VERSİYON 1.0

Kamu Bilgi Teknolojileri Denetimi Rehberi

İç Denetim Koordinasyon Kurulu

ANKARA |Ocak 2014

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

SUNUŞ

Bilgi teknolojileri ve iletişim alanındaki gelişmeler ve bilgi toplumuna geçiş sürecindeki gereklilikler kamu idarelerimizi de önemli şekilde etkilemekte ve faaliyetler düne göre daha fazla bilgi teknolojileri üzerinden yürütülmektedir. Bilgi teknolojileri kullanımına yönelik olarak önemli miktarlarda kamu yatırımları yapılmaktadır. Bilgi teknolojilerinin kullanımına yönelik bu hızlı trend, beraberinde bilgi teknolojilerinin barındırdığı risklerin yönetimi sorununu da gündeme getirmektedir. İşte iç denetimin önemi burada ortaya çıkmakta ve iç denetim birimlerinin, idarelerin kullandığı bilgi teknolojilerinin barındırdığı risklerin ne şekilde yönetildiği konusunda üst yöneticilerine güvence vermesi gerekmektedir.

İşlemlerini büyük ölçüde bilgi teknolojilerine dayalı olarak gerçekleştiren kamu idarelerinde, bilgi teknolojileri kullanımından kaynaklanan risklerin değerlendirilebilmesi, bilgi teknolojilerine ilişkin iç kontrollerin yeterliliği ve etkinliği hakkında bir değerlendirmede bulunulabilmesi ve uygunluk, mali, performans ve sistem denetimlerinden daha anlamlı sonuçlar elde edilebilmesi için bilgi teknolojileri denetimi yöntemlerinden yararlanılması gerekmektedir. Ayrıca, hem genel kabul görmüş uluslararası iç denetim standartları hem de Kamu İç Denetim Standartları, denetimler sırasında bilgi teknolojilerine yönelik risklerin de mutlaka değerlendirilmesini zorunlu kılmaktadır.

5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu gereğince iç denetim alanında merkezi uyumlaştırma görev ve fonksiyonu, İç Denetim Koordinasyon Kurulu (İDKK) tarafından yerine getirilmektedir. Bu fonksiyon kapsamında İDKK; standart ve yöntemleri belirlemek, gerekli mevzuat düzenlemelerini yapmak, koordinasyonu sağlamak, rehberlik ve eğitim hizmeti vermekle görevli ve yetkilidir.

Bu Rehber, 5018 sayılı Kanunun 67 nci maddesi ile İç Denetçilerin Çalışma Usul ve Esasları Hakkında Yönetmeliğin 7, 8, 10, 14, 36, 37 ve 55 inci maddelerine dayanılarak hazırlanmış ve İDKK'nın 22.01.2014 tarih ve 1 sayılı Kararıyla kabul edilmiştir. İç denetim birimleri, yürüttükleri iç denetim faaliyetlerinde bu Rehberle belirlenen esas ve yöntemlere uyarlar. Ayrıca, kavramsal birliğin tesis edilmesi amacıyla Rehbere, Terimler Sözlüğü eklenmiştir. Rehber, iç denetçilerin denetim yeteneklerini sınırlamaz ve iç denetim uygulamalarının geliştirilmesine engel teşkil etmez. İç denetim birimleri, ihtiyaç duymaları halinde ilave politika ve prosedürler belirleyebilir ve bunların bir örneğini de İDKK'ya gönderirler.

Kapsamlı bir çalışmanın ürünü olan bu Rehber, İDKK'nın web sitesinde görüşe açılmış, gelen görüş ve öneriler dikkate alınarak Rehbere son şekli verilmiştir. Rehberin, idarelerimizde yürütülen bilgi teknolojileri denetimi faaliyetlerine ivme kazandıracağına ve bu kapsamda yapılacak denetim sonuçlarıyla da bilgi teknolojilerinin kullanımından kaynaklanan risklerin yönetimine önemli oranda katkı yapılacağına inanıyorum.

İ.İlhan HATİPOĞLU

İç Denetim Koordinasyon Kurulu Başkanı

KISALTMALAR

Kısaltma	Tanım
AD	Active Directory (Aktif Dizin)
AES	Advanced Encryption Standard (İleri Şifreleme Standardı)
AI	Acquire & Implement (Edinim ve Kurulum, COBIT 4.1 etki alanı)
AICPA	American Institute of Certified Public Accountants (Amerikan Yeminli Mali Müşavirler Enstitüsü)
ANSI	American National Standards Institute (Amerikan Ulusal Standartlar Enstitüsü)
BAI	Build Acquire and Implement (Kur, Edin ve Uygula, COBIT 5 etki alanı)
BGYS	Bilgi Güvenliği Yönetim Sistemi
BT	Bilgi teknolojileri
CD	Compact Disc (Kompakt Disk)
CGEIT	Certified in the Governance of Enterprise IT (Kurumsal BT Yönetişim Sertifikası)
CIA	Certified Internal Auditor (Sertifikalı İç Denetçi)
CIPP	Certified Information Privacy Professional (Sertifikalı Bilgi Gizliliği Uzmanı)
CISA	Certified Information Systems Auditor (Uluslararası Sertifikalı Bilgi Sistemleri Denetçisi)
CISM	Certified Information Security Manager (Sertifikalı Bilgi Güvenliği Yöneticisi)
CISSP	Certified Information Systems Security Professional (Sertifikalı Bilgi Sistemleri Güvenlik Uzmanı)
COBIT	Control Objectives for IT and related Technologies (Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri)
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRISC	Certified in Risk and Information Systems Control (Sertifikalı Risk ve Bilgi Sistemleri Kontrolleri Uzmanı)
CRMA	Certification in Risk Management Assurance (Risk Yönetimi Güvence Sertifikası)
DBA	Database Administrator (Veritabanı Yöneticisi)
DES	Data Encryption Standard (Veri Kriptolama Standartı)
DGS	Denetim Gözetim Sorumlusu
DMZ	Demilitarized Zone
DS	Delivery & Support (Hizmet Sunumu ve Destek, COBIT 4.1 etki alanı)
DSS	Deliver, Service and Support (Hizmet Sunumu ve Destek, COBIT 5 etki alanı)
DVD	Digital Versatile Disc (Sayısal Çok Yönlü Disk)
EDM	Evaluate, Direct and Monitor (Değerlendir, Yönlendir ve İzle, COBIT 5 etki alanı)
FIPS	Federal Information Processing Standards
GAIT	Guide to the Assessment of IT Risk (BT Riski'nin Değerlendirilmesi Rehberi)
GIAC	Global Information Assurance Certification (Küresel Bilgi Güvencesi Sertifikası)
GTAG	Global Technology Audit Guides (Küresel Teknoloji Denetimi Rehberleri)
HR	Human Resources (İnsan Kaynakları)

Kısaltma	Tanım
HSA	Hizmet Seviyesi Anlaşması
IAPP	International Association of Privacy Professionals (Uluslararası Gizlilik Uzmanları Birliği)
İDB	İç Denetim Birimi
İDB Başkanı	İç Denetim Birimi Başkanı
İDKK	İç Denetim Koordinasyon Kurulu
IDS	Intrusion Detection System (Saldırı Tespit Sistemleri)
IEC	International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)
IIA	The Institute of Internal Auditors. (İç Denetim Enstitüsü)
IP	Internet Protocol
İSA	İşletim Seviyesi Anlaşmaları
ISACA	Information Systems Audit and Control Association (Bilgi Sistemleri Denetim ve Kontrol Derneği)
ISC^2	International Information Systems Security Certification Consortium (Uluslararası Bilgi Sistemleri Güvenliği Sertifikasyon Konsorsiyumu)
ISO	International Organization for Standardization (Uluslararası Standardizasyon Teşkilatı)
ITAF	IT Assurance Framework (BT Güvence Çerçevesi)
ITGI	IT Governance Institute (BT Yönetişim Enstitüsü)
ITIL	Information Technology Infrastructure Library (Bilgi Teknolojileri Altyapı Kütüphanesi)
KİDR	Kamu İç Denetim Rehberi
KİDS	Kamu İç Denetim Standartları
KRP	Kurumsal Risk Puanı
LDAP	Lightweight Directory Access Protocol (Basit Dizin Erişim Protokolü)
MD5	Message-Digest Algorithm 5
ME	Monitor & Evaluate (İzleme ve Değerlendirme, COBIT 4.1 etki alanı)
ÖD	Önerilen Değer
OE	Order Entry
PDA	Personal Digital Assistant
PO	Plan & Organize (Planlama ve Organizasyon, COBIT 4.1 etki alanı)
SH	Sales History
SQL	Structured Query Language
SSAS	SQL Server Analiz Servisleri
SY	Süreklilik Yönetimi
ÜG	Üzerinden Gitme
UPS	Uninterrupted Power Supply (Kesintisiz güç kaynağı)
URP	Uygulama Risk Puanı
USB	Universal Serial Bus
VPN	Virtual Private Network

Bilgi Teknolojileri Denetimi 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 idareleri, teknolojideki söz konusu gelişmelere paralel olarak hızlı bir değişim sürecinden geçmektedir. Bu çerçevede hem diğer idarelere 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 idareleri 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. Kamu BT Denetimi Rehberi (Rehber), kamu idarelerinde Bilgi Teknolojileri Denetimi gerçekleştirilmesi sırasında izlenmesi ve uygulanması gereken metodoloji ve denetim testleri ile ilgili bir yöntem sunmaktadır. Rehber'in amacı, iç denetim birimlerinin (İDB) idarelerinde 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 iç denetimi ihtiyaçları ve BT denetim kapasitesi dikkate alınarak özellikle pratik ve uygulanabilir bir düzenleme yapılması gözetilmiştir.

Kamuda BT denetimi uygulamalarının hayata geçirilmesiyle birlikte, aşağıda belirtilen faydaların ortaya çıkmasının mümkün olacağı düşünülmektedir:

- BT kullanımından kaynaklanan risklerin kurum bazında değerlendirilmesi,
- Kurumlarda BT kontrol ortamının etkinliğinin araştırılarak kontrollere ilişkin eksikliklerin ve iyileştirme fırsatlarının tespit edilmesi,
- Tespit edilen bulgu ve önerilerden hareketle kurumların BT stratejilerine girdi sağlanması,

- BT yönetişimi ve BT yönetimi alanlarında dünya ve ülke çapında kabul gören öncü uygulamaların hayata geçirilmesine destek sağlanması,
- Bilgi güvenliği, veri gizliliği vb. hususlarda mevzuat uyumluluğunun sağlanmasına destek verilmesi,
- Gerçekleştirilecek denetimler neticesinde, yürütülmekte olan üst seviye programlara (örneğin siber güvenlik inisiyatifi) girdi sağlanabilmesi,
- BT kontrollerinin önemine ilişkin farkındalık düzeyinin ve kontrol bilincinin arttırılması,
- Kamu iç denetiminde bütünleşik denetim yaklaşımının benimsenmesine destek sağlanması ve diğer denetim türlerinin etkinliğinin arttırılması,
- İDB'lerin BT denetim kapasitesinin geliştirilmesi.

Rehber'in Yapısı ve Özellikleri

Rehber'in yapısı

Rehber 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 kontrolleri ile yönetişim kontrollerine ve bunlar ile ilgili denetim testlerine yer verilmektedir.
- Bölüm 4'de; BT Yönetim Süreçlerine ilişkin denetim yaklaşımı ele alınmakta ve bu süreçlere ait BT genel kontrollerine ve ilgili denetim testlerine 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 testlerine yer verilmektedir.

Rehberin özellikleri

Rehber, Kamu İç Denetim Rehberi'ne (KİDR) uyumlu olacak şekilde hazırlanmış olup, KİDR'da ele alınan iç denetim yaklaşımının ve ortak terminolojinin gözetilmesine azami özen gösterilmiştir. Buna paralel olarak Rehber, ağırlıklı olarak bilgi teknolojilerine özgü hususlara yoğunlaşmış olup, KİDR'la belirlenen 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 İDB'lerin 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 testleri
- Ek kaynaklar

Belirtilen detaylar, her kurumda genel anlamda uygulanması mümkün olabilecek temel ve yaygın denetim testlerini içermekle birlikte Rehber'deki yaklaşım, gerektiğinde ilave risk ve kontrollerin ele alınmasına, belirtilenlerden farklı denetim testlerinin ve tekniklerinin uygulanmasına ve ilave kaynaklara başvurulabilmesine imkân tanıyacak şekilde hazırlanmıştır. Böyle bir ihtiyaç duyulması halinde Rehber içerisinde ilgili bölümlerin sonunda yer verilen "**Ek Kaynaklar**"da referans olarak belirtilen standartlara ve çerçevelere başvurulması uygun olacaktır.

Rehberin kullanımı ile ilgili olarak aşağıdaki hususlara dikkat edilmesi önerilmektedir:

- BT denetimi birçok noktada iç 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 teknolojileri 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, Rehber'de 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/denetim için ilgili bölümlerde belirtilen "**Ek Kaynaklar**"ın kullanılması ve denetim testlerinin denetim amacına uygun olarak detaylandırılması konusu, yetkin bir iç denetçi tarafından değerlendirilmelidir.
- Rehber'in etkin bir şekilde uygulanması için denetimi gerçekleştirecek denetçinin iç denetim tecrübesine sahip olmasının yanı sıra, temel düzeyde bir BT denetimi eğitimini de tamamlaması beklenmektedir. Rehber'deki daha ileri düzey konular için ileri düzey ve uygulamalı eğitimlerin ve buna ek olarak eğitim amaçlı pilot denetimlerin de gerçekleştirilmesi önerilir. Rehber bir denetim yöntemi sunmakta olup, Rehber'i kullanacak iç denetçilerin almaları gereken eğitimleri ve denetimde saha tecrübesini tek başına ikame etme amacını taşımamaktadır. Rehber'in etkin kullanımı için birinci bölümde de bahsi geçen yetkinliklere sahip olmak tavsiye edilmektedir.

Bu çerçevede Rehber'i kullanarak denetim faaliyeti yürütecek iç denetçilerin, Rehber'in her bir bölümü için sahip olmaları beklenen genel asgari yetkinlik seviyelerine (YS) aşağıdaki tabloda yer verilmektedir:

Tablo 1 – Rehber bölümleri ve yetkinlik düzeyi ilişkisi

Rehber bölümleri	**Artan Yetkinlik Seviyesi (+)**			
	Tanımlar ve Esaslar	Zorunlu Denetim Adımları	Seçeneğe Bağlı Denetim Adımları	Detay Referanslar
Bölüm 1: BT Denetimi Temel Kavramlar				
Bölüm 2: BT Denetim Metodolojisi				
Bölüm 3: BT Kurum Seviyesi ve Yönetişim Süreçleri Denetimi				
Bölüm 4: BT Genel Kontrolleri (Yönetim Süreçleri) Denetimi				
Bölüm 5: BT Uygulama Kontrollerinin Denetimi				
Bölüm 6: BT Genel Kontrolleri (BT Altyapı) Denetimi				

Gerekli asgari yetkinlik düzeyi	**1. Seviye (Başlangıç)**	**2. Seviye (Gelişmekte)**	**3. Seviye (Uzman)**	**Uygulanabilir Değil**

Yukarıda belirtilen gerekli asgari yetkinlik düzeyleri için beklentiler kısaca şu şekilde özetlenebilir:

- 1.Seviye (Başlangıç seviyesi): Kamu idarelerinde iç denetim faaliyetlerinde bulunmuş ve Temel BT Denetimi Eğitimi'ne katılmış iç denetçinin bulunduğu seviye olarak tarif edilebilir.

- 2.Seviye (Gelişme olan seviye): Kamu idarelerinde iç denetim faaliyetlerinde bulunmuş ve Temel BT Denetimi ve İleri BT Denetimi Eğitimlerine katılmış ve kamu kurumlarında en az 1-2 yıl BT denetimi çalışmalarında bulunmuş iç denetçinin bulunduğu seviye olarak tarif edilebilir.
- 3.Seviye (Uzman seviyesi): CISA sertifikasına sahip ya da sınavı almaya hazır seviyede gerekli eğitimlerini tamamlamış, BT denetimi alanında en az 2-3 yıl tecrübeye sahip iç denetçinin bulunduğu seviye olarak belirtilebilir.

Yukarıda genel hatlarıyla verilmiş olan sınıflandırmaya ek ve paralel olarak, Bölüm 3'ten itibaren Rehber içinde yer alan detay denetim testlerinin her biri belirtilen sınıflandırmaya tabi tutulmuş ve **1/2/3** numaraları kullanılarak ilgili detay denetim testinin hangi yetkinlik seviyesince uygulanabileceği ayrıca belirtilmiştir. Söz konusu yetkinlik değerlendirmesi, iç denetçilere yol gösterici olarak hazırlanmış olup, her denetim ortamının kendi karmaşıklık seviyesi de planlamada mutlaka göz önünde bulundurulmalıdır.

1. BİLGİ TEKNOLOJİLERİ DENETİMİ 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 durum 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 bir "**bütünleşik denetim**" çerçevesinde de yürütülebilir.

1.2. BT denetiminin uygulama alanları

Yukarıda belirtilen hedefler doğrultusunda, BT denetimi aşağıda listelenmiş farklı denetim türlerinin biri veya birkaçı ile bütünleşik olarak gerçekleştirilebilir. Bilgi teknolojilerine ilişkin kontroller, iç kontrol sisteminin önemli bir parçası olduğu için, söz konusu bütünleşik denetimlerde de BT kontrollerinin incelenmesi önemli bir yer tutar. Ayrıca BT denetimi, bütünleşik denetimlerin haricinde tek başına ayrı bir kapsamla da yürütülebilir. Bilgi sistemlerinin güvenliğinin denetimi amacıyla gerçekleştirilebilen denetimler buna bir örnek olup, bu konu Rehber'de ayrı bir kapsam örneği (güvenlik denetimi) olarak incelenmiştir.

1.2.1. Sistem denetimi

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 bir 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 güvenceyle, süreç kontrollerinde yürütülecek çalışmalarda ve harcanacak iş gücünde tasarruf edilmesi mümkün olabilir. Bu çerçevede BT kontrollerinin denetlenmesi, iç kontrol sistemi üzerindeki denetim stratejisini etkileyen önemli bir faktördür.

1.2.2. Performans denetimi

Performans denetimi, yönetimin bütün kademelerinde gerçekleştirilen faaliyet ve işlemlerin planlanması, uygulanması ve kontrolü aşamalarındaki etkililiğin, ekonomikliğin ve verimliliğin değerlendirilmesidir.

Bu çerçevede yürütülecek BT denetimi çalışmaları, 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 performansı üzerindeki etkisi de değerlendirilebilir. BT yönetişimi 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.

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 değerlendirilmesini gerektirmenin yanında, mali denetimin niteliğini, zamanlamasını ve kapsamını da etkiler.

1.2.4. Uygunluk denetimi

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 denetlenmesine 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 denetimler de, bilgi teknolojileri denetimini içeren birer uygunluk denetimi olarak ele alınabilir.

1.2.5. Güvenlik denetimi

Bilgi teknolojileri denetimi yukarıda listelenmiş denetim uygulamalarına ek olarak, müstakil bir şekilde 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 yapılandırmalarının uygunluğu, denetim izlerinin oluşturulması ve takibi, güvenlik olaylarının yönetimi vb. alanlarda değerlendirme çalışmaları yürütülür. Bu kapsamdaki 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 türleri kapsamı içerisinde de değerlendirilmektedir.

1.3. Mesleki etik kurallar

Etik kurallar, bireylerin ve kuruluşların davranışlarını düzenleyen ilkeleri ve beklentileri belirtir. Risk yönetimi, kontrol ve yönetişim konularında güvence/denetim çalışmalarının güven üzerine kurulu olmasından dolayı, iç denetçinin de birincil görevi çalışmalarında etik kurallara uygun hareket etmektir. İç denetçilerin uyması gereken etik kurallar, 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununun 67 nci maddesinin (k) bendinde İç Denetim Koordinasyon Kurulu'nca belirleneceği hükme bağlanmış ve bu kapsamda Kamu İç Denetçileri Meslek Ahlak Kuralları belirlenmiştir. Buna göre iç denetçi mesleğini icra ederken dürüstlük, tarafsızlık, nesnellik, bağımsızlık, gizlilik, yetkinlik gibi etik kurallara uymalı ve bu

kuralların uygulanmasını desteklemelidir. Bu kurallar dışında iç denetçi, Uluslararası İç Denetim Enstitüsü (IIA) tarafından oluşturulan Etik Kuralları ve ISACA tarafından oluşturulan Profesyonel Etik Kuralları'nı da dikkate almalıdır. Bu kurallardan yola çıkarak, denetçi aşağıda listelenen etik kurallara ve bağımsızlık ilkesine uygun hareket etmelidir:

- İç denetçi, tüm mesleki hayatı boyunca sorumluluk ve doğruluk duygusuyla hareket etmelidir.
- İç denetçi, kanun dışı bir faaliyete bilerek veya isteyerek taraf olmamalı, hukukun ve mesleğin gerektirdiği özel durum açıklamalarını yapmalıdır.
- İç denetçi, görev alanındaki sorunları ve konuları ele alma konusunda bağımsız ve tarafsız olmalıdır.
- İç denetçi tutarlı olarak dürüst davranmalıdır. Bu, kendisine ve yaptığı denetime güven duyulmasını sağlamaktadır.
- İç denetçi, 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.
- İç denetçi, mesleki veya yasal zorunluluk olmadıkça, elde ettikleri bilgilerin değerinin korunmasına ve gizliliğine özen göstermeli, gereken onay ve yetkileri almadan kurum bilgilerini başkalarıyla paylaşmamalıdır.
- İç denetçi, denetimi gerçekleştirebilecek bilgi ve beceriye sahip olmalı ve sadece görevin gerektirdiği bilgi, beceri ve tecrübeye sahip olduğu işleri üstlenmelidir. BT denetimi yapacak iç denetçi sahip olduğu profesyonel yetkinlikleri sürekli geliştirmekle sorumludur.
- BT denetimi bir ekip çalışması halinde gerçekleştiriliyorsa iç denetçi, ekip üyelerinin profesyonel etik kurallarına uygun şekilde çalıştıklarından emin olmalıdır. İç denetçi, denetim süresince karşılaştığı her sorunla profesyonel etik kurallarına ve denetim standartlarına uygun şekilde mücadele etmelidir.
- İç denetçi çıkar çatışmalarından kaçınmalı, baskıcı, hakaret edici ve tehdit edici uygulamalarda bulunmamalıdır.
- Profesyonel etik kurallarına veya denetim standartlarına uymayan iç denetçi hakkında disiplin işlemleri başlatılmalıdır.
- Uyulması gereken etik kurallar profesyonel denetçilerin taleplerine ve gelişmelere göre güncellenir. İç denetçi etik kurallardaki değişiklikleri takip etmekle sorumludur.

Denetimde bağımsızlık ve tarafsızlık ilkesi

İDB, yürüttüğü faaliyetleriyle denetlenenden fonksiyonel olarak bağımsız olmalıdır. Denetim ancak böylece tarafsız bir şekilde tamamlanabilir. BT denetimi yapacak iç denetçinin denetlenen alanda doğrudan bir kontrolü varsa veya denetlenen alanda doğrudan kontrolü olan kişilere rapor verme sorumluluğu varsa, iç denetçi bağımsızlığını ve tarafsızlığını kaybeder. Eğer iç denetçi bir durumun veya ilişkinin bağımsızlığını ve tarafsızlığını etkilediğini fark ederse, mümkün olduğunca kısa sürede İDB başkanını bilgilendirmelidir.

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 iç denetçinin, denetlenen birime ve iş süreçlerine ilişkin riskler ve kontrollerle ilgili bir anlayış geliştirmiş olması da kritiktir.

İç denetçi 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.

İç denetçi 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 konusu için gerekli profesyonel ve teknik bilgi ve beceriye sahip olan iç denetçinin 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

ISACA tarafından önerilen Bilgi Sistemleri Denetimi ve Kontrolü Müfredat Modelinde (Model Curriculum for IS Audit and Control), BT denetimlerini 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: Edinme, 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 güvencesinin verilmesi.

1.4.2. Teknik Olmayan Yetkinlikler

İç denetçiden beklenen teknik olmayan yetkinlikler IIA'nın İç Denetçi Yetkinlik Çerçevesi modelinde aşağıdaki şekilde belirlenmiştir.

- Etki (ikna) ve iletişim
  - İkna gücünü etkili kullanır ve geliştirir
  - Açık ve ikna edici mesajlar vererek ve aktif dinleyerek, etkin bir şekilde iletişim kurar
  - Liderlik ve ekip çalışmasına yatkındır
  - Kurumsal politika ve prosedürleri etkin bir şekilde uygular
  - İşe alma, seçme ve personeli 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 yaparak etkin bir biçimde çalışır
  - Ortak hedefler doğrultusunda ekip sinerjisi oluşturur
- Değişiklik yönetimi
  - Değişime ve yeniliğe açıktır
- Anlaşmazlık çözümü
  - Anlaşmazlıkları müzakereler ile etkin olarak yönetir ve çözümler

1.5. Sertifikasyonlar

BT denetimi konusunda uzmanlaşmak isteyen iç denetçilerin 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 de 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.

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, 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 uluslararası düzeyde tanınırlar.

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, yönetimsel sorumluluklar gibi konulara yönelik olarak bağımsız bir kuruluş olan Uluslararası Bilgi Sistemleri Güvenliği Sertifikasyon Konsorsiyumu ($(ISC)^2$) tarafından verilmektedir. CISSP, en önemli uluslararası bilgi güvenliği sertifikaları arasında kabul edilmektedir.

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 güvenliği ve gizli tutulması konusunda bir anlayışa sahip olurlar.

Sertifikalı Bilgi Güvenliği Yöneticisi (Certified Information Security Manager):

CISM sertifikası, 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 çeşitli düzeylerde 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 sağlanması, risk optimizasyonu, kaynak optimizasyonu gibi konulara yönelik olarak geliştirilen bir uzmanlık sertifikasıdır.

Risk Yönetimi Güvence Sertifikası (Certification in Risk Management Assurance)

CRMA sertifikası, IIA tarafından verilmektedir. CRMA, risk güvencesi, yönetişim süreçleri, kalite güvence ya da kontrol öz değerlendirme konularında sorumluluğu veya tecrübesi olan iç denetçiler ve risk yönetimi uzmanları için tasarlanmıştır.

1.6. Uluslararası Standartlar ve Çerçeveler

Rehber hazırlanırken gerekli noktalarda aşağıdaki çerçeve, standart ve referanslardan faydalanılmış ve bunlar ilgili bölümlerde kaynak olarak gösterilmiştir. Söz konusu kaynaklar bir iç denetçi için gerektiğinde başvurulmak üzere kullanılabilecek ilave kaynaklar için önemli bir başlangıç noktası teşkil etmektedir.

