir kurum bünyesinde uygulama kontrollerine ilişkin denetim çalışmalarının belirlenmesi amacıyla aşağıdaki karar ağacı oluşturulmuş olup, denetçi bu karar ağacındaki yönlendirmeler uyarınca denetim çalışmalarını revize etmelidir.

Şekil 5.1 – Genel BT Kontrollerindeki Eksikliklerin Uygulama Kontrollerine Etkisinin Değerlendirmesi

6. BT ALTYAPI GENEL KONTROLLERİ

- 6.1. Kapsam Deęerlendirilmesine İlişkin Esaslar
- 6.2. İşletim Sistemleri
- 6.3. Veritabanı Sistemleri
- 6.4. Ağ Sistemleri
- 6.5. Uzaktan erişim

6.1. İŐLETİM SİSTEMLERİ

6.1.1. Solaris (Unix) İŐletim Sistemleri

Risk – Kontrol EŐleŐmeleri

Riskler	K1	K2	K3	K4
R1. Bilgi sistemleri üzerinde otomatik olarak tanımlanan varsayılan kullanıcılar kullanılarak diđer kullanıcıların yetkilerinin artırılması	+			
R2. Bilgi sistemleri üzerinde kritik veri, bilgi ve cihazlara yetkisiz erişimlerin gözlemlenmesi	+	+	+	+
R3. Güvenlik ve şifre parametrelerinin, yetkisiz erişimleri önleyecek şekilde atanmaması	+		+	+
R4. Yetkisiz erişim girişimlerinin yönetim tarafından fark edilememesi	+	+	+	+
R5. Kritik dosya ve kaynakların bilinçli ya da farkında olmadan deđiŐtirilmesi		+	+	

Kontroller

K1 - Kullanıcı Hesap Yönetimi ve Şifreler

Bilgi sistemleri üzerinde tanımlı, cihazların fabrika çıkışı ya da sistemlerin ve yazılımların ilk kurulumu sonrası otomatik olarak oluşturulan kullanıcı ve sistem hesapları bulunur. Benzer şekilde, bu hesaplara ait kullanıcı şifresi gibi güvenlik parametreleri de başlangıta sabit deęerlere tanımlanmıştır. Bu gibi kullanıcı hesaplarına varsayılan (*default*) kullanıcı hesapları denir.

Bilgi sistemleri üzerindeki varsayılan kullanıcı hesap şifreleri genellikle bilindiğinden ya da kolay tahmin edilebilir olduğundan, sistem kurulumu sonrası deęiştirilir. Ek olarak, varsayılan kullanıcı hesapları hizmet dışı kalacak şekilde yetkileri kaldırılır. Bu sayede, tüm kullanıcı işlemleri; inkâr edilemezlik ve sorumluluk atama ilkesine göre kaydedilir. Bu ilkeye göre bilgi sistemleri üzerinde yapılan kritik işlemlerin benzersiz kullanıcı hesapları bazında denetim izleri saklanabilir.

Unix sistemlerinde “*sistem*” ve “*kullanıcı*” olmak üzere iki tip varsayılan kullanıcı profili bulunmaktadır. Varsayılan sistem hesapları, normal kullanıcı hesaplarının erişimine kapalı olan çeşitli sistem süreçlerinde ve dięer sistem dosyaları üzerinde sahiplik oluşturmak için kullanılmaktadır. Varsayılan normal kullanıcılar ise UNIX işletim sistemi kurulumunu takiben sisteme erişimlerin gerçekleştirilebilmesi amacıyla otomatik olarak tanımlanmaktadır. UNIX sistemlerde kullanıcı hesap yönetiminde sistem dizini olan *etc* dizini altındaki *passwd* and *shadow* olmak üzere iki tip dosya kullanılmaktadır.

- *passwd* dosyası sistem hesaplarının bir listesini tutmaktadır. Kullanıcı kimliği, grup kimliği, ev dizini, kabuk (shell) ve benzeri bilgileri göstermektedir.
- *shadow* dosyası kullanıcı hesaplarının şifreli (kriptolu) parola bilgilerini ve isteğe baęlı olarak kullanıcı hesabının sona erme süresine ilişkin bilgilerini içermektedir.

etc/passwd dosyasının içeriğindeki kayıtlar aşağıdaki formatta gösterildiği şekilde saklanır:

Örnek kayıt:

```
myilmaz:x:210:15000:MehmetYılmaz:/home/users/myilmaz:/usr/bin/ksh
```

myilmaz: kullanıcı adı

x: kullanıcı şifresi – şifreli (kriptolu) saklandığı durumlarda ”x” işareti ile belirtilir ve *etc/shadow* dosyasında saklıdır.

210: kullanıcı kimlik numarası

15000: kullanıcının üyesi olduğu birincil grup numarası

Mehmet Yılmaz: kullanıcı bilgileri

/home/users/myilmaz: kullanıcının sistem girişi sonrasında baęlandığı kök dizin

/usr/bin/ksh: kullanıcı komut satırı (shell) programı tipi

etc/shadow dosyasının içeriğindeki kayıtlar aşağıdaki formatta gösterildiği şekilde saklanır. Bu dosya içerisinde kullanıcı şifresi belli kriptolama algoritmalarıyla (MD5, DES, DES5 vb.) işlenerek kriptolu (*hashed*) şekilde saklanır.

Örnek kayıt:

myilmaz:51X3vWqgK0BDw:15453:0:99999:3:x:y:z

myilmaz: kullanıcı adı

51X3vWqgK0BDw: kriptolu kullanıcı şifresi (*hashed password*)

15453: kullanıcı şifresinin en son deęiştirildiğinden beri geçen gün sayısı (1 Ocak 1970 tarihinden itibaren)

0: şifrenin deęiştirilmeden önce kullanılması gereken minimum gün sayısı

99999: şifrenin kullanılabilmesi maksimum gün sayısı

3: geçerliliğini doldurmak üzere olan şifre için ne kadar gün öncesinden uyarı verileceğini gösteren deęer

x: şifrenin geçerliliği dolduktan sonra kaç gün içerisinde kullanıcı hesabının pasif hale getirileceğini gösterir deęer

y: kullanıcı hesabının pasif hale gelmesi için kalan gün sayısı

z: bu parametre alanı kullanılmaz, özel kullanım amaçlarına karşı rezerve edilmiştir

Denetim Prosedürleri

#	Denetim prosedürleri	T/i	Z/O
K1.1	BT güvelliğine ilişkin prosedür temin edilerek prosedürde yayımlanan UNIX sistem güvenliğine ilişkin standartların, sektörde kabul gören en iyi uygulamalara yönelik yapılandırıldığı gözlemlenir.	T	Z
K1.2	etc/passwd dosyası temin edilerek içeriğindeki kullanıcı adlarından sonra gelen alanda “x” işaretlinin varlığı gözlemlenir. Bu bağlamda tüm kullanıcı şifrelerinin/parolalarının şifreli (kriptolu) bir şekilde saklandığı teyit edilir.	İ	Z
K1.3	etc/passwd and etc/shadow dosyaları temin edilip içeriğindeki aktif kullanıcı hesapları tespit edilir*. Aktif kullanıcı hesapları arasından denetim dönemi içerisinde yaratılan kullanıcı hesapları içerisinde örneklem yöntemiyle seçilen kullanıcılar için kullanıcı yetki talep ve onay dokümanları sorgulanarak resmi prosedürün uygulandığı teyit edilir. * Aktif olmayan kullanıcı hesapları, kullanıcı ismini takiben “LK” (locked) ya da “NP” (No Password) parametrelerine sahiptir. (Ör: “listen:*LK*:::::” ya da “nobody:NP:6445:::::”)	İ	Z
K1.4	Varsayılan kullanıcı hesapları (Ör: admin, guest, kullanıcı1, yönetici vb.) gözden geçirilir ve kritik yetkilerin sadece olması gereken kullanıcılara atandığı kontrol edilir. Varsayılan hesaplar aktif halde ise ilgili hesapların varsayılan şifrelerinin, kurumun bilgi güvenliği politikalarına uygun olarak deęiştirildiğinden emin olunmalıdır.	İ	Z
K1.5	Kullanıcı kayıtlarında, UNIX sistemlerde en yüksek yetkili kullanıcı olan “root” kullanıcısı hariç dięer kullanıcıların kimlik ve grup numaralarının 0 (sıfır) olarak atanmadığı teyit edilir.	İ	Z

TASLAK

Umask değeri

“Umask” değeri UNIX ve Linux sistemleri üzerinde yaratılan her yeni dosya için varsayılan olarak atanan erişim yetkilerini belirler. Bu yetkiler “Umask” değeri olarak adlandırılır. “Umask” değerleri üç haneli rakamlardan oluşur; ilk hane dosya sahibinin, ikinci hane dosya sahibinin üye olduğu gruptaki kullanıcıların, son değer ise önceki iki tanıma uymayan tüm kullanıcıların yetkilerini belirlemek için kullanılır. Genel UNIX yetkilerinden farklı olarak, bu değerlerin karşılıkları mantıksal olarak ters çevrilerek (negate) ifade edilir.

Umask değeri için belirlenmesi gereken değeri hesaplamak için; atanması istenen erişim yetkisi değeri dizinler için 777’den, dosyalar için ise 666’dan çıkartılır. Kalan değer “Umask” değerini belirler.

Örnek olarak, bir UNIX sistem üzerinde varsayılan olarak bir kullanıcının yarattığı dizinlere ilişkin;

- kullanıcının kendisinin *okuma, yazma ve çalıştırma* (7),
- kullanıcının ait olduğu grubun *okuma* (4),
- diğer bütün kullanıcıların ise sadece *okuma* (4) yetkisinin olması isteniyor.

Bu durumda sistem üzerinde atanması gereken “Umask” değeri 777 değerinden 744 değeri çıkartılarak elde edilen 033 değeridir.

033 olarak tanımlanan “Umask” değeri sonrasında yeni yaratılan /test/deneme klasörüne ait yetkiler aşağıdaki şekilde görüntülenebilir:

```
-rwxr--r-- 1 root sys 5309 May 15 09:28 /test/deneme
```

“Umask” değeri için atanan değerlere ilişkin yetkiler sağdaki tabloda gösterilmiştir.

Değer	Açıklama	UNIX kodlaması
0	okuma, yazma, çalıştırma	rwx
1	okuma, yazma	rw-
2	okuma, çalıştırma	r-x
3	okuma	r--
4	çalıştırma, okuma	r-x
5	yazma	-w-
6	çalıştırma	--x
7	erişim izni mevcut değil	---

Denetim Prosedürleri

#	Denetim prosedürleri	T/i	Z/O
K2.1	BT güvenliğine ilişkin prosedür temin edilerek prosedürde yayımlanan UNIX sistem güvenliğine ilişkin standartlar incelenir.	T	Z
K2.2	Komut satırı (shell) aracılığı ile /etc dizininde “ls -l” komutu çalıştırılarak dizin içerisinde yer alan passwd, group ve shadow dosyalarına ait erişim yetkileri incelenir.	İ	Z
K2.3	passwd ve group dosyası için erişimlerin '-rw -r- -r- -' şeklinde; tek kullanıcının yazma ve okuma yetkisi, diğer kullanıcıların ise yalnızca okuma yetkisi olacak şekilde atandığı gözlenir.	İ	Z
K2.4	shadow dosyası için erişimlerin '-rw - - - - - - -' ya da '-r- - - - - - - - -' tek kullanıcının yazma ve/veya okuma yetkisi, diğer kullanıcıların ise yalnızca okuma yetkisi olacak şekilde atandığı gözlemlenir.	İ	Z
K2.5	/etc/default/login dosyası temin edilerek içeriğinde ‘CONSOLE = /dev/console’ parametresinin aktif durumda olduğu teyit edilir. Bahsi geçen parametre uzak bağlantı aracılığıyla direkt olarak “root” hesabı ile sisteme giriş yapılmasını kısıtlar. Uzaktan bağlanacak kullanıcı hesapları, “root” hesabına ancak “su” komutu ile erişebilir. “su” komutu ile hesaplar arası yapılan geçişler /usr/bin/cat /var/adm/sulog doyasında saklanır.	İ	Z

K3 - Şifre ve Güvenlik Parametreleri

Bilgi sistemleri üzerinde tanımlı güvenlik ve şifre parametreleri, yetkisiz erişimleri önleyecek şekilde yapılandırılmıştır.

UNIX sistemlerde oturum açma aşamasında veya oturumlar arası bir kullanıcıdan başka bir kullanıcıya geçilirken, ilgili kullanıcının kullanıcı adı ve şifresi girilerek yetki sorgusu yapılabilir. Buna paralel olarak, kullanıcılar, şifrelerini belli kısıtlamalar çerçevesinde yaratabilir ya da değiştirebilirler. Bu kısıtları sistem üzerinde tanımlanan güvenlik politikaları ve şifre parametreleri belirler.

Denetim Prosedürleri

#	Denetim prosedürleri	T/İ	Z/O
K3.1	Sistem üzerinde <code>/etc/default/login</code> dosyası içeriği temin edilir. Temin edilen dosya içeriğinde <code>PASSREQ</code> parametresinin <code>YES</code> değerine atandığı (<code>PASSREQ = YES</code>) teyit edilir.* * Bu parametre, başında “#” imleci olmadığı sürece etkindir. Parametrenin başında “#” imleci mevcut ise, sisteme girişte kullanıcılar <i>kullanıcı adı</i> ya da <i>şifre</i> girmeleri için sistem tarafından zorlanmazlar. Bu parametre etkin değil ise, diğer test adımları da geçerliliğini kaybedebilir.	İ	Z
K3.2	Sistem üzerinde <code>/etc/shadow</code> dosyası içeriği temin edilir. Temin edilen dosya içeriğindeki kullanıcılara ait dizideki 3’üncü parametre gözlemlenir. İlgili parametre 1 Ocak 1970 tarihinden itibaren saniye cinsinden, kullanıcı hesabına ait şifrenin hangi tarihte değiştiğini gösterir. Yeni yaratılan kullanıcılar için bu parametrenin 0 (Sıfır) değerine atandığı gözlemlenerek, kullanıcıların sisteme ilk girişlerinde şifrelerini değiştirmeye zorlandıkları teyit edilir.	İ	Z
K3.3	Sistem üzerinde <code>/etc/default/login</code> dosyasının içeriği temin edilir. Temin edilen dosya içeriğinde; <ul style="list-style-type: none"> Aktif olmayan oturumların kaç saniye sonra kilitlenmesi gerektiğini belirleyen <code>TIMEOUT</code> parametresinin 3600 (60 dakika) değerinden daha düşük bir değere atandığı teyit edilir. Sistem üzerinde bir kullanıcı hesabının kaç hatalı giriş denemesi sonrası kilitleneceğini belirleyen <code>RETRIES</code> parametresinin uygun değere atandığı teyit edilir. Bu parametrenin atandığı değer kadar hatalı giriş denemesi olduğunda hesap sistem tarafından otomatik olarak kilitlenir. Etkinleştirildiği takdirde varsayılan olarak 5 değerine atanmıştır. Hatalı şifre girişleri sonrası kullanıcı hesaplarının sistem tarafından kilitlendikten sonra sistemin bu kilidi kaldırma süresini belirleyen <code>DISABLETIME</code> parametresinin uygun değere atandığı teyit edilir. Etkinleştirildiği takdirde varsayılan olarak 20 değerine atanmıştır. 	İ	Z
K3.4	Sistem üzerinde <code>/etc/default/passwd</code> dosyası içeriği temin edilir. Temin edilen dosya içeriğinde;	İ	Z

	<ul style="list-style-type: none"> • Şifre uzunluğu değerinin saklandığı <code>PASSLENGTH</code> parametresinin, • Şifrede kullanılması gereken en az harf sayısını gösteren <code>MINALPHA</code> parametresinin*, • Şifre içerisinde aynı karakterin en fazla kaç defa yan yana kullanılabileceğini belirten <code>MAXREPEATS</code> parametresinin**, • Kullanıcının eski ve yeni şifresi arasındaki olması gereken minimum karakter farkı sayısının atandığı <code>MINDIFF</code> parametresinin***, • Şifre içerinde bulunması gereken en az rakam sayısını gösteren <code>MINDIGIT****</code> parametresinin**, • Şifre içerisinde bulunması gereken en az küçük harf sayısını belirten <code>MINLOWER**</code> parametresinin, • Şifre içerisinde bulunması gereken en az büyük harf sayısı <code>MINUPPER</code> parametresinin**, • Şifre içerisinde bulunması gereken en az özel karakter (%, !, +, vb.) sayısını belirten <code>MINSPECIAL****</code> parametresinin**, • Şifre içerisinde bulunması gereken en az alfa-nümerik karakter (%, !, +, vb.) sayısını belirten <code>MINNONALPHA*****</code> parametresinin*****, • Kullanıcı şifresinin kullanıcı adı ile aynı olmasını önleyen <code>NAMECHECK</code> parametresinin uygun olarak atandığı gözlemlenir. <p>* <code>MINALPHA</code> parametresi herhangi bir değere atanmamış ise varsayılan olarak 2 değeri alır.</p> <p>** parametre herhangi bir değere atanmamış ise varsayılan olarak 0 değeri alır.</p> <p>*** <code>MINDIFF</code> parametresi herhangi bir değere atanmamış ise varsayılan olarak 3 değeri alır.</p> <p>**** <code>MINNONALPHA</code> parametresi ile aynı anda kullanılamaz.</p> <p>***** <code>MINNONALPHA</code> parametresi belirtilmediği durumlarda, varsayılan değer olarak atanan 1 değeri etkindir. Ek olarak, <code>MINDIGIT</code> veya <code>MINSPECIAL</code> parametresi ile beraber kullanılamaz.</p> <p>***** <code>MINNONALPHA</code> parametresi herhangi bir değere atanmamış ise varsayılan olarak 1 değeri alır.</p>	
--	--	--

K4 - Kullanıcı Oturum Ama Giriřimlerinin Gzden Geirilmesi

Bilgi sistemleri zerindeki gvenlik nlemleri, yetkisiz eriřimleri nleyecek řekilde minimum standartları karřılamalıdır.

UNIX sistemlerde herhangi bir kullanıcı oturumu aık iken; farklı bir kullanıcı hesabı ile oturum amak iin “su” (switch user-kullanıcı deęiřtir) komutu kullanılır. Kullanıcı geiřlerini gsteren denetim izleri “sulog” dosyasında; tarih, kullanıcı adı ve kullanıcı geiř giriřim sonularının detaylarını ierecek řekilde kayıt altına alınır.

Denetim Prosedrleri

#	Denetim prosedrleri	T/i	Z/O
K4.1	<p>etc/default/su dosyası ierisindeki SULOLOG parametresinin var/adm/sulog deęerine atandıęı (SULOLOG = var/adm/sulog) incelenir.*</p> <p>/usr/bin/cat/var/adm/sulog dosyası temin edilerek “su” (switch user) komutu ile hesaplar arası gerekleřtirilen oturum geiřlerinin, kullanıcıların yetki seviyelerine uygun olarak yapıldıęı kontrol edilir.</p> <p>* Bu parametre, bařında “#” imleci olmadıęı srece etkindir. Parametrenin bařında “#” imleci mevcut ise, “su” komutu ile yapılan kullanıcı oturum deęiřikliklerinin denetim izleri kayıt altına alınmaz. Bu parametre etkin deęil ise, dięer test adımları da geerlilięini kaybedebilir.</p>	İ	O
K4.2	<p>Ařaęıdaki rnek kayıta grldę gibi, sulog dosyası ierisinde kayıt altına alınan kullanıcı oturumu geiřleri incelenir:</p> <p>SU 02/03 11:40 + pts/10 guestuser-root</p> <p>Bu rnekte guestuser kullanıcısı pts/10 terminalinden “su” komutunu kullanarak 02/03 tarihinde saat 11:40'ta system zerinde root hesabına bařarılı bir řekilde (+) geiř yaptıęı grlmektedir.</p>	İ	O
K4.3	Denetim dnemine ait kayıtlar ierisinde “root” gibi yksek yetkili hesaplara řpheli ya da yetkisiz geiřlerin varlıęı kontrol edilir.	İ	O
K4.4	<p>Ařaęıdaki komutlar alıřtırılarak sistem zerindeki denetim olaylarına iliřkin konfigrasyonların tutulduęu dosyalara sadece “root” kullanıcısının eriřebildięi teyit edilir:</p> <p>ls -l /etc/default/su ls -l /var/adm/sulog ls -l /var/adm/loginlog ls -l /etc/security/audit_class ls -l /etc/security/audit_user ls -l /etc/security/audit_control ls -l /etc/security/audit_event</p>	İ	O

K4.5	<p>Ařağıdaki komut alıřtırılarak “loginlog” dosyasını ieriğı temin edilir:</p> <p style="text-align: center;">cat /var/adm/loginlog</p> <p>Dosya ieriğinde sistem üzerinde oturum ama iřlemine iliřkin bařarısız kullanıcı giriřimlerinin kaydedildiğı gözlemlenir. İlgili personel ile görüřülerek bu olayların gözden geçirildiğine iliřkin kanıtlar temin edilir.</p>	İ	O
------	--	---	---

TASLAK

Ek Kaynaklar

- Bankacılık Düzenleme ve Denetleme Kurumu. (2010, 06 01). BANKALARDA BİLGİ SİSTEMLERİ YÖNETİMİNDE ESAS ALINACAK İLKELERE İLİŞKİN TEBLİĞ.
- Hafele, S. I.-D. (2004, February 23). Three Different Shades of Ethical Hacking: Black, White and Gray.
- International Organization for Standardization(ISO)-International Electrotechnical Commission(IEC). (2005). ISO/IEC 20000. Geneva, Switzerland, Europe.
- International Organization for Standardization(ISO)-International Electrotechnical Commission(IEC). (2005, October). ISO/IEC 27001:2005-Information Technology-Security Techniques-Information Security Management Systems-Requirements. Geneva, Switzerland, Europe.
- International Standards Organization. (2012, 05 15). Societal security – Business continuity management systems - Requirements. Geneva, Switzerland.
- ISACA. (2007). COBIT 4.1 Framework. Rolling Meadows, Illinois, United States of America.
- ISACA. (2012). COBIT 5 Enabling Processes. Rolling Meadows, Illinois, United States of America.
- Kotter, J. (1996). Leading Change. Boston, Massachusetts, USA.
- The Institute of Internal Auditors. (2008, July). Business Continuity Management. Altamonte Springs, Florida.
- The Institute of Internal Auditors. (2012, March). Global Technology Audit Guide (GTAG) 2 Change and Patch Management Controls: Critical for Organizational Success 2nd Edition.
- The Institute of Internal Auditors. (2007, November). Global Technology Audit Guide (GTAG) Identity and Access Management. Altamonte Springs, Florida, USA.
- The Institute of Internal Auditors. (2012, March). Global Technology Audit Guide (GTAG®) 1 Information Technology Risk and Controls 2nd Edition.
- The Institute of Internal Auditors. (2007, November). Identity and Access. Altamonte Springs, FL, US.
- UK Cabinet Office. (2011). ITIL Service Design. Norwich, UK.
- UK Cabinet Office. (2011). ITIL Servis Transition. Norwich, UK.
- UK Cabinet Office. (2009). Projects in Controlled Environment(PRINCE 2). Norwich, United Kingdom.

6.1.2. MS Windows İşletim Sistemleri

Riskler	K1	K2	K3
R1. Bilgi sistemleri üzerinde kritik veri, bilgi ve cihazlara yetkisiz erişimlerin gözlemlenmesi	+	+	+
R2. Bilgi sistemleri üzerinde otomatik olarak tanımlanan varsayılan kullanıcılar kullanılarak diğer kullanıcıların yetkilerinin artırılması	+		+
R3. Güvenlik ve şifre parametrelerinin, yetkisiz erişimleri önleyecek şekilde atanmaması	+		+
R4. Bilgi sistemlerine yetkisiz erişimlerin ya da erişim girişimlerinin yönetim tarafından fark edilememesi	+	+	+
R5. Kritik dosya ve kaynakların bilinçli ya da farkında olmadan değiştirilmesi	+	+	
R6. Kullanıcılar tarafından bilinçli ya da farkında olmadan bilgi sistemleri üzerinde erişim yetkisi artırma işlemlerinin gerçekleştirilmesi	+		+

- Aktif Dizin’de (Active Directory) kullanıcı ve bilgisayar yapılandırmaları politikalar (policy) ile yönetilir. Politikalar, Aktif Dizin Politika Yöneticisi (Active Directory Policy Manager) üzerinden ilgili kullanıcılarla, gruplara, organizasyonlara veya bilgisayarlara tanımlanarak uygulanır. Aktif Dizin’deki politikalar; politikaların kendileri ve politikaların linkleri olmak üzere iki kısımdan oluşmaktadır. Yönetimi kolaylaştırmak ve yapılandırmaları bir tutmak için yapılandırma değişiklikleri politikaların kendileri üzerinden yapılır. Daha sonra bu yapılandırmalar linkler ile ilgili gruplara atanır. “Active Directory Policy Manager”, ağaç dizin şemasını (gruplar, organizasyon grupları, klasörler vb.) direk olarak Aktif Dizin’den temin eder. Dolayısıyla Aktif Dizin’de yapılacak değişiklikler politikaların uygulanacakları alanları etkiler.

Kontroller

K1 - Kullanıcı Hesap Yönetimi ve Şifreler

Bilgi sistemleri üzerinde tanımlı, cihazların fabrika çıkışı ya da sistemlerin ve yazılımların ilk kurulumu sonrası otomatik olarak oluşturulan kullanıcı ve sistem hesapları bulunur. Benzer şekilde, bu hesaplara ait kullanıcı şifresi gibi güvenlik parametreleri de başlangıçta sabit değerlere tanımlanmıştır. Bu gibi kullanıcı hesaplarına varsayılan (*default*) kullanıcı hesapları denir.

Bilgi sistemleri üzerindeki varsayılan kullanıcı hesap şifreleri genellikle bilindiğinden ya da kolay tahmin edilebilir olduğundan, sistem kurulumu sonrası değiştirilir. Ek olarak, varsayılan kullanıcı hesapları hizmet dışı kalacak şekilde yetkileri kaldırılır. Bu sayede, tüm kullanıcı işlemleri; inkâr edilemezlik ve sorumluluk atama ilkesine göre kaydedilir. Bu ilkeye göre bilgi sistemleri üzerinde yapılan kritik işlemlerin benzersiz kullanıcı hesapları bazında denetim izleri saklanabilir.

Windows tabanlı işletim sistemlerinde Aktif Dizin (Active Directory) Etki Alanı (Domain) yapısı kullanılarak, kurum bünyesindeki tüm Windows tabanlı sistemlerin güvenlik ve şifre politikaları ve bu sistemler üzerinde tanımlı kullanıcı hesapları, bu kullanıcı hesaplarının sahip olduğu yetkiler ve ilgili diğer cihazlar (ör: yazıcılar) tek kaynaktan kontrol edilebilir.

Kullanıcı ve grupların listesi;

Sistem dili **Türkçe** olan sistemlerde;

[Başlat] -> [Tüm Programlar] -> [Yönetim Araçları] -> [Aktif Dizin Kullanıcıları ve Bilgisayarlar]

Sistem dili **İngilizce** olan sistemlerde;

[Start] -> [Programs] -> [Administrative Tools] -> [Active Directory Users and Computers] adımları takip edilerek açılan menüde ilgili etki alanı (Domain) adı seçilerek gözlemlenebilir.