- COBIT 5 - ISACA
- COBIT 4.1 - ISACA
- BT Güvence Rehberi (IT Assurance Guide Using COBIT 4.1) - ISACA
- ITAF - ITGI
- Denetim Kılavuzları - ISACA
- BT Risk'inin Değerlendirilmesi Rehberi (Guide to the Assessment of IT Risk) - The IIA
- Küresel Teknoloji Denetimi Rehberi (Global Technology Audit Guides) - The IIA
- Uygulama Kılavuzları - Türkiye İç Denetim Enstitüsü
- Kurumsal Risk Yönetimi (Enterprise Risk Management) - COSO
- ISO 2700x Bilgi Güvenliği Standartları - ISO
- Bilgem Kılavuzları - TÜBİTAK
- BT Altyapı Kütüphanesi (IT Infrastructure Library v3) – Office of Government Commerce
- ISO 22301 Sosyal Güvenlik İş Sürekliliği Yönetim Sistemleri - ISO

2. BT DENETİM METODOLOJİSİ

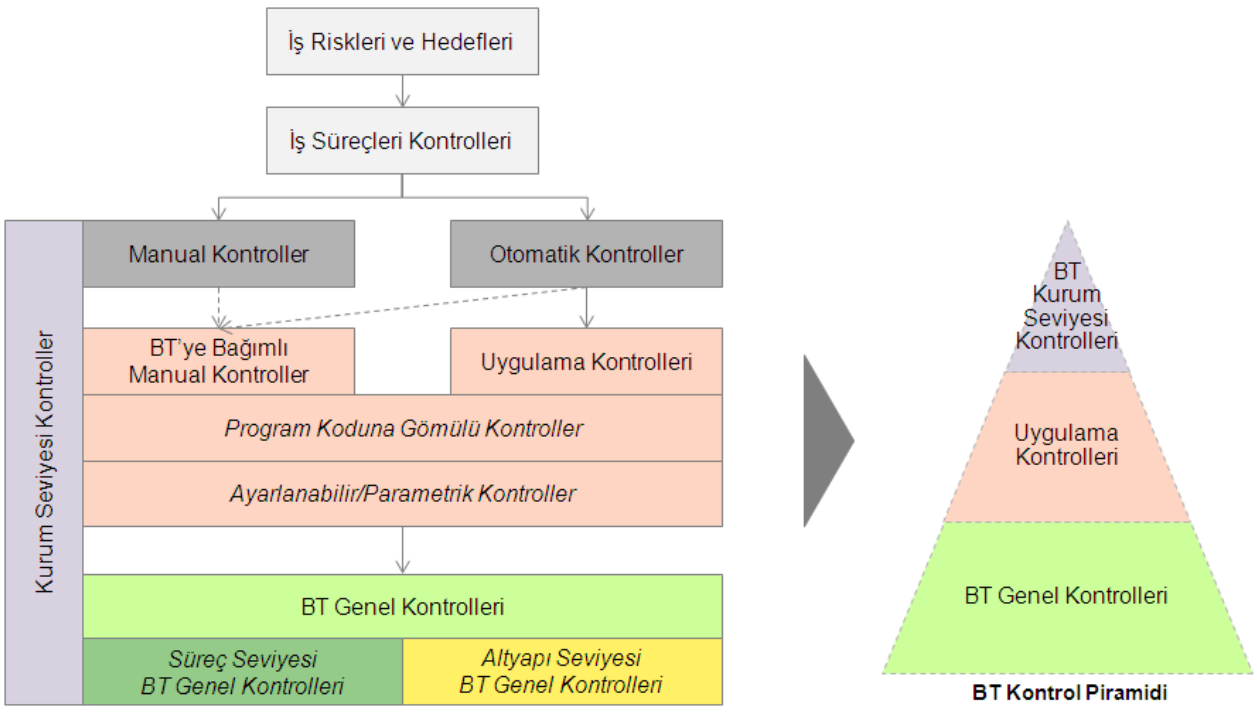
2.1. BT Denetim Metodolojisine Giriş

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 konumlandırılmasında yarar görülmektedir.

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

Şekil 1 - Kontrollerin ilişkilendirilmesi



Şekilde görüldüğü üzere, iç kontrol sisteminin iş risklerini ve hedeflerini karşılayabilmesi açısından, iki ana kontrol grubu (manuel 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 teknolojileriyle ilgili üst seviye kontrolleri ifade etmekle birlikte, aynı zamanda BT yönetişimiyle ilgili hususlara da değinir.

BT yönetişimi 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 konuyla ilişkilendirilmiştir. COBIT çerçevesinde BT yönetişimi, 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 niteliğiyle konuya ilişkin kontroller, yukarıdaki şekilde gösterilen BT kontrol piramidinin en tepe noktasını oluşturmaktadır.

COBIT çerçevesi, özellikle COBIT 5 versiyonu ile birlikte, BT yönetişim ve yönetim süreçleri ile ilgili net bir ayrıma gitmiştir. Bu husus iç denetçinin kontrollerin niteliğini doğru algılayabilmesi açısından önem arz etmektedir. Bu çerçevede BT yönetişimi, yukarıda da belirtildiği üzere genel anlamda kurumu yönlendiren bir katman olarak düşünülebilir. BT yönetimi ise kurumun amaçlarına ulaşabilmesi için yönetişim 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 kontrolleri 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 iç 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 manuel 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 temelde beş grup olarak ele alınmaktadır:

- Kaynak Veri Hazırlığı ve Yetkilendirme: Bilgi sistemlerine 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 değişikliklerle 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 BT denetimi yetkinliklerine sahip iç denetçilerin katkısıyla ele alınmaktadır.

- ***BT'ye bağımlı manüel kontroller***

BT'ye bağımlı manüel kontroller, hem manüel 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 süreci bilgi sistemlerine bağlı olmadan yürütüldüğü için kontrolün bu unsuru bir manüel kontrol gibi değerlendirilir. Denetimde her iki unsur da kendi metodolojileri çerçevesinde ayrı ayrı değerlendirilir. Bu çerçevede BT'ye bağımlı manüel kontrollerin otomatik unsurları, uygulama kontrollerine benzer şekilde ele alınmaktadır. Rehber'de genel olarak uygulama kontrolü kavramından bahsedilirken BT'ye bağımlı manüel kontrollerin bu unsuru da kastedilmektedir.

BT Genel Kontrolleri

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

- 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 süreçleriyle 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 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" 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 kontrollerinin ayrılmaz bir parçası olmakla birlikte, BT denetim çalışma

planının hazırlanması, iç denetçilere görev dağılımının yapılabilmesi ve saha çalışmaları hususlarında önemli bir pratiklik sağladığından, ayrı bir grup olarak ele alınmıştır.

2.1.2. BT Denetim Metodolojisi: Büyük Resim

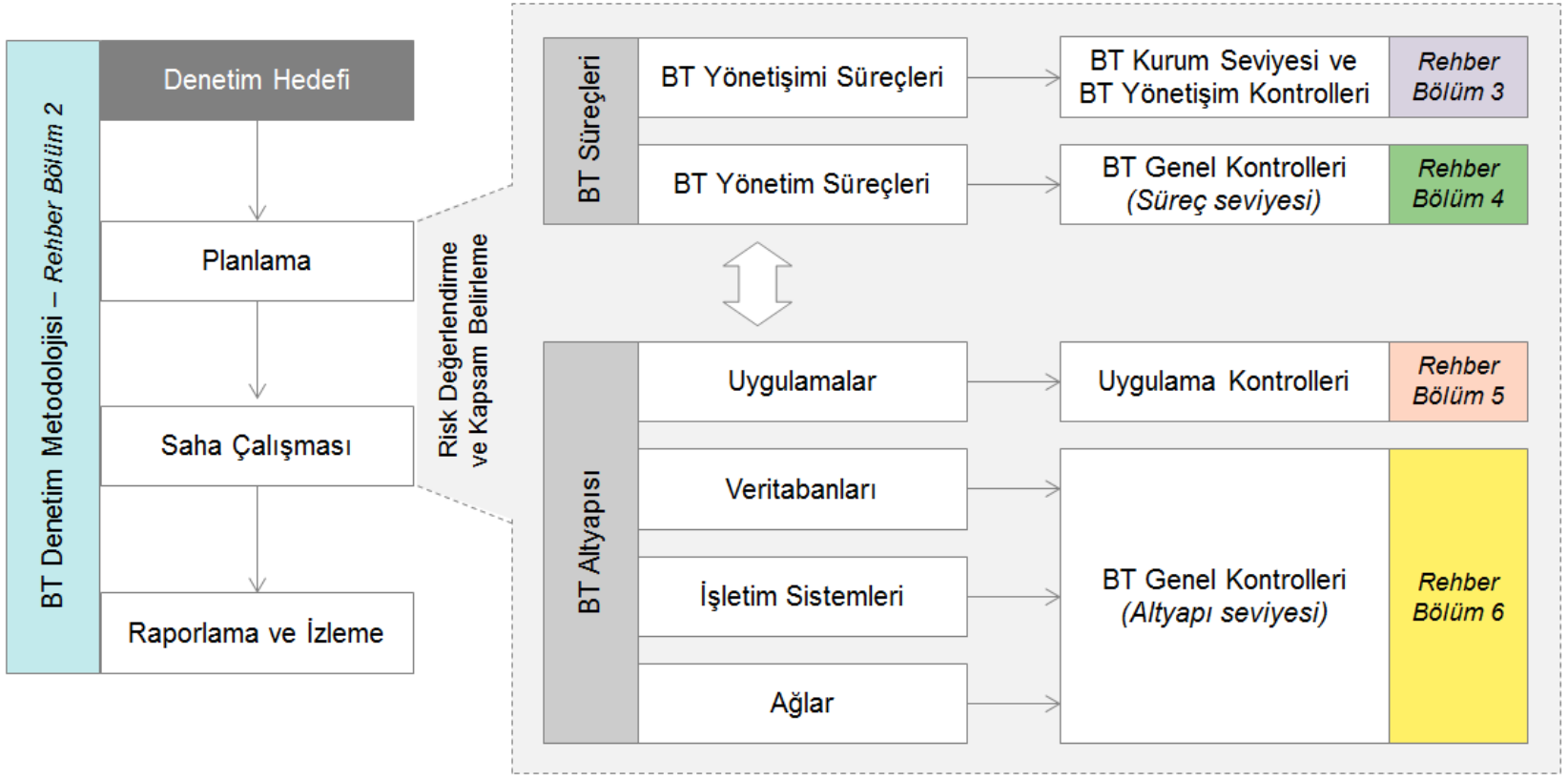
BT denetim metodolojisinin ana adımlarına, BT denetiminin konusu olan unsurlara ve bir önceki kısımda belirtilen kontrol türlerinin metodolojideki yerlerine işaret eden genel bir şemaya bir sonraki sayfada yer verilmektedir.

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

Şekil 2'de ayrıca her bir BT kontrol grubuna ilişkin detaylı denetim testlerinin, Rehber'in hangi bölümünde ele alındığı da renk kodlarıyla gösterilmiştir. Aynı renk kodları kontrollerin birbiriyle olan ilişkisinin gösterildiği Şekil 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.

Şekil 2 – BT Denetim Metodolojisi



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 yapılacağının bilinçli olarak belirlenmesi ve BT denetim ekibinin bu doğrultuda yönlendirilmesi kritiktir. Bu amaçla kurumun 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 ölçümlenmesi gibi farklı beklentiler de yer alabilir.

Denetim hedeflerinin belirlenmesi açısından, planlama aşamasından detaylı denetim görevlerine 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 küçültebilecek olası mali kaynak sorunları bu etkenlerden bazılarıdır.

Denetim hazırlıkları başlatılırken öncelikle kurum fonksiyonları, paydaş beklentileri, kurumun organizasyonel yapısı, teknolojik değişiklikler, yasal mevzuat, iş ihtiyaçları ve kuruma ve faaliyet alanına özgü risklerin bütününü 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. Planlama yapılırken denetim hedeflerine uygun BT hedeflerinin belirlenmesi ve bu hedeflerle ilişkilendirilebilen denetim görevlerinin 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 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 yapılandırılmasına yönelik unsurlar öne çıkabilir. Bu unsurlar, denetim hedefi ve denetim konuları 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

İç denetçiler denetim çalışmasını yürütecekleri birimle ilgili belirli konuları denetime başlamadan önce anlamaya yönelik bir araştırma ve bilgi toplama faaliyeti gerçekleştirmelidir. Bu sayede denetimin daha verimli ve etkin olması sağlanabilecektir. Ön araştırmanın yapılması sırasında aşağıda belirtilen konularda bilgiler toplanır, gerekli ön analizler yapılır ve kayıt altına alınır.

- *Kurum/Birim ile ilgili temel mevzuatın anlaşılması*

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 görevlerine ilişkin kapsamın belirlenmesine doğrudan etki edebilecek alanların belirlenmesine yardımcı olacak ve aynı zamanda mevzuat açısından gerekli bir hususun denetim kapsamı dışında bırakılmasına engel olacaktır.

- *Kurum/Birim iş süreçlerinin anlaşılması*

İç 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 itibariyle anlamak adına mevcut durumda hazır bulunan belge ve dokümanları inceleyerek gerekli bilgileri edinmeye çalışır. Söz konusu bilgilerin bir bölümü kurumun hazırlamış olduğu Stratejik Plan ve Faaliyet Raporu gibi kaynaklarda bulunabilir.

- *Önceki denetim raporlarının incelenmesi*

Denetlenecek süreçler ve faaliyetlerde ya da BT ile ilgili başka bir alanda daha önceden yapılmış iç denetim ve dış denetim çalışmaları 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 denetim ekibi, denetlenecek birimdeki ilgili yöneticileri, BT birimi yöneticileri ve sorumluları ve ilgili diğer sorumlu personelin katılacağı bir açılış toplantısı yapar. Bu toplantının amacı aşağıdaki hususlar üzerinde bilgi paylaşımı yapmaktır:

- 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 organizasyonunun yapısı, BT altyapısının genel şematik yapısı, altyapı ve uygulamaların entegrasyon düzeyi ve dış ortamlarla olan bilgi alış verişi gibi konular da tartışılarak sonraki bölümlerde yürütülecek anlayış geliştirme ve analiz aşamaları öncesi ön bilgi edinilmelidir.

Açılış toplantısında görüşülen konular tutanak ile kayıt altına alınır ve denetim dosyasında muhafaza edilir.

BT Organizasyonunun Anlaşılması

İç denetçi, BT biriminin kurumun genel organizasyon yapısı içerisindeki yerini, BT birimi yönetiminin kurum seviyesinde temsil seviyesini, BT biriminin kendi içerisindeki organizasyon yapılanmasını, görev dağılımını ve bunlara ilişkin ilişki, iletişim ve raporlama yapılarını inceleyerek BT organizasyonunu anlamalıdır. Bu doğrultuda denetçi, denetlenen kurum/birim organizasyon şeması ile beraber ilgili BT biriminin de organizasyon şemasını temin etmeli ve incelemelidir. Söz konusu inceleme, iç denetçiye kurum içerisinde BT'ye ilişkin faaliyetlerin organizasyon seviyesinde nasıl yürütüldüğü konusunda bilgi verebileceği gibi, iç denetçinin denetim sırasında karşılaşacağı belirli aksaklıkların kök nedenlerinin belirlenmesinde yol gösterici de olabilecektir.

Ek olarak denetçi hem kurum/birim organizasyonunu daha iyi anlamak hem de denetim testleri sırasında yardımcı olması amacıyla güncel birim personel listesini ve denetim dönemi içerisinde işe başlamış ve işten ayrılmış birim personellerinin listesini temin etmeli ve incelemelidir.

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 ve 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, 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, Rehber'in ilerleyen bölümlerinde bahsedilecek olan risk değerlendirme ve kapsam belirleme adımlarına girdi olarak kullanılacaktır.

Yukarıda bahsedilen ve genel olarak BT ortamının anlaşılmasına yardımcı olacak bilgilerin bir bölümünün sonraki aşamalarda kullanılabilmesi açısından kayıt altına alınması gerekmektedir. Bu doğrultuda oluşturulmuş olan Bilgi Toplama Formu (***Ek 1 – Bilgi Toplama Formu***), "Genel Bilgiler" ve "Teknik Bilgiler" adında iki ana bölümden oluşmaktadır. Bu formun amacı denetim saha çalışmalarına başlamadan önce denetlenen birimden planlama, kapsam belirleme ve risk analizi aşamaları için girdi sağlayacak verilerin sağlanmasıdır.

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

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

2.2.3.Risk değerlendirmesinin yapılması

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

Bir kurumda iç denetim sürecini etkileyen şartlar zamanla değişebildiğinden, hiçbir risk değerlendirme yaklaşımı tek başına tüm şartlarda en ideal risk değerlendirme stratejisi olarak değerlendirilemez. Riskler, kurumun süreç ve hedefleri göz önünde bulundurularak denetim görevlerinin 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/birim/faaliyet 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 temel risk faktörleri ve risk değerlendirme yaklaşımı göz önünde bulundurularak, kurumun karşı karşıya kaldığı bilgi teknolojileri risklerinin,

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

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

Risk değerlendirme aşamasında Uluslaralarası Standartlar Teşkilatı (International Organization for Standards – ISO) tarafından yayınlanmış olan ISO 31000:2009, Risk Yönetimi – Prensip ve Kılavuzlar (Risk Management – Principles and Guidelines) standardından da faydalanılabilir.

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

- Denetim testlerinin içeriği, kapsamı ve zamanlaması,
- Denetlenecek alt süreçlerin, alt faaliyetlerin ve fonksiyonların belirlenmesi,
- Denetim için ayrılacak kaynak ve zamanın belirlenmesi

konularında yardımcı olur.

Denetim görevlerinin planlanması ve denetimin kapsamının belirlenmesi amacıyla, hem kurumun bütününe ilişkin genel BT risk seviyesi, hem de BT uygulamalarının risk seviyeleri iki ayrı çalışma ile tespit edilir. 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 (***Ek 2-Risk Değerlendirme Formu***).

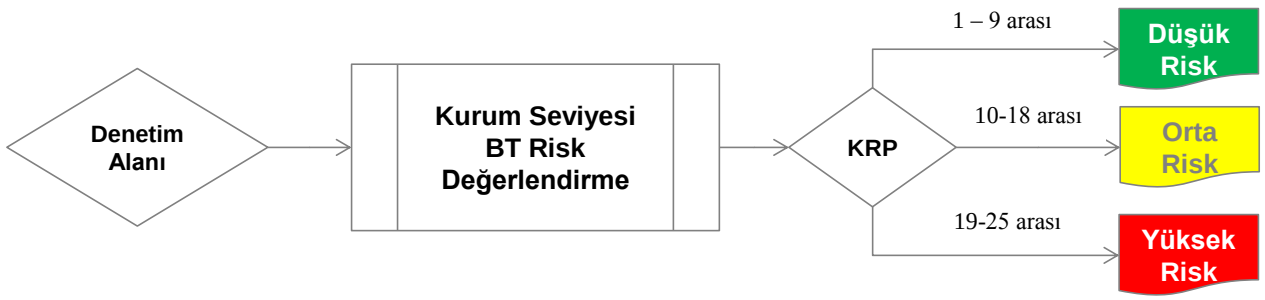
Kurum seviyesi BT risk değerlendirmesi

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 kapalı uçlu sorudan oluşur (***Ek 2.1 - Kurum Seviyesi Risk Değerlendirme Formu)***. Formdaki tüm sorular iç denetçi tarafından denetlenenin durumu değerlendirilerek cevaplanır. Kurum seviyesi risk puanının hesaplanabilmesi amacıyla formda bulunan her sorunun ve her soruya verilecek karşılıkların Rehber'in ilgili ekinde de ifade edildiği şekilde önceden belirlenmiş bir katsayısı bulunmaktadır. Bu katsayılar iç denetçinin kurum/birimle ilgili değerlendirmesine ve yargısına göre ihtiyaç halinde denetçi tarafından değiştirilebilir. Risk değerlendirme katsayılarında yapılacak bu değişiklikler sebepleri de belirtilecek şekilde belgelendirilmelidir.

Kurum Seviyesi Risk Değerlendirme Formu'nda bulunan sorulara verilecek cevaplar neticesinde kurumun kurumsal BT risk derecesini temsil eden ve 25 üzerinden hesaplanan bir değer – Kurum Risk Puanı (KRP) elde edilir. Söz konusu sorular genel itibariyle KİDR'da belirtilen temel risk faktörlerine ilişkin değerlendirmelere imkân sağlamakla birlikte, kurumun faaliyet alanı ya da sunduğu hizmetler göz önünde tutularak özelleştirilebilir. KRP'si 1 ila 9 arasında olan kurumlar görece az riskli (Düşük Risk) olarak değerlendirilebilirken, 19 ila 25 değeri ise yüksek riski (Yüksek Risk) işaret etmektedir. KRP'si 10 ila 18 arasında olan kurumlar Orta Riskli olarak değerlendirilir. Söz konusu puan aralıkları kurumun faaliyet alanına ve BT ortamının karmaşıklığına bağlı olarak değiştirilebilir.

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

Şekil 3 – KRP: Kurum Seviyesi Risk Puanı



Uygulama seviyesi BT risk değerlendirmesi

Kurum/birim bünyesinde bulunan uygulamaların temel olarak faaliyetleri ve iş süreçlerini destekleme seviyeleri ve belirli teknik özellikleri açısından değerlendirilmesi sırasında kullanılacak olan kuruma ait uygulamaların kapsama alınma gerekliliklerini değerlendirmek amacı ile sorulmuş toplam 16 adet kapalı uçlu sorudan oluşmaktadır (***Ek 2.2 Uygulama Seviyesi Risk Değerlendirme Formu***). Söz konusu form içine öncelikle kurum bünyesindeki tüm uygulamalar yazılır ve belirtilen soruların her biri tüm uygulamalar için ayrı ayrı cevaplandırılır. Uygulama seviyesi risk puanının hesaplanabilmesi amacıyla formda bulunan her sorunun ve her soruya verilecek cevabın Rehber'in ilgili ekinde de belirtildiği şekilde belirli bir katsayısı bulunmaktadır. Bu katsayılar iç denetçinin uygulama ile ilgili değerlendirmesine ve yargısına göre ihtiyaç halinde değiştirilebilir. Risk değerlendirme katsayılarında yapılacak değişiklikler sebepleri de belirtilecek şekilde belgelendirilmelidir. Uygulama Seviyesi Risk Değerlendirme Formu'nda bulunan bu sorulara verilecek cevaplar neticesinde uygulama risk seviyesini temsil eden 25 üzerinden bir değer – Uygulama Risk Puanı (URP) elde edilir. Uygulama risk seviyesi 1 ila 9 arasında olan uygulamalar görece az riskli (Düşük Risk) olarak değerlendirilebilirken, 19 ila 25 değeri ise yüksek (Yüksek Risk) riski işaret etmektedir. URP'si 10 ila 18 arasında hesaplanan uygulamalar Orta Riskli olarak değerlendirilir. Söz konusu puan aralıkları kurumun/birimin faaliyet alanına, BT ortamının ve ilgili uygulamanın karmaşıklığına bağlı olarak değiştirilebilir.

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

Şekil 4 – URP: Uygulama Seviyesi Risk Puanı

Uygulama seviyesi risk değerlendirme formu üzerinde gerçekleştirilen çalışmaya ilave olarak, önceki iç ve dış denetim raporları, yönetimin denetimden beklentisi, kaynak planlaması veya iç 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. Burada önemli olan husus, ilave ya da çıkarmaların hangi gerekçeye dayanılarak yapıldığının net bir biçimde ortaya konulabilmesidir.

Uygulama seviyesinde risk değerlendirmesi yapılmasından sonra kapsama alınacak uygulama envanterinin teknoloji envanteri formuyla kayıt altına alınması gerekmektedir. Teknoloji envanteri formu, iç denetçi tarafından doldurulmalıdır (***Ek 3 – Örnek Teknoloji Envanteri Formu***). Denetim hedefleri ve uygulama risk değerlendirmesi sonucu olarak kapsama alınan uygulamaların kurulu olduğu platformlar, işletim sistemleri, veritabanları ve uygulamayla ilgili süreç sahipleri bu form üzerinde kaydedilir.

Risk değerlendirme ve bir sonraki bölümde verilmiş olan kapsam belirleme için kullanılacak yönlendirme tablolarının kullanımı neticesinde belirlenecek kapsam uyarınca gerçekleştirilmesi gereken detay denetim testleri ve çalışmaları Rehber'in ilerleyen bölümlerinde sunulmuştur.

2.2.4. Kapsamın belirlenmesi

Kapsam Belirlenmesine İlişkin Esaslar

BT denetimi kapsamının, denetim türüne bağlı olarak ne şekilde belirlenebileceğine ilişkin karar mekanizmaları her bir denetim türü için ayrı ayrı olarak aşağıdaki bölümde verilmiştir.

Aşağıda belirtilen kapsam tabloları dışında kalan Uygulama Kontrollerinin denetimi başta mali ve sistem denetimlerinde olmak üzere belirli ölçüde değerlendirme kapsamına alınır. Uygulama kontrollerinin doğası gereği kurumların faaliyet alanı ve uygulanan iş süreçleri ile iş uygulamaları kullanımı ve karmaşıklığı açısından farklılık göstermesinden dolayı, denetim kapsamına alınacak uygulama kontrolleri her denetimde denetim ekibi tarafından yukarıda belirtilen hususlar dikkate alınarak belirlenir ve uygulanır. Bu kontrollere ilişkin örnekler, Rehber'in 5. Bölümünde yer almaktadır.

Mali Denetim Kapsamında Yürütülecek BT Denetimi Kapsamı

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

Kurum Seviyesi Risk Değerlendirme	**Düşük Risk** **KRP: 1-9**	**Orta Risk** **KRP: 10-18**	**Yüksek Risk** **KRP: 19-25**
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 testleri kapsamda.	• Zorunlu denetim testleri kapsamda. • Opsiyonel denetim testleriniın kapsama alınması önerilir.	Zorunlu ve Opsiyonel denetim testlerinin 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.	• Zorunlu denetim testleri kapsamda. • Denetlenen kurumun faaliyetlerine ya da denetim dönemi içinde sistem değişikliği olup olmadığına bağlı olarak seçilecek süreçler (ör: DS2, AI2) için Opsiyonel denetim testleri kapsamda.	Zorunlu ve Opsiyonel denetim testlerinin tamamı kapsamda.

Uygulama Seviyesi Risk Değerlendirme	Düşük Risk URP: 1-9	Orta Risk URP: 10-18	Yüksek Risk URP: 19-25
İş Uygulamaları	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen Zorunlu denetim testlerinden ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim testlerinin tümü ve 2. Grup içinde belirtilen denetim testlerinden Zorunlu olanlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim testlerinin tümü ve 2. Grup içinde belirtilen denetim testlerinden Zorunlu olanlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır. Buna ilave olarak 2. Grup içinde belirtilen Opsiyonel denetim testlerinin 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 testleri 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 testlerinin 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 testleri 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	Seçilen iş uygulamasının çalışma mantığına ve veritabanı sistemi ile olan etkileşimine, veritabanı sistemi seviyesindeki son kullanıcı hesabı sayısına, veritabanı seviyesine erişim	Seçilen iş uygulamasının çalışma mantığına ve veritabanı sistemi ile olan etkileşimine, veritabanı sistemi seviyesindeki son kullanıcı hesabı sayısına, veritabanı seviyesine erişim

Uygulama Seviyesi Risk Değerlendirme	Düşük Risk URP: 1-9	Orta Risk URP: 10-18	Yüksek Risk URP: 19-25
	yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim testleri kapsama alınması önerilir.	yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim testleri kapsama alınması önerilir.	yöntemlerine ve veritabanı sistemi üzerinde doğrudan çalıştırılabilen programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim testleri 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 testleri 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 testleri 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 testleri kapsama alınır.

Sistem Denetimi Kapsamında Yürütülecek BT Denetimi Kapsamı

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

Kurum Seviyesi Risk Değerlendirme	**Düşük Risk** **KRP: 1-9**	**Orta Risk** **KRP: 10-18**	**Yüksek Risk** **KRP: 19-25**
BT Kurum Seviyesi Kontrolleri	Kapsamda.	Kapsamda.	Kapsamda.
BT Yönetişim Kontrolleri	Kapsamda değil.	Kapsamda.	Kapsamda.
BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup	Zorunlu denetim testleri kapsamda.	• Zorunlu denetim testleri kapsamda. • Seçime bağlı denetim testlerinin kapsama alınması önerilir.	Zorunlu ve Opsiyonel denetim testlerinin 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.	• Zorunlu denetim testleri kapsamda. • Denetlenen kurumun faaliyetlerine ya da denetim dönemi içinde sistem değişikliği olup olmadığına bağlı olarak seçilecek süreçler (ör: DS2, AI2) için Opsiyonel denetim testleri kapsamda.	Zorunlu ve Opsiyonel denetim testlerinin tamamı kapsamda.

Uygulama Seviyesi Risk Değerlendirme	Düşük Risk URP: 1-9	Orta Risk URP: 10-18	Yüksek Risk URP: 19-25
İş Uygulamaları	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen Zorunlu denetim testlerinden ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim testlerinin tümü ve 2. Grup içinde belirtilen denetim testlerinden Zorunlu olanlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim testlerinin tümü ve 2. Grup içinde belirtilen denetim testlerinden Zorunlu olanlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır. Buna ilave olarak 2. Grup içinde belirtilen Opsiyonel denetim testlerinin 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 testleri 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 testlerinin 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 testleri 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	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	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 Risk Değerlendirme	Düşük Risk URP: 1-9	Orta Risk URP: 10-18	Yüksek Risk URP: 19-25
	programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim testleri kapsama alınması önerilir.	programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim testleri kapsama alınması önerilir	programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim testleri 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 testleri 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 testleri 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 testleri kapsama alınır.

Performans Denetimi Kapsamında Yürütülecek BT Denetimi Kapsamı

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

Kurum Seviyesi Risk Değerlendirme	**Düşük Risk** **KRP: 1-9**	**Orta Risk** **KRP: 10-18**	**Yüksek Risk** **KRP: 19-25**
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 ekonomik bir şekilde kullanıldığının değerlendirilmesi olduğundan, BT altyapı bileşenleri üzerinde gerçekleştirilecek bir genel kontrol 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: 1-9**	**Orta Risk** **URP: 10-18**	**Yüksek Risk** **URP: 19-25**
İş Uygulamaları	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen Zorunlu denetim testlerinden 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 testlerinden 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 testlerinden veri üretimine ve iş ihtiyaçlarının karşılanmasına doğrudan etki edebilecek olanlar kapsama alınır. Buna ilave olarak 1. ve 2. Grup içinde Opsiyonel 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 testlerinden 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 testlerinden 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 testlerinden özellikle veri üretimine doğrudan etki edebilecek olanlar kapsama alınır.

Uygulama Seviyesi Risk Değerlendirme	Düşük Risk URP: 1-9	Orta Risk URP: 10-18	Yüksek Risk URP: 19-25
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 testlerinden 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 testlerinden 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 testlerinden 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 testleri 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 testleri 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 testleri özellikle veri üretimine doğrudan etki edebilecek olanlar kapsama alınır.

Uygunluk Denetimi Kapsamında Yürütülecek BT Denetimi Kapsamı

Uygunluk denetimi kapsamında Kurum Seviyesi Risk Değerlendirme ve Uygulama Risk Değerlendirme sonuçlarına göre yürütülebilecek denetimler için belirlenebilecek kapsama ilişkin yönlendirme aşağıda belirtilmiştir.

Kurum Seviyesi Risk Değerlendirme	**Düşük Risk** **KRP: 1-9**	**Orta Risk** **KRP: 10-18**	**Yüksek Risk** **KRP: 19-25**
BT Kurum Seviyesi Kontrolleri	Kapsamda.	Kapsamda.	Kapsamda.
BT Yönetişim Kontrolleri	Uygunluk gerektiren mevzuat ya da diğer kriterler uyarınca kapsama alınabilir.	Uygunluk gerektiren mevzuat ya da diğer kriterler uyarınca kapsama alınabilir.	Uygunluk gerektiren mevzuat ya da diğer kriterler uyarınca kapsama alınabilir.
BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup	• Zorunlu denetim testleri kapsamda. • Opsiyonel denetim testlerinden seçilecekler ilgili mevzuat ya da kritere göre kapsama alınabilir.	• Zorunlu denetim testleri kapsamda. • Opsiyonel denetim testlerinden 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: 1-9	Orta Risk URP: 10-18	Yüksek Risk URP: 19-25
İş Uygulamaları	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen Zorunlu denetim testlerinden ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim testlerinin tümü ve 2. Grup içinde belirtilen denetim testlerinden Zorunlu olanlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim testlerinin tümü ve 2. Grup içinde belirtilen denetim testlerinden Zorunlu olanlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır. Buna ilave olarak 2. Grup içinde belirtilen Opsiyonel denetim testlerinin 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 testleri 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 testlerinin 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 testleri 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 testleri 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 Risk Değerlendirme	Düşük Risk URP: 1-9	Orta Risk URP: 10-18	Yüksek Risk URP: 19-25
			programların niteliğine bağlı olarak Altyapı seviyesindeki BT Genel Kontrolleri'ne ilişkin denetim testleri 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 testleri 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 testleri 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 testleri kapsama alınır.

Güvenlik Denetimi Kapsamında Yürütülecek BT Denetimi Kapsamı

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

Kurum Seviyesi Risk Değerlendirme	**Düşük Risk** **KRP: 1-9**	**Orta Risk** **KRP: 10-18**	**Yüksek Risk** **KRP: 19-25**
BT Kurum Seviyesi Kontrolleri	Kapsamda.	Kapsamda.	Kapsamda.
BT Yönetişim Kontrolleri	Güvenlik ile ilgili denetim testleri kapsama alınır.	Güvenlik ile ilgili denetim testleri kapsama alınır.	Güvenlik ile ilgili denetim testleri kapsama alınır.
BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup	• Güvenlik Hizmetleri Yönetimi sürecinin tüm denetim testleri kapsama alınır. • Diğer süreçlerde bulunan denetim testleri arasından kurum güvenlik süreçleri ile ilgili düşünülenler kapsama alınabilir.	• Güvenlik Hizmetleri Yönetimi sürecinin tüm denetim testleri kapsama alınır. • Diğer süreçlerde bulunan denetim testleri arasından 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 testleri seçilebilir.	Denetlenen kurumun faaliyetleri ile denetim dönemi içinde sistem değişikliği olup olmadığına bağlı olarak ve denetlenen kurumdaki güvenlik faaliyetleri uyarınca süreçlerdeki ilgili denetim testlerinin seçilmesi önerilir.	

Uygulama Seviyesi Risk Değerlendirme	Düşük Risk URP: 1-9	Orta Risk URP: 10-18	Yüksek Risk URP: 19-25
İş Uygulamaları	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen Zorunlu denetim testlerinden ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır. Buna ilave olarak 1. Grup içinde Opsiyonel olarak belirtilen denetim testleri da kapsama alınabilir.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim testlerinin tümü ve 2. Grup içinde belirtilen denetim testlerinden Zorunlu olanlarından ilgili iş uygulaması üzerinde yürütülebilecek olanlar kapsama alınır. Buna ilave olarak 2. Grup içinde Opsiyonel olarak belirtilen denetim testlerinin da kapsama alınması önerilir.	BT Genel Kontrolleri (Yönetim Seviyesi Kontroller) – 1. Grup içinde belirtilen denetim testlerinin tümü ve 2. Grup içinde belirtilen tüm denetim testlerinin 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 testleri 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 testleri 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 testlerinin tümü kapsama alınabilir.		

2.2.5. Çalışma Planının Hazırlanması

BT denetimi saha çalışması öncesinde denetimin amaçlarını karşılayacak, genel denetim stratejisine uygun, denetim boyunca kişi ve birimlerin yükleneceği sorumlulukları dikkate alan, bağımsızlık ilkesi, yasal yükümlülük ve standartlar ile uyumlu bir çalışma planı oluşturulmalıdır. Çalışma planı oluşturulurken, denetlenecek birimin 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 çalışma planı; denetim sırasında ortaya çıkabilecek riskleri, hatalı varsayımları ya da o ana kadar tamamlanan denetim testlerindeki hatalı tespitler sonucu doğan düzeltme gereksinimlerini de karşılayabilecek esneklikte oluşturulmalıdır. Diğer bir deyişle, önemlilik değerlendirmesi profesyonel bir bakış açısı ve tecrübe gerektirir.

Oluşturulacak çalışma planı KİDR'da belirtilen prensipler göz önünde tutularak hazırlanır. Denetim kapsamının belirlenmesini takiben her bir denetim görevi için denetimin amacı ve denetim zaman planı belirlenir. Bu kapsamda 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

Çalışma Planının ekinde; risk ve kontrollere ilişkin değerlendirmeler sonucunda hazırlanan "Risk Kontrol Matrisi" ile hangi denetim testlerinin kim tarafından, nerede, hangi tarihler arasında yapılacağını gösteren bir görev iş programı yer alır. Hem Risk Kontrol Matrisi hem de Görev İş Programı için KİDR ekinde yer alan ilgili örneklerden faydalanılabilir.

Çalışma planı hazırlandıktan sonra İDB Başkanı tarafından onaylanır ve denetim ekibi ile paylaşılır. Denetim süresince elde edilebilecek yeni bilgiler, düzenlemelerdeki değişiklikler, gerçekleşebilecek önemli olaylar ve denetimi etkileyebilecek diğer hususlar nedeniyle, çalışma planında güncellemelerin yapılması gerekebilir.

2.3. Saha Çalışması

2.3.1. Kontrollerin Değerlendirilmesi

BT denetimlerinde kontrollerin önemli bir bölümü için kontrol tasarımlarının anlaşılabilmesi amacıyla fiilen sahaya çıkılmasına ihtiyaç duyulmaktadır. Bu durum bilgi teknolojilerinin doğasına özgü bir husus olup, tasarım ve işletim etkinliklerinin kimi zaman iç içe geçmiş olmasından kaynaklanmaktadır. Örneğin, kontrol tasarımının ilgili sistem parametrelerinin doğru olarak yapılandırılmasını gerektiren noktalarda bu durum karşımıza çıkmaktadır. Kontrolün işletim etkinliği de benzer şekilde ilgili sistem parametrelerinin yapılandırıldığı şekilde çalışmaya devam etmesi ile ilgilidir ve bu noktada iç denetçi kontrolün tasarımına geri döner. Benzer nedenlerden ötürü bir çok kontrol için tasarım etkinliklerinin doğrudan politika, prosedür vb. dokümanların incelenmesi yoluyla anlaşılması mümkün olmayabilir. Özellikle BT ile ilgili dokümantasyonun yetersiz olduğu durumlarda bu imkân ciddi ölçüde azalır. Böyle durumlarda fiilen sahaya inerek, tasarıma konu olan bilgileri bizzat BT personeli ile görüşmeler yaparak ve sistem yapılandırmalarını inceleyerek temin etmek gerekir.

Yukarıda belirtilen nedenlerden dolayı, KİDR'dan farklı olarak kontrollerin tasarımına ilişkin değerlendirme bu Rehber içinde Planlama bölümünden Saha Çalışması bölümüne alınmıştır. Bu farklılık sürecin işleyişiyle ilgili önemli bir farklılık olmayıp, sadece kavram bütünlüğü açısından BT denetimleri için geçerli olan bir hususun Rehber'de daha tutarlı gösterilmesi amacıyla yapılmıştır.

Denetim görevlerinin kapsamının belirlenmesi sırasında denetim türüne göre zorunlu ve zorunlu olmayan alanların seçimi ve uygulamasıyla ilgili yönlendirmelere, Rehber'in 2.2.4 Kapsam Belirleme bölümü içerisinde yer verilmiştir.

BT denetim görevleri;

- 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 testlerine, Rehber'in sonraki bölümlerinde yer verilmiştir. Bu bölümlerin nasıl ele alınabileceği ve kullanılabileceği aşağıda belirtilmiştir.

Anahtar Kontrollerin Tespit Edilmesi

Anahtar kontroller, süreç içinde tasarlandığı şekilde çalışmadığında 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 çalışmalarının verimli ve etkin bir şekilde planlanmasına ve uygulanmasına yardımcı olacaktır.

İç denetçi, faaliyet, süreç ve BT ortamını anladıktan ve Rehber içinde belirtilen kontrollerden hangilerinin kurum içinde uygulandığını tespit ettikten sonra, bunlar içinden anahtar kontrolleri ayrıştırıp önceliği bu kontrollerin denetlenmesine vermelidir. Bu anlamda Rehber içinde ilerleyen bölümlerde denetim testleri içinde "zorunlu" olarak belirtilmiş denetim testlerine sahip kontrollerin öncelikle ele alınması ve değerlendirilmesi iç denetçiye yardımcı olacaktır.

Tasarım Etkinliğinin Değerlendirilmesi

Denetimin yürütülmesi sırasında yararlanılan denetim tekniklerinden olan "Tasarımın Değerlendirilmesi" ya da "Üzerinden Gitme" veya "İz Sürme" ile örneklem seçimi ve uygulamanın değerlendirilmesi testleri genel itibariyle KİDR'da belirtildiği şekliyle kullanılacaktır.

Tasarımın Değerlendirilmesi / Üzerinden Gitme / İz Sürme: Herhangi bir kontrolün, tasarım etkinliği ve yeterliliği açısından ilgili olduğu riskleri karşılayıp karşılamadığının değerlendirilmesi ve rastgele seçilecek tek bir örnek işlem üzerinden kontrolün denetime tabi tutulmasıdır. Bu değerlendirme sırasında 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 bulunan denetim prosedürleri içerisinde verilmiş olan kontrollere ilişkin denetim testlerinin bir kısmı ilgili kontrolün tasarım etkinliğinin değerlendirilmesine yönelik hazırlanmış olup (T) harfiyle belirtilerek ayrıştırılmıştır.

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.

Örneklem Seçimi

Denetim çalışmaları sırasında iç denetçinin kurum BT ortamı ilgili süreçlerinde, uygulamalarda ya da sistemlerde oluşan tüm işlem ya da kayıtları incelemesine, *özel bir nedenin bulunmaması halinde*, gerek yoktur. Uygun yöntemlerle seçilecek yeterli sayıda kaydın ya da işlemin incelenmesi makul bir güvence oluşturmak açısından yeterlidir.

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

Örneklem seçimi, istatistiki ya da istatistiki olmayan yöntemler kullanılarak, ilgili kontrole ilişkin denetim dönemi boyunca oluşmuş kayıt, belge ve diğer çıktıların tamamı üzerinden (iç denetçinin hakkında kanaate varmayı istediği veri topluluğu, ana kütle) belirli bir sayıda rastgele örnek seçimiyle gerçekleştirilir.

Seçilecek örnek sayısı aşağıdaki hususlara bağlıdır:

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

Örneklem sayısının belirlenmesi amacıyla KİDR'da da verilmiş olan aşağıdaki tablo kullanılabilir.

Tablo 2 - Örneklem 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 iç denetçi, riskli gördüğü alanlara ilişkin kontrollerin denetimi sırasında örnek sayısında artış yapabilir. Seçilen örnekler içinde hatalara ya da istisnalara rastlanılması durumunda da iç denetçi benzer bir yaklaşımla daha fazla örnek seçerek ilgili kontrole dair güvence seviyesini artırma yoluna gidebilir.

Yukarıdaki tablo manuel ya da yarı-otomatik (BT'ye bağımlı manüel) kontrollerin test edilmeleri sırasında kullanılması beklenen örneklem yöntemini vermektedir. Buna ek olarak uygulama kontrollerinin (ör: otomatik kontroller) denetimi sırasında BT genel kontrollerinin etkinliğine bağlı olarak tek bir örnek üzerinden ilgili testleri gerçekleştirmek mümkün olabilmektedir. Söz konusu ilişki Rehberin 5.2. - Uygulama kontrolleri – BT genel kontrolleri ilişkisi bölümünde ifade edilmiştir.

Örneklem seçimi ile ilgili alternatif yöntemlerden kısaca bahsetmek gerekirse, bu yöntemlerden en çok kullanılanı ve istatistiki olarak makul güvence vermeye aday yöntem, bir rastgele sayı üreteci vasıtasıyla yapılacak "rassal" seçimdir. Bu yöntemde, ana kütle içinde her bir kayıta bir numara verilir. Bilgisayar üzerinde çalıştırılabilecek bir rastgele sayı üreteci 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 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. Denetim dönemi, gerçekleştirilecek olan denetimin türüne göre farklılık gösterebilir. Çalışma planı aksini belirtmedikçe sistem denetimi ve mali denetimlerde cari yıl ya da daha önceki yıllara kadar denetim dönemi uzatılabilir. Performans denetimlerinde, denetlenecek alana ve denetimin amacına göre denetim dönemi farklılık gösterebilirken güvenlik denetimi için denetim döneminin en az son altı ayı içermesi, tavsiye olarak ise son bir yılı kapsaması önerilmektedir.

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.

Rehberdeki denetim prosedürleri içerisinde verilmiş olan kontrollere ilişkin denetim testlerinin 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 türüne bağlı olarak risk değerlendirme ve kapsam belirleme sonuçlarına göre seçilecek olan BT Kurum Seviyesi Kontrolleri ve/veya BT Yönetişim Kontrolleri'ne ilişkin denetim testleri, Rehber'in üçüncü bölümünde verilmiş olup, belirtilen kontrollere ilişkin detay denetim testlerinin hepsi zorunlu kılınmıştır. Bu bölümde gerek BT Kurum Seviyesi Kontrolleri gerekse de BT Yönetişim Kontrolleri için verilmiş olan denetim testlerine ilişkin akış şu şekildedir:

Şekil 5 – BT Kurum Seviyesi Kontrolleri ve BT Yönetişim Kontrolleri Denetimi İçin Denetim Prosedürlerinin Akışı

Daha önce de belirtildiği üzere, Rehber içerisinde belirtilen denetim testleri iç denetçi yetkinliğine göre üç farklı seviyeye ayrılmıştır. Tablo 1'de tanımlanan bu seviyeler dikkate alınarak gerekli görülen durumlarda belirli prosedürlerin yerine getirilmesi için farklı seviyedeki iç denetçilerin görev alması değerlendirilmelidir.

BT Genel Kontrollerinin (Yönetim Süreçlerinin) Denetimi

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

Seçilecek süreçlerde "zorunlu" olarak ifade edilen denetim testlerinin uygulanması zorunludur. "Opsiyonel" olarak belirtilen denetim testlerinin uygulanması ise, denetlenen kurumun yapısına, iç denetçinin profesyonel yargısına ve kurum ile ilgili risk algısına göre ele alınabilecektir.

BT Yönetim Süreçleri denetimine ilişkin akışa Rehber'in 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 (Z)" ve "Opsiyonel (O)" detay denetim testleri
- Sürecin ve kontrollerin gösterildiği örnek bir akış şeması

verilmiştir. Söz konusu akış aşağıdaki şekilde de gösterilebilir.

Şekil 6 – BT Yönetim Süreçleri Denetimi İçin Denetim Prosedürlerinin Akışı

Daha önce de belirtildiği üzere, Rehber içerisinde belirtilen denetim testleri iç denetçi yetkinliğine göre üç farklı seviyeye ayrılmıştır. Tablo 1'de tanımlanan bu seviyeler dikkate alınarak gerekli görülen durumlarda belirli prosedürlerin yerine getirilmesi için farklı seviyedeki iç denetçilerin görev alması değerlendirilmelidir.

Uygulama Kontrolleri Denetimi

Uygulama kontrollerinin denetiminde gündeme gelebilecek uygulama kontrolleri tipleri ve bunlara ilişkin örnek kontrollere Rehber'in 5. bölümünde yer verilmiştir. Bununla birlikte gerek faaliyet alanı ve iş süreçlerindeki gerekse de BT uygulama altyapısının karmaşıklık seviyelerindeki farklılıklar sebebiyle uygulama kontrolleri kurumdan kuruma farklılaşabilir ve her kurum için ortak denetim testlerinin oluşturulması pratikte mümkün değildir. Bu nedenle kurum içindeki uygulama kontrollerinin iç 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 muhtemel aksaklıkların ortaya konması
- Faaliyet alanı ve iş süreçlerini destekleyen iş uygulamalarının çalışma mantıklarının, birbiriyle olan veri akışlarının, süreç içerisinde kullanılan verilerden hangilerini ilettiklerinin, işlediklerinin ve sakladıklarının ve ayrıca kurumun muhasebe bilgi sistemi işleyişinin anlaşılması
- Belirlenen riskler ve yaşanması muhtemel hataların önlenebilmesi 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 kontrollerin hangilerinin mevcut durumda ilgili iş uygulaması üzerinde bulunduğunun anlaşılması

Yukarıda belirtilen hususların tamamlanmasını takiben iç denetçi her bir uygulama kontrolü için Rehber'in beşinci bölümünde belirtilen yönlendirmeler ışığında denetim görevlerini gerçekleştirir ve sonuçlarını değerlendirir.

BT Altyapı Genel Kontrolleri Denetimi

Uygulama risk değerlendirmesi sonucu kapsama alınan BT uygulamaları ve teknoloji envanterinde belirtildiği üzere bu uygulamaların üzerinde çalıştığı ve kullandığı altyapı bileşenleri üzerinde yürütülebilecek denetim testleri Rehber'in altıncı bölümünde belirtilmiştir.

BT Altyapı Genel Kontrolleri, denetimin uygulama alanı ve gerçekleştirilecek risk değerlendirme sonuçlarına bağlı olarak kapsama alınan uygulamalar üzerinde gerçekleştirilen denetim görevlerini altyapı seviyesine de uygulanması gereken durumlarda ele alınabilecek ve özellikle güvenlik odaklı bakış açısına sahip nitelikte kontrollerdir. Bunun yanı sıra, kapsama alınan uygulamalar üzerinde gerçekleştirilen kontrol etkinliği çalışmalarını desteklemek ve bu uygulamalar üzerine verilecek güvence seviyesine destek olunması amacıyla da 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 seviyelerde (işletim sistemi, veritabanı, ağ) ele alınabileceği gibi, iç denetçinin yargısına ve risk algısına bağlı olarak belirli seviyeler ya da seçilen seviyelerden belirli kontroller de 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 konu hakkında bilgi alınabilir.

Denetim testlerini gerçekleştirecek olan iç denetçi, öncelikle Rehber'de açıklanmış olan ilgili sürecin tanımını ve kontrol hedeflerini anlamalıdır. Buna ek olarak örnek kontrol akışının incelenmesi, kontrol akışının bir kurumda nasıl işleyebileceğini anlamak açısından yardımcı olacaktır. Akışın ardından süreçle ilgili riskler ve bu risklerin etkin bir şekilde karşılanması amacıyla belirlenen kontroller tablo halinde listelenmektedir. Bu tabloda, seçilen belirli risklere karşı gelecek kontroller bulunabilir. Devamında ise bu kontroller incelenir ve etkinliğini değerlendirmek üzere tasarlanmış olan detay denetim testleri uygulanır.

Denetim testlerinin uygulama zorunluluğu "Zorunlu" ve "Opsiyonel" 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 "Opsiyonel" olarak işaretlenmiş denetim testleri de uygulanabilir. Bununla birlikte, Rehber'in sınırlayıcı olmadığı da dikkate alınmalı ve denetlenen kuruma özgü durumların mevcudiyeti halinde, ek kaynaklardan da yararlanılarak riskler, kontroller ve ilgili denetim testleri denetimin hedefine uygun şekilde güncellenmelidir.

Çalışma Kâğıtlarının Kullanımı

Denetim çalışmalarının belgelendirdiği en önemli araç, çalışma kâğıtlarıdır (***Ek 4 – Örnek Çalışma Kâğıdı***). Çalışma kâğıtları, form şeklinde ve iç denetçi tarafından doldurulmak üzere hazırlanmıştır.

Söz konusu Örnek Çalışma kâğıdının ilk sütunu denetlenen süreci (değişiklik yönetimi, operasyon yönetimi vb.) 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 testinin numarası ve kontrolün gerçekleşme frekansı/sıklığı belirtilir.

Çalışma kâğıdı doldurulurken aşağıdaki hususlara dikkat edilmelidir:

- Denetlenen Süreç: Bu bölüme gerçekleştirilen testin bağlı bulunduğu süreç Rehber'deki adıyla yazılır. (Ör: Değişiklik Yönetimi)
- İlgili Birim: Teste konu olan durumun ilgilendirdiği birim (Ör: BT Değişiklik ve Konfigürasyon Yönetimi Bölümü)
- Denetim Testi No: Testin numarası Rehber'de belirtildiği şekliyle yazılır (Ör: K1.T1).
- Denetim Testi: Testin açıklaması Rehber'de belirtildiği şekliyle yazılır.
- Kontrol Frekansı: Test edilen konunun gerçekleştirilme sıklığıdır.

Üzerinden gitme (ÜG) çalışmaları ilgili sütunda:

- Çalışmayı gerçekleştiren kişinin ismi,
- Çalışmanın gerçekleştirildiği tarih,
- Seçilen örnek
- Açıklama ve
- Kanıt numarası/referansı

belirtilecek şekilde belgelenir.

Gerçekleştirilen test çalışması yine aynı ÜG için yapılan çalışmaya benzer şekilde belgelenir, ek olarak test çalışması ile ilgili örneklem popülasyonu ve seçilen örneklere ilişkin bilgiler sağlanır.