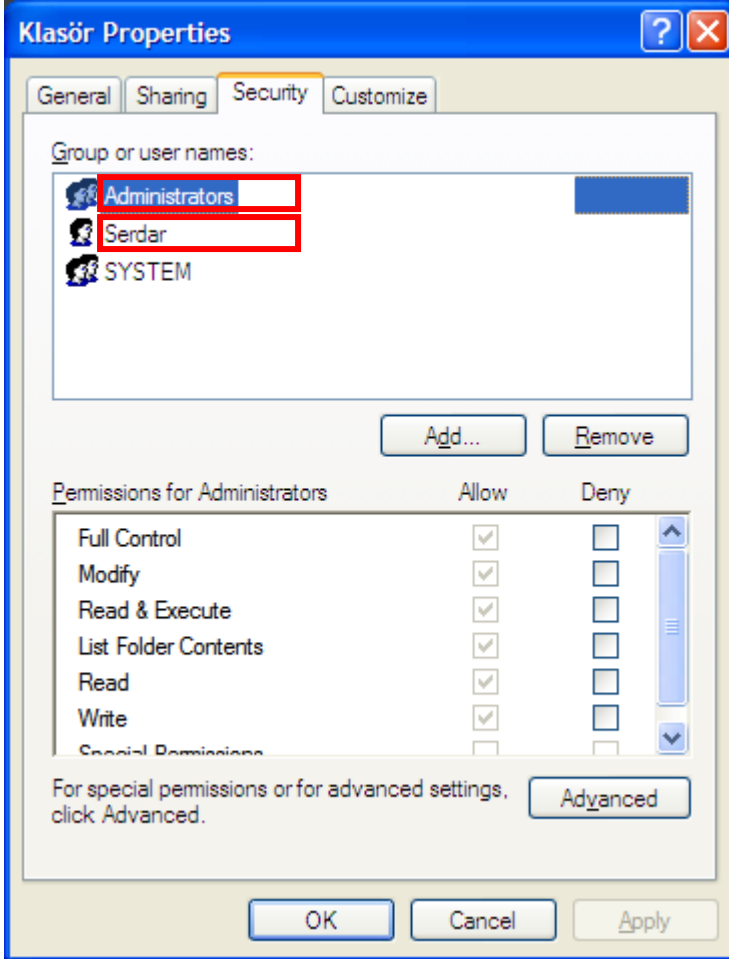
Denetim Prosedürleri

#	Denetim prosedürleri	T/i	Z/O
K1.1	BT güvenliğine ilişkin prosedür temin edilerek prosedürde yayımlanan Windows sistem güvenliğine ilişkin standartların, üretici kılavuzları ve genel kabul görmüş uygulamalar uyarınca yapılandırıldığı gözlemlenir.	T	Z
K1.2	Kullanıcı ve grup listeleri temin edilerek içeriğindeki aktif kullanıcı hesapları tespit edilir. <ul style="list-style-type: none"> Kullanıcı ikonu üzerindeki “İptal” simgesi olan aktif olmayan kullanıcı hesapları ile tespit edilir. Varsayılan “Misafir” (<i>Guest</i>) hesabının erişime kapalı olduğu gözlemlenir. Genel isimlendirmeye sahip (ör: admin, system_user, kullanıcı1, guest vb.) kullanıcı hesapları erişimlerinin system üzerinde kapalı olduğu gözlemlenir. 	İ	Z
K1.3	Kullanıcı ve grup listeleri temin edilerek; kötü niyetli kişiler tarafından kolay tahmin edilen ve siber saldırılar sırasında saldırı aracı olarak sıkça kullanılan varsayılan “Yönetici” (<i>Administrator</i>) hesabının isminin değiştirildiği teyit edilir.	İ	Z
K1.4	Varsayılan kullanıcı hesapları gözden geçirilir ve kritik yetkilerin sadece olması gereken kullanıcılara atandığı kontrol edilir. <ul style="list-style-type: none"> Varsayılan hesaplar aktif halde ise ilgili hesapların varsayılan şifrelerinin, kurumun bilgi güvenliği politikalarına uygun olarak değiştirildiğinden emin olunmalıdır. 	İ	Z
K1.5	Kullanıcı gruplarına ilişkin temin edilen liste üzerinde “Yönetici” (<i>Administrators</i>) grubuna dahil olan kullanıcıların yetkilerinin uygunluğu teyit edilir.	İ	Z

K2 - Kritik Dosyalara Erişim

Windows sistemlerinde “*kullanıcı*” ve kullanıcıların dâhil olabildiği “*grup*” olmak üzere bir dosya ya da dizin üzerinde iki farklı şekilde erişim yetkisi atanabilir.

Windows sistemlerde herhangi bir dosya ya da klasör üzerindeki kullanıcı ve grupların erişim yetkileri; dosya/klasör üzerinde farenin sağ tuşu ile tıklanıp “Özellikler” (Properties) seçeneği tıklandıktan sonra “Güvenlik” (Security) sekmesi seçilerek, ilgili grup ya da kullanıcı hesabı üzerine tıklanıp “Kullanıcı Yetkileri” (Permissions) penceresinden gözlemlenebilir.



- **Read / Okuma:** Dizin/dosya üzerinde okuma fonksiyonuna sahip olduğunu gösterir.
- **Modify / Değişirme:** Dizin/dosya üzerinde değiştirme fonksiyonuna sahip olduğunu gösterir.
- **Write / Yazma:** Dizin/dosya üzerinde yazma fonksiyonuna sahip olduğunu gösterir.
- **Read & Execute / Okuma ve Çalıştırma:** Dizin/dosya üzerinde okuma ve çalıştırma fonksiyonlarına sahip olduğunu gösterir.
- **List Folder Contents / Dizin İçeriklerini Listele:** Dizine ilişkin alt dosya ve dizin içeriklerini listeleme fonksiyonuna sahip olduğunu gösterir.
- **Full Control / Tam Yetki:** Dizin/dosya üzerinde yazma, okuma, değiştirme ve listeleme fonksiyonlarının tümüne sahip olduğunu gösterir.

Yukarıdaki örnekte ilgili dizine “Administrators” ve “SYSTEM” gruplarına dahil olan kullanıcılar dışında “Serdar” kullanıcısının eriştiği gözlemlenebilir.

TASLAK

Denetim Prosedürleri

#	Denetim prosedürleri	T/i	Z/O
K2.1	<p>Kurum bünyesinde bilgi sistemleri denetimi kapsamına alınan uygulamaların çalışması için kaynak olarak kullanılan dosya ve klasörlere (exe, dll, lib vb.) erişimlerin uygunluğu gözlemlenir:</p> <ul style="list-style-type: none"> Denetim kapsamına alınan uygulamalara ait sunucu listesi temin edilir. Windows platformu üzerinde çalışan uygulama sunucuları içerisinde örneklem seçilir. Seçilen örneklem için ilgili kurum BT personeli ile görüşülüp, kaynak dizin ve dosyalar tespit edilir. Belirlenen kaynak dizinlere ilişkin kullanıcı erişim yetkileri gözlemlenerek kurum politikalarına; ilgili politika mevcut değilse kullanıcının pozisyonu, görev tanımı ve / veya çalıştığı bölüm göz önünde bulundurularak uygunluğu teyit edilir. 	İ	Z
K2.2	<p>Windows üzerindeki sistem kayıt defteri içerisinde (Registry) hiyerarşik bir veritabanı yapısında genel sistem konfigürasyon seçenekleri ve ayarları tutulur. Aşağıdaki adımlar izlenerek bu kayıt defterine ilişkin kullanıcı erişimlerinin uygunluğu teyit edilir:</p> <ul style="list-style-type: none"> [Başlat] -> [Çalıştır] -> "regedit32" (ya da "regedit") yazdıktan sonra "Giriş" (Enter) tuşuna basarak "Registry Editor" (Regedit32.exe) çalıştırılır. HKEY_LOCAL_MACHINE sekmesinin altında -> [SYSTEM] -> [CurrentControlSet] -> [Control] -> [SecurePipeServers] -> [Winreg] anahtarına ulaşılır. [Winreg] sekmesi üzerinde fare ile sağ tuşa tıkladıktan sonra "Yetkiler" (Permissions) seçeneğine tıklanır. Bu anahtar üzerinde sadece yüksek yetkili (administrator) kullanıcıların erişimi olduğu gözlemlenir.* <p>* İlgili anahtar üzerindeki kullanıcı yetkilerinin gözlemlenebilmesi için sunucu üzerinde yüksek yetkili (Administrator) bir kullanıcı hesabı ile testin gerçekleştirilmesi gerekmektedir.</p>	İ	O
K2.3	<p>Sistem üzerinde tanımlı grupların listesi temin edilerek, her grup için, grubun üzerinde iken farenin sağ tuşuna tıklayarak "üyeler" seçeneği seçilir ve örnek olarak Account Operators, Yönetici (Administrators), Enterprise Admins, Schema Admins ve Domain Admins gibi kritik gruplara ait olan kullanıcılar gözlemlenir.</p> <p>Bu gruplara fazla sayıda kullanıcının, varsayılan veya genel isimlendirmeye sahip kullanıcıların dahil olmadığı; ve bu gibi yönetim guruplarına başka gurupların da dahil edilmemiş olduğu teyit edilir.</p>	İ	Z

K3 - Varsayılan Şifre ve Güvenlik Parametreleri

Bilgi sistemleri üzerinde tanımlı güvenlik ve şifre parametreleri, yetkisiz erişimleri önleyecek şekilde yapılandırılmıştır.

Aktif Dizin altyapısına sahip olan kurumların bilgi sistemleri altyapısına ilişkin hesap kilitleme (Account Lockout) ve şifre politikaları (Password Policy) da mevcut tek bir kontrol paneli üzerinden yönetilebilir. Buna paralel olarak kullanıcılar; şifrelerini bu kısıtlamalar çerçevesinde yaratabilir ya da değiştirebilirler. Bu kısıtları sistem üzerinde tanımlanan güvenlik politikaları ve şifre parametreleri belirler.

TASLAK

Sistem dili **İngilizce** olan sistemlerde Hesap Kitleme Politikası (Account Lockout Policy);

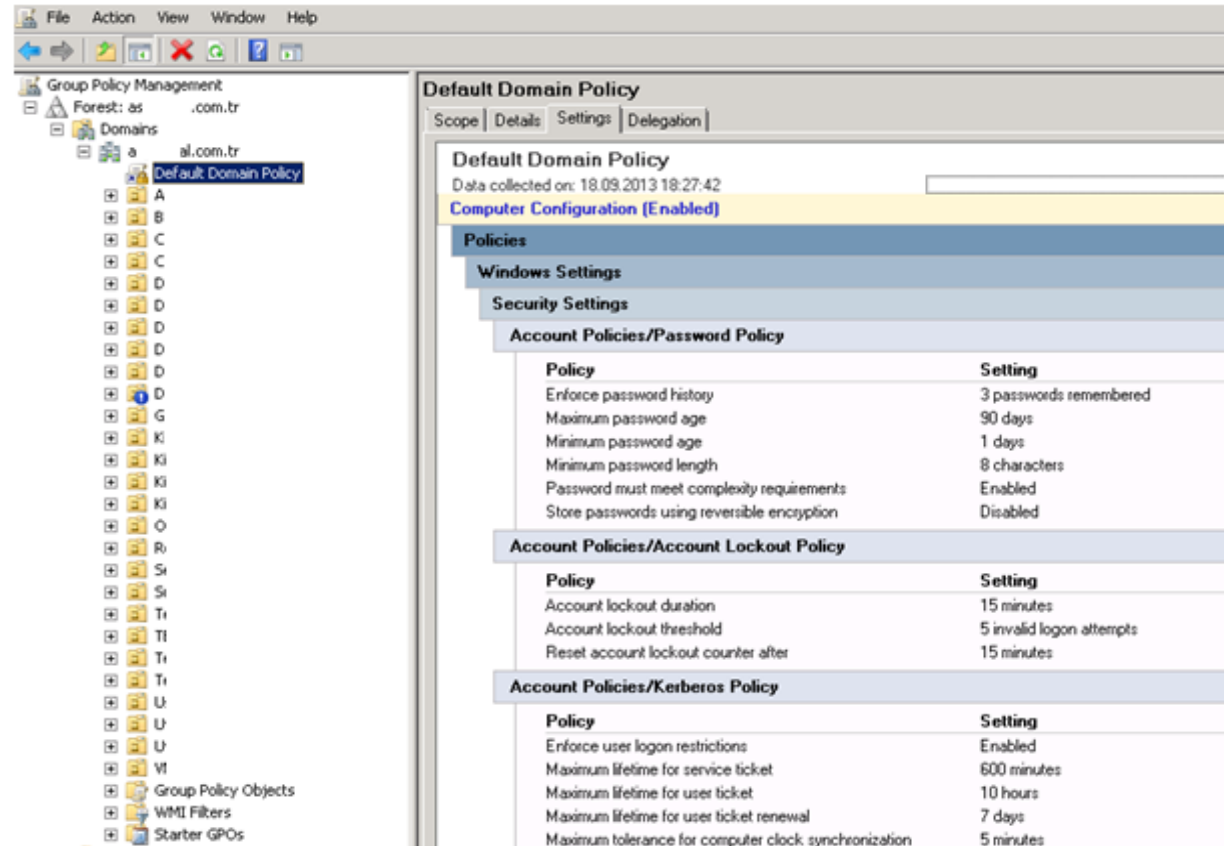
[Start] -> [Programs] -> [Administrative Tools] -> [Group Policy Management],

Türkçe sistemler için;

[Başlat] -> [Programlar] -> [Yönetim Araçları] -> [Grup Politikası Yönetimi] seçilerek gözlemlenebilir

Açılan Pencerede sol kısımdan ilgili etki alanı (Domain) ve politika seçilir.

Sağdaki ekrandan (mavi bölge) settings / ayarlar (gri sekme) seçilir.



Windows tabanlı sistemlerde, yukarıda da görüldüğü gibi şifre politikasına ilişkin aşağıdaki parametreler tanımlanabilir:

Parametre	Tanım
Enforce password history	Yeni şifre tanımlanırken, tanımlanan sayı kadar geriye dönük şifre sayısını tutar ve değiştirilen şifrenin bu şifrelerden farklı olması beklenir.
Maximum password age	Şifrenin azami kullanma süresini gün bazında belirtir.
Minimum password age	Şifrenin en az kaç gün kullanılması gerektiğini belirler.
Minimum password length	İzin verilen en kısa şifre uzunluğunu belirtir.
Password must meet complexity requirements	Şifre içerisinde rakam, küçük harf, büyük harf ve özel karakterlerin (+, %, ! vb.) kullanılmasını zorunlu kılar.
Store passwords using reversible encryption	Bu parametre kullanıcı şifrelerinin geri döndürülebilir şekilde kriptolanmasını (encrypted) belirler. Güvenlik açısından bakıldığında şifrenin sistem üzerinde düz metin olarak saklanılmasından farksızdır. Bu nedenle kullanıcı güvenliğini riske atmamak için etkinleştirilmemelidir.

Benzer şekilde hesap kilitleme politikasına ilişkin aşağıdaki parametreler atanabilir:

Parametre	Tanım
Account lockout duration	Sistem üzerinde belli bir süre işlem yapılmadığında hesabın ne kadar süre sonra kilitleneceğini belirler.
Account lockout threshold	Sisteme azami başarısız giriş deneme sayısını belirler. Bu parametrenin atandığı değer kadar hatalı giriş denemesi olduğunda hesap sistem tarafından otomatik olarak kilitlenir.
Reset account lockout counter after	Yanlış giriş denemeleri sonucunda kilitlenen kullanıcı hesabının ne kadar süre kilitli kalacağını belirler.

Windows tabanlı sistemlerde olayları kayıt altına almaya ilişkin aŐağıdaki parametreler tanımlanabilir:

Parametre	Tanım
Audit Account Logon Events	Hesap oturumu açma olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit Account Management	Hesap yönetim olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit Process Tracking	İŐlem takibi olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit System Events	Sistem olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit Privilege Use	Yetki kullanımı olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit Policy Change	Politika deęiŐiklięi olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit Object Access	Obje erişimi olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit Logon Events	Oturum açma olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit Directory Service Access	Dizin erişim servisi olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.

Windows tabanlı sistemlerde, yukarıda da görüldüęü gibi boŐta kalan oturumların yönetilmesine ilişkin aŐağıdaki parametreler tanımlanabilir:

Parametre	Tanım
Define this policy setting in the template	Bu yapılandırmanın kullanılıp kullanılmayacağını tanımlamak için kullanılır.
Minutes	Sistemin hareketsiz kaldığı durumlarda dakika cinsinden oturumu ne kadar süre sonra boŐta (idle) olarak tanımlayacağını belirtir.

Denetim Prosedürleri

#	Denetim prosedürleri	T/i	Z/O
K3.1	<p>Sistem üzerinde şifre politikaları (Password Policy) içeriği temin edilir. Şifre politikaları üzerinde tanımlanan parametrelerin kurum bilgi güvenliği politikalarına uygun olarak, aşağıdaki önerilen değerler (Ö.D.) doğrultusunda atandığı gözlemlenir:</p> <ul style="list-style-type: none"> • <i>Enforce password history</i>: Ö.D. \geq 3-5 • <i>Maximum password age</i>: Ö.D. = 60-90 gün • <i>Minimum password age</i>: Ö.D. $>$ 1 gün • <i>Minimum password length</i>: Ö.D. \geq 8 karakter • <i>Password must meet complexity requirements</i>: Ö.D. = “Aktif” (Enabled) • <i>Store passwords using reversible encryption</i>: Ö.D. = “Pasif” (Disabled) 	İ	Z
K3.2	<p>Sistem üzerinde hesap kitleme politikaları (Account Lockout Policy) içeriği temin edilir. Politika üzerinde tanımlanan parametrelerin kurum bilgi güvenliği politikalarına uygun olarak, aşağıdaki önerilen değerler (Ö.D.) doğrultusunda atandığı gözlemlenir:</p> <ul style="list-style-type: none"> • <i>Account lockout duration</i>: Ö.D. \leq 15 dakika • <i>Account lockout threshold</i>: Ö.D. = 3-5 • <i>Reset account lockout counter after</i>: Ö.D. $>$ 30 dakika* <p>* Bu değer 0 olarak atandığında süresiz olarak kilitlenir ve ancak kullanıcı hesap yöneticileri tarafından tekrar aktif hale getirilebilir. Ancak bu gibi bir uygulama bilgi sistemleri personeli üzerinde ek yük doğuracağından ve operasyonel açıdan verimli değildir.</p>	İ	Z
K3.3	<p>Sistem üzerinde yaratılan yeni kullanıcı hesaplarına ilişkin şifrelerin, ilk oturum açıldığında sistem tarafından otomatik olarak değiştirilmeye zorlandığı (Maximum password age = 0) gözlemlenir. Bu değer kullanıcı ya da grup bazında atanabilir.</p> <ul style="list-style-type: none"> • İlgili sunucu üzerinde örnek bir kullanıcı hesabı yaratılarak ilk kez oturum açılır. Kullanıcı adı ve parola girildikten sonra; sistemin, kullanıcıyı yeni parola oluşturmaya zorlandığı teyit edilir. 	İ	Z
K3.4	<p>Sistem üzerinde boşta kalmış oturumların (IDLE Session Timeout) içeriği temin edilir. Politika üzerinde tanımlanan parametrelerin kurum bilgi güvenliği politikalarına uygun olarak, aşağıdaki önerilen değerler (Ö.D.) doğrultusunda atandığı gözlemlenir:</p> <ul style="list-style-type: none"> • <i>Define this policy setting in the template</i> için Ö.D. = kutu seçili; • <i>Minutes</i> için Ö.D. = 15; 	İ	O

K3.5	<p>Sistem üzerinde gerekleřen olayların kayıt altına alma politikası (Auditing Policies) ieriđi temin edilir. Politika üzerinde tanımlanan parametrelerin kurum bilgi gvenliđi politikalarına uygun olarak, aŗađıdaki nerilen deđerler (.D.) dođrultusunda atandıđı gzlemlenir:</p> <ul style="list-style-type: none">• <i>Audit Account Logon Events</i> iin .D. = Success and Failure;• <i>Audit Account Management</i> iin .D. = Success and Failure;• <i>Audit Directory Service Access</i> iin .D. = Failure;• <i>Audit Logon Events</i> iin .D. = Success and Failure;• <i>Audit Object Access</i> iin .D. = Failure;• <i>Audit Policy Change</i> iin .D. = Success and Failure;• <i>Audit Privilege Use</i> iin .D. = Failure;• <i>Audit Process Tracking</i> iin .D. = None; and• <i>Audit System Events</i> iin .D. = Failure.	İ	O
------	---	---	---

TASLAK

6.2. VERİTABANI SİSTEMLERİ

6.2.1. MS SQL Server Veritabanı Sistemleri

Risk – Kontrol Eşleşmeleri

Riskler	K1	K2	K3
R1. Veritabanı sistemleri üzerinde kritik veri, bilgi ve cihazlara yetkisiz erişimlerin gözlemlenmesi	+	+	+
R2. Veritabanı sistemleri üzerinde otomatik olarak tanımlanan varsayılan kullanıcılar kullanılarak diğer kullanıcıların yetkilerinin artırılması	+		+
R3. Güvenlik ve şifre parametrelerinin, yetkisiz erişimleri önleyecek şekilde atanmaması			+
R4. Veritabanı sistemlerine yetkisiz erişimlerin ya da erişim girişimlerinin yönetim tarafından fark edilememesi			+
R5. Kritik veri, bilgi ve cihazların bilinçli ya da farkında olmadan değiştirilmesi	+	+	
R6. Kullanıcılar tarafından bilinçli ya da farkında olmadan bilgi sistemleri üzerinde erişim yetkisi artırma işlemlerinin gerçekleştirilmesi	+	+	

Kontroller

K1 - Varsayılan Kullanıcı Hesapları ve Şifreler

MS SQL veritabanının fiziksel bileşenleri, MS SQL yazılımından ve işletim sistemleri kontrolleri tarafından korunan sunucu üzerindeki çeşitli depolama/konfigürasyon dosyalarından oluşur.

MS SQL Server veritabanı sistemlerinde sunucu tabanlı yetkilendirmeden yararlanıldığında, işletim sistemi kontrolleri gibi veritabanı dışındaki güvenlik kontrolleri, veritabanı kimlik doğrulama kontrollerini destekler. Sunucu tabanlı doğrulama işlemleri bulunuyorsa veritabanı dışındaki güvenlik kontrolleri değerlendirilir.

TASLAK

Denetim Prosedürleri

#	Denetim prosedürleri	T/i	Z/O
K1.1	<p>Veritabanı sisteminin üzerinde çalıştığı işletim sistemi güvenlik ayarlarının MS SQL veritabanı dosyalarına erişimi kısıtlayacak şekilde yapılandırıldığı değerlendirilir:</p> <ul style="list-style-type: none"> İşletim sistemi güvenlik ayarları gözden geçirilirken, hem grupların hem de kullanıcıların veritabanı dosyaları üzerinde değişiklik yapma yetkileri temin edilir. Güncel erişim listesinde genel isimlendirmeye sahip (kullanıcıya özel olmayan) hesaplar bulunuyorsa, bu hesaplara erişimi kısıtlayacak kontrollerin bulunduğu değerlendirilir. Windows tabanlı sunucularda erişim yetkileri kontrolleri detaylı denetim adımı için lütfen 6.1.2 MS Windows İşletim Sistemleri – K2. Kritik Dosyalara Erişim bölümüne bakınız. 	İ	Z
K1.2	<p>Veritabanı üzerinde “<i>select * from sys.syslogins</i>” komutu çalıştırılarak kullanıcı ve grup listeleri temin edilir. Tablo içeriğindeki aktif kullanıcı hesapları tespit edilir:</p> <ul style="list-style-type: none"> Windows Authentication (Windows kimlik doğrulama) yöntemi kullanılıyor olsa dahi “sa” hesabına karmaşık bir şifrenin atandığı doğrulanır. Şifre alanı boş olsa dahi, MS SQL Server veritabanı sistemlerindeki tüm şifreler karmaşık şekilde (kriptolu) halde görünür. “sa” hesabını da içeren tüm ayrıcalıklı hesaplara şifre atandığını doğrulamak için veritabanı yöneticisi (Database Administrator) oturumu kullanılarak tüm ayrıcalıklı hesaplara erişim girişimleri gerçekleştirilir. Genel isimlendirmeye sahip (ör: admin, system_user, kullanıcı1, guest vb.) kullanıcı hesapları erişimlerinin system üzerinde kapalı olduğu gözlemlenir. 	İ	Z
K1.3	<p>“<i>BUILTIN\Administrators</i>” grubuna ait sistem girişlerinin kaldırıldığı ve bu girişin veritabanı yöneticileri için özel olarak yaratılmış bir Windows grubu ile değiştirildiği teyit edilir:</p> <ul style="list-style-type: none"> <i>SQL Server Management Studio</i> başlatılır. <i>Microsoft SQL Server -> Güvenlik (Security) -> Logins</i> sekmesine tıklanır. “<i>BUILTIN\Administrators</i>” girişinin <i>Windows</i> grubu ile değiştirildiği doğrulanır. Sistem yöneticisi ile görüşmeler gerçekleştirilerek bu gruba kullanıcı eklenmesinde izlenen yetkilendirme süreci değerlendirilir. (Bkz: 4.2 Güvenlik Hizmetleri Yönetimi) 	İ	Z

K1.4	<p>Varsayılan kullanıcı hesapları gözden geçirilir ve kritik yetkilerin sadece olması gereken kullanıcılara atandığı kontrol edilir:</p> <ul style="list-style-type: none">Varsayılan hesaplar aktif halde ise ilgili hesapların varsayılan şifrelerinin, kurumun bilgi güvenliği politikalarına uygun olarak değiştirildiğinden emin olunmalıdır.	İ	Z
K1.5	<p>Kullanıcı gruplarına ilişkin temin edilen liste üzerinde yüksek yetkili yönetici gruplarına dahil olan kullanıcıların yetkilerinin uygunluğu teyit edilir.</p>	İ	Z

TASLAK

K2 - Kritik Dosyalara Erişim

Denetim Prosedürleri

#	Denetim prosedürleri	T/i	Z/O
K2.1	<p>Kullanıcı yönetimi, değişiklik yönetimi ve veritabanı operasyonları gibi anahtar kontrolleri destekleyen süreçler için ayrıcalıklı kullanıcı haklarının yer aldığı bir liste temin edilir. (Örn: tüm sisteme veya güvenlik yönetimi fonksiyonlarına erişim yetkisi olan kullanıcı listesi)</p> <ul style="list-style-type: none"> • Ayrıcalıklı haklara sahip olan kullanıcı listesi gözden geçirilir ve kullanıcı sayısının uygunluğu olduğu değerlendirilir. • Kullanıcıların sahip oldukları iş tanımına / iş fonksiyonuna uygun yetkilere sahip olduklarını değerlendirmek için kullanıcı hacmine ve bu kontrolün doğasına dayalı olarak bir test tekniği geliştirilir. • Aşağıdaki prosedürler kullanılarak ayrıcalıklı haklara sahip kullanıcı listesi temin edilir: <ul style="list-style-type: none"> ○ <i>sp_helprolemember 'db_securityadmin'</i> ○ <i>sp_helprolemember 'db_owner'</i> ○ <i>sp_helprolemember 'db_accessadmin'</i> ○ <i>sp_helpsrvrolemember 'sysadmin'</i> ○ <i>sp_helpsrvrolemember 'serveradmin'</i> ○ <i>sp_helpsrvrolemember 'securityadmin'</i> • Atanan ayrıcalıklı erişim haklarının uygunluğu gözden geçirilir ve ayrıcalıklı erişim haklarının sadece iş tanımları ile uyumlu kişilere verildiği teyit edilir. 	İ	Z

K3 - Şifre ve Güvenlik Parametreleri

Denetim Prosedürleri

#	Denetim prosedürleri	T/i	Z/O
K3.1	<p>Sistem üzerinde şifre politikaları (<i>Password Policy</i>) içeriği temin edilir. Şifre politikaları üzerinde tanımlanan şifre uzunluğu, hesap kitleme süresi, şifre karmaşıklığı, şifre ömrü gibi parametrelerin kurum bilgi güvenliği politikalarına uygun olarak atandığı gözlemlenir:</p> <ul style="list-style-type: none"> • <i>SQL Server Management Studio</i> başlatılır. • Uygun sunucu objesine sağ tıklanır. • [<i>Properties</i>] seçeneğine tıklanır. • [<i>Security</i>] sekmesine tıklanır. • [<i>Server Authentication (Sunucu Doğrulama)</i>] seçeneğinin altında [<i>Windows Authentication mode</i>] seçeneğinin işaretli olduğu teyit edilir: <ul style="list-style-type: none"> ○ Eğer [<i>Windows Authentication mode</i>]* seçeneğini aktif ise, Windows seviyesinde hesap kitleme politikası gözden geçirilir. (Bkz: 6.1.2 MS Windows İşletim Sistemleri – K3. Güvenlik ve Şifre Parametreleri) • SQL Server veritabanı üzerinde <i>select * from sys.sql_logins</i> komutu çalıştırılır. • [<i>is_policy_checked</i>] =1 durumu doğrulanıyor ise Windows hesap kitleme ayarları SQL hesapları için geçerlidir. <p>* [<i>Windows Authentication mode</i>] seçeneği işaretli ise ve SQL Server veritabanı sistemi MS Windows Server işletim sistemi üzerinde çalışıyorsa, SQL kullanıcı hesapları üzerinde Windows şifre politikası uygulanabilir.</p>	İ	Z