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 kâğıtlarında belirtilen kontroller ve yürütülen çalışmalar denetim gözetim sorumlusu tarafından gözden geçirilir ve denetim gözetim sorumlusunun ismi ve gözden geçirme tarihi "Gözden Geçirme" sütununa yazılır.

2.3.2. Bulguların Değerlendirilmesi

Denetim 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. 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 ardından olumsuz bir kanaate varılması gerekmektedir.

İç 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 arz eden konular mümkün mertebe birleştirilmeye çalışılır.

Hazırlanmış olan bulgu denetlenen birim tarafından okunduğunda, bulgunun içeriğini, nedenini, bulgunun yaratabileceği riskleri net olarak anlatacak 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, değerlendirilmeleri sırasında belirli bir ölçeklendirme yöntemine göre sınıflandırılmaları gerekebilir. Söz konusu sınıflandırma için KİDR'da verilmiş olan bulgu önem düzey tablosu kullanılır.

Tablo 3 - Bulgu Önem Düzey Tablosu

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 durdurmasına 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 uğratacak 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 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, Uluslararası genel kabul görmüş standartlar ve Ulusal ya da uluslararası iyi uygulamalar)

Bulguların kayıt altına alınması ve takip edilmesi amacıyla KİDR ekinde yer alan örnek formlar kullanılabilir.

2.4. Raporlama ve İzleme

2.4.1. Denetim raporunun hazırlanması ve sunumu

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

Tespit edilen bulgular, rapor aşamasına geçmeden denetlenen birim yöneticileri ve sorumluları ile paylaşılır ve bulgular üzerine mutabakat aranır.

Bulguların öncelikle denetlenen birim yöneticileri ve sorumlularına sunulmasının sebebi, gerek iç denetçinin gözünden kaçan bilgi, belge ve kanıtlar sebebiyle gerekse de denetlenen birim tarafından zamanında iç denetçiye iletilememiş ek bilgiler ya da belgeler sebebi ile bulgu olarak nitelendirilmemesi gerekirken bulgu olarak belirtilen hususların tespit edilmesi ve buna istinaden yapılabilecek güncellemeler sonrasında denetim ekibi ile denetlenenin bulgular üzerinde mutabakata varmasına izin vermesidir.

Denetim bulguları, Bulgu Paylaşım Formları aracılığıyla DGS tarafından denetlenen birime/birimlere gönderilir. Bildirimde, kapanış toplantısının tarihi, yeri, kimlerin katılmasının faydalı olacağı hususu ile toplantının gündemi belirtilir. Ayrıca bu bildirimde Bulgu Paylaşım Formlarının, ne kadar süre içerisinde cevaplanarak İDB'ye iletilmesi gerektiği de belirtilir. Bulgu ve önerilerin, karar alıcı konumda bulunan yöneticilerle paylaşılması yerinde olacaktır.

Kapanış toplantısı denetlenen birim yöneticileri ve sorumluları ile gerçekleştirilir. Bu toplantıda bulgular denetlenen birimle paylaşılır, bulgulara dair öneriler sunulur ve denetlenen birimin bulgular için ne gibi düzeltici ya da önleyici aksiyonlar alacağı hakkında görüşleri alınır.

Kapanış toplantısında denetim ekibi, 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, denetim ekibi tarafından ek prosedürler uygulanarak tespitlerde düzeltme ve güncelleme yapılabilir.

Bulgular üzerinde denetim ekibi ile denetlenen arasında bir uyuşmazlık olduğunda KİDR'da verilmiş olan karar mekanizması kullanılır.

Tablo 4 - 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. (Düzeltilebilir husus)	Denetlenen birimin görüşüne katılıyor.	→		Düzeltme yapılarak raporda yer verilir.
Bulguya katılmıyor.	Denetlenen birimin görüşüne katılmıyor.	Uzlaşılamayan 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.

Denetim raporu içinde bulunması gereken en temel unsurlar 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.

Denetim raporu aşağıdaki içerikte sunulmalıdır:

a) Rapor kapağı: Rapor kapağında, İDB'nin adına, denetim adına, denetim alanına, denetimi gerçekleştiren iç denetçilere, gözetim sorumlusuna, 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 (Tablo 5'e bakınız),
- Denetlenen faaliyet ve süreçle ilgili yaygınlaştırılmasında fayda görülen hususların yer aldığı "Başarılı performans ve iyi uygulama örnekleri" bölümü.

Denetim raporunun gözden geçirilmesi, dağıtım listesinin hazırlanması ve resmi bir şekilde iletilmesi için gerekli esas ve yöntemler ile kullanılabilecek şablona, KİDR'da yer verilmiştir.

Tablo 5 - Denetim Görüşü Oluşturma Tablosu		
	Açıklamalar	**Kurallar**
1	BT kontrol ihtiyacının farkına varılmıştır. BT risklerinin ve kontrollerinin belirlenmesine yönelik gelişi güzel ve kişilere bağlı bir yaklaşım söz konusudur. Kontrol zayıflıkları belirlenmemektedir. Kontrollere ilişkin sorumlulukların belirlenmesinde yetersizlikler bulunmaktadır. BT'nin kendinden beklenenleri yerine getirebilme durumu ile ilgili bir değerlendirme bulunmamaktadır.	Denetlenen faaliyetle ilgili olarak "1 – Başlangıç" değerlendirmesi yapılabilmesi için, iki veya daha fazla kritik önem düzeyine sahip bulgunun olması gerekir.
2	BT ortamında kontroller uygulanmakla birlikte, dokümantasyonda eksiklikler bulunmaktadır. Kontrollerin çalışması, ilgili kişilerin bilgi ve motivasyonlarına bağlı olarak değişmektedir. Kontrollerin etkililiği değerlendirilmemektedir. Kontrol zayıflıkları tam olarak ortaya konamamakta ve öncelik sırasına göre çözüme kovuşturulmamaktadır. Kontrollere ilişkin sorumluluklar kısmen belirlenmiştir. BT'den beklenenler bilinmektedir ancak sistematik olarak takip edilmemektedir.	Denetlenen faaliyetle ilgili olarak "2 – Sınırlı/Sistematik Olmayan" değerlendirmesi yapılabilmesi için, bir kritik veya iki ve daha fazla yüksek önem düzeyine sahip bulgunun olması gerekir.
3	BT ortamında kontroller uygulanmakta ve yeterli düzeyde kayıt altına alınmaktadır. Düzenli olarak kontrollerin çalışıp çalışmadığı kontrol edilmektedir. Ancak bu değerlendirme süreci yazılı olarak belirlenmemiştir. Yönetim, büyük ölçüde kontrolleri takip edebilmekte, ancak gözden kaçan hususlar olabilmektedir. BT'nin kendinden beklenenleri ne ölçüde karşılayabildiği takip edilmektedir, ancak bu faaliyet yazılı olarak gerçekleştirilmemektedir.	Denetlenen faaliyetle ilgili olarak "3 – Gelişime açık" değerlendirmesinin yapılabilmesi için, kritik önem düzeyine sahip bulgu bulunmaması ve en fazla bir yüksek önem düzeyine sahip bulgunun olması gerekir.
4	BT için bir risk yönetimi ve iç kontrol ortamı bulunmaktadır. Yazılı olarak tanımlanmış ve düzenli olarak yürütülen bir kontrol değerlendirme süreci bulunmaktadır. Yönetim kontrollerle ilgili sorunları hızla tespit ederek öncelik sırasına uygun ve tutarlı bir şekilde çözüme kovuşturabilmektedir. BT'nin kendinden beklenenleri karşılama düzeyini yazılı olarak takip edilmekte ve değerlendirilmektedir.	Denetlenen faaliyetle ilgili olarak "4 – Yeterli" değerlendirmesinin yapılabilmesi için kritik, yüksek veya orta düzeyde bir bulgunun bulunmaması gerekir.
5	BT ile ilgili risk ve kontrol değerlendirme faaliyetleri, kurum kontrolleri ile entegre olarak yürütülmektedir. BT süreçlerindeki kontroller sürekli olarak takip edilmektedir. . Sorun tespit edilen alanlarda kök neden analizleri yapılarak gerçekçi çözümler üretilebilmektedir. Çalışanlar kontrollerin geliştirilmesi ve iyileştirilmesi sürecine aktif olarak katılmaktadır. BT kendinden beklenenleri takip etmekte ve sürekli gelişim için faaliyet göstermektedir.	Denetlenen faaliyetle ilgili olarak "5 – Gelişmiş" değerlendirmesinin yapılabilmesi için, her hangi bir bulgunun bulunmaması gerekir.

2.4.2. Denetim sonuçlarının izlenmesi

Denetim çalışması sonucunda denetlenen birim ile mutabık kalınan ve hazırlanmış olan Denetim Raporu eşliğinde belirtilmiş olan bulgulara ilişkin denetlenen birim tarafından verilmiş olan iyileştirici, düzeltici ya da önleyici aksiyon planlarının, yine bu aksiyon planlarının tamamlanması için öngörülen 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 testlerinin yapılması vasıtasıyla yerine getirilir. Bu çalışmalar sonrasında gerekli aksiyonların alındığına kanaat getirildiği durumlarda ilgili bulgu "TAMAMLANMIŞ" olarak kapatılır. Bulgulara ilişkin aksiyon planlarının öngörülen tarih itibariyle tamamlanmadığının ya da tamamlanamayacağının anlaşıldığı durumlarda 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.

2.5. Kalite güvence

Denetim görevlerinin, denetim amaç ve kapsamına uygun yürütülüp yürütülmediği, buna ilave olarak gerçekleştirilen denetim testlerinin Rehber'de belirtilen hususlara, genel itibariyle KİDR'a ve ilgili olabilecek diğer mevzuat hükümlerine uygun ele alınıp alınmadığının kalite güvence açısından değerlendirilmesi gerekir. Kalite güvence çalışmasının temel amacı denetim sırasında karşılaşılan zorluklar, iç denetçilerin yaptıkları hatalar ya da denetim sırasında temel alınan rehber ve kılavuzlarda karşılaşılabilecek eksikliklerin zamanında tespit edilebilmesi ve bunlara ilişkin düzeltici önlemlerin zamanında alınabilmesine olanak sağlamaktır.

İDB Başkanı her bir denetim görevinin KİDS ile KİDR ve Rehber'e uygun olarak yürütülmesini sağlamak amacıyla kıdemli bir iç denetçiyi, yılı iç denetim programıyla DGS olarak görevlendirir. Yılı iç denetim programıyla üst yöneticiden yetki alması halinde İDB başkanı, yıl içerisinde DGS'lerde değişiklik yapabilir. Denetim gözetim sorumluluğu ile denetim gözetim sorumlularının belirlenmesinde KİDR'daki esaslar dikkate alınır.

Kalite güvence çalışmaları gerçek zamanlı olarak ve tamamlanan her denetim adımından sonra ele alınır. Kalite güvence 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 görevinde gerekli risk değerlendirmelerinin doğru bir şekilde tamamlanıp tamamlanmadığı
- Risk değerlendirmesi sonucunda denetim kapsamının doğru bir şekilde belirlenip belirlenmediği
- Önceki dönemlerden devam eden açık bulgu ya da risk alanlarının risk değerlendirmesinde ve kapsam belirlenmesinde göz önünde bulundurulup bulundurulmadığı
- 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 kâğıtlarının ve ilgili kanıtlara ilişkin belgelerin uygun şekilde hazırlanıp hazırlanmadığı
- Yapılan tüm çalışmalara ilişkin uygun kayıtların ve belgelerin hazırlanıp hazırlanmadığı
- Rehber, KİDR, ilgili diğer kılavuz ve yönergeler uyarınca denetim sırasında yerine getirilmesi gereken bir faaliyetin tamamlanamadığı durumlar için ilgili durumun gerekçesi ile birlikte kayıt altına alınıp alınmadığı

Öte yandan, her bir denetim raporu İDB Başkanı tarafından gözden geçirilir. Bu kapsamda KİDR ekinde yer alan Rapor Gözden Geçirme Kontrol Listesinden yararlanılabilir.

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 Seviyesi Kontroller

Genel Tanım

Bu bölüm kurum seviyesi kontrollerin değerlendirilmesi amacı ile uygulanması önerilen denetim testlerini 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. Kurumun BT organizasyonu, süreçleri ve altyapısı üzerinde de tüm kurumu etkileyen kapsayıcı iç kontroller bulunmaktadır.

Kurum seviyesi kontroller, bir hata ya da dolandırıcılık sonucu olarak mali tablolarda herhangi bir yanıltıcı bilgi bulunma riskinin değerlendirilmesi, gerçekleştirilecek denetim süreçlerinin yapısının tasarlanması ve bütçe ve kapsamının belirlenmesi amacı ile denetçi tarafından iyi anlaşılmalıdır. Bu sebeple, mali raporlamaların BT üzerinde ilerlediği kurumlarda BT kurum seviyesi kontrollerinin de kapsamlı olarak değerlendirilmesi gereklidir. Ancak BT kurum seviyesi kontroller, kurumun yönetiminin yönerge ve talimatlarının bir bütün olarak anlaşılması açısından tüm denetim tipleri için geçerlidir. Netice itibariyle kurumsal risk yönetiminin de önerdiği ana bileşenlerden biri olan kontrol ortamının anlaşılması ve değerlendirilmesi sırasında yukarıda bahsi geçen BT kurum seviyesi kontrollerinin anlaşılması önem arz etmektedir.

Yukarıda belirtilen çerçevede BT kurum kontrolleri olarak politika ve prosedür yapısı, kurumsal mimari, proje ve portföy yönetim çerçevesi, BT performansının değerlendirilmesi ve BT iç kontrolünün izlenmesi gibi temel faaliyetlere yer verilmiştir. Çeşitli kaynaklarda BT kurum kontrolleri olarak da ele alınabilen bazı kontrollere ise BT Yönetim süreçlerinin zorunlu denetim testlerinde yer verilmiştir.

Kurum Seviyesi Kontroller

Süreçte yer alan tipik kontrollere aşağıdaki tabloda yer verilmiştir:

Kurum Seviyesi Kontroller	
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.
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.
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.
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.
K5	Kurum BT iç kontrol ortamı düzenli olarak izlenir ve değerlendirilir. Bu değerlendirmelere öz değerlendirmeler ile iç ve dış 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.

Risk – Kontrol Eşleşmeleri

Kurum Seviyesi Kontroller Risk – Kontrol Eşleşmeleri					
Riskler	**K1**	**K2**	**K3**	**K4**	**K5**
R1. Kurumun yönetim yaklaşımının BT tarafından doğru anlaşılamaması	+			+	
R2. Kurum stratejisinin ve hedeflerinin BT tarafından desteklenmemesi	+	+	+		
R3. Kurum hedefleri doğrultusunda çalışmayan BT yapısı sebebiyle 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 Testleri

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 testleri**	**T/İ[1]**	**Z/O[2]**	**YS[3]**
K1.T1	BT'nin kurum içerisindeki önemi değerlendirilerek organizasyonel yapı içerisinde hangi seviyede konumlandırıldığı gözlemlenir.	T	Z	2
K1.T2	Kurum bünyesindeki BT organizasyon yapısı incelenir ve yapının iş hedeflerine ve BT önceliklerine uygun şekilde yapılandırıldığı kontrol edilir.	T	Z	2
K1.T3	Kurum bünyesinde tüm BT personelinin rol ve sorumluluklarının tanımlanmış olduğu ve bunların kurum BT hedeflerini gerçekleştirmesi için en uygun şekilde belirlendiği gözlemlenir.	T	Z	2
K1.T4	Kurum bünyesinde BT yönetimi ile ilgili politika ve prosedürlerin oluşturulduğu gözlemlenir. Bunların kurum ihtiyaçlarına uygun şekilde yapılandırıldığı gözlemlenir.	T	Z	2
K1.T5	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.	T	Z	2
K1.T6	Kurum bünyesindeki prosedürlerin ve süreçlerin sürekli geliştirilmeye açık olduğu ve bu doğrultuda gerekli çalışmaların yapıldığı kontrol edilir. Bu çalışmaların izlemeyi, kalite yönetimini, otomasyonu ve eğitim aşamalarını içerdiği değerlendirilir.	İ	Z	1
K1.T7	Oluşturulmuş olan politika ve prosedürlere kurum bünyesinde uyum sağlanması için çalışmaların (eğitimler, duyurular, yaptırımlar) gerçekleştirildiği kontrol edilir.	İ	Z	1
K1.T8	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. Aşağıda örnek bir görevler ayrılığı kontrol tablosu bulunmaktadır.	İ	Z	1

[1] T/İ: Tasarım/İşletim
[2] Z/O: Zorunlu/Opsiyonel
[3] YS: Yetkinlik Seviyesi, (bkz. Tablo 1)

Görevler Ayrılığı Kontrol Tablosu													
	Kontrol Grubu	**Sistem Analisti**	**Uygulama Programcısı**	**Yardım Masası ve Destek Müdürü**	**Son Kullanıcı**	**Veri Girişi**	**Bilgisayar Operatörü**	**Veritabanı Yöneticisi**	**Ağ Yöneticisi**	**Sistem Yöneticisi**	**Güvenlik Yöneticisi**	**Sistem Programcısı**	**Kalite Güvencesi**
Kontrol Grubu		x	x	x		x	x	x	x	x		x	
Sistem Analisti	x			x	x		x				x		x
Uygulama Programcısı	x			x	x	x	x	x	x	x	x	x	x
Yardım Masası ve Destek Md.	x	x	x		x	x		x	x	x		x	
Son Kullanıcı		x	x	x			x	x	x			x	x
Veri Girişi	x		x	x			x	x	x	x	x	x	
Bilgisayar Operatörü	x	x	x		x	x		x	x	x	x	x	
Veritabanı Yöneticisi	x		x	x	x	x	x		x	x		x	
Ağ Yöneticisi	x		x	x	x	x	x	x					
Sistem Yöneticisi	x		x	x		x	x	x				x	
Güvenlik Yöneticisi		x	x			x	x					x	
Sistem Programcısı	x		x	x	x	x	x	x		x	x		x
Kalite Güvencesi		x	x		x							x	

(x) ile belirtilen alanlardaki görevlerin aynı kişide bulunması kontrol zayıflığına neden olabilir.

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 testleri**	**T/İ**	**Z/O**	**YS**
K2.T1	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	2
K2.T2	Hedeflenen mimari yapıya ulaşılması için kurum tarafından yapılması gerekenlerin bir plan çerçevesinde belirlendiği ve hayata geçirildiği gözlemlenir. Mevcut durumda uygulanan ya da gelecekte uygulanacak çözümlere ilişkin değerlendirmelerin gerçekleştirildiği ve kurum yapısına en uygun ve en verimli çözümün seçilmesi için azami gayret gösterildiği kontrol edilir. Belirlenen zaman planında bir gecikme olup olmadığı ve varsa bunun nedenleri tartışılır.	İ	Z	2
K2.T3	Kurumsal mimari bileşenleri arasındaki etkileşimlerin ve ilişkilerin tanımlanmış ve kayıt altına alınmış olduğu kontrol edilir.	T	Z	2
K2.T4	Mimari yapının kurum bünyesinde yerleştirilmesi için bir uygulama planının oluşturulduğu ve düzenli olarak gözden geçirilerek gerektiği durumlarda güncellendiği gözlemlenir.	İ	Z	2

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 testleri**	**T/İ**	**Z/O**	**YS**
K3.T1	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 özellikler gösterebilen ya da kaynak kullanımı ya da zamanlama gibi belirli kriterlerde ortak unsurlar taşıyan birçok projenin merkezi bir şekilde yönetimini ifade eden portföy ve projelerin yönetimi amacıyla bir çerçevenin ya da politikanın tanımlandığı kontrol edilir.	T	Z	2
K3.T2	Kurum ve BT stratejisine uygunluk, maliyet, getiri ve risk gibi etmenlerin değerlendirilmeye alınarak projelerin önceliklendirildiği gözlemlenir.	İ	Z	2
K3.T3	BT program, portföy ve projelerinin yürütülmesi için gereken bütçenin belirlendiği ve farklı finansman yöntemlerinin göz önünde bulundurulduğu örneklem bazında gözlemlenir. Bütçe takibinin düzenli olarak yapılıp yapılmadığı incelenir.	İ	Z	2
K3.T4	Yüksek öncelikte olan programların ve projelerin fizibilite çalışmaları ve maliyet-fayda analizleri dikkate alınarak seçildiği ve buna uygun şekilde yürütüldüğü gözlemlenir.	İ	Z	2
K3.T5	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	2
K3.T6	Kurum bünyesinde programların ve bunların dâhil olduğu BT yatırım portföylerinin düzenli olarak takip edildiği ve güncellendiği gözlemlenir.	İ	Z	2
K3.T7	Gerçekleştirilen projelerin ve programların ardından faydaların gözlemlendiği ve öğrenilen derslerin saptanarak kaydedildiği gözlemlenir.	İ	Z	2

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 testleri**	**T/İ**	**Z/O**	**YS**
K4.T1	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	2
K4.T2	Oluşturulan performans ölçüm ve değerlendirme sistemi için hedef performans değerlerinin belirlendiği ve ilgili yönetim birimlerince onaylandığı gözlemlenir.	T	Z	2
K4.T3	Performans değerlerinin belirlenen ölçütler çerçevesinde düzenli olarak ölçüldüğü ve kayıt altına alındığı kontrol edilir.	İ	Z	1
K4.T4	BT fonksiyonunun performansının son kullanıcılar tarafından da değerlendirilmesine imkan tanıyan bir son kullanıcı memnuniyet çalışmasının (anket, vb.) yapıp yapılmadığı sorgulanır. Çalışmanın yapılması durumunda dile getirilen hususlar BT yönetimi ile görüşülür ve mevcut aksiyon durumu tartışılır.	İ	Z	1
K4.T5	Toplanan performans değerlerinin analiz edildiği ve raporlandığı gözlemlenir. Raporların ilgili paydaşlarla ve yönetim kademeleriyle paylaşıldığı kontrol edilir.	İ	Z	1
K4.T6	Performans incelemelerinin sonucu olarak düzeltici ya da önleyici faaliyetlerin gerçekleştirildiği teyit edilir.	İ	Z	1

K5 - Kurum BT iç kontrol ortamı düzenli olarak izlenir ve değerlendirilir. Bu değerlendirmelere öz değerlendirmeler ile iç ve dış 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 testleri**	**T/İ**	**Z/O**	**YS**
K5.T1	Kurum bünyesindeki BT kontrollerinin 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	2
K5.T2	Süreç sahiplerinin, süreçler üzerindeki kontrollerin etkinliğini ve geçerliliğini ölçmek için öz değerlendirmeler gerçekleştirdiği gözlemlenir.	İ	Z	2
K5.T3	Gerçekleştirilen BT iç kontrol değerlendirmelerinde mevzuata uyum kriterinin dikkate alınmış olduğu gözlemlenir.	İ	Z	2
K5.T4	Kurum hedeflerine ulaşılabilmesi için BT iç kontrol ortamının sürekli olarak izlendiği ve en iyi uygulamalar incelenerek geliştirildiği gözlemlenir.	İ	Z	2
K5.T5	Kurum bünyesinde denetim faaliyeti gerçekleştiren bölüm ve kişilerin bağımsız olduğu ve bu faaliyetleri gerçekleştirmek için yeterli yetkinliğe sahip oldukları değerlendirilir.	İ	Z	2

Ek Kaynaklar

- ISACA, (2007). COBIT 4.1 Framework – PO1, PO2, PO4, PO9, PO10. Rolling Meadows, Illinois, ABD.
- ISACA, (2012). COBIT 5 Enabling Processes – APO01, APO02, APO03, APO12. Rolling Meadows, Illinois, ABD.
- ISO/IEC, (2005). ISO/IEC 20000 3.1 Management Responsibility.
- ISO/IEC, (2005). ISO/IEC 20000 4.0 Planning and Implementing Service Management.
- ISO/IEC, (2005). ISO/IEC 20000 4.4 Continual Improvement.
- ISO/IEC, (2005). ISO/IEC 20000 5.0 Planning and implementing new or changed services.
- UK Cabinet Office, (2011). ITIL V3 2011 Continual Service Improvement, 4.1 The 7 Step Improvement Process.
- UK Cabinet Office, (2011). ITIL V3 2011 Service Strategy, 4.1 Strategy Management for IT Services.

3.2. BT Yönetişim Süreci Denetimi

Sürecin Genel Tanımı

Yönetişim süreçleri, kurumun amaçlarının uzlaşma dâhilinde belirlenebilmesi için paydaş ihtiyaçlarının, koşulların ve alternatiflerin değerlendirilmesi; önceliklendirme ve karar verme mekanizmaları sayesinde kuruma yön verilmesi ve nihayetinde kararlaştırılan yön ve amaçlara uyumun izlenmesi unsurlarını kapsamaktadır. Bu çerçevede BT yönetişimi de kuruma BT açısından yön verilmesi ile ilgilenmektedir.

Yönetişim ile yönetim arasında önemli bir farklılık bulunmaktadır. COBIT 5 çerçevesinde de belirtildiği üzere, yönetim süreçleri yönetişimden daha farklı bir katmana odaklanır. Buna göre yönetim süreçleri, kurumun amaçlarına ulaşabilmesi için yönetişim organları tarafından belirlenen yönün takip edilebilmesini sağlayan aktivitelerin planlanması, geliştirilmesi (oluşturulması), işletilmesi ve izlenmesi faaliyetlerini içerir. Özetle BT yönetişimi kurumun BT ile ilgili yön ve amaçlarının belirlenmesine odaklanırken, BT yönetimi ise bu yön ve amaçların operasyonel anlamda hayata geçirilmesi üzerinde durmaktadır. BT yönetimine ilişkin süreçlerin denetimi Rehber'de bir sonraki bölümde ele alınmıştır.

BT yönetişim süreçlerinin denetlenmesi sayesinde, kurumu ilgilendiren BT kararlarının nasıl alındığı, BT ile ilgili yönlendirmenin nasıl yapıldığı, hedeflerin nasıl oluşturulduğu, fayda-risk-kaynak dengesinin nasıl gözetildiği gibi hususlarla birlikte, kurumsal yönetim ilkelerinin de temel olarak BT fonksiyonu üzerinde nasıl uygulandığı konusunda genel bir değerlendirme yapmak mümkün olmaktadır.

Yönetişim Süreci Kontrolleri

Süreçte yer alan tipik kontrollere aşağıdaki tabloda yer verilmiştir:

Yönetişim Kontroller	
K1	Kurum bilgi teknolojileri yönetişim 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.
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.
K3	Yatırımlar sonucu iş süreçlerinden, BT hizmetlerinden ve BT varlıklarından sağlanan fayda uygun maliyetlerle en iyi seviyeye yükseltilir.
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 teknolojilerinin kullanımı ile ilgili riskler de belirlenir ve yönetilir.
K5	Kurumun kaynak ihtiyaçları kurum hedeflerini destekleyecek şekilde karşılanır, BT'ye dair kaynak harcamaları optimize edilir.
K6	Paydaşların performans ve uyum takibi şeffaf bir şekilde paydaşlarla mutabık kalınarak gerçekleştirilir. İyileştirici faaliyetler için paydaşlarla iletişimler etkili ve zamanlı bir şekilde yürütülür.