K3.2	<p>Microsoft SQL Server Analiz Servisleri (<i>SSAS – Analyses Services</i>) aktif olmayan oturumların zaman aşımına uğraması özelliğini destekler. Veritabanı sistemleri üzerinde uzaktan açılan oturumlar ve uzaktan yapılan sorgular için aktif olmayan oturumların zaman aşımına uğradığı teyit edilir. Analiz Servislerinin bu özelliğini incelemek için aşağıdaki adımlar gerçekleştirilir:</p> <ul style="list-style-type: none"> • SQL Server Management Studio açılır. • Veritabanı motoruna analiz sunucusuna (<i>Analysis Server</i>) bir bağlantı açıldığına emin olunur. • <i>Object Explorer</i> bölümünde bağlantı kurulan sunucuya sağ tıklanır. • Menüde <i>Properties</i> sekmesine tıklanır. • Varsayılan olarak <i>General (Genel)</i> sayfasının seçildiğinden emin olunur. • <i>Show Advanced (All) Properties</i> kutusu işaretlenir. • <i>IdleConnectionTimeout (Aktif Olmayan Oturumların Zaman Aşımına Uğraması)</i> parametresi gözlemlenir: <ul style="list-style-type: none"> ○ 32-bit uzunluğunda işaretli (<i>signed</i>) sayı değeri, pasif bağlantıların zaman aşımına uğrama süresini saniye cinsinden değeridir. Bu özellik için varsayılan değer, tüm aktif olmayan bağlantıların zaman aşımına uğramayacağını ifade eden <i>sıfır (0)</i> değeridir. 	İ	Z
K3.3	<p>SQL Server Management Studio çalıştırılarak denetleme ayarlarını üzerinden başarısız oturum açma girişimlerinin kaydedildiği teyit edilir:</p> <ul style="list-style-type: none"> • Uygun sunucu objesine sağ tıklanır. • [<i>Properties</i>] seçeneğine tıklanır. • [<i>Security</i>] sekmesine tıklanır. • [<i>Login Auditing</i>] alanında [<i>Both failed and successful logins</i>] (Başarılı ve başarısız oturum açma girişimleri) seçeneğinin işaretli olduğu teyit edilir. • Oturum açma girişimleri denetleniyor ise, aşağıdakileri özellikleri değerlendirmek için sistem yöneticisinden aşağıdaki konular ile ilgili bilgi alınır: <ul style="list-style-type: none"> ○ Başarısız oturum açma girişimlerinin denetlenme sıklığı ○ Şüpheli oturum açma girişimlerine ve gerçekten yanlış oturum açma denemelerine yer veren prosedürlerin varlığı ○ Başarısız oturum açma girişim raporları dosyalanması ve güvenli bir şekilde saklanması • Başarısız oturum açma girişimlerine ilişkin raporlanan dokümanlar gözden geçirilir. Tekrar eden ve şüpheli başarısız oturum açma girişimleri belirlenir ve ne gibi aksiyonlar alındığı değerlendirilir. 	İ	O

6.2.2. Oracle Veritabanı Sistemleri**Risk – Kontrol Eşleşmeleri**

Riskler	K1	K2	K3
R1. Veritabanı sistemleri üzerinde kritik veri, bilgi ve cihazlara yetkisiz erişimlerin gözlemlenmesi	+	+	+
R2. Veritabanı sistemleri üzerinde otomatik olarak tanımlanan varsayılan kullanıcılar kullanılarak diğer kullanıcıların yetkilerinin artırılması	+		+
R3. Güvenlik ve şifre parametrelerinin, yetkisiz erişimleri önleyecek şekilde atanmaması			+
R4. Veritabanı sistemlerine yetkisiz erişimlerin ya da erişim girişimlerinin yönetim tarafından fark edilememesi			+
R5. Kritik veri, bilgi ve cihazların bilinçli ya da farkında olmadan değiştirilmesi	+	+	
R6. Kullanıcılar tarafından bilinçli ya da farkında olmadan bilgi sistemleri üzerinde erişim yetkisi artırma işlemlerinin gerçekleştirilmesi	+	+	

K1 - Kullanıcı Hesap Yönetimi ve Şifreler**Denetim Prosedürleri**

#	Denetim prosedürleri	T/İ	Z/O																								
K1.1	<p>Varsayılan kullanıcı hesapları için varsayılan şifrelerin değiştirildiği teyit edilir:</p> <ul style="list-style-type: none"> “sqlplus” aracı “system” hesabı ile çalıştırılır. Aşağıdaki komutlar SQL penceresine girilir: <pre>SQL> SET ECHO OFF SQL> SET MARKUP HTML ON SPOOL ON SQL> SPOOL dba_users_with_defpwd.html SQL> SELECT * FROM DBA_USERS_WITH_DEFPWD; SQL> SET MARKUP HTML OFF SQL> SET ECHO ON SQL> SPOOL OFF</pre> Oluşturulan 'dba_users_with_defpwd.html' dosyası temin edilir. 'dba_users_with_defpwd.html' dosyası incelenerek aşağıdaki varsayılan kullanıcı hesapları için varsayılan şifrelerin değiştirildiği teyit edilir: <p>Varsayılan Oracle veritabanı kullanıcıları</p> <table border="1"> <tr><td>SYS</td></tr> <tr><td>SYSTEM</td></tr> <tr><td>OUTLN</td></tr> <tr><td>SCOTT</td></tr> <tr><td>ADAMS</td></tr> <tr><td>JONES</td></tr> <tr><td>CLARK</td></tr> <tr><td>BLAKE</td></tr> <tr><td>HR (Human Resources)</td></tr> <tr><td>OE (Order Entry)</td></tr> <tr><td>SH (Sales History)</td></tr> <tr><td>DEMO</td></tr> <tr><td>ANONYMOUS</td></tr> <tr><td>AURORA\$ORB\$UNAUTHENTICATED</td></tr> <tr><td>AWR_STAGE</td></tr> <tr><td>CSMIG</td></tr> <tr><td>CTXSYS</td></tr> <tr><td>DBSNMP</td></tr> <tr><td>DIP</td></tr> <tr><td>DMSYS</td></tr> <tr><td>DSSYS</td></tr> <tr><td>EXFSYS</td></tr> <tr><td>LBACSYS</td></tr> <tr><td>MDSYS</td></tr> </table>	SYS	SYSTEM	OUTLN	SCOTT	ADAMS	JONES	CLARK	BLAKE	HR (Human Resources)	OE (Order Entry)	SH (Sales History)	DEMO	ANONYMOUS	AURORA\$ORB\$UNAUTHENTICATED	AWR_STAGE	CSMIG	CTXSYS	DBSNMP	DIP	DMSYS	DSSYS	EXFSYS	LBACSYS	MDSYS	İ	Z
SYS																											
SYSTEM																											
OUTLN																											
SCOTT																											
ADAMS																											
JONES																											
CLARK																											
BLAKE																											
HR (Human Resources)																											
OE (Order Entry)																											
SH (Sales History)																											
DEMO																											
ANONYMOUS																											
AURORA\$ORB\$UNAUTHENTICATED																											
AWR_STAGE																											
CSMIG																											
CTXSYS																											
DBSNMP																											
DIP																											
DMSYS																											
DSSYS																											
EXFSYS																											
LBACSYS																											
MDSYS																											

	<table border="1"> <tr><td>ORACLE_OCM</td></tr> <tr><td>ORDPLUGINS</td></tr> <tr><td>ORDSYS</td></tr> <tr><td>PERFSTAT</td></tr> <tr><td>TRACESVR</td></tr> <tr><td>TSMSYS</td></tr> <tr><td>XDB</td></tr> </table>	ORACLE_OCM	ORDPLUGINS	ORDSYS	PERFSTAT	TRACESVR	TSMSYS	XDB		
ORACLE_OCM										
ORDPLUGINS										
ORDSYS										
PERFSTAT										
TRACESVR										
TSMSYS										
XDB										
K1.2	<p>Oracle veritabanı sistemlerinde denetim sürecinde oluşturulmuş hesapların listesi temin edilir. “DBA_USERS” tablosundaki “CREATED” sütünü incelenerek kullanıcı hesaplarının oluşturulma tarihleri belirlenir.</p> <ul style="list-style-type: none"> • “sqlplus” aracı “system” hesabı ile çalıştırılır. • Aşağıdaki komutlar SQL penceresine girilir: <pre>SQL> SET ECHO OFF SQL> SET MARKUP HTML ON SPOOL ON SQL> SPOOL dba_users.html SQL> SELECT * FROM DBA_USERS; SQL> SET MARKUP HTML OFF SQL> SET ECHO ON SQL> SPOOL OFF</pre> • Oluşturulan 'dba_users.html' dosyası temin edilir. • Uygun örneklem teknikleri kullanılarak kullanıcılara erişim yetkileri atama sürecinin gerekli talep ve onaylar alınarak yürütüldüğü ve bu kullanıcılara atanan yetkilerin, kullanıcının görevi tanımına uygun olduğu teyit edilir.* <p>* Denetim sürecinde, “DBA_USERS” tablosundaki “Account Status” alanında “EXPIRED” (zamanı geçmiş) veya “LOCKED” (kilitlemiş) değeri bulunan hesaplar belirlenip, denetim sürecindeki testlerden muaf tutulabilirler.</p>	İ	Z							

K2 - Kritik Dosyalara Eriřim

Denetim Prosedürleri

#	Denetim prosedürleri	T/İ	Z/O
K2.1	<p>İřletim sisteminin belirtilen dosyalar gibi Oracle veritabanı dosyalarını erişimi kısıtlayacak şekilde yapılandırıldığını onaylanır.</p> <ul style="list-style-type: none"> İřletim sistemi güvenliđi incelenirken, ařađıdaki dosyalara erişimi olan kullanıcı ve gruplar hakkında güvenlik ve erişim bilgileri temin edilir. Eđer güncelleme (okuma-yazma) yetkisi olan kullanıcı hesaplarına ilişkin genel isimlendirmeye tabi hesaplar mevcut ise, bu tür hesapların erişimlerinin sadece gerekli kullanıcılarda bulunduđunun teyidi için ne tür kontrollerin mevcut olduđu tespit edilir: <ul style="list-style-type: none"> Aralar ve İkili Kodlar (Binaries): veritabanına destek olan dosya ve aralardır. Tablo alanı (tablespace) veri dosyaları: Oracle veritabanı sistemleri çeřitli tablo içeriklerini (örn. tablolar, paketler, prosedürler vb.) tablo alanlarında (tablespace) tutar. Bunlar çođunlukla “.dbf” uzantılı dosyalardır ve \$ORACLE_BASE/oradata/<sid>/ klasöründe tutulur. Başlangı dosyası: Başlangı parametrelerinin saklandıđı dosyasıdır. Bu dosya, Oracle veritabanı alıřtırıldıđında, varsayılan başlangı parametrelerini yapılandırmak için kullanılır. INIT.ORA dosyası olarak belirtilir; genellikle INIT<veritabanı ismi>.ORA olarak isimlendirilir. Bu dosya üzerindeki parametrelere ilişkin yapılan deđiřikler, veritabanı yeniden başlatılıncaya kadar veritabanına etki etmez. Kontrol dosyaları: Bu dosyalar veritabanının fiziksel yapısına ilişkin durumun deđiřiminin takibi için kullanılır. Veritabanı başlangıı esnasında ve veritabanı kurtarımında kullanılır. Kontrol dosyalarının sayıları ve buldukları konumlar, Oracle başlangıı sırasında alıřtırılan “INIT.ORA” dosyası içerisinde “CONTROL_FILES” parametresinde listelenir. Yapılandırma dosyası: “CONFIG.ORA” dosyası “INIT.ORA” dosyasında bulunmayan ek yapılandırma ayarlarını içerir. Bu dosyanın varlıđı isteđe bađlı olduđundan tüm Oracle kurulumlarında bulunmayabilir. “CONFIG.ORA” dosyası sistem güvenliđi ve yapılandırması hakkında önemli bilgiler içermektedir. Veritabanı dinleyici dosyası: Veritabanına erişim sađlamak için, veritabanı dinleyicisinin řifresinin tutulduđu dosyadır. orapwd<veritabanı ismi> dosyası: Bu dosya yüksek yetkili SYS, SYSDBA veya SYSOPER rollerine sahip kullanıcıların řifrelerinin kriptolanmış (hashed) halini tutar. 	İ	Z
K2.2	Veritabanı üzerindeki PUBLIC rolüne atanmış olan yetkilerin uygunluđu teyit edilir. Varsayılan olarak, tüm kullanıcı hesaplarının PUBLIC rolüne erişimi vardır ve PUBLIC rolüne ilişkin tanımlanan güvenlik hakları tüm kullanıcılara uyarlanır.	İ	Z

<p>Hassas roller, nesnelere ve sistem yetkileri PUBLIC rolüne atanmamış olmalıdır:</p> <ul style="list-style-type: none">• “DBA_SYS_PRIVS” tablosu temin edilir:<ul style="list-style-type: none">○ “sqlplus” aracı “system” hesabı ile çalıştırılır.○ Aşağıdaki komutlar SQL penceresine girilir: SQL> SET ECHO OFF SQL> SET MARKUP HTML ON SPOOL ON SQL> SPOOL dba_sys_privs_privs.html SQL> SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='CREATE USER' OR PRIVILEGE='BECOME USER' OR PRIVILEGE='ALTER USER' OR PRIVILEGE='DROP USER' OR PRIVILEGE='CREATE ROLE' OR PRIVILEGE='ALTER ANY ROLE' OR PRIVILEGE='DROP ANY ROLE' OR PRIVILEGE='GRANT ANY ROLE' OR PRIVILEGE='CREATE PROFILE' OR PRIVILEGE='ALTER PROFILE' OR PRIVILEGE='DROP PROFILE' OR PRIVILEGE='CREATE ANY TABLE' OR PRIVILEGE='ALTER ANY TABLE' OR PRIVILEGE='DROP ANY TABLE' OR PRIVILEGE='INSERT ANY TABLE' OR PRIVILEGE='UPDATE ANY TABLE' OR PRIVILEGE='DELETE ANY TABLE' OR PRIVILEGE='CREATE ANY PROCEDURE' OR PRIVILEGE='ALTER ANY PROCEDURE' OR PRIVILEGE='DROP ANY PROCEDURE' OR PRIVILEGE='CREATE ANY TRIGGER' OR PRIVILEGE='ALTER ANY TRIGGER' OR PRIVILEGE='DROP ANY TRIGGER' OR PRIVILEGE='CREATE TABLESPACE' OR PRIVILEGE='ALTER TABLESPACE' OR PRIVILEGE='DROP TABLESPACES' OR PRIVILEGE='ALTER DATABASE' OR PRIVILEGE='ALTER SYSTEM'; SQL> SET MARKUP HTML OFF SQL> SET ECHO ON SQL> SPOOL OFF○ Oluşturulan 'dba_sys_privs_privs.html' dosyası temin edilir.○ 'dba_sys_privs_privs.html' dosyası incelenerek, PUBLIC rolüne atanmış olan sistem yetkilerinin uygunluğu teyit edilir. <p>“DBA_TAB_PRIVS” tablosu temin edilir:</p> <ul style="list-style-type: none">○ “sqlplus” aracı “system” hesabı ile çalıştırılır.		
---	--	--