Yönetişim Kontrolleri Risk – Kontrol Eşleşmeleri						
Riskler	**K1**	**K2**	**K3**	**K4**	**K5**	**K6**
R1. İş ve bilgi teknolojileri stratejilerinin eşgüdümlü olmaması	+	+				
R2. Performans ölçütlerinin iş, yönetişim ve yönetim ihtiyaçlarını karşılamayacak şekilde tanımlanması	+					
R3. İş birimlerinin beklenti ve ihtiyaçlarının yeterli şekilde tanımlanamaması ya da anlaşılamaması	+	+	+	+		
R4. Gelişim fırsatlarının belirlenememesi		+	+			
R5. Üst düzey 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 önceliklendirmesinin yapılamaması	+				+	
R10. Kurum ve bilgi teknolojileri kaynak yönetim stratejilerinin uyumsuz olması	+				+	
R11. Kurum paydaşlarının performansının beklentileri karşılayamaması						+
R12. Paydaşlarla kurum arasında hedefler konusunda anlaşmazlıkların çıkması						+

Denetim Testleri

K1 - Kurum bilgi teknolojileri yönetişim 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 testleri**	**T/İ**	**Z/O**	**YS**
K1.T1	Kurum hedeflerinin gerçekleşmesi açısından BT'nin öneminin anlaşıldığı ve bu yöndeki rolünün belirlendiği gözlemlenir. Bu doğrultuda kurum BT stratejisi ve yönetişim ile ilgili politika, yönerge ve diğer dokümanlar incelenir. Bu dokümanlar tasarlanırken kamu ve kurum ihtiyaçlarının gözetildiği teyit edilir.	T	Z	2
K1.T2	Yönetişim rol ve sorumluluklarının tanımlandığı, kurum ve BT fonksiyonlarının iletişim kanallarının tesis edildiği ve iletişim yöntemlerinin önceden belirlenmiş olduğu teyit edilir.	T	Z	1
K1.T3	Kurumun BT ile ilgili kararlarının nasıl alındığına ilişkin sürecinin ve buradaki rol ve sorumlulukların tanımlı olduğu teyit edilir. Yetki devri söz konusu ise bunun hangi kurallar çerçevesinde yapıldığı incelenir.	T	Z	1
K1.T4	Kurumun BT yönetişim performans ölçütlerinin tanımlı olduğu BT yönetişiminin söz konusu ölçütler kullanılarak düzenli olarak değerlendirildiği teyit edilir.	İ	Z	2

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 testleri**	**T/İ**	**Z/O**	**YS**
K2.T1	BT stratejisi ile ilgili tüm planlarda ve diğer belgelerde kurum hedeflerinin temel alındığı incelenir. Bu dokümanların kurum hedeflerinin dikkate alınarak oluşturulduğu gözlemlenir.	T	Z	2
K2.T2	Mevcut BT yeteneklerinin ve dışarıdan sağlanan BT hizmetlerinin kurum hedeflerinin gerçekleştirilmesi konusunda yeterlilik açısından değerlendirildiği gözlemlenir.	T	Z	2
K2.T3	Ulaşılmak istenen BT yapısı için bir stratejik plan oluşturulduğu ve izlenecek yolun tanımlandığı gözlemlenir.	T	Z	2
K2.T4	Tanımlanan BT stratejisi ve yönünün kurum bünyesinde ilgili kişilerle paylaşıldığı kontrol edilir.	İ	Z	1
K2.T5	Kurum BT stratejisinin düzenli olarak gözden geçirildiği ve yenilendiği gözlemlenir. Bu sayede, kısa, orta ve uzun vadede yapılacakların belirlendiği gözlemlenir.	İ	Z	1
K2.T6	Kanun, yönetmelik ve yasalardaki değişikliklerin düzenli olarak izlenerek kurum stratejilerinin güncellendiği teyit edilir.	İ	Z	1
K2.T7	Üst yönetim strateji toplantı tutanakları incelenir ve bu toplantılarda alınan kararların alt birimlerce uygulandığı değerlendirilir.	İ	Z	1

K3 - Yatırımlar sonucu iş süreçlerinden, BT hizmetlerinden ve BT varlıklarından sağlanan fayda uygun maliyetlerle en iyi seviyeye yükseltilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K3.T1	Bilgi teknolojileri yatırım planı ve kurum stratejilerinin uyumu değerlendirilir. Yatırım planının hangi hedef ve ölçütler doğrultusunda oluşturulduğu incelenir.	T	Z	2
K3.T2	Bilgi teknolojileri yatırım planının ve proje gereksinimlerinin birbirleriyle örtüştüğü gözlemlenir. Projelerin, yatırım planının hangi unsurları veya hedefleri doğrultusunda belirlendiği incelenir.	T	Z	2
K3.T3	Projelerde fayda maliyet analizlerinin gerçekleştirildiği ve üst yönetimle paylaşıldığı teyit edilir. Fayda maliyet analizlerinin proje kararlarında bir ölçüt olarak kullanılıp kullanılmadığı araştırılır.	İ	Z	2
K3.T4	Bilgi teknolojileri yatırımlarının düzenli gerçekleşen komitelerde ya da çalışma gruplarında paydaşlar tarafından değerlendirildiği kontrol edilir. Bu değerlendirmelerde BT yatırımlarından sağlanan faydalara ilişkin bir gözden geçirmenin yapılıp yapılmadığı sorgulanır.	İ	Z	1
K3.T5	Bilgi teknolojileri fonksiyonu ve hizmetleri bazında proje ve yatırımların değerlendirilebilmesini sağlayacak izlemenin gerçekleştirildiği teyit edilir.	İ	Z	2

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 teknolojilerinin kullanımı ile ilgili riskler de belirlenir ve yönetilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K4.T1	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	2
K4.T2	BT risk iştahı ve toleransı temel alınarak hazırlanmış BT risk yönetimi dokümanları incelenir, yeterlilikleri değerlendirilir.	İ	Z	2
K4.T3	BT risk yönetim süreci, ana BT kontrol hedeflerini ve BT yönetim süreçlerini kapsaması açısından değerlendirilir.	T	Z	2
K4.T4	Risk yönetimi süreci, BT risk iştahı ve toleranslar ile belirlen ana BT kontrol hedefleri ve süreçlerinin birlikte değerlendirilmesi sonucunda hazırlanan risk envanterleri incelenir, yeterlilikleri değerlendirilir.	İ	Z	2
K4.T5	Düzenli hazırlanan risk değerlendirme raporları incelenir, süreç etkinliği bakımından değerlendirilir.	İ	Z	2
K4.T6	Risk envanterinde bulunmayan risklerin tespiti amacıyla düzenli gözlem yapıldığı değerlendirilir.	İ	Z	1
K4.T7	Tespit edilen BT risklerinin, kurumun genel risk yönetimi çerçevesinde bir girdi olarak değerlendirilip değerlendirilmediği incelenir. BT risk yönetiminin kurumun bütününde uygulanan risk yönetimi yaklaşımı ile ne ölçüde uyumlu olduğu araştırılır.	İ	Z	2

K5 - Kurumun kaynak ihtiyaçları kurum hedeflerini destekleyecek şekilde karşılanır, BT'ye dair kaynak harcamaları optimize edilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K5.T1	Personel yönetim dokümanlarının ve standartlarının kurum stratejisine uygun şekilde oluşturulduğu teyit edilir.	T	Z	2
K5.T2	Proje kaynak atamaları ve genel kurum stratejisi birbiriyle uyum açısından değerlendirilir.	T	Z	2
K5.T3	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	1
K5.T4	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	1

K6 - Paydaşların performans ve uyum takibi şeffaf bir şekilde paydaşlarla mutabık kalınarak gerçekleştirilir. İyileştirici faaliyetler için paydaşlarla iletişimler etkili ve zamanlı bir şekilde yürütülür.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K6.T1	Kurum bünyesinde paydaşlar için performans ve uyum raporlama ihtiyaçlarının kurum hedefleri ile uygun olarak tanımlandığı gözlemlenir.	T	Z	2
K6.T2	Kurum paydaşları ile iletişim şekillerinin kurum standartlarına uygun olarak belirlendiği, paydaş raporlamalarının kime iletileceği ve kim tarafından onaylanacağı gibi konuların kurum prensiplerine uygun olduğu teyit edilir.	T	Z	2
K6.T3	Kurum paydaşlarının raporlamalarının düzenli olarak takip edildiği, izlendiği ve bu izlemeler neticesinde iyileştirici eylemlerin alındığı gözlemlenir.	İ	Z	1
K6.T4	Paydaşlar ile ilişkilerin kurum hedeflerini destekleyecek şekilde yürütüldüğü gözlemlenir.	İ	Z	2

Ek Kaynaklar

- COSO, (2013). Integral Control – Integrated Framework Dunham, North Carolina, ABD.
- ISACA, (2007). COBIT 4.1 Framework – ME4. Rolling Meadows, Illionis, ABD.
- ISACA, (2012). COBIT 5 Enabling Processes – EDM01, EDM02, EDM03, EDM04, EDM05. Rolling Meadows, Illinois, ABD.
- ISACA, (2013). COBIT 5 for Risk. Rolling Meadows, Illinois, ABD.

4. BİLGİ TEKNOLOJİLERİ YÖNETİM SÜREÇLERİ DENETİMİ

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

- 4.1. Değişiklik 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. Değişiklik Yönetimi

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 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 suiistimallerden 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 denetimlerinde 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.

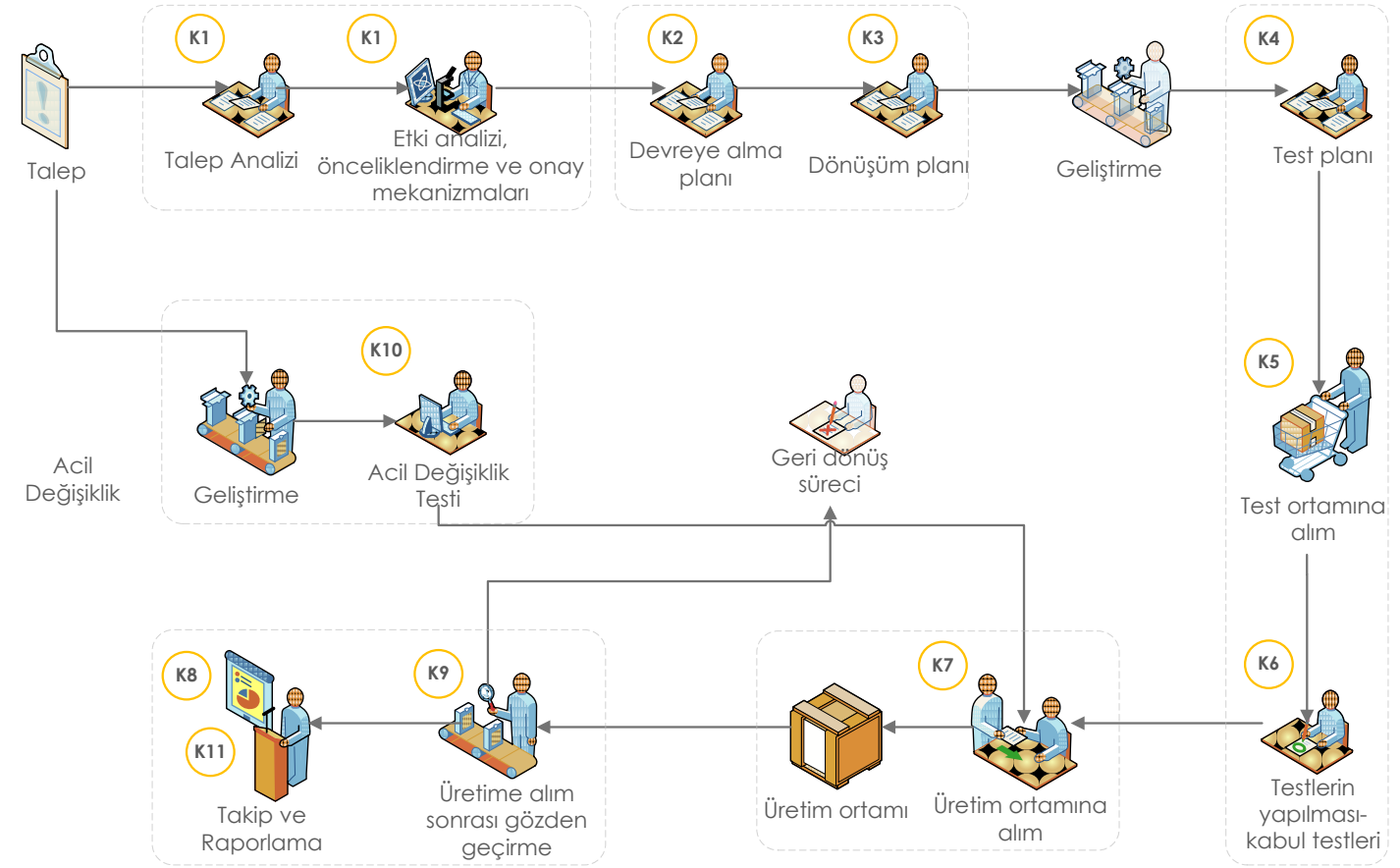
Kontrollere İlişkin Örnek Akış

Süreçte yer alan tipik kontrollere aşağıdaki tabloda yer verilmiştir:

Değişiklik Yönetimi – Kontroller	
K1	Değişiklik yönetimi sürecinde ilgili birimler tarafından 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 değişikler ile ilgili olarak canlı sistemde izlemeler ve geçiş sonrası tespit edilebilecek sorun ve problemlerin hızı çözümüne olanak sağlamak adına 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 indirgemek adına izleme ve takip faaliyetleri yürütülür.
K11	Reddedilen ve gerçekleştirilen tüm değişikliklerin raporlamaya uygun şekilde kayıt altına alınması amacıyla bir takip ve raporlama sistemi oluşturulur.

Bahsi geçen kontrollere ilişkin <u>örnek</u> akış şeması aşağıda yer almaktadır:

Değişiklik Yönetimi – Kontrollere İlişkin Örnek Akış



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. Yedekleme işlemi yapılmadan yeni sisteme geçilmesi nedeniyle ihtiyaç duyulan eski verilere ulaşılamaması	+	+	+				+				
R6. Değişikliklerin kayıt altına alınamaması 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 kalması				+	+	+		+			

Denetim Testleri

K1 - Değişiklik yönetimi sürecinde ilgili birimler tarafından gerçekleştirilecek etki analizi, önceliklendirme ve onay mekanizmaları vasıtasıyla, değişiklik yapılan uygulama ve/veya altyapı bileşenlerinin veri bütünlüğü ve güvenilirliğini olumsuz etkileyecek riskler azaltılır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K1.T1	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	1

K1.T2	Değişiklik yönetimi ile ilgili dokümanların (ör: politika, prosedür, akış, vb.) aşağıdakileri içerip içermediği kontrol edilir.
	• Süreçte rol alan personelin görev ve sorumluluklarının tanımı
	• Değişiklik kavramının ve tiplerinin tanımı (değişik tiplerine ilişkin örnekler aşağıdadır):
	  • Sürüm/versiyon yükseltmeleri ya da diğer program değişiklikleri,
	  • 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 ya da dış kaynak (destek hizmeti) kullanımıyla ilgili 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
		T	Z	2

	değerlendirilmesi • Değişiklik süreci içinde birbirinden ayrılması gereken sorumluluklara (değişikliklerin geliştirilmesi, test edilmesi, devreye/kullanıma alınması, izlenmesi/değerlendirilmesi) ilişkin görevler ayrılığı ilkesi			

K1.T3	• Kapsama alınan uygulama ve sistemler üzerinde denetim dönemi içerisinde gerçekleşmiş olan değişiklerin listesi temin edilir. Bu listenin temininde tercih edilecek ilk yöntem, mümkün olduğu durumlarda değişikliğin yapıldığı sistemin kendisi üzerinden ve değişikliklere ilişkin detayları içeren denetim izleri / log'ların temin edilmesidir. Bunun en önemli avantajı, yapılan değişiklerin tümünün (yani istatistiksel açıdan tüm değişiklik popülasyonunun) elde edilebilmesi ve böylece "tamlık" konusunda bir güvence sağlanabilmesidir.
	• Bazı sistemler kendi özelliklerinin bir parçası olarak bu denetim izlerini sağlayabilirler. Bazı yapılarda ise değişiklikler, bu amaçla üretilmiş özel araçlar yardımıyla canlıya alınır ve bu araçlar yardımıyla ilgili denetim izleri sağlanabilir. Böyle bir imkan bulunması durumunda canlı sistemden doğrudan temin edilen değişiklik listesi içerisinden, uygun görülen örneklem yöntemi kullanılarak gerekli sayıda örnek değişiklik seçilir.
	• Değişikliklerin listesine doğrudan canlı sistemden ulaşılamaması 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 tamlığından emin olunur ve ardından değişiklik yönetimi sürecinin değerlendirilmesi için gerekli örnekler bu manüel liste üzerinden seçilebilir.
	• Ek olarak işletim sistemleri ve veritabanı sistemleri üzerinde gerçekleştirilebilecek değişiklikler de bu kapsamda değerlendirilir. Söz konusu sistemler üzerinde gerçekleştirilebilecek değişikliklere örnek olarak aşağıdakiler sayılabilir:
	  • Versiyon yükseltmeleri
	  • Yama geçişleri
		İ	Z	2

	• Uygulama ve program kütüphanelerinde değişiklikler • Veritabanı sistemi üzerinde program ya da veri değişiklikleri			
K1.T4	Seçilen örnek değişiklikler üzerinden: • Faaliyet ya da süreç sahiplerinin, kendi alanları, faaliyetleri ya da süreçleri ile ilgili talep ettikleri değişiklikleri onayladıkları 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, sözleşmelerden ve hizmet seviyesi anlaşmalarından kaynaklanan gereksinimlerle uyumun sağlanıp sağlanamadığı 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. • Not: Yukarıda belirtilen unsurların bir kısmı kurum tarafından tüm değişiklik tipleri için yerine getirilmiyor olabilir. Kurumun mevcut prosedürleri, gerçekleştirilen risk analizleri, değişikliğin önem seviyesi, büyüklüğü, kapsamı ve etkisi gibi birçok etken hangi unsurların yerine getirileceği konusunda belirleyici olabilir. Denetçi çalışmalarında bu hususu da göz önüne almalı ve değişikliklerin yönetimi ve kontrolü konusunda bir belirsizliğin bulunmadığına yönelik incelemelerini derinleştirilmiştir.	İ	Z	2

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 testleri**	**T/İ**	**Z/O**	**YS**
K2.T1	Bir önceki adımda seçilen örnek değişiklikler üzerinden: • 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	2

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 testleri**	**T/İ**	**Z/O**	**YS**
K3.T1	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*	2
K3.T2	Dönüşüm planlarında, iş ve BT sürekliliği ile ilgili başarısız bir durumda ilgili sistemin ya da uygulamanın çalışır durumda bulunan bir önceki haline mevcut bulunan yedeklerden geri dönülmesi unsurlarına yer verildiği gözlemlenir.	T	O	1
K3.T3	Dönüşüm gerçekleştirilmiş değişikliklerden seçilen örnekler incelenir ve gerekli tüm dokümanların oluşturulduğu (dönüşüm planları, test dokümanları vb.), testlerin eksiksiz olarak gerçekleştirildiği, geri dönüşün gerekmesi ihtimaline karşı yapılacakların planlandığı ve ilgili denetim izlerinin toplanarak saklandığı gözlemlenir.	İ	O	2

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

K4 - Değişikliklerin testine yönelik rolleri, sorumlulukları, testlere ilişkin kriterleri ve test sonuçlarına ilişkin beklentileri tanımlayan bir değişiklik test planı oluşturulur.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K4.T1	İş ve BT süreç/sistem sahipleri ile iletişime geçilerek kurum standartlarıyla uyumlu bir test planının varlığı araştırılır.	T	O	1
K4.T2	Test planının, risk değerlendirmelerini, gerekli fonksiyonel ve teknik gereksinimleri, testi gerçekleştirmeye olanak sağlayacak kaynakları ve kabul kriterlerini içerdiği incelenir.	T	O	1
K4.T3	Test planının uygulanacak detaylı test aşamalarını içerdiği kontrol edilir. *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.*	T	O	2
K4.T4	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	3
K4.T5	Örnek olarak seçilecek değişikliklerde test adımlarının ilgili iş süreç sahipleri ve BT personeli tarafından belirlenen başarı kriterlerine göre değerlendirildiği kontrol edilir.	İ	O	2

K5 - Değişiklikler sonrasındaki durumu iş süreçleri ile BT uygulama ve altyapı bileşenleri açısından yansıtacak güvenli bir test ortamı oluşturulur.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K5.T1	Test ortamının üretim ortamından (canlı ortam) bağımsız olduğu ve fiziksel ya da mantıksal olarak üretim ortamından ayrıştırıldığı gözlemlenir.	T, İ	Z	2
K5.T2	Test ortamı içinde bulunan verilerin yetkisiz erişim açısından güvenliğinin sağlandığı ve test ortamında bulundurulan verilere erişimlerin kontrollü olduğu gözlemlenir.	İ	Z	3
K5.T3	Test ortamında kullanılacak test verileri üretim ortamından kopyalama suretiyle oluşturuluyorsa, bu verilerin bilgi gizliliği açısından üretim ortamından test ortamına aktarılması sırasında asıl/orijinal verilerin anlaşılamayacak bir şekilde karmaşık hale getirildiği incelenir. *Örnek olarak üretim ortamında bulunan ve vatandaşlara ait gerçek TC kimlik numaralarının test ortamına aynen değil, karıştırılarak aktarılması verilebilir.*	İ	O	3
K5.T4	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	3

K6 - Değişikliğin devreye alınması öncesinde "değişiklik kabul testleri" önceden belirlenmiş test planına ve/veya kriterlere göre gerçekleştirilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K6.T1	Değişikliklerin üretim ortamına taşınmalarından önce gerçekleştirilen son kabul test sonuçlarının, iş süreç sahipleri ile gerekiyorsa ilgili BT personeli ve ilgili olabilecek taraflarca, ilgili test planlarına uygun olarak onaylandığı kontrol edilir.	İ	Z	1
K6.T2	Test sürecinde ortaya çıkan hataların kaydedildiği, düzeltildiği ve düzeltilmiş değişikliğin tekrar test edildiği gözlemlenir.	İ	O	1

K7 - Test sonuçları başarılı olarak değerlendirilen değişikliklerin üretim ortamına aktarımı ve devreye alınması yazılım sürecinde görev almayan birim ya da kişiler tarafından gerçekleştirilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K7.T1	Değişikliklerin devreye alınmasının devreye alma planına uygun olarak gerçekleştirildiği gözlemlenir.	İ	Z	1
K7.T2	Değişikliklerin devreye alınması ve canlı/üretim ortama aktarımı otomatik olarak gerçekleşiyorsa, otomatik aktarım mekanizması incelenir; aktarımın sadece doğru hedeflere yapıldığı gözlemlenir. Eğer değişikliklere ilişkin dağıtım el yordamıyla (manüel) yapılıyorsa doğru hedeflere dağıtım yapıldığının nasıl kontrol edildiği sorgulanır. Bu amaçla ilgili personelle mülakat gerçekleştirilir ve aktarım yöntemine ilişkin detaylar (aktarıma ilişkin olası script (betik), batch (toplu iş), kopyalanan dosyalar, denetim izleri, vb.) incelenir.	İ	Z	3
K7.T3	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 (özellikle bu bilginin sağlanabildiği araçların varlığında) tüm değişiklikler için de yürütülebilir. Söz konusu incelemelerin yapılamadığı durumlarda, bilgi sistemleri üzerinde üretilmiş olan denetim izleri (loglar) temin edilip yetkisiz işlemlerin gerçekleştirilip gerçekleştirilmediği ya da işlemlerin onaylı personel tarafından gerçekleştirildiği değerlendirilir.	İ	Z	2
K7.T4	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	2
K7.T5	Değişikler sonrasında ilgili değişikliğin niteliğine bağlı olarak gerekli durumlarda ilgili iş süreçlerinin, sistem ve kullanıcı dokümantasyonunun ve varsa konfigürasyon yönetiminin takip edildiği sistemlerdeki konfigürasyon bilgilerinin güncellendiği gözlemlenir.	İ	O	2

K8 - Gerçekleştirilen değişikler ile ilgili olarak canlı sistemde izlemeler ve geçiş sonrası tespit edilebilecek sorun ve problemlerin hızı çözümüne olanak sağlamak adına belirli bir süre destek sağlanır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K8.T1	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	1
K8.T2	Devreye alınan değişiklikler ile ilgili açılan olay kayıtları incelenir ve bu olayların çözümlendiği teyit edilir.	İ	O	1

K9 - Değişikliklerin devreye alınmasını takiben çıktıları ve sonuçları gözlemlemek için bir "devreye alma sonrası gözden geçirme" çalışması gerçekleştirilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K9.T1	Uygulama sonrası gözden geçirme yöntemlerinin belirlendiği ve/veya prosedürlerinin oluşturulduğu gözlemlenir.	T	O	1
K9.T2	Devreye alma sonrası gözden geçirme adımlarının/prosedürlerinin aşağıdaki unsurları içerdiği gözlemlenir. • Hangi iş ihtiyaçları karşılanmıştır? • Projeden beklenen hangi faydalar sağlanmıştır? • Sistem ne kadar kullanılabilirdir? • 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	1
K9.T3	Devreye alma sonrası gözden geçirmelerde kullanılacak başarı kriterlerinin belirlenmesinde ilgili iş süreci ve/veya talep sahiplerinin de yer aldığı teyit edilir. *Talep sahibi iş birimi ya da değişikliklerden etkilenen birimler olabilir.*	T	O	1
K9.T4	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	2

K10 - Acil değişiklikler sonrası oluşabilecek ek sorunlar ya da güvenlik hususları en aza indirgenir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K10.T1	Acil değişiklik prosedürleri temin edilir ve acil değişiklik tanımının, acil değişiklerde uygulanacak aşamaların ve gerekli olabilecek ek erişim / yetkilendirme mekanizmasının söz konusu prosedür içinde belirtildiğinden emin olunur.	T	Z	1
K10.T2	Denetim dönemi içerisinde gerçekleşmiş acil değişikliklerin içinden örneklem seçilerek: • Acil değişikliğin prosedürlere uygun olarak gerçekleştirildiği, • Ek bir sistemsel erişim hakkı sağlanmış olması durumunda bu erişim hakkının temin ve kullanımına ilişkin kayıtların ve denetim izlerinin (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	2

K11 - Gerçekleştirilen ve reddedilen tüm değişikliklerin raporlamaya uygun şekilde kayıt altına alınması amacıyla bir takip ve raporlama sistemi oluşturulur.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K11.T1	Değişiklik raporlama ve takip sisteminin tüm birimlerce talep edilen ve sonrasında tamamlanan, reddedilen, onaylanan fakat başlatılmaya işlem gören tüm değişiklik taleplerini içerip içermediği kontrol edilir.	İ	Z	1
K11.T2	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. Söz konusu denetim testi, değişiklik yönetimi sürecinde beklenen talep, test kabulü ve canlı sisteme aktarım onayı gibi belirli adımlarda beklenen kontrollerin eksikliği durumlarda telafi edici faaliyetlerin tespitine yönelik olarak da kullanılabilir.	İ	Z	2

Ek Kaynaklar

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

4.2. Güvenlik Hizmetleri Yönetimi

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 gittikçe artmaktadır.