	<ul style="list-style-type: none">○ Aşağıdaki komutlar SQL penceresine girilir*: <pre>SQL> SET ECHO OFF SQL> SET MARKUP HTML ON SPOOL ON SQL> SPOOL dba_tab_privs_IUADE.html SQL> SELECT UNIQUE GRANTEE, <TABLO_ADI> FROM DBA_TAB_PRIVS WHERE (PRIVILEGE='INSERT' OR PRIVILEGE='UPDATE' OR PRIVILEGE='ALTER' OR PRIVILEGE='DELETE' OR PRIVILEGE='EXECUTE');</pre>○ Oluşturulan 'dba_tab_privs_IUADE.html' dosyası temin edilir.○ 'dba_tab_privs_IUADE.html' dosyası incelenerek, PUBLIC rolüne atanmış olan nesne yetkilerinin uygunluğu teyit edilir. <p>* Sorguda geçen <TABLO_ADI> kısmına kurum için finansal önem taşıyan tablo ismi yazılmalıdır. Finansal olarak önem taşıyan tabloları kurum yetkilileri ile görüşerek belirleyebilirsiniz.</p> <ul style="list-style-type: none">● “DBA_ROLE_PRIVS” tablosu temin edilir:<ul style="list-style-type: none">○ “sqlplus” aracı “system” hesabı ile çalıştırılır.○ Aşağıdaki komutlar SQL penceresine girilir*: <pre>SQL> SET ECHO OFF SQL> SET MARKUP HTML ON SPOOL ON SQL> SPOOL dba_role_privs.html SQL> SELECT * FROM DBA_ROLE_PRIVS; SQL> SET MARKUP HTML OFF SQL> SET ECHO ON SQL> SPOOL OFF</pre>○ Oluşturulan 'dba_role_privs.html' dosyası temin edilir.○ 'dba_role_privs.html' dosyası incelenerek, PUBLIC rolüne atanmış olan rollerin yetkilerinin uygunluğu teyit edilir.	
--	--	--

K3 - Şifre ve Güvenlik Parametreleri

Denetim Prosedürleri

#	Denetim prosedürleri	T/i	Z/O
K3.1	<p>Global ve kurumsal roller kullanıldığı durumlarda, veritabanı güvenlik kontrolleri LDAP teknolojisi ile merkezleştirilmektedir. Bu tür durumlarda veritabanı için global bir rol oluşturulur ve o global rol LDAP sunucusu üzerinde bir kurum rolü ile bağdaştırılır. Kurum kullanıcıları LDAP sunucusu tarafından doğrulanır ve sonrasında, veritabanı üzerinde global bir role erişim sağlayacak şekilde, LDAP üzerinden veritabanı erişimleri kurum rolü bazında sağlanır. Global ve kurumsal roller kullanıldığında ilgili prosedürleri çoğu zaman değiştirilerek merkezi güvenlik modeline uyum sağlamaları gerekir.</p> <ul style="list-style-type: none"> • “DBA_USERS” tablosu temin edilir: <ul style="list-style-type: none"> ○ “sqlplus” aracı “system” hesabı ile çalıştırılır. ○ Aşağıdaki komutlar SQL penceresine girilir: <pre>SQL> SET ECHO OFF SQL> SET MARKUP HTML ON SPOOL ON SQL> SPOOL dba_users.html SQL> SELECT * FROM DBA_USERS; SQL> SET MARKUP HTML OFF SQL> SET ECHO ON SQL> SPOOL OFF</pre> ○ Oluşturulan 'dba_users.html' dosyası temin edilir. ○ 'dba_users.html' dokümanı incelenir ve kullanıcılardan “PASSWORD” değişkeni ‘GLOBAL’ değeri almış olanları tespit edilir. Bu yapılandırma global kimlik doğrulama mekanizmasının (<i>Global Authentication and Authorization</i>) kullanıldığını gösterir. • ‘GLOBAL’ değerinin mevcut oluşu tespit edilen durumlarda, kurum çalışanları ile görüşerek, kimlik tespiti yapılan mekanizmanın detaylarına ulaşılır. 	İ	Z
K3.2	<p>Sunucu tabanlı kimlik doğrulaması kullanıldığında veritabanı dışında (işletim sistemi) güvenlik kontrolleri kullanılır. Sunucu tabanlı kimlik doğrulama kullanılan durumlarda veritabanı dışındaki güvenlik kontrolleri de veritabanı-seviyesi test prosedürlerine dâhil edilir.</p> <ul style="list-style-type: none"> • “DBA_USERS” tablosu temin edilir: <ul style="list-style-type: none"> ○ “sqlplus” aracı “system” hesabı ile çalıştırılır. ○ Aşağıdaki komutlar SQL penceresine girilir: <pre>SQL> SET ECHO OFF SQL> SET MARKUP HTML ON SPOOL ON SQL> SPOOL dba_users.html SQL> SELECT * FROM DBA_USERS;</pre> 	İ	O

	<pre>SQL> SET MARKUP HTML OFF SQL> SET ECHO ON SQL> SPOOL OFF</pre> <ul style="list-style-type: none"> ○ Oluşturulan 'dba_users.html' dosyası temin edilir. • 'dba_users.html' dosyasını incelenir ve “DBA_USERS” tablosundaki kullanıcıların herhangi birinin “PASSWORD” alanına karşılık gelen değer “EXTERNAL” olup olmadığı teyit edilir. “EXTERNAL” değerinin varlığı sunucu tabanlı kimlik doğrulamanın bulunduğunu gösterir. • Eğer “EXTERNAL” değerini almış bir değer mevcut ise aşağıdaki adımları izleyerek Oracle başlangıç dosyasının (V\$PARAMETER2) bir kopyasını temin etmek için aşağıdaki komut çalıştırılır: <pre>SELECT * FROM V\$PARAMETER2 WHERE NAME in (remote_os_authent,'os_authent_prefix');</pre> • V\$PARAMETER2 tablosunun çıktısı aşağıdaki adımları uygulayarak alınır: <ul style="list-style-type: none"> ○ “sqlplus” aracı “system” hesabı ile çalıştırılır. ○ Aşağıdaki komutlar SQL penceresine girilir: <pre>SQL> SET ECHO OFF SQL> SET MARKUP HTML ON SPOOL ON SQL> SPOOL v_parameter2_external.html SQL> SELECT * FROM V\$PARAMETER2 WHERE NAME in (remote_os_authent,'os_authent_prefix'); SQL> SET MARKUP HTML OFF SQL> SET ECHO ON SQL> SPOOL OFF</pre> ○ Oluşturulan 'v_parameter2_external.html' dosyası temin edilir. • “v_parameter2_external.html” dosyasında, “os_authent_prefix” parametresi incelenir. Bu parametre sunucu tabanlı kimlik doğrulama için tanımlanmış hesapları belirtir. Veritabanı sunucusunda “os_authent_prefix” parametresindeki değer ile başlayan tüm kullanıcılar, veritabanı seviyesinde kimlik doğrulamayı atlarlar. Bu parametre için varsayılan değer “ops\$”tur. “ ” değerini almış bir “os_authent_prefix value” değişkeni bu özelliğin kapalı olduğunu gösterir. Bu parametre için tavsiye edilen değer “ ” değeridir. • Ek olarak, “v_parameter2_external.html” dosyasında, “remote_os_authent” parametresi incelenir. Parametre “TRUE” değerine atanmış ise veritabanı ağdaki diğer veritabanı sunucuları ile güven ilişkisi oluşturmaktadır. Bu parametre “TRUE” değerine atanmış ve “os_authent_prefix” parametresi aktif ise; varsayılan “ops\$” ön ekine sahip hesaplar ağ üzerindeki tüm veritabanlarında kimlik doğrulamayı atlayabilir. • “DBA_USERS” tablosundaki kullanıcıların herhangi birinin “PASSWORD” alanına karşılık gelen değer “EXTERNAL” değerlerinin mevcut olduğu tespit edildiğinde, kurum yetkilileri ile görüşüp kullanıcı kimlik doğrulama mekanizmalarını incelenir ve veritabanı üzerinde mantıksal erişimlere ilişkin kontroller belirlenir. Bu 	
--	---	--

	kontroller test edilir.* * Kullanıcı kimlik doğrulama mekanizması olarak Kerberos, SecureID veya Identix kullanıldığında, o kullanıcıya ilişkin "PASSWORD" alanı "EXTERNAL" değerini alır.		
K3.3	<p>Veritabanı sistemi üzerinde tanımlı şifre parametre değerleri temin edilir. Şifre parametreleri üzerinde tanımlanan değerlerin kurum bilgi güvenliği politikalarına uygun olarak atandığı gözlemlenir:</p> <ul style="list-style-type: none"> • "DBA_USERS" tablosu temin edilir: <ul style="list-style-type: none"> ○ "sqlplus" aracı "system" hesabı ile çalıştırılır. ○ Aşağıdaki komutlar SQL penceresine girilir: <pre>SQL> SET ECHO OFF SQL> SET MARKUP HTML ON SPOOL ON SQL> SPOOL dba_users.html SQL> SELECT * FROM DBA_USERS; SQL> SET MARKUP HTML OFF SQL> SET ECHO ON SQL> SPOOL OFF</pre> ○ Oluşturulan 'dba_users.html' dosyası temin edilir. • "DBA_USERS" tablosu temin edilir: <ul style="list-style-type: none"> ○ "sqlplus" aracı "system" hesabı ile çalıştırılır. ○ Aşağıdaki komutlar SQL penceresine girilir: <pre>SQL> SET ECHO OFF SQL> SET MARKUP HTML ON SPOOL ON SQL> SPOOL dba_profiles.html SQL> SELECT * FROM DBA_PROFILES; SQL> SET MARKUP HTML OFF SQL> SET ECHO ON SQL> SPOOL OFF</pre> ○ Oluşturulan 'dba_profiles.html' dosyası temin edilir. • "DBA_SOURCE" tablosu temin edilir: <ul style="list-style-type: none"> ○ "sqlplus" aracı "system" hesabı ile çalıştırılır. ○ Aşağıdaki komutlar SQL penceresine girilir: <pre>SQL> SET ECHO OFF SQL> SET MARKUP HTML ON SPOOL ON SQL> SPOOL password_verify_function.html SQL> SELECT NAME,TEXT FROM DBA_SOURCE WHERE NAME in (SELECT LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME = 'PASSWORD_VERIFY_FUNCTION') ORDER BY NAME, LINE; SQL> SET MARKUP HTML OFF SQL> SET ECHO ON SQL> SPOOL OFF</pre> 	İ	Z

	<ul style="list-style-type: none"> ○ Oluřturulan ‘password_verify_function.html’ dosyası temin edilir. • Her bir kullanıcı hesabı için belirtilen parametrelerin uygunluęunu denetlenir: <ul style="list-style-type: none"> ○ Oracle veritabanında řifre yapılandırılmaları profillere atanmıřtır. řifre yapılandırmalarına iliřkin parametreler “DBA_PROFILES” tablosu içinde tanımlanmıřtır. Her kullanıcı bir profil ile baędařtırılmıřtır. Her řifre yapılandırması için: <ul style="list-style-type: none"> - Her bir profil için güvenlik ve řifre parametrelerine iliřkin yapılandırmaların uygunluęu teyit edilir. - Kullanıcı hesaplarının uygun profillere atandıkları ve bu profillerdeki güvenlik ve řifre yapılandırmalarının ilgili kullanıcıya uygun olup olmadıęı gözlemlenir. • Kabul edilen en kısa řifre uzunluęu Oracle veritabanı belirli řifre yapılandırmalarını kontrol etmek için řifre onaylama fonksiyonu (PASSWORD_VERIFY_FUNCTION) atanır. Kabul edilen en kısa řifre uzunluęu da bunlara dâhildir. “DBA_PROFILES” tablosu içinde, “PASSWORD_VERIFY_FUNCTION” parametresinde dosya veya dosyaların tanımlandıęı teyit edilir. Parametrede dosya tanımlı ise ilgili dosyaları temin ederek, dosya içerięinde ařaęıda belirtilen kodun varlıęı teyit edilir (en kısa řifre uzunluęu için tavsiye edilen deęer 6-8 veya daha büyük bir deęerdir): <i>IF length(password) < 6 THEN raise_application_error(-20002, 'Password length less than 6')</i> “DBA_USERS” tablosundaki her kullanıcının, řifre onaylama fonksiyonu uygun yapılandırılmıř bir profile atandıęı teyit edilir. • İlk oturum açılıřı için tek kullanımlık řifre Oracle veritabanlarında “PASSWORD_VERIFY_FUNCTION” içerisinde ilk oturum açılıřından sonra kullanıcıların řifrelerini deęiřtirmeleri için bir yapılandırma sunulmaktadır. Kullanıcı hesabı açılırken ařaęıdaki SQL komutu alıřtırılırsa, kullanıcıların řifrelerini deęiřtirmeleri zorunlu kılınır: <i>ALTER USER <kullanıcı_adı> PASSWORD EXPIRE</i> Hesap açılıř sürecini incelerken yukarıdaki kodun kullanıldıęı teyit edilir.* * Buradaki <kullanıcı_adı> parametresinin yerine kullanıcı hesabının varlıęı gözlemlenmelidir. • řifre karmařıklıęı Oracle veritabanlarında “PASSWORD_VERIFY_FUNCTION” içerisinde ařaęıdaki parametreler için gerekli yapılandırmalar tanımlanabilir: <ul style="list-style-type: none"> ○ Kullanıcı adı ile řifrenin aynı olmaması ○ Kullanıcı řifresinin, basit kelimelerin bulunduęu bir listesi ile karřılařtırılarak, “ok basit” olmamasının saęlanması 	
--	--	--