Bilgi güvenliği, kuruma ait bilgilerin iş sürekliliğini sağlamak, iş risklerinin etkilerini azaltmak ve BT yatırımlarından ve fırsatlarından azami faydayı sağlamak adına yetkisiz erişimlere, ifşa edilmelerine, değiştirilmelerine, kopyalanmalarına ya da imha edilmelerine karşı 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 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 bir gerekliliktir. 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. denetim açısından kritiklik taşıyan işlevselliklerinin kontrollü bir biçimde korunduğuna, uygulamalar üzerindeki yetkilerin kontrollü bir biçimde verildiğine 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 denetimlerinde sıklıkla ele alınan konulardan biri olmaktadır.

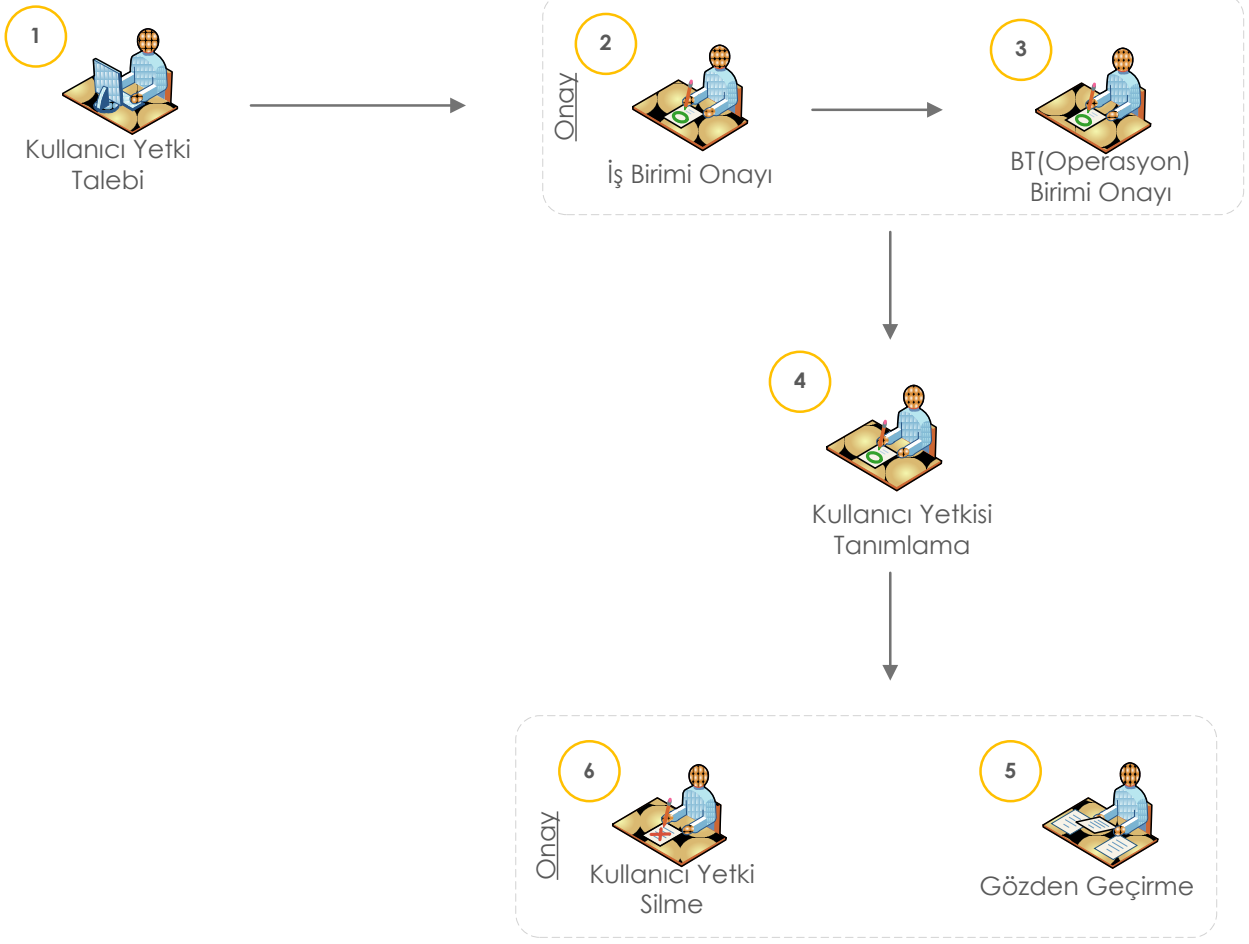
Kontrollere İlişkin Örnek Akış

Süreçte yer alan tipik kontrollere aşağıdaki tabloda yer verilmiştir:

Güvenlik Hizmetleri Yönetimi - Kontroller	
K1	Kurum bünyesinde güvenliğe dair standart, onaylı 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 değişikliklerin gerçekleştirilmesi ve kurum bünyesinde bu değişikliklere paralel olarak güvenlik yamalarının ve anti-virüs uygulamalarının kullanılması gibi önlemlerin alınması ile BT uygulamaları ve altyapılarının 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, vatandaşlara, 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.

Kullanıcı yetkilendirme kontrollerine ilişkin örnek akış şeması aşağıda yer almaktadır. Bu şemada belirtilen kontrol numaraları sadece gösterim amaçlı olup yukarıda belirtilen numaralardan bağımsızdır:

Güvenlik Hizmetleri Yönetimi – Yetkilendirme Kontrollerine İlişkin Örnek Akış



Kontrol numaraları

Risk – Kontrol Eşleşmeleri

Güvenlik Hizmetleri Yönetimi Risk – Kontrol Eşleşmeleri										
Riskler	**K1**	**K2**	**K3**	**K4**	**K5**	**K6**	**K7**	**K8**	**K9**	**K10**
R1 Kurum bünyesinde gerekli anlayışın ya da farkındalığın oluşmaması sebebiyle bilgi güvenliği sürecinin etkin bir şekilde yönetilememesi	+	+	+				+			+
R2 Bilgi güvenliği olaylarının takip edilmemesi denetim izlerinin tutulmaması ve zamanında çözülmemesinin sonucu olarak kurum bilgi sistemlerine sızılması, kurum bilgilerinin çalınması ve iş kesintilerinin oluşması.	+	+	+	+	+	+				+
R3. Bilgi güvenliği stratejisinin BT stratejisi ile uyumsuzluk göstermesi	+	+	+							
R4. Kurum veri bütünlüğünün bozulması ve veri işleyen sistemlerin iş gerekliliklerine uygun çalışamaması	+	+	+	+	+	+	+	+	+	+
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. Bilgi sistemleri uygulamaları üzerinde kritik veri, bilgi, donanım ve cihazlara yetkisiz erişimlerin gerçekleştirilmesi				+	+	+	+	+	+	
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						+		+		
R11. Cihazlarda izinsiz konfigürasyon değişikliklerinin gerçekleştirilmesi				+	+	+		+		

Güvenlik Hizmetleri Yönetimi Risk – Kontrol Eşleşmeleri										
Riskler	**K1**	**K2**	**K3**	**K4**	**K5**	**K6**	**K7**	**K8**	**K9**	**K10**
R12. Bilgi güvenliği konusundaki yasal yükümlülüklerin yerine getirilememesi; kanun ve yükümlülüklere 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 arttırılması				+	+	+	+			
R14. Bilgi sistemleri uygulamaları üzerinde gerçekleşen erişimlerin izlenmemesi sonucu yetkisiz erişimlerin ya da erişim girişimlerinin yönetim tarafından fark edilememesi						+				+
R15. Bilgi sistemleri ve ilgili ağ yapısı üzerinden şifrelenmeden (kriptolanmadan) iletilen kullanıcı adı ve kullanıcı parolalarının yetkisiz kişiler tarafından ele geçirilmesi					+	+	+			
R16. Kullanıcılar tarafından bilinçli ya da farkında olmadan bilgi sistemleri üzerinde erişim yetkisi arttırma işlemlerinin gerçekleştirilmesi							+			
R17. Kısıtlanmayan medya yüklemeleri (download) (dosya paylaşımı, video, ses vb.) sonucunda bilgi sistemleri sürekliliği, performans ve kapasitesini etkileyecek hususların oluşması										
R18. Kontrolsüz dosya paylaşımlarının (ör: dosya paylaşım ağları üzerinden yapılan paylaşımlar) gerçekleşmesi sonucu olarak fikri mülkiyet haklarının ihlal edilmesi	+	+	+							
R19. Bilgi sistemleri üzerindeki güvenlik ve parola parametrelerinin, yetkisiz erişimleri önleyecek şekilde tanımlanmaması				+		+	+			

Denetim Testleri

K1 - Kurum bünyesinde güvenliğe dair standart, onaylı ve sürekli gelişim bakış açısıyla bir bilgi güvenliği yönetim sistemi (BGYS) oluşturulur.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K1.T1	Kurumun stratejisi, genel güvenlik yapısı, risk iştahı, konumu, varlıkları ve teknolojik yapısına göre tasarlanmış bir BGYS'nin varlığı sorgulanır.	T	Z	2
K1.T2	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	2
K1.T3	Kurum bünyesinde uygulanan BGYS'nin üst yönetici tarafından onaylı olduğu gözlemlenir.	İ	Z	1
K1.T4	Kurum üst düzey yöneticilerine aşağıdaki görevlerin atanmış olduğu ve bu görevlerin gerçekleştirilmekte olduğu gözlemlenir. • Bilgi güvenliği ile ilgili risk yönetimi ve uyum programlarının denetlenmesi. Bu doğrultuda dönemsel olarak risk değerlendirme sonuçları ve etki analizleri ilgili üst düzey yöneticiler ile paylaşılır • Korunacak bilgi varlıklarının kurum içi kritiklik değerlendirmesinin onaylanması • Stratejik ortaklar ve diğer üçüncü şahıslarla ilgili bilgi güvenliği politikalarının incelenmesi • Üst seviye bilgi güvenliği yöneticilerinin tayinlerinin onaylanması • Bilgi güvenliğine uyumsuzluk vakaları ile ilişkin yaptırımların belirlenmesi	İ	Z	2
K1.T5	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	1
K1.T6	Bilgi güvenliği politikası içerisinde güvenlik yönetimi fonksiyonunun kapsamını, hedeflerini, rol ve sorumluluklarının yanında ilgili mevzuat uyarınca gerekli uyum ve risk etmenlerini de içeren bilgilerin bulunup bulunmadığı araştırılır.	T	O	1

K1.T7	Kurum bünyesinde güncel ve üst yönetici tarafından onaylanmış bir bilgi güvenliği politikasının varlığı incelenir. Bilgi güvenliği politikasının aşağıdaki unsurları içermesi beklenir • 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	1
K1.T8	Bilgi güvenliği politikasının, bilgi güvenliği konusunda üst düzey yöneticilerin 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	1
K1.T9	Kurum bünyesinde hazırlanmış, güncel ve kullanılan detay güvenlik standartları ve prosedürleri incelenir. Bu dokümanların en azından aşağıdaki konuları içerdiği gözlemlenir: • 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 • Internet kullanımı güvenliği • Ağ güvenliği • Denetim izleri güvenliği • Fiziksel ve çevresel güvenlik • Lisans yönetimi • Temiz masa politikası	T	Z	1
K1.T10	Bilgi güvenliği yönetiminin altında bulunduğu hiyerarşik yapı incelenir. Bilgi güvenliği ile ilgilenen birimlerin hangi karar verme yetkilerine sahip olduğu gözlemlenir.	T	O	2

K2 - Bilgi güvenliğinden kaynaklanabilecek risklerin nasıl yönetileceğinin belirlendiği, kurumsal strateji ve kurumsal mimariye uygun bir bilgi güvenliği planı hazırlanır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K2.T1	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	2
K2.T2	Bilgi güvenliği planının oluşturulmasında veri yönetişiminin, teknoloji standartlarının, güvenlik ve kontrol politikalarının, risk yönetiminin ve ilgili mevzuat yükümlülüklerinin dikkate alındığı gözlemlenir.	T	Z	2
K2.T3	Bilgi güvenliği planının en azından aşağıdaki unsurları içerdiği gözlemlenir: • Kurum çapında geçerli olacak güvenlik standartları • Politikaların kurum genelinde uygulanması amacıyla oluşturulmuş alt politikalar ya da prosedürler • Bilgi güvenliği personel ihtiyacı ve planlaması • Bilgi güvenliği yatırımları	İ	Z	2
K2.T4	Kurumsal mimarinin bir parçası olarak güvenlik yönetimi için kullanılan çözümlerin (ör: sistem, araç, vb.) bir envanterinin tutulduğu kontrol edilir.	İ	O	1
K2.T5	Kurum bünyesinde kullanıcıların bilgi güvenliği farkındalığını artırmak amacı ile bilgi güvenliği eğitimlerinin düzenlendiği ve bunlara katılımın sağlandığı kontrol edilir.	İ	Z	1
K2.T6	Kurum bünyesinde sosyal mühendislik saldırılarına karşı yapılan farkındalık çalışmaları incelenir, çalışanlarla görüşülerek farkındalık çalışmalarının etkinlikleri değerlendirilir. Sızma testleri kapsamında sosyal mühendislik testleri gerçekleştirildiyse, bunlar da incelenir ve sonuçlarına karşı alınmış aksiyonlar değerlendirilir.	İ	O	2

K3 - Kurum bünyesinde bilgi güvenliği uygulamalarının sürekli olarak gelişmesi için BGYS izlenir ve gözden geçirilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K3.T1	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	2
K3.T2	Kurum bünyesinde uygulanmakta olan BGYS ile ilgili düzenli olarak iç denetim faaliyetlerinin yürütüldüğü gözlemlenir. Eğer varsa, söz konusu iç denetim raporları temin edilir ve incelenir. Bulgulara ilişkin aksiyonların son durumları hakkında bilgi alınır.	İ	Z	1
K3.T3	BGYS'nin yönetim tarafından düzenli olarak değerlendirmeye tabi tutulduğu ve gerektikçe kapsam değişikliklerine ve geliştirmelere gidildiği gözlemlenir.	İ	O	1
K3.T4	BT güvenlik planının izleme ve gözden geçirme çalışmaları neticesinde ihtiyaç ve gereksinimler uyarınca güncellendiği gözlemlenir.	İ	Z	1

K4 - Kurum bilgi sistemleri üzerinde önleyici, tespit edici ve düzeltici değişikliklerin gerçekleştirilmesi ve kurum bünyesinde bu değişikliklere paralel olarak güvenlik yamalarının ve anti-virüs uygulamalarının kullanılması gibi önlemlerin alınması ile BT uygulamaları ve altyapılarının kötü amaçlı yazılımlardan etkilenme riski azaltılır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K4.T1	Kurum bünyesinde zararlı yazılımların önlenmesine ilişkin bir politikanın ya da prosedürün oluşturulduğu, belgelendiği ve tüm kurum çapında farkındalığın yaratıldığı teyit edilir.	T, İ	Z	1
K4.T2	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	1
K4.T3	Zararlı yazılımları saptayan uygulamaların (ör: anti-virüs, kişisel güvenlik duvarı tanımları gibi) düzenli olarak güncellendiği gözlemlenir.	İ	Z	2
K4.T4	Örnek personel bilgisayarları ve sunucular seçilerek, bunlar üzerinde anti-virüs programının kurulu olduğu, virüs tanımlarını içeren dosyaların son güncellenme tarihleri gözlemlenir.	İ	Z	2
K4.T5	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	1
K4.T6	Tüm güvenlik yazılımlarının ve güncellemelerinin merkezi bir konfigürasyon ve değişiklik yönetimi kullanılarak yönetildiği, dağıtıldığı ve izlendiği gözlemlenir.	İ	Z	2
K4.T7	Kurum bünyesinde BT güvenliğini sağlamakla sorumlu personelin kullanılan mevcut yazılımlar ile ilgili güvenlik tehditlerini düzenli olarak takip ettiği teyit edilir.	İ	Z	2
K4.T8	Kurum bünyesinde kullanılan tüm uygulamaların bir envanterinin tutulduğu kontrol edilir. Bu envanter ile uygulamaların hangi sürümlerinin de kullanıldığının takip edildiği teyit edilir.	İ	Z	1
K4.T9	Kurum bünyesinde dışarıdan tedarik edilmiş tüm uygulamaların lisanslarının güncelliğinin takip edildiği gözlemlenir. Geçerliliğini yitiren lisansların otomatik veya manüel olarak tespit edildiği gözlemlenir.	İ	Z	1

K4.T10	Kurum bünyesinde Yazılım Varlık Yönetimi (Software Asset Management) sürecinin uygulanmakta olduğu kontrol edilir. Lisanssız yazılımların özellikle güvenlik açısından kurum bilgi sistemlerine tehdit oluşturabileceği düşünüldüğünde söz konusu süreç kullanılan yazılımların orijinal yazılımlar olup olmadığına dair içerdiği kontroller açısından önemli arz etmektedir. *Yazılım varlık yönetimi, kurumun BT varlıklarını yönetmesi ve ihtiyaçları doğrultusunda optimize etmesi için bir dizi süreç ve prosedürlerden oluşan bir iyi uygulama şeklidir. Yazılım varlık yönetimi sürecini uygulayan kurumlar/birimler ISO19770 Yazılım Varlık Yönetimi Sertifikasyonu ile uygulanmakta olan sürecin etkinliğini tasdikleyebilirler. ISO19770 sertifikasının varlığı yazılım varlık yönetimi sürecinin değerlendirmesinde sorgulanabilir.*	İ	O	2
K4.T11	Kurum e-posta servisine gelen e-postaların, personelce indirilen dosyaların ve dışarıdan diğer veri girişlerinin (taşınabilir diskler vs.) filtrelendiği ve tehdit oluşturabilecek e-posta ve dosyaların engellendiği kontrol edilir. Kuruma giren ve çıkan verilerin otomatik bir araçla izlenip izlenmediği ve kural dışı veri paylaşımlarının engellenip engellenmişi sorgulanır.	İ	Z	2

K5 - Bilgi sistemleri bileşenleri ve iletişim ortamındaki bilgilerin korunması için kurum bünyesindeki bilgi sistemleri ağının güvenliği sağlanmalıdır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K5.T1	Kurum bünyesinde bir ağ güvenlik politikasının (verilen hizmetler, izinli trafik ve bağlantı türleri vb. içerecek şekilde) oluşturulduğu ve uygulandığı teyit edilir. Politikanın iş ihtiyaçları ve risk değerlendirmeleri baz alınarak oluşturulduğu kontrol edilir.	T	Z	3
K5.T2	Sadece kurum tarafından yetkilendirilmiş cihazların kurum ağına ve bilgi sistemlerine erişebileceği ve bu cihazların sadece en azından bir parola erişimi ile kullanılabildiği kontrol edilir.	T	Z	2
K5.T3	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	3
K5.T4	Tüm kritik ağ bileşenlerinin (ana router'lar, DMZ, VPN switch'leri) 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 izlenebilirliğinin sağlandığı doğrulanır.	İ	Z	2
K5.T5	Kurum ağ bileşenlerinin standart konfigürasyonlarının tanımlanıp tanımlanmadığı kontrol edilir. Her ağ bileşeninden örneklem seçilerek, kurum ağ güvenliğini sağlayacak şekilde standart olarak kabul edilen konfigürasyonlara uygun şekilde ayarlanmış olduğu kontrol edilir.	İ	Z	3
K5.T6	Kurum ağ bileşenlerinde yapılacak konfigürasyon değişikliklerinin değişiklik yönetimi sürecine uygun olarak gerçekleştirildiği kontrol edilir.	İ	Z	2
K5.T7	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	2
K5.T8	Kurum bünyesindeki verilerin belirlenen kriterlere göre (dışarıya açıklık seviyeleri, içerdiği bilgi vb.) göre gizlilik ve hassaslık konusunda sınıflandırıldıkları kontrol edilir.	İ	O	3
K5.T9	Kurum dışına iletilen verilerin, sınıfına göre güncel yöntemler ile kriptolandığı (şifreleyerek karmaşıklaştırma) gözlemlenir.	İ	O	3

K5.T10	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	3
K5.T11	Özel anahtarların gizlilik ve bütünlüğünü korumak için bulunan kontrollerin değerlendirilerek, özel imzalama anahtarlarının güvenli kriptolama aracılığıyla (FIPS 140-1, ISO 15782-1, ANSI X9.66 gibi) depolandığı, özel anahtarların güvenli kriptolama modülünden üretildiği, özel anahtarların yedeklendiği ve sadece yetkili personel tarafından saklandığı ve güvenli fiziksel ortamdan geri alınabileceği teyit edilir.	İ	O	3

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 testleri**	**T/İ**	**Z/O**	**YS**
K6.T1	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	2
K6.T2	Kurum bünyesindeki tüm uygulamalara, işletim sistemlerine, veri tabanlarına, cihazlara, sistemlere ve diğer teknolojik cihazlara erişim sağlanması için kullanılan parolaların kurum bünyesinde tanımlanmış olan parola parametrelerine uygun olarak belirlendiği gözlemlenir.	İ	Z	2
K6.T3	Örnek kullanıcı bilgisayarları seçilerek, bu bilgisayarların kurum güvenlik politikalarına uygun şekilde, belirli bir süre kullanılmadıklarında otomatik olarak kilitlendiği kontrol edilir. Söz konusu kontrolün, merkezi yönetim sistemleri aracılığı ile yönetilen ve uygulanan bir kural vasıtası ile zorunlu kılındığı durumlarda ilgili kuralların varlığı merkezi yönetim sistemlerinde tespit edilir. Söz konusu denetim testleri için altıncı bölümde detaylı denetim testleri sunulmuştur.	İ	O	1
K6.T4	Kurum bünyesinde iş ihtiyaçlarına göre belirlenmiş olan veri sınıflarına göre gizlilik açısından kritiklik arz eden verilerin, uygunsuz kişilerin eline geçmemesi için kriptolanarak ya da ilgili diğer önlemler alınarak saklandığı gözlemlenir.	İ	O	2
K6.T5	Kurum bilgi kaynaklarına kurum dışından erişim gerçekleştirilmesi süreci ile ilgili politika dokümanlarının mevcut olduğu gözlemlenir.	T	Z	1
K6.T6	Kurum bilgi kaynaklarına erişimin uygun bir kimlik doğrulama yöntemi ile (örn: kullanıcı adı/parola, iki faktörlü vb.) gerçekleştirildiği gözlemlenir.	İ	Z	2
K6.T7	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.) tutulacağının belirlendiği kontrol edilir.	T	Z	2
K6.T8	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	2
K6.T9	Örnek ağ cihazları seçilerek (güvenlik duvarı, IDS gibi) bunların kurum güvenlik politikalarına ve genel kabul görmüş güvenlik prensiplerine uygun şekilde yapılandırıldıkları gözlemlenir.	İ	Z	3

K6.T10	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	3
K6.T11	Son kullanıcı bilgisayarlarının ağ trafiklerini filtreleyen kişisel güvenlik duvarı, web içerik filtrelemesi gibi mekanizmaların kurulu olduğu gözlemlenir.	İ	Z	3
K6.T12	Son kullanıcı cihazlarının imhası ile ilgili kurum politikalarının mevcut olduğu gözlemlenir. Örnek seçilecek imha kayıtları incelenir ve seçilen cihazların bu politikalara göre kurum bilgilerinden arındırıldığı ve imha edildiğine dair kayıtlar incelenir.	T, İ	O	2

K7 - Tüm kullanıcılar, bilgi sistemleri üzerinde iş tanımları ile paralel, ihtiyaç duyacakları en az seviyede erişim yetkilere sahip olmalıdır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K7.T1	Kurum bünyesindeki bilgi kaynaklarına erişim sağlanması ile ilgili kontrolleri belirleyen bir erişim ve yetkilendirme politikası ya da prosedürünün mevcut olduğu gözlemlenir. Erişim yetkilendirme prosedürleri görevler ayrılığı ilkesine uygun olarak tasarlanmalıdır. Görevler ayrılığı, bir görevi (özellikle kritik bir işlemi) 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 (bkz: ***Görevler Ayrılığı Kontrol Tablosu***). Bu doğrultuda önce 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. Bunun yanında erişim ve yetkilendirme politikalarının ya da prosedürlerinin en azından aşağıdaki unsurları içermesi beklenir: • 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	2
K7.T2	Kurum bünyesindeki uygulamalarda ve sistemlerde kullanıcı adlarının belli standartlara göre oluşturulduğu teyit edilir.	İ	Z	1
K7.T3	Tüm kullanıcıların birbirinden ayrı eşsiz kullanıcı isimlerine veya tanımlayıcılara sahip olduğu gözlemlenir.	İ	Z	1

K7.T4	Uygulama kullanıcılarının yetkilendirmelerinin görevlerine ve unvanlarına göre tanımlandığı kontrol edilir. Bu amaçla gerekirse görev tanımları ya da ilgili mevzuat da temin edilerek incelenir. 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	2
K7.T5	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. • 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 • parolaların oluşturulması, kullanıcıya iletilmesi ve değiştirilmesi *Söz konusu kontrollerin belirli sistemler üzerinde nasıl yapılabileceğine dair teknik adımlar Rehber'in 6. Bölümü'nde listelenmiştir.*	İ	Z	3
K7.T6	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	1
K7.T7	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	1
K7.T8	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	2
K7.T9	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	1