	<ul style="list-style-type: none"> ○ En az bir harf, bir rakam ve bir karakter iermesi ○ Őifrenin, en son kullanılan son u (ya da en az u) Őifreden farklı olması <p>Yukarıda listelenen maddeler, Őifre onaylama fonksiyonu ierisinde özelleŐtirilerek ilave Őifre kontrolleri eklenebilir.</p>		
K3.4	<p>Daha önceki denetim adımlarında temin edilen 'dba_profiles.html' dosyası ieriğindeki aŐağıdaki parametrelerin her kullanıcı hesabına karŐılık gelecek profiller iin tanımlandığı teyit edilir;</p> <ul style="list-style-type: none"> • Zorunlu Őifre deėiŐtirme sıklığı (Őifre ömrü) “PASSWORD_LIFE_TIME” deėerinin belirlendiėi durumlarda, “DBA_USERS” tablosundaki her aktif kullanıcı hesabı iin, ilgili kullanıcı hesabının Őifre ömrü yapılandırması yapılandırılmış bir profile atandığı teyit edilir. (Önerilen deėer: 90 gün ya da daha az) • Hesap kilitlenmeden önce izin verilen yanlış oturum açma denemesi sayısı “DBA_PROFILES” tablosu ierisinde, “FAILED_LOGIN_ATTEMPTS” deėerinin 3 ile 5 arasında olduėu teyit edilir. Bu deėer kullanıcı hesabı kilitlenmeden önce yapılabilecek yanlış oturum açma deneme sayısını gösterir. • Őifrenin kilitli kalacağı süre “DBA_PROFILES” tablosun ierisinde, “PASSWORD_LOCK_TIME” deėerinin en az 1 gün olduėu teyit edilir. Bu deėer “FAILED_LOGIN_ATTEMPTS” (izin verilen en fazla yanlış oturum açma denemesi sayısı) deėeri ulaŐıldıktan sonra hesabın yöneticiler tarafında bir müdahale olmazsa ne kadar kilitli kalacağını tanımlar. • Aynı Őifre tekrar kullanılmadan önce kullanılması gereken farklı Őifre sayısı “DBA_PROFILES” tablosu ierisinde, “PASSWORD_REUSE_MAX” veya “PASSWORD_REUSE_TIME” deėerlerinin belirlenen kullanıcı profilleri iin tanımlandığı teyit edilir. “PASSWORD_REUSE_MAX” deėeri daha önceden kullanılan bir Őifreyi kullanmadan önce en az kaç defa farklı Őifreler kullanılarak Őifre deėiŐikliėi yapılabileceėini belirler. Tavsiye edilen deėer 4 veya daha yüksektir. “PASSWORD_REUSE_TIME” daha önceden kullanılan bir Őifrenin en az kaç gün sonra tekrar kullanılabilceėini belirtir. Tavsiye edilen deėer 365 (gün) veya daha fazlasıdır. • BoŐ Oturum Zaman AŐımı “DBA_PROFILES” tablosu ierisinde belirlenen kullanıcı profilleri iin “IDLE_TIME” deėerinin 30 veya daha az bir deėere atandığı teyit edilir.* Bu deėer kullanıcı hesaplarının oturumu açık iken kaç dakika iŐlem yapılmaması sonrasında sonlandırılacağını belirtir. <p>* Kurum iŐleyici iin belirli kullanıcı hesaplar ve profiller iin zaman aŐımı parametresinin atanmaması beklenebilir (Örn. yazılım ara yüzleri, sistem araçları vb.)</p>	İ	Z

K3.5	<p>Oracle veritabanı dinleyicisi (<i>Oracle database listener</i>) ağ üzerinden veritabanına gönderilen bağlantıları yönetir. Dinleyici, yapısal olarak veritabanı önünde konumlandırıldığından saldırıya maruz kalma riski artmaktadır. Oracle 11g versiyonu ile birlikte dinleyicinin varsayılan davranışı güvenliği arttırmak için diğer makinelerden gelen “<i>lsnrctl</i>” isteklerini reddetmektedir.</p> <p>Örnek olarak;</p> <ul style="list-style-type: none"> - En güvenli = şifre yok, varsayılan. - Daha az güvenli = şifre belirtilmiş. <p>Yerel makinede varsayılan olarak DBA grubuna ait kullanıcılar için şifre kontrolü yapılmaz.</p> <ul style="list-style-type: none"> • “LISTENER.ORA” dosyasının bir kopyası temin edilir ve şifrelerin etkin olup olmadığı ve şifre girişinde şifrelenmiş bir değer olup olmadığı belirlenir. Şifrelenmiş bir şifre mevcut ise aşağıdaki gibi bir parametre gözlemlenir: <pre>PASSWORDS_LISTENER=(<şifrelenmiş değer>)</pre> • “LISTENER.ORA” dosyasının bir kopyası temin edilir ve varsayılan olarak dinlenen portun değiştirilip değiştirilmediği belirlenir. Varsayılan port 1521’dir. Aşağıdaki örnekte LISTENER.ORA dosyasında port ayarının temin edilebileceği kısmın bir örneği yer almaktadır: <pre>LISTENER= (DESCRIPTION= (ADDRESS_LIST= (ADDRESS=(PROTOCOL=tcp)(HOST=sale- server)(PORT=1521)) (ADDRESS=(PROTOCOL=ipc)(KEY=extproc))))</pre> 	İ	Z
K3.6	<p>Oracle veritabanları üzerinde denetleme (auditing) ayarları üzerinden başarısız oturum açma girişimlerinin kaydedildiği teyit edilir:</p> <ul style="list-style-type: none"> • “DBA_STMT_AUDIT_OPTS” tablosu temin edilir: <ul style="list-style-type: none"> ○ “sqlplus” aracı “system” hesabı ile çalıştırılır. ○ Aşağıdaki komutlar SQL penceresine girilir*: <pre>SQL> SET ECHO OFF SQL> SET MARKUP HTML ON SPOOL ON SQL> SPOOL dba_stmt_audit_opts_session.html SQL> SELECT USER_NAME,FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='CREATE SESSION'; SQL> SET MARKUP HTML OFF SQL> SET ECHO ON SQL> SPOOL OFF</pre> ○ Oluşturulan 'dba_stmt_audit_opts_session.html' dosyası temin edilir. • Tüm başarısız oturumların denetlenmesi için yukarıdaki sorgunun, aşağıdaki örnekte görüldüğü gibi “user_name” (kullanıcı adı) alanında boş bir satır çıkarması gereklidir: 	İ	O

USER_NAME	FAILURE		
----- BY ACCESS			
<p>Eğer başarısız oturum açma denemeleri kayıt altına alınmakta ise, aşağıdaki maddeler belirlenir:</p>			
<ul style="list-style-type: none">• Oturum açma girişimleri denetleniyor ise, aşağıdakileri özellikleri değerlendirmek için sistem yöneticisinden aşağıdaki konular ile ilgili bilgi alınır:<ul style="list-style-type: none">○ Başarısız oturum açma girişimlerinin denetlenme sıklığı○ Şüpheli oturum açma girişimlerine ve gerçekten yanlış oturum açma denemelerine yer veren prosedürlerin varlığı○ Başarısız oturum açma girişim raporları dosyalanması ve güvenli bir şekilde saklanması• Başarısız oturum açma girişimlerine ilişkin raporlanan dokümanlar gözden geçirilir. Tekrar eden ve şüpheli başarısız oturum açma girişimleri belirlenir ve ne gibi aksiyonlar alındığı değerlendirilir.			

TASLAK

6.2.3. Ağ Sistemleri

Risk – Kontrol Eşleşmeleri

Riskler	K1	K2	K3
R1. Bilgi sistemleri ağ altyapısı içerisindeki kritik donanımlara yetkisiz erişimlerin görülmesi	+	+	+
R2. Veri kaybı		+	+
R3. Veri sızıntısı		+	+
R4. Bilgi sistemleri üzerinde tutulan verilerin tahrip edilerek bütünlüğünün bozulması		+	
R5. Veri hırsızlığı		+	+
R6. Kısıtlanmayan medya yüklemeleri (dosya paylaşımı, video, ses vb.) sonucunda bilgi sistemleri sürekliliği, performans ve kapasitesini etkileyecek hususların oluşması		+	
R7. Veri trafiği yönlendirmelerinin yanlış yapılandırılması sonucunda performans kaybı oluşması		+	
R8. Zararlı yazılımların bilgi sistemleri ağına sirayet etmesi		+	
R9. Yasadışı içeriklere erişim		+	
R10. Bilgi sistemleri üzerinden geçen ağ trafiğinin içeriğinin yetkisiz kişilerce görüntülenmesi		+	+
R11. Bilgi sistemleri üzerinden şifrelenmeden iletilen kullanıcı adı ve kullanıcı şifrelerinin yetkisiz kişiler tarafından ele geçirilmesi			+

K1 - Ađ ayrıştırması (segmentasyon)

Ađ ayrıştırması; kurum içerisindeki bilgi sistemlerinin bađlı olduđu ađların organizasyon yapısı, i ađ yapısı ya da farklı bir kořula gre her biri ayrı bir gvenlik emberine sahip olacak Őekilde birbirlerinden ayrılmasıdır.

Ađ ayrıştırmasının amacı; bilgi sistemleri ađ gvenliđini ve kullanıcı yetki kontrol seviyesini arttırmaktır. Ađ ayrıştırması ile bir ađ içerisinde meydana gelebilecek sorunların diđer ađlara sirayet etmemesinin nne geilir. Ađ ayrıştırması sayesinde bilgi sistemleri ađı içerisinde kademeli kontroller uygulanabilmektedir. Farklı gvenlik gereksinimleri ve uygun bir risk deđerlendirmesi sonucu bilgi sistemleri ađı mantıksal olarak; dıřarıdan serbeste eriřilebilen sistemler, i ađlar ve kritik varlıklar gibi alanlara ayrıştırılabilir. Ađ ayrıştırmasının bulunmadıđı kurumlarda, ađ ynetimi ve buna bađlı olarak olay/problem ynetimi etkin bir Őekilde yapılamayabilmektedir.

Kurum içerisinde bilgi sistemleri ađ altyapısı; kurumun eriřim ve ađ gvenliđi politikaları ile uyumlu bir Őekilde yapılandırılmalıdır. Ađ ynetim sistem ve cihazları zerinde tanımlı kullanıcı yetkileri gncel ve kurumun yetki ve eriřim kurallarına uygun olarak atanmalıdır.

TASLAK

Denetim Prosedürleri

#	Denetim prosedürleri	T/İ	Z/O
K1.1	Kurumun bilgi sistemleri ağ altyapısı yapılandırmasına ilişkin politika ve prosedürler temin edilerek fiziksel ya da sanal ağ ayrıştırmasının varlığı gözlemlenir.	T	Z
K1.2	Kurum içerisinde bir ağ ayrıştırması mevcut ise bilgi sistemleri ağı şemalarında bu durumun gösterildiği teyit edilir.	İ	Z
K1.3	Kurum bilgi sistemleri ağ altyapısı üzerinde ağ ayrıştırmasına ilişkin yapılan kural ve altyapı değişikliklerinin kontrollü gerçekleştirildiği ve düzenli olarak gözden geçirildiği teyit edilir. <i>(Bkz: 6.3 Ağ Sistemleri - K2. Ağ cihazları güvenliği)</i>	İ	Z
K1.4	Bilgi sistemleri ağ altyapısı sistemleri üzerinde tanımlı kullanıcı yetkileri temin edilip, kullanıcı yetkilendirmelerinin ağ şemasına uygun biçimde yapıldığı teyit edilir. <i>(Bkz: 4.2 Güvenlik Hizmetleri Yönetimi ve 6.3 Ağ Sistemleri - K2. Ağ cihazları güvenliği)</i>	İ	Z
K1.5	Bilgi sistemleri ağ altyapısı sistemleri üzerindeki kullanıcı yetkilerinin düzenli aralıklarla gözden geçirildiği teyit edilir. <i>Bkz: 4.2 Güvenlik Hizmetleri Yönetimi ve 6.3 Ağ Sistemleri - K2. Ağ cihazları güvenliği)</i>	İ	Z

K2 - Ağ cihazları güvenliği

Dışarıya açık olan bilgi sistemlerinde güvenlik duvarları (*firewall*), saldırı tespit sistemleri (*intrusion detection system - IDS*), saldırı önleme sistemleri (*intrusion prevention systems – IPS*) genelde dış ağlar ile kurum ağı arasındaki ilk savunma hattıdır. Bu sistemler üzerinde yalnızca olması gereken servislerin ve ağ kanallarının açık tutulması ve güvenlik riski doğurabilecek gereksiz diğer tüm servislerin kapalı olması gerekmektedir. Güvenlik duvarlarının yapılandırmasının yanlış veya eksik olması, tüm bilgi sistemleri ağı üzerindeki güvenlik riskini arttırmaktadır.

Kurum içerisindeki bilgi sistemlerinin, yerel ağların birbirleriyle ve kurum dışı ağlar ile arasındaki veri akış trafiğini yöneten yönlendirici (*router*) ve anahtarlar (*switch*) gibi cihazların yönetimi, kurumun dâhili ve harici tehdit risklerini yönetmesinde önde gelen faktörlerden biridir. Kurumun; kendi iç ağları ve harici ağlar arasında kurduğu veri trafiği güvenliğinin sağlanamaması, aradaki adam saldırısı (*man in the middle attack*) ya da kritik veri ve bilgilere yetkisiz erişimlerin görülmesi gibi ciddi bilgi güvenliği açıkları doğurabilir.

Ağ cihazları güvenliği başlığı altında aşağıdaki kontroller uygulanabilir:

- Güvenlik duvarı, sızma tespit ve sızma önleme sistemleri gibi güvenlik cihazlarının konumu ve yönlendirici (*router*) ve anahtarların (*switch*), kurumun bilgi sistemleri ağ topolojisi içerisinde uygun şekilde yapılandırılmıştır.
- Bilgi sistemleri ağlarına dâhil olan cihazlar veya ağ yazılımlarının tüm güvenlik ayarları güncel, etkin ve kurum standartlarına uygun şekilde tanımlanmıştır.
- Ağ cihazlarının ayarları kurum ihtiyaçlarını karşılayacak ve en performanslı çalışacak şekilde; minimum kural sayısı ve karmaşıklığı ile tanımlanmıştır.
- Ağ cihazları üzerinde gerçekleştirilen kural değişiklikleri, yapılandırmalar ve yamalar kontrollü şekilde gerçekleştirilmekte ve düzenli aralıklarla gözden geçirilmektedir.
- Ağ cihazları, kurumun bilgi sistemleri ağı dışından gelecek siber saldırılara karşı gerekli alarm ve uyarı mekanizmalarına sahiptir.

Denetim Prosedürleri

#	Denetim prosedürleri	T/İ	Z/O
K2.1	Bilgi sistemleri ağı şemasının temin edilerek tüm ağ cihazlarının konumunun uygun şekilde yapılandırıldığı kontrol edilir.	T	Z
K2.2	Ağ cihazları ile ilgili varsayılan yapılandırma ve güvenlik ayarlarının tanımlandığı politika temin edilerek, bu politikanın kurum hedeflerine, ihtiyaçlarına ve varsa yasal gereksinimlere uygun, güncel ve onaylı olduğu kontrol edilir.	T	Z
K2.3	Ağ cihazları yönetim konsolu üzerindeki ağ adreslerini tanımlayan IP (<i>Internet Protocol</i>) ve içerik filtreleme ayarlarının yanı sıra alarm ve bildiri gibi tanımlamaların ilgili güvenlik politikası ile uyumluluğu gözlemlenir.	T	Z
K2.4	Güvenlik duvarı üzerinde tanımlı güvenlik parametrelerine ilişkin varsayılan değerlerde her zaman tüm kanalları ve servisleri reddedecek şekilde (<i>DENY ALL</i>) yapılandırılmış olduğu; istisnaların (<i>exception</i>) ise bu varsayılan değer üzerine tanımlandığı gözlemlenir.	İ	Z
K2.5	Ağ cihazları yapılandırılması ve kural değişikliklerinin düzenli olarak gözden geçirildiği gözlemlenir.	İ	Z
K2.6	Ağ cihazları yönetim konsolu üzerindeki şifre politikalarının, kurumun şifre standartları politikası ile uyumluluğu kontrol edilir.	İ	Z
K2.7	Ağ cihazları üzerinde tanımlı kullanıcıların listesi temin edilir ve örneklemeler üzerinden mevcut erişim yetkileri ilgili güvenlik politikalarına uygunluğu kontrol edilir.	İ	Z
K2.8	Ağ cihazları üzerindeki sürüm ve yama listesi kayıtları temin edilerek denetim dönemi içerisinde gerçekleşen yapılandırma değişiklikleri ve yamalar arasından rastgele örneklemeler seçilir. Bu örneklemelere karşılık gelen kural değişikliği talepleri ve onay dokümanları temin edilerek kontrol sürecine uygunluğu incelenir.	İ	Z
K2.9	Ağ cihazları yönetim konsolundan kurum bilgi sistemleri üzerinde meydana gelen şüpheli trafiğe karşı üretilen alarm kurallarının tanımlandığı gözlemlenir. Ek olarak, ilgili alarmlar aracılığı ile bilgilendirilen kişilerin yeterliliği ve uygunluğu teyit edilir.	İ	Z
K2.10	Şüpheli ağ trafiği sonucu üretilen alarm raporlarının ve bildirimlerin kaydedildiği teyit edilerek düzenli aralıklarla gözden geçirildiği teyit edilir.	İ	Z
K2.11	Güvenlik duvarı üzerindeki varsayılan güvenlik ayarlarının ve tanımlı varsayılan kullanıcıların uygun şekilde değiştirildiği kontrol edilir.	İ	Z

K3 - Güvenli iletişim

Bilgi sistemleri aracılığı ile kurum içi ve dışı kişilerle, ya da diğer kurumlar ile gizlilik açısından kritik olarak tanımlanan verileri içeren yazışma, iletişim, aktarım ve paylaşım gibi işlemler; ilgili veri sınıfına uygun olarak güvenli bir ortam aracılığı ile gerçekleştirilir. Güvenli olmayan bir bilgi sistemleri ağı üzerinden yapılan bu gibi işlemler, aktarılan verilerin yetkisiz kullanıcılar tarafından görüntülenmesine ve veri sızıntısına olanak sağlar.

Güvenli iletişim başlığı altında aşağıdaki kontroller uygulanabilir:

- Bilgi sistemleri ağı üzerindeki veri haberleşme kanallarının güvenliği ile ilgili politika ve prosedürler kurum hedeflerine, ihtiyaçlarına ve varsa yasal gereksinimlere uygun, güncel ve onaylıdır.
- Bilgi sistemleri ağı üzerinde iletilen veriler, gizlilik seviyelerine göre sınıflandırılmış ve ilgili sınıflar için aktarım sırasında kullanılacak şifreleme yöntemleri tanımlanmıştır.
- Bilişim sistemleri ağına dahil olan tüm donanım ve yazılımlar, kurum yönetimi tarafından belirlenen BT güvenlik politikalarına uyumludur.
- Bilgi sistemleri aracılığı ile kimlik doğrulama amaçlı iletilen kullanıcı adı ve kullanıcı şifresi gibi bilgiler ağ üzerinde şifreli olarak iletilir.
- Bilgi sistemleri ağı üzerindeki veri trafiği, yalnızca yetkili kullanıcılar tarafından yönetilmektedir.

Denetim Prosedürleri

#	Denetim prosedürleri	T/İ	Z/O
K3.1	Bilgi sistemleri ağı üzerindeki veri haberleşme kanallarının güvenliği ile ilgili politika ve prosedürlerin güncelliği ve onaylı olduğu teyit edilir.	T	Z
K3.2	Bilişim sistemleri ağına dâhil olan tüm donanım ve yazılımların kurum yönetimi tarafından belirlenen BT güvenlik politikalarına uyumluluğu kontrol edilir.	T	Z
K3.3	Bilgi sistemleri aracılığı ile kurum içi ve dışı kişilerle, ya da diğer kurumlar ile gizlilik açısından kritik olarak tanımlanan verileri içeren yazışma, iletişim, aktarım ve paylaşım gibi işlemlerin; ilgili veri sınıfına uygun olarak güvenli bir ortam aracılığı ya da şifreleme yöntemi ile gerçekleştirildiği teyit edilir.	T	Z
K3.4	Diğer kurum ve kişiler ile gerçekleştirilen veri paylaşımı ve veri aktarımlarına ilişkin yöntemlerin ve gizlilik anlaşmaları gibi protokollerin mevcut olduğu gözlemlenerek söz konusu verilerin güvenlik, hassasiyet ve kritiklik seviyelerinin tanımlı olduğu teyit edilir.	T	O
K3.5	Çevrimiçi işlemler için vatandaş ya da kurum çalışanlarına ait özlük bilgileri gibi gizli veriler; mevcut yasa ve mevzuatlarla uyumlu şekilde iletilir.	İ	O
K3.6	Bilgi sistemleri üzerinden kimlik doğrulama amaçlı iletilen kullanıcı adı ve kullanıcı şifresi gibi bilgilerin ağ üzerinde şifreli olarak iletildiği teyit edilir.	İ	Z
K3.7	Bilgi sistemleri ağı aracılığı ile aktarılan şifrelenmiş verilerin, AES (<i>Advanced Encryption Standard</i>) gibi güçlü algoritmalar aracılığı ile şifrelendiği teyit edilir.	İ	O

6.2.4. Uzaktan erişim

Uzaktan erişim yetkileri, kullanıcıların fiziksel olarak kurum ağı dışında iken, bu amaç için yapılandırılmış uzaktan erişim istemcileri (*remote access client*) sayesinde Internet üzerinden kurum ağı içerisindeki sistemlere bağlanarak çalışmalarına olanak sağlamaktadır. Kurum bilgi sistemleri üzerinde tanımlanan uzaktan erişim yetkilerinin operasyonel açıdan daha fazla verimlilik sağlaması ile beraber bu erişimlerin kontrollü ve güvenli bir ortamda gerçekleştirilmesi ve kötü niyetli kişilerin yetkisiz erişim girişimlerine ve siber saldırılar aracılığıyla bilgi sızmalarına karşı kapsamlı önlemlerin alınabilmesi ile mümkündür.

Uzaktan erişim başlığı altında aşağıdaki kontroller gözlemlenebilir:

- Uzaktan erişim politikaları kurum hedeflerine, ihtiyaçlarına ve varsa yasal gereksinimlere uygun, günceldir.
- Uzaktan erişim yetkileri ek onaya istinaden tanımlanır.
- Uzaktan erişim sistemleri güvenli bir ağ yapısı içerisinde konumlandırılmıştır.
- Uzaktan yetkisiz erişim saldırılarına ilişkin alarm ve rapor mekanizmaları yapılandırılmıştır ve uzaktan erişim girişimleri kayıt altına alınarak düzenli aralıklarla gözden geçirilmektedir.

Risk – Kontrol Eşleşmeleri

Riskler	K1	K2	K3
R1. Bilgi sistemleri ağ altyapısı içerisindeki kritik donanımlara yetkisiz erişimlerin görülmesi	+	+	+
R2. Veri kaybı		+	+
R3. Veri sızıntısı		+	+
R4. Bilgi sistemleri üzerinde tutulan verilerin tahrip edilerek bütünlüğünün bozulması		+	
R5. Veri hırsızlığı		+	+
R6. Kısıtlanmayan medya yüklemeleri (dosya paylaşımı, video, ses vb.) sonucunda bilgi sistemleri sürekliliği, performans ve kapasitesini etkileyecek hususların oluşması		+	
R7. Veri trafiği yönlendirmelerinin yanlış yapılandırılması sonucunda performans kaybı oluşması		+	
R8. Zararlı yazılımların bilgi sistemleri ağına sirayet etmesi		+	
R9. Yasadışı içeriklere erişim		+	
R10. Bilgi sistemleri üzerinden geçen ağ trafiğinin içeriğinin yetkisiz kişilerce görüntülenmesi		+	+
R11. Bilgi sistemleri üzerinden şifrelenmeden iletilen kullanıcı adı ve kullanıcı şifrelerinin yetkisiz kişiler tarafından ele geçirilmesi			+

Denetim Prosedürleri

#	Denetim prosedürleri	T/İ	Z/O
K1.1	Bilgi sistemleri uzaktan erişim politikası ve uzaktan erişim yetkisine sahip kullanıcı listesi temin edilerek, kurum yönetimi tarafından onaylı ve güncel olduğu gözlemlenir.	T	Z
K1.2	Bilgi sistemlerine uzaktan erişimler sırasında kullanılan kullanıcı doğrulama mekanizmalarının kurumun bilgi güvenliği politikasına uygun yapılandırıldığı kontrol edilir.	T	Z
K1.3	Bilgi sistemleri ağına uzaktan erişimler sırasında kullanıcının bildiği bir parolanın yanı sıra, sahip olduğu değişken şifreler ile (SMS, değişken parola üretici aygıtlar "token" vb araçlar ile) erişim yapabildiği teyit edilir. (The Institute of Internal Auditors, 2007)	İ	O
K1.4	Bilgi sistemleri güvenlik donanımı ve ağ cihazlarının kurumun bilgi sistemleri ve uzaktan erişim politikalarına uygun yapılandırıldığı gözlemlenir. (Bkz: 6.3 Ağ Sistemleri - K2. Ağ cihazları güvenliği)	T	Z
K1.5	Bilgi sistemleri veritabanları, işletim sistemleri ve ağ cihazları gibi bilgi güvenliği ve denetim açısından kritik sistemler üzerinde denetim dönemi içerisinde uzaktan erişim yetkisi tanımlanan kullanıcıların listesi içerisinde örnek kullanıcılar seçilerek ilgili kullanıcılara ait yetkilendirmenin kontrollü ve ilgili sürece uygun olarak gerçekleştirildiği gözlemlenir.	İ	Z
K1.6	Denetim dönemi için kurumun bilgi sistemleri üzerinde gerçekleştirilen uzaktan erişimlere ilişkin denetim izleri temin edilerek kullanıcıların uygunluğu test edilir.	İ	Z

Ek Kaynaklar

- Bankacılık Düzenleme ve Denetleme Kurumu. (2010, 06 01). BANKALARDA BİLGİ SİSTEMLERİ YÖNETİMİNDE ESAS ALINACAK İLKELERE İLİŞKİN TEBLİĞ.
- Hafele, S. I.-D. (2004, February 23). Three Different Shades of Ethical Hacking: Black, White and Gray.
- International Organization for Standardization(ISO)-International Electrotechnical Commission(IEC). (2005). ISO/IEC 20000. Geneva, Switzerland, Europe.
- International Organization for Standardization(ISO)-International Electrotechnical Commission(IEC). (2005, October). ISO/IEC 27001:2005-Information Technology-Security Techniques-Information Security Management Systems-Requirements. Geneva, Switzerland, Europe.
- International Standards Organization. (2012, 05 15). Societal security – Business continuity management systems - Requirements. Geneva, Switzerland.
- ISACA. (2007). COBIT 4.1 Framework. Rolling Meadows, Illinois, United States of America.
- ISACA. (2012). COBIT 5 Enabling Processes. Rolling Meadows, Illinois, United States of America.
- Kotter, J. (1996). Leading Change. Boston, Massachusetts, USA.
- The Institute of Internal Auditors. (2008, July). Business Continuity Management. Altamonte Springs, Florida.
- The Institute of Internal Auditors. (2012, March). Global Technology Audit Guide (GTAG) 2 Change and Patch Management Controls: Critical for Organizational Success 2nd Edition.
- The Institute of Internal Auditors. (2007, November). Global Technology Audit Guide (GTAG) Identity and Access Management. Altamonte Springs, Florida, USA.
- The Institute of Internal Auditors. (2012, March). Global Technology Audit Guide (GTAG®) 1 Information Technology Risk and Controls 2nd Edition.
- The Institute of Internal Auditors. (2007, November). Identity and Access. Altamonte Springs, FL, US.
- UK Cabinet Office. (2011). ITIL Service Design. Norwich, United Kingdom.
- UK Cabinet Office. (2011). ITIL Servis Transition. Norwich, UK.
- UK Cabinet Office. (2009). Projects in Controlled Environment(PRINCE 2). Norwich, United Kingdom.