K7.T10	Kritik verilerin bulunduğu uygulamalara, veritabanlarına veya işletim sistemlerine girişlerde ek güvenlik mekanizmalarının kullanıldığı teyit edilir *(örnek olarak parola, token (yetkili kullanıcılara BT servislerine erişim için otomatik anahtar üreten fiziksel cihazlara verilen isim), dijital imza, vb).*	İ	Z	2
K7.T11	Denetim döneminde açılmış hesaplar listesi temin edilir. Örnek olarak seçilen hesapların yetkilendirme süreçleri aşağıdaki hususlar doğrultusunda kontrol edilir: • 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	2
K7.T12	Tüm kritik verilere kullanıcı erişimlerinin denetim izlerinin tutulduğu ve bu denetim izlerine, ilgili veriler üzerinde yetkileri bulunan kullanıcılarının hiçbir şekilde erişemediği kontrol edilir. Bunun yanında, ayrıcalıklı erişim haklarına sahip kullanıcıların denetim izlerinin de tutulduğu ve bu hesapların yaptığı işlemlerin izlerinin düzenli ve daha sık olacak şekilde izlendiği kontrol edilir.	İ	Z	2

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, vatandaşlara, tedarikçilere veya tüm üçüncü şahıslar dahil olmak üzere herkese uygulanmalıdır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K8.T1	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 vb.)	T	Z	1
K8.T2	Sistem odalarına giriş yetkilendirmelerinin nasıl yapılması gerektiğine dair güvenlik adımlarını içeren politika ve prosedürlerin varlığı gözlemlenir.	T	Z	1
K8.T3	Sistem odalarına yapılan tüm giriş denemelerinin (başarılı ya da başarısız) kaydedildiği teyit edilir.	İ	Z	1
K8.T4	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	1
K8.T5	Sistem odasında bulunan tüm kişilerin kimliklerini dışarıdan görülebilecek şekilde taktıkları ya da taşıdıkları gözlemlenir.	İ	Z	1
K8.T6	Sistem odasına giriş yetkisi bulunmayan ziyaretçilere her an yetkili bir çalışanın eşlik ettiği gözlemlenir.	İ	Z	1
K8.T7	Düzenli olarak fiziksel güvenlik ve bunlara ilişkin hususların ele alındığı eğitimlerin düzenlendiği teyit edilir.	İ	O	1
K8.T8	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	1
K8.T9	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	1
K8.T10	Sistem odasının kameralar ile izlenildiği ve bu kameraların sistem odasının her noktasını görecek şekilde konumlandırıldığı gözlemlenir.	İ	Z	1

K8.T11	Kurum bünyesinde temiz masa politikasının uygulandığı gözlemlenir. Bu kapsamda örnek çalışanlar seçilir ve aşağıdaki kurallara uydukları gözlemlenir: • Masada o sırada ihtiyaç duyulan belgelerin haricinde belge bulunmaması • Parola ve kullanıcı adı bilgilerinin açıkta bulunabilecek kağıt vb. malzemeler üzerine yazılmaması • Kurum bilgileri içeren kağıtların çöpe atılmaması, kağıt imha makinelerinde kırpılması • Masalarda cep telefonu, akıllı telefon, tablet bilgisayar, USB bellek, harici disk, CD, DVD gibi elektronik veri içeren cihaz ve medyaların başıboş bırakılmaması • Masalarda vatandaşlık bilgileri, TCKN ve kuruma ait kritik bilgiler içeren dokümanların başıboş bırakılmaması • Proje dosyaları gibi önemli dokümanların kilitli dolaplarda tutulması • Kullanıcılar bilgisayarın başında değilken parola korumasının aktif olması	İ	Z	1

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 testleri**	**T/İ**	**Z/O**	**YS**
K9.T1	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	1
K9.T2	Hassas dokümanlara ve çıktı cihazlarına erişim yetkilerinin, "ihtiyaç duyulacak en düşük seviyede yetki" prensibine göre verildiği kontrol edilir.	İ	O	2
K9.T3	Hassas dokümanların ve çıktı cihazlarının envanterinin tutulduğu ve düzenli olarak sayımların yapılarak bu envanter ile karşılaştırmaların yapıldığı gözlemlenir.	İ	O	1
K9.T4	Hassas dokümanlar ve çıktı cihazları için fiziksel koruma önlemlerinin alındığı gözlemlenir.	İ	O	1
K9.T5	Hassas dokümanların ve çıktı cihazlarının, içerdikleri veya içerebilecekleri bilgilerin sonradan bir daha kullanılamayacak şekilde imha edildiği gözlemlenir.	İ	O	2

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 testleri**	**T/İ**	**Z/O**	**YS**
K10.T1	Altyapı güvenliği izleme araçları tarafından üretilen güvenlik ile ilgili kayıtların (ör: güvenlik duvarı logları, denetim izleri, güvenlik olay kayıtları vb.) risk seviyelerine göre kayıt altına alındığı gözlemlenir.	T, İ	Z	2
K10.T2	Güvenlik olaylarının belirlenip analiz edildiği, çözüldüğü ve kayıt altına alınıp kurum bünyesinde üst düzey yöneticilere ve ilgili paydaşlara raporlandığı kontrol edilir.	İ	Z	2
K10.T3	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	2

Ek Kaynaklar

- The IIA, (2007). Global Technology Audit Guide (GTAG), Identity and Access Management.
- ISACA, (2007). COBIT 4.1 Framework – DS5. Rolling Meadows, Illionis, ABD.
- ISACA. (2012). COBIT 5 Enabling Processes – APO13, DSS05. Rolling Meadows, Illinois, ABD.
- UK Cabinet Office, (2011). ITIL V3 2011 Service Operation, 4.5 Access Management.
- ISO/IEC, (2005). ISO/IEC 27002, Code of Practice for Information Security Management.

4.3. Yardım Masası, Olay ve Problem Yönetimi

Sürecin Genel Tanımı

Yardım masası bir kurumda, ürün ve hizmetler ile ilgili son kullanıcılara ve son kullanıcılara 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 kurumlarda hizmet masası olarak da isimlendirilebilir.

BT hizmetlerinde oluşan beklenmedik kesintilere ya da BT hizmet kalitesinin düşmesine sebep olacak durumlar "olay" olarak değerlendirilmektedir. Olay yönetimi sürecinin hedefi, olay tanımına uyan durumlar ile karşılaşıldığı 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 dönmesinin 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 olarak veya sürece uygun bir şekilde olay yönetimi sürecine aktarır ve ilgili uzmanlara yönlendirir.

Çözülemeyen, 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 çözümlemeyi, çözümlenemeyen problemlerin iş süreçleri üzerindeki etkilerini 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 kadarki 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 sürekliliğinin sağlanması ve işlevselliğinin artırılması konularında fayda sağlar.

Sürecin BT Denetimi Açısından Önemi

Yardım masası, olay ve problem yönetimi, BT ve BT'ye bağımlı iş süreçlerinin sürdürülebilirliği ve kritik BT işlevselliğinin denetim dönemi açısından devamlılığının sağlanması açılarından önemli olması sebebiyle, BT denetimlerinde sıkça incelenen süreçler arasında yer alır. Bu süreçlerin değerlendirilmesi ile süreçleri ve kritik BT işlevselliğini 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 olayların, hataların ve olumsuzlukların, denetim dönemi içerisinde kontrollü bir biçimde tespit edilip, değerlendirilip çözümlendiğine ve bunların tekrarlanmamasına dair gerekli önlemlerin alındığına ilişkin bir kanaat oluşturulabilir. Bu çerçevede yardım masası, olay ve problem yönetimi süreçlerinin denetimi, özellikle mali ve sistem denetimlerde sıklıkla ele alınan konulardan biri olmaktadır.

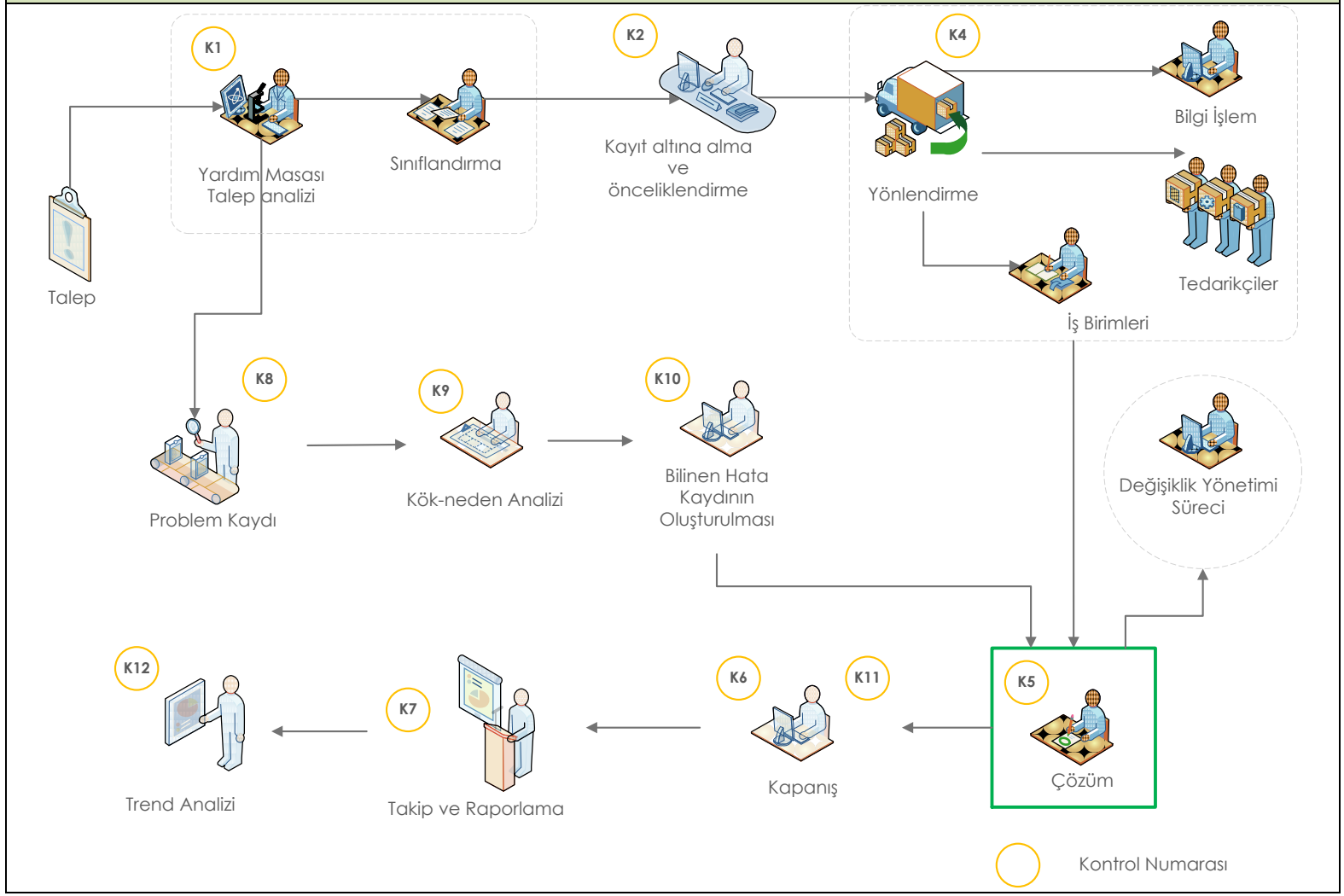
Yardım masası, olay ve problem yönetimi, BT denetimi açısından aşağıdaki süreç ve kontroller üzerinden takip edilebilir. Söz konusu akış her kurum için farklı olabileceği gibi, süreç içerisinde ele alınan olay ve problem tipleri, kullanılan olay ve problem yönetimi araçları ve takip ve raporlama mekanizmaları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

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

Yardım Masası, Olay ve Problem Yönetimi – Kontrollere İlişkin Örnek Akış



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. Çözülemeyen 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	+	+				+			+		
R10. BT hizmetlerinde kalite eksikliği	+	+	+	+	+	+	+	+	+	+	+
R11. Olay yönetimi ile ilgili geri dönüşlerde BT hizmetlerinden memnuniyetsizlik	+	+	+	+	+	+	+	+	+	+	+

Denetim Testleri

K1 - İlgili BT birimi tarafından olay ve yardım masası yönetim süreci belirlenir, talep sınıflandırma yöntemleri ve modelleri tanımlanır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K1.T1	Kurum bünyesinde bir BT yardım masasının varlığı tespit edilir.	T	Z	1
K1.T2	Yardım masasının işleyişinin tanımlandığı politika ve prosedürlerin varlığı araştırılır.	T	Z	1
K1.T3	Mevcut politika ve/veya prosedürlerde olay ve hizmet taleplerinin sınıflandırıldığı olay önceliklendirme yöntemlerinin ve/veya kriterlerinin tanımlandığı gözlemlenir.	T	Z	1
K1.T4	Verimli ve etkin çözümler sağlamak amacıyla, daha önceden yaşanan ve çözümü bilinen olaylar için çözüm yöntemlerinin tanımlanmış olduğu kontrol edilir.	T	O	1
K1.T5	Standart hizmetlerde kişinin kendi kendine ve etkili bir şekilde çözüm üretmesinde, yardım talebi çeşidine göre yardım türü modellerinin tanımlanmış olduğu kontrol edilir.	T	O	1
K1.T6	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	1
K1.T7	Olay yönetimi için kullanılan araçlar incelenir. Olay yönetimi için sadece bu tanımlanmış araçların kullanıldığı doğrulanır. Araçların kullanımı hakkında son kullanıcılara bilgilendirme yapıldığı teyit edilir.	İ	Z	1

K2 - Yardım talepleri ve olaylar, ilgili BT birimi tarafından iş kritikliğine ve yürürlükteki hizmet seviyesi sözleşmesine göre tanımlanır, kayıt altına alınır ve sınıflandırılır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K2.T1	Yardım masası ve olay yönetimi sürecinde kullanılan araç(lar) incelenir. Bu araç(lar) üzerinden denetim dönemi boyunca açılmış kayıtlar temin edilir ve içerisinden uygun örneklem 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	1
K2.T2	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	2
K2.T3	Bir üst adımda seçilen örnek yardım talepleri ve olayların, tanımlanan hizmet seviyesi anlaşmalarındaki iş etkisi ve aciliyetine göre önceliklendirilmiş olduğu gözlemlenir.	İ	Z	1

K3 - Geçmiş olaylara ilişkin belirtiler tanımlanır ve kaydedilir, olası nedenler belirlenir ve çözüm planı hazırlanır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K3.T1	Geçmişte karşılaşılmış olaylara yol açan kök nedenlerin ve aksaklıkların tanımlandığı ve gelecekte oluşabilecek olaylar için bu belirtilerin izlendiği gözlemlenir.	İ	O	2
K3.T2	Olayların saptanması için belirtilerin kayıt altına alınmış olduğu bir bilgi kaynağının (ör: veritabanının) varlığı gözlemlenir.	T	O	2
K3.T3	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 barındırmıyorsa, yeni bir problem olarak kaydedildiği kontrol edilir.	İ	O	1
K3.T4	Kurum bünyesindeki uzman birimlere, uzmanlıkları ile ilgili olay tiplerinin atanmış olduğu gözlemlenir. Uzmanlık gerektiren durumlarda, ilgili birimin uygun seviyede katılım göstermiş olduğu kontrol edilir.	İ	O	2

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 testleri**	**T/İ**	**Z/O**	**YS**
K4.T1	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	1
K4.T2	Seçilen örnek olayların çözümlenmesinde kullanılan geçici çözümlerin kayıt altına alındığı ve takip edildiği gözlemlenir.	İ	Z	1
K4.T3	Gerekli durumlarda bilgi sistemleri üzerinde bilgi ya da veri kurtarma eylemlerinin gerçekleştirilip gerçekleştirilmediği sorgulanır.	İ	O	2
K4.T4	Olay çözümlerinin belgelendiği ve çözümün daha sonra benzer olaylar oluştuğunda bilgi kaynağı olarak kullanılıp kullanılmayacağının değerlendirildiği kontrol edilir.	İ	O	1
K4.T5	Çözümlenen olayların çözüm yöntemlerinin kaydedildiği gözlemlenir.	İ	Z	1

K5 - Olay çözümünün yeterli olduğu ve talebin karşılandığı doğrulanır ve olay kaydı sonlandırılır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K5.T1	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	2
K5.T2	Örnek olarak seçilen olay kayıtlarının, olayı bildiren personelin onayı alınarak kapatıldığı teyit edilir.	İ	Z	1

K6 - Problemlerin sınıflandırması ve raporlanması için gerekli kriter ve prosedürler tanımlanır ve uygulanır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K6.T1	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	1
K6.T2	Durum ya da olayların, problem olarak tanımlanması için gerekli kriterlerin belirlenmiş olduğu gözlemlenir.	T	Z	1
K6.T3	Problem önceliklendirme kriterlerinin ilgili iş süreçlerinin niteliği dikkate alınarak belirlendiği gözlemlenir.	T	Z	2
K6.T4	Problemlerin sınıflandırmasına ilişkin yöntemlerin tanımlanmış olduğu gözlemlenir.	T	Z	1
K6.T5	Denetim dönemi boyunca gerçekleşen tüm problemlerin kayıt altına alındığı ve belgelerinin prosedürlere uygun olarak oluşturulduğu sorgulanır.	İ	Z	1
K6.T6	Değişiklik yönetimi sisteminden gelen girdiler de dahil olacak şekilde örnek seçilecek problemlerin politika ve/veya prosedürlere uygun şekilde ele alınmış olduğu incelenir.	İ	O	1
K6.T7	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	1

K7 - Gerçekleşen problemlere ilişkin kök nedenleri değerlendirmek ve analiz etmek için ilgili konuda uzmanlar görevlendirilerek problemler araştırılır ve teşhis edilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K7.T1	Farklı tipte problemlerin çözümü için, gerekli olduğu düşünülen durumlarda farklı yetkinliklere sahip uzman kişilerin görevlendirildiği gözlemlenir.	İ	O	1
K7.T2	Kök neden analizi sırasında, bilinen hataların tutulduğu bilgi kaynaklarından ve veri tabanlarından yararlanılmış olduğu gözlemlenir.	İ	O	1
K7.T3	Problemlerin çözümünde raporların oluşturularak çözüme ilişkin ilerleyişin bildirildiği kontrol edilir. Çözülemeyen problemlerin süregelen etkilerinin izlendiği gözlemlenir.	İ	O	1

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 testleri**	**T/İ**	**Z/O**	**YS**
K8.T1	Problemin kök analizi tanımlandıktan sonra probleme ilişkin olarak bilinen hata kayıtlarına ilişkin bilgi tabanının güncellendiği ve probleme ilişkin uygun çözümlerin kayıt altına alındığı gözlemlenir.	İ	O	2
K8.T2	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	2

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 testleri**	**T/İ**	**Z/O**	**YS**
K9.T1	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	1
K9.T2	Örnek olarak seçilen problemlerin ancak ilgili paydaşların onayı ile "çözümlendi/tamamlandı/giderildi vb." durumuna alındığı gözlemlenir.	İ	Z	1
K9.T3	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 vatandaşların bu durum ile ilgili haberdar edildiği kontrol edilir.	İ	O	1
K9.T4	Açık durumdaki problemlerin listesi temin edilir. Bu problemlerin durumlarının BT yönetiminin ve kullanıcıların haberdar olması için yardım masasına raporlandığı gözlemlenir.	İ	Z	1
K9.T5	Problemin çözümüne ilişkin yürütülen çalışmalara ait kayıtların hazırlanmış olduğu gözlemlenir.	İ	O	2
K9.T6	Problemlerin ve bilinen hataların hizmetler üzerindeki etkisinin izlendiği kontrol edilir.	İ	Z	2
K9.T7	Problemlerin çözümlerinin gözden geçirildiği ve onaylandığı gözlemlenir.	İ	Z	1

K10 - Yeni problemlere neden olabilecek eğilimleri gözlemleyebilmek ve tespit edebilmek için özellikle olay ve değişiklik kayıtları verileri toplanır ve analiz edilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K10.T1	Problem yönetimi sürecinin değişiklik yönetimi ve olay yönetimi süreçleri ile entegre olacak şekilde ele alındığı değerlendirilir.	İ	Z	2
K10.T2	Olay, problem, değişiklik yönetimi süreç sahipleri ve yöneticilerinin bilinen problemler ile ilgili düzenli olarak görüştükleri sorgulanır.	İ	O	1
K10.T3	Problemler sonucu oluşan toplam maliyetin belirlendiği, kurumsal olarak izlendiği ve harcanan iş gücünün takip edildiği kontrol edilir.	İ	O	1
K10.T4	İş gereksinimleri ve hizmet seviyesi anlaşmalarına göre problem çözümlerinin izlendiği raporların hazırlanmış olduğu gözlemlenir. Ayrıca daha önceden belirlenen kriterlere göre problemin daha üst bir seviyeye aktarılması, dış tedarikçilerle iletişime geçilmesi gibi problem seviye yükseltme sürecinin işletildiği kontrol edilir.	İ	Z	2
K10.T5	Kaynakların kullanılmasını optimize etmek ve geçici çözümleri azaltmak adına problem eğilimlerinin izlendiği gözlemlenir.	İ	Z	1
K10.T6	Kök nedene yönelik kalıcı çözümlerin belirlenerek uygulandığı ve değişiklik yönetimi sürecine uygun şekilde değişikliklerin gerçekleştirildiği kontrol edilir.	İ	O	2

K11 - Olay yönetimi sürecinin sürekli iyileştirilmesini sağlamak için, olay ve taleplerin çözümlenme yöntemleri, süreleri ve eğilimleri düzenli olarak izlenir, analiz edilir ve raporlanır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K11.T1	Kritik veya çözülemeyen olayların eskalasyon (seviye yükseltme) süreçleri incelenir. Problem yönetimi sürecinin varlığı ve bu tip olaylar için sürecin nasıl tetiklendiği araştırılır.	T, İ	Z	1
K11.T2	Çözülmemiş durumda olan problemlere ilişkin durumların düzenli olarak takibinin yapıldığı ve ilgili yönetim birimine raporlandığı kontrol edilir.	İ	Z	1
K11.T3	Olay yönetimi raporlama ihtiyaçlarının tanımlanmış olduğu gözlemlenir. Raporlama zamanlamaları ve dönemlerinin belirlendiği gözlemlenir. Raporların hazırlanması için hangi araçlardan ve verilerden yararlanıldığı sorgulanır.	T	Z	1
K11.T4	Eğilim göstergelerini oluşturmak, tekrarlanan sorunların modellerini 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	2
K11.T5	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	2
K11.T6	Sıkça karşılaşılan olaylar için bir bilgi kaynağının ya da veritabanının (sıkça sorulan sorular gibi) varlığı gözlemlenir.	İ	Z	1
K11.T7	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	Z	1
K11.T8	Yardım masası performansının artırılması için düzenli olarak son kullanıcı memnuniyeti anketlerinin yapıldığı gözlemlenir. Bu anketlerin sonuçlarına göre eylem planlarının oluşturulduğu kontrol edilir.	İ	Z	1

Ek Kaynaklar

- ISACA, (2007). COBIT 4.1 Framework – DS8, DS10. Rolling Meadows, Illionis, ABD.
- ISACA, (2012). COBIT 5 Enabling Processes – DSS02, DSS03. Rolling Meadows, Illinois, ABD.
- UK Cabinet Office, (2011). ITIL V3 2011 Service Operation, 4.2 Incident Management.
- UK Cabinet Office, (2011). ITIL V3 2011 Service Operation, 4.3 Request Fulfilment.
- UK Cabinet Office, (2011). ITIL V3 2011 Service Operation, 4.4 Problem Management.
- ISO/IEC (2005). ISO/IEC 27002, 13. Information Security Incident Management.

4.4. BT Operasyon ve Yedekleme Yönetimi

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" üzerinde doğrudan ve dolaylı etkilere sahiptir. Kritik işlevselliğin denetim dönemi boyunca sürdürülebilmesi için, özellikle yığın (batch) ve zamanlanmış (otomatik olarak önceden belirlenmiş zamanlarda gerçekleşen) işlerin düzgün çalıştığının teyidi ve hataların izlenip düzeltilmesi önemlidir. Yığın ve zamanlanmış işler, özellikle sistemler arası veri aktarımlarında, gün ya da dönem sonu işlemlerinde ve online ya da gerçek zamanlı (real-time) olarak gerçekleştirilmesi gerekmeyen birçok işlem için sıklıkla kullanılmaktadır. Bu nedenle söz konusu işlerin doğru çalışması denetçi açısından önemlidir. Bununla birlikte sistemlerin takip edilmesi, veri yedeklemelerinin yapılması, sistemlere ilişkin çevresel önlemlerin takip edilmesi gibi bir dizi diğer BT operasyonu da kritik BT işlevselliği açısından BT denetimini ilgilendirmektedir. Bahsi geçen hususlarla birlikte veri yönetimine ilişkin bazı temel esaslar da bu süreç içerisinde ele alınmaktadır.

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, ilgili olaylar kayıt altında tutulur ve raporlanır.
K4	Kurum bilgi sistemlerini oluşturan tüm unsurların çevresel etkenlere karşı uygun şekilde korunmasını sağlayacak önlemler alınır.

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 vb. işlerin takip edilememesi ve bu sebeple ortaya çıkan sıkıntıların zamanında çözülememesi ve raporlanamaması	+			

Denetim Testleri

K1 - Kurum bünyesinde gerçekleştirilen BT faaliyetleri ve işlemleri tutarlı ve güvenilir bir biçimde tanımlanır ve yönetilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K1.T1	Kurum bünyesinde yürütülen 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	1
K1.T2	İncelenen BT faaliyetlerine dair prosedürlerde ve kılavuzlarda personele ilişkin rol ve sorumlulukların tanımlanmış olduğu gözlemlenir.	T	Z	1
K1.T3	Yığın (batch) ve zamanlanmış (otomatik olarak önceden belirlenmiş zamanlarda gerçekleşen) işlere ilişkin çalıştırma prosedürleri incelenir. Bu prosedürlerin onaylı olduğu ve izleme faaliyetlerini de içerdiği gözlemlenir.	T	Z	2
K1.T4	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 birim yöneticisi tarafından onaylandığı gözlemlenir.	İ	Z	2
K1.T5	Örnek olarak seçilen yığın ve zamanlanmış işleri gerçekleştirmiş olan operatörlerin kim olduğu öğrenilir, ilgili kişilerin görev tanımı incelenir ve bu kişilerin aynı zamanda söz konusu işlere ait denetim izlerinin değerlendirilmesinden sorumlu olmadıkları gözlemlenir.	İ	Z	2
K1.T6	BT faaliyetlerini gerçekleştiren ve izleyen ekipler için vardiya takviminin oluşturulduğu ve yönetim ile paylaşıldığı gözlemlenir.	İ	O	1
K1.T7	Yığın işlerin gerçekleştirilmesi için, vardiya günlükleri incelenerek vardiyaların her an yeterli sayıda operatörün çalışacağı şekilde ayarlandığı gözlemlenir.	İ	O	1
K1.T8	Vardiyalar sırasında tespit edilen sorunlar incelenir. Bu sorunlar için olay yönetimi sürecine uygun şekilde kayıt açıldığı gözlemlenir.	İ	O	1

K2 - Kurum bünyesinde iş ihtiyaçlarına uygun olarak veri oluşturma, işleme, saklama, yedekleme ve imha mekanizmaları ve bunlara ilişkin süreçler tesis edilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K2.T1	Kurum bünyesinde sistemlerin, uygulamaların ve verilerin yedekleme politika ve prosedürlerinin oluşturulmuş olduğu ve aşağıda belirtilen örnek konuları içerdiği gözlemlenir. • Yedekleme sıklığı • Yedekleme tipi (tam yedekleme, artımlı yedekleme vb.) • Yedekleme ortamı tipi • Yedekleme tipi (otomatik, manüel) • 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	2
K2.T2	Kurum BT bünyesinde saklanan ve işlenen veri tiplerinin tanımlandığı ve gizlilik, bütünlük ve erişilebilirlik seviyelerine göre değerlendirildiği incelenir.	T	O	2
K2.T3	Kapsama alınan uygulamalara/sistemlere ait verilerin iş ihtiyaçlarına ve süreklilik planlarına göre sınıflandırıldığı gözlemlenir.	T	O	2
K2.T4	Kapsama alınan uygulamalara ait verilerin yedeklenmesinin ve bu yedeklerin saklanmasının, verilerin kategorilerine, yasal zorunluluklara ve prosedürlere uygun şekilde gerçekleştirildiği uygun bir örneklem üzerinden incelenir.	İ	Z	2
K2.T5	Yedekleme sürecinin izlenmesi ile ilgili rol ve sorumlulukların atanmış olduğu gözlemlenir.	T	Z	1
K2.T6	Yedeklerin sorunsuz olarak alındığına ya da yedeklerin alınması ile ilgili sorunların çıktığı durumlara dair bilgilendirmelerin ilgili personele yapıldığı gözlemlenir. Otomatik yedekleme yapan cihazların durum raporlarının oluşturulduğu ve izlemeden sorumlu personel tarafından incelendiği gözlemlenir.	İ	Z	2
K2.T7	Yedekleme sürecinde çıkan sorunlar için olay yönetimi sürecine uygun şekilde kayıt açıldığı gözlemlenir.	İ	Z	2
K2.T8	Yedeklerin envanter listesi incelenir ve örnek olarak seçilen yedeklerin fiziksel varlığı gözlemlenir, varsa yedeklerin üzerindeki etiketlerin doğruluğu araştırılır.	İ	O	2

K2.T9	Yedekleme ortamlarının çalıştığından ve geri dönülebilir olduğundan emin olmak adına, kapsamdaki sistemlerin, uygulamaların ve verilerin yedeklerinden 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	3
K2.T10	Kurum bünyesinde kullanılmayan ya da saklama süresi dolan verilerin ve ilgili saklama medyalarının (disk, DVD, vb.) imhasına ilişkin bir sürecinin mevcut olduğu gözlemlenir.	İ	O	1
K2.T11	Veri imhası ile ilgili rol ve sorumlulukların açık bir şekilde belirlendiği gözlemlenir.	T	O	1
K2.T12	Tekrar kullanılacak ortamlarda bulunan verilerin üzerine yazma, de-gauss, vb yöntemlerle kesin bir şekilde yok edildiğinden (wipe) emin olunduğu gözlemlenir.	İ	Z	2
K2.T13	İmha sürecine sokulan verilerin ve saklama ortamlarının tüm imha sürecinin bir kurum görevlisi tarafından izlenip raporlandığı kontrol edilir.	İ	Z	1
K2.T14	İmha sürecinde yer alan (varsa) taşeron firmaların fiziksel güvenlik gereksinimlerini sağladığı kontrol edilir.	İ	O	2

K3 - Kurum BT altyapısı izlenir ve ilgili olaylar kayıt altında tutulur ve raporlanır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K3.T1	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.	T, İ	Z	2
K3.T2	İzlenecek altyapı bileşenlerinin iş ihtiyaçlarına bağlı olarak kritikliklerine göre önceliklendirildikleri kontrol edilir.	İ	O	3
K3.T3	İzlenen altyapı bileşenlerinin için eşik değerlerinin belirlendiği ve bu eşik değerlerini aşan göstergeler için ilgili birimin harekete geçtiği ve gerekli önlemlerin alındığı gözlemlenir.	İ	O	3
K3.T4	İzlenen altyapı bileşenlerinin izlenen özelliklerindeki değişimlerinin ve eğilimlerinin düzenli olarak kontrol edildiği, probleme yol açabilecek eğilimler için gerekli önlemlerin alındığı gözlemlenir.	İ	O	2
K3.T5	Denetim dönemi boyunca gerçekleşmiş BT altyapısını ilgilendiren olaylar arasından örneklem seçilir ve bu örnek olaylar için olay kaydının açılıp açılmamış olduğu kontrol edilir.	İ	Z	2

K4 - Kurum bilgi sistemlerini oluşturan tüm unsurların çevresel etkenlere karşı uygun şekilde korunmasını sağlayacak önlemler alınır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K4.T1	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 açılabildiği ve turnike vb. yöntemlerle tek seferde sadece bir kişinin kapıdan girişine izin verildiği gözlemlenir.	İ	Z	1
K4.T2	Sistem odasının bulunduğu yerin seçiminde şirketin iş ve güvenlik ihtiyaçlarının değerlendirildiği çevresel etmenlerin ve risklerin (hırsızlık, ısı, yangın, duman, sel, deprem, terör, kimyasallar, patlayıcılar vb.) dikkate alındığı gözlemlenir.	İ	Z	1
K4.T3	Sistem odasının maruz kaldığı risklerin değerlendirildiği ve bu risklerin gerçekleşmesi durumunda işe olan etkilerinin ölçüldüğü gözlemlenir. Söz konusu değerlendirme ayrı bir prosedür içerisinde belirtilmişse ilgili prosedür incelenir.	İ	O	2
K4.T4	Sistem odasında önceden belirlenmiş eşik değerlerin aşılması halinde alarm veren ısı, nem, duman ve yangın detektörleri gibi izleme ve alarm sistemlerinin bulunduğu gözlemlenir.	İ	Z	1
K4.T5	Sistem odası yangın söndürme sistemi incelenir. Sistem odasında yangın söndürme sistemi olarak gazlı, su bazlı ya da benzeri sistemlerin olduğu kontrol edilir.	İ	Z	1
K4.T6	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 (ör. kabloların personelin ayaklarına takılmayacak şekilde derli toplu bir biçimde tutulduğu) gözlemlenir.	İ	Z	1
K4.T7	Acil durum anında sistem odasının boşaltılmasına dair bir prosedürün bulunduğu ve bu prosedürün acil durum esnasında neler yapılması gerektiğini ve personelin rol ve sorumluluklarını detaylı olarak içerdiği gözlemlenir.	T	Z	1
K4.T8	Acil durumda sistem odasının boşaltılabilmesi için sistem odasının gerekli tasarıma sahip olduğu (acil olarak boşaltılmasının mümkün olduğu) acil durum şalter düğmesinin olduğu, acil durumda basılacak düğmelerin, yere düşmüş bir kişi tarafından basılabilecek yükseklikte olduğu teyit edilir.	İ	Z	1
K4.T9	BT teçhizatının elektrik altyapısının korunması ve çalışırlığının sağlanması için voltaj regülatörlerinin, kesintisiz güç kaynaklarının (UPS) ve jeneratörlerin varlığı araştırılır. Bunların BT teçhizatı için yeterli olup olmadığı teyit edilir.	İ	Z	2

K4.T10	Kesintisiz güç kaynaklarının, yangın söndürme sistemlerinin, sistem odasında bulunan soğutma sistemlerinin ve çevresel etkilere karşı tesis edilmiş diğer cihaz ve ekipmanların bakımlarına ilişkin prosedür ya da talimatlar temin edilir ve bakımların düzenli olarak gerçekleştirildiği gözlemlenir. Bunun için denetim döneminde gerçekleşmiş bakımlar arasından bir örneklem seçilir ve bakım belgeleri incelerek, bakımın gerçekleştiği teyit edilir.	T, İ	Z	1
K4.T11	Sistem odasında alternatif güç ve iletişim hatlarının varlığı kontrol edilir.	İ	O	1
K4.T12	Sistem odasına giriş yetkisi olan personelin sistem odasında uyulması gereken iş sağlığı ve güvenliği kuralları hakkında bilgilendirildiği gözlemlenir.	İ	Z	1
K4.T13	Sistem odası ile ilgili gerçekleşen olayların yönetiminin olay yönetimi sürecine uygun şekilde takip edildiği ve kayıt altına alındığı kontrol edilir.	İ	O	1

Ek Kaynaklar

- ISACA, (2007). COBIT 4.1 Framework – DS12, DS13. Rolling Meadows, Illionis, ABD.
- ISACA, (2012). COBIT 5 Enabling Processes DSS01 Manage Operations. Rolling Meadows, Illinois, ABD.
- UK Cabinet Office, (2011). ITIL V3 2011 Service Operation, 4.1 Event Management

4.5. Süreklilik Yönetimi

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 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, insanların 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 alternatif veri kurtarma yöntemleri ve çalışma lokasyonları tespit edilir.

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, süreçlerini ve bu çerçevede "kritik BT işlevselliği"ni kesintisiz bir şekilde sürdürebilmesi ile doğrudan ilgili olduğundan BT denetimlerinde sıklıkla değerlendirilen konulardan biridir. Bu sürecin değerlendirilmesi ile herhangi bir felaket veya kriz anında süreç ve faaliyetlerin asgari düzeyde etkileneceğine ve önceden kabul edilen makul bir 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 oluşturulmasına destek sağlanabilir.

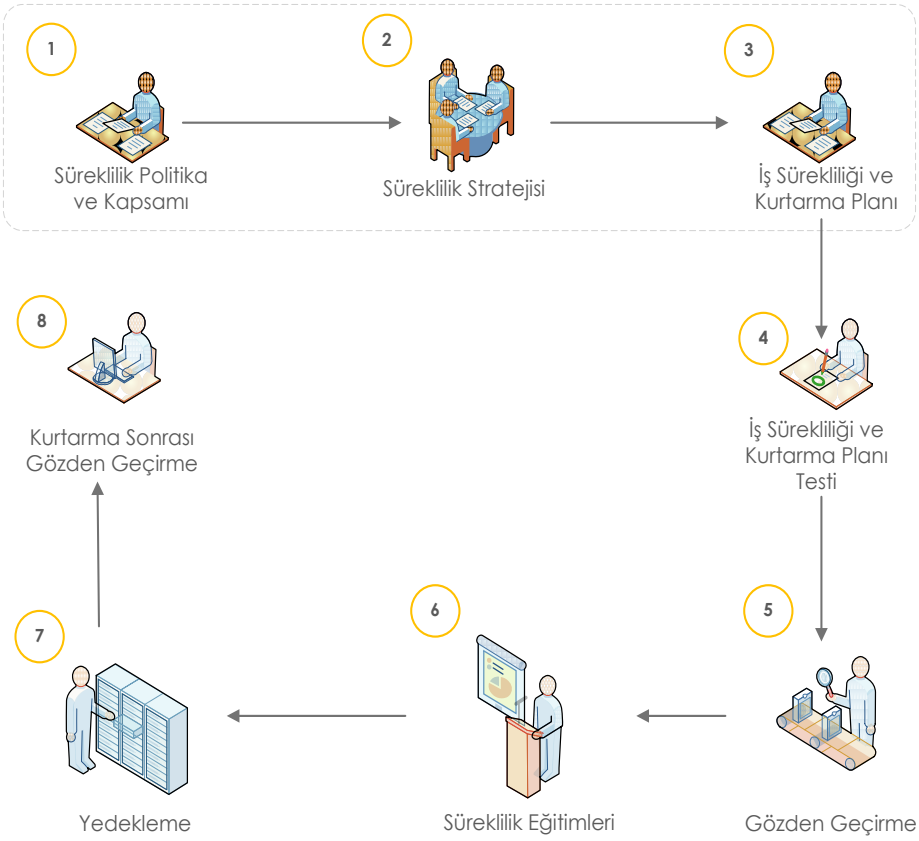
Süreklilik yönetimi, BT denetimi açısından aşağıda belirtilen süreç akışı üzerinden takip edilebilir. Söz konusu akış her kurum için farklı olabileceği gibi, süreç içerisinde ele alınan planlama şekilleri, iş etki değerlendirme yöntemleri, yedekleme araçları, yedekleme ve olağanüstü durum mimarisi ve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

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 iş sürekliliği ve 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 erişilebilirliği sağlanır. Bu doğrultuda kritik uygulamaların yedekleri düzenli olarak alınır ve güvenli olarak saklanır. (Bu kontrol BT Operasyon ve Yedekleme Yönetimi başlığı altındaki süreç içerisinde ayrıca 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 alınmasının (ayağa kaldırılmasının) ardından süreklilik planının süreçteki yeterliliği değerlendirilir.

Süreklilik Yönetimi – Kontrollere İlişkin Örnek Akış



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	+	+	+			+		
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 eksikliğinin olması	+	+	+	+	+	+		+

Denetim Testleri

K1 - Kurum ve paydaş hedefleri ile uyumlu bir süreklilik politikası ve kapsamı belirlenir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K1.T1	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 onaylandıkları teyit edilir.	T	Z	2
K1.T2	SY dahilinde hedef ve kapsama ilişkin tanımların net bir şekilde yapılmış olduğu gözlemlenir.	T	Z	2
K1.T3	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.	T	Z	2
K1.T4	SY dâhilinde, kritik iç ve dış süreçler ile bu süreçleri destekleyen temel süreçler ve ilgili BT hizmetlerinin ve sistemlerinin tanımlanmış olduğu tespit edilir.	T	Z	2
K1.T5	Süreklilik politikası ve kapsamı üzerinde anlaşma yapılmış olan tüm paydaşların ve süreç içinde yer alacak personelin görev ve sorumluluklarının tanımlanmış olduğu kontrol edilir.	T	Z	1
K1.T6	SY dahilinde herhangi bir kesintinin gerçekleşmesi durumunda, bu durumdan etkilenecek olan paydaşların süreklilik ile ilgili ihtiyaçlarının belirlendiği gözlemlenir.	T	Z	1
K1.T7	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.	T	Z	2
K1.T8	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	1

K2 - Süreklilik yönetimi seçenekleri değerlendirilir ve felaket anında kurum iş süreçlerinin kurtarılmasını sağlayacak düşük maliyetli, sürdürülebilir bir süreklilik stratejisi ortaya koyulur.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K2.T1	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.	T	Z	1
K2.T2	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.	T	Z	1
K2.T3	Kesinti sonrasında kritik faaliyetlerin tekrar devreye alınması ve ayağa kaldırılması işlemleri için, iş ve teknik gereksinimlerin belirlenmiş olduğu teyit edilir.	T	Z	1
K2.T4	Süreklilik yönetimine ilişkin gereksinimler göz önünde bulundurarak maliyet analizlerinin yapılmış olduğu teyit edilir.	T	O	1
K2.T5	İş sürekliliği stratejisinin ve ilgili diğer plan, politika ve prosedür gibi dokümanların işe ve teknolojik ihtiyaçlara göre düzenli olarak gözden geçirildiği ve gerekli durumlarda güncellendiği gözlemlenir.	İ	Z	1

K3 - Bir kesinti ya da felaket olduğu durumlarda yapılması gerekenleri belgeleyen, kurumun kritik faaliyetlerine süreklilik stratejisine dayalı bir iş sürekliliği planı hazırlanır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K3.T1	Tüm kritik iş birimleri ve süreçleri için süreklilik planlarının oluşturulduğu ya da mevcut planın tüm ilgili birimleri ve kritik süreçleri kapsadığı gözlemlenir.	T	Z	1
K3.T2	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.	T	Z	1
K3.T3	Faaliyetleri açısından kritik olarak değerlendirilen tedarikçilerin süreklilik planında yer aldığı ve tedarik edilen hizmetlerin de sürekliliğinin dikkate alındığı gözlemlenir.	T	Z	1
K3.T4	Süreklilik planlarını destekleyecek şekilde ilgili BT sistemlerinin yedekleme ihtiyaçlarının belirlendiği gözlemlenir.	T	Z	2
K3.T5	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	1
K3.T6	Süreklilik yönetimi sürecinde görev alan personelin hangi becerilere ve yeteneklere sahip olması gerektiğinin tanımlandığı kontrol edilir.	T	O	1
K3.T7	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.	T	Z	2

K4 - Kritik iş süreçlerinin ve faaliyetlerinin başarı ile ayağa kaldırılmasından emin olunması amacı ile kurtarma planı düzenli olarak test edilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K4.T1	İş ve faaliyetlere ilişkin risklerin doğru şekilde karşılanması ve etkilerinin azaltılması için Süreklilik Planı'nın ve ilgili diğer politika ve prosedürlerin bütünlüğünün sağlanması doğrultusunda süreklilik planlarının test edilmesine ilişkin hedeflerin tanımlandığı gözlemlenir.	T	Z	2
K4.T2	Süreklilik Planı üzerinde gerçekleştirilecek test çalışmalarının, herhangi bir felaketin kritik iş süreçleri ve faaliyetleri üzerinde 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	2
K4.T3	Süreklilik Planı'nda tanımlandığı şekilde test faaliyetleri takviminin hazırlandığı kontrol edilir.	İ	Z	1
K4.T4	Süreklilik ve felaket kurtarma testlerinin düzenli olarak gerçekleştirildiği incelenir. Bu testler kapsamında olağanüstü durum merkezinin de çalışırlığının test edildiği gözlemlenir.	İ	Z	2
K4.T5	Testlerin, en güncel süreklilik planının dikkate alınarak gerçekleştirildiği gözlemlenir.	İ	Z	3
K4.T6	Gerçekleştirilen test sonrası sonuçların ve sonuç analizlerinin belgelendirildiği gözlemlenir.	İ	Z	2
K4.T7	Gerçekleştirilen testler sonucunda süreklilik planının iyileştirilmesi amacıyla önerilerin geliştirildiği ve raporlandığı gözlemlenir.	İ	Z	2

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 testleri**	**T/İ**	**Z/O**	**YS**
K5.T1	Mevcut operasyonel ve stratejik hedeflere uygun olarak iş sürekliliği ve felaket kurtarma planlarına yönelik düzenli olarak gözden geçirme çalışmalarının yapılıp yapılmadığı sorgulanır.	İ	Z	1
K5.T2	Planın gözden geçirilmesinin ardından değişikliği tetikleyen herhangi bir durum oluştuğunda, plan üzerinde yapılması gereken değişiklikler için takip edilecek süreç adımlarının belirlendiği gözlemlenir.	T	Z	2
K5.T3	İş sürekliliği planı üzerinde yapılacak değişiklikler ile ilgili üst düzey yöneticilerin onayının alındığının teyidi yapılır.	İ	Z	1
K5.T4	Güncellenen planlarda sürüm değişikliklerinin açıkça belirtildiği gözlemlenir.	İ	O	1

K6 - Tüm iç ve dış taraflar ve paydaşlar için iş sürekliliği konusunda eğitimler düzenlenir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K6.T1	SY dahilinde ilgili personel ve paydaşlar tarafından alınması gereken eğitimlerin sıklığına ve eğitim yöntemlerine (ör: sınıf eğitimi, e-eğitim) plan içerisinde yer verildiği gözlemlenir.	T	Z	1
K6.T2	Süreklilik yönetimi sürecinde planlama, etki değerlendirme, risk analizi, iletişim ve acil müdahale konularında gerekli eğitimlerin, verildiği katılımcı listeleri incelenerek teyit edilir. Eğitimler neticesinde yapılacak sınav vb. yöntemler ile eğitimlerin etkinliğinin ölçüldüğü gözlemlenir.	İ	Z	1
K6.T3	Süreklilik yönetimi sürecinde görev alan personelin bilgi birikimi ve yeteneklerinin testler düzenlenerek ölçüldüğü gözlemlenir.	İ	O	1

K7 - Süreklilik ile ilgili yedekleme faaliyetlerine yönelik olarak felaket anında ve sonrasında iş için kritik olan verilerin erişilebilirliği 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 testleri	T/İ	Z/O	YS
K7.T1	Yedekleme politika ve prosedürleri incelenir. Bu dokümanlar içerisinde iş ihtiyaçlarına göre yedekleme gereksinimlerinin, takvimlerinin, kullanılacak yedekleme araçlarının ve sistemlerinin bulunduğu ve tanımlandığı gözlemlenir.	T	Z	2
K7.T2	Kritik uygulamalar, veriler, dokümanlar ve sistemlerin belirtildiği bir envanterin mevcudiyeti sorgulanır.	İ	Z	1
K7.T3	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 vb. gibi belgeler incelenerek teyit edilir.	İ	Z	2
K7.T4	Yedeklenen verilerin kurumun tesis/yerleşkesi dışında, ana sistemlerin bulunduğu ortamla benzer riskleri içermeyen başka bir ortamda saklandığı teyit edilir.	İ	Z	1
K7.T5	Yedeklenen verilerin tesis/yerleşke dışına taşınırken güvenliğinin sağlandığı ve bulunduğu ortamın fiziksel ve mantıksal güvenliğinin sağlanmış olduğu teyit edilir.	İ	Z	2
K7.T6	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	2
K7.T7	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	2

K8 - İş süreçlerinin ve faaliyetlerin başarılı şekilde devreye alınmasının (ayağa kaldırılmasının) ardından süreklilik planının süreçteki yeterliliği değerlendirilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K8.T1	Bir felakete veya operasyonel kesintiye neden olan bir olayı takiben süreç boyunca süreklilik planına ne kadar uyulduğunun değerlendirildiği gözlemlenir.	İ	O	2
K8.T2	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	2

Ek Kaynaklar

- The IIA, (2008). Global Technology Audit Guide (GTAG), Business Continuity Management.
- ISACA, (2007). COBIT 4.1 Framework – DS4. Rolling Meadows, Illionis, ABD.
- ISACA, (2012). COBIT 5 Enabling Processes – DSS04. Rolling Meadows, Illinois, ABD.
- ISO/IEC, (2005). ISO/IEC 20000 6.3 Service Continuity and Availability Management.
- UK Cabinet Office, (2011), ITIL V3 2011 Service Design, 4.6 IT Service Continuity Management.
- ISO/IEC (2005). ISO/IEC 27002, 14 Business Continuity Management.
- ISO (2012). ISO 22301 Societal Secuirty – Business Continuity Management Systems.

4.6. BT Altyapı ve Yazılım Edinim, Kurulum ve Bakımı

Sürecin Genel Tanımı

BT altyapı ve yazılım edinim, kurulum ve bakımı süreci, kurumun stratejik ve operasyonel hedeflerini yerine getirebilmesi için zamanlı ve uygun maliyetli BT çözümlerinin uygulamaya konması amacını taşımaktadır. Bu çözümler, yazılımı kurum tarafından gerçekleştirilecek veya dışarıdan tedarik edilecek uygulamaları, 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 bakım 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.

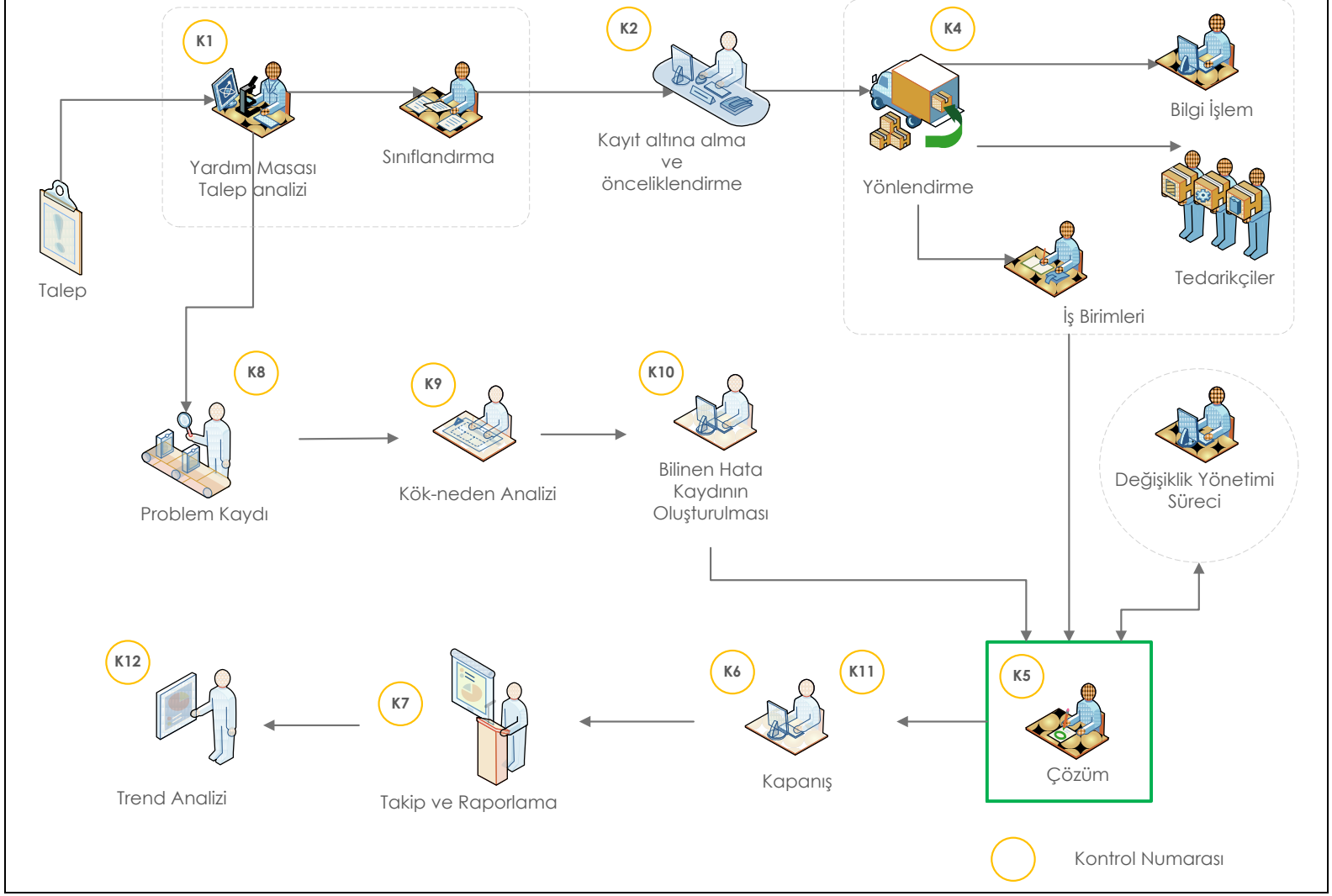
BT altyapı ve yazılım edinim, kurulum ve bakımı süreci, BT denetimi açısından aşağıdaki örnek süreç akışı üzerinden takip edilebilir. Söz konusu akış her kurum için farklı olabileceği gibi, süreç içerisinde ele alınan altyapı, yazılım veya hizmet tipleri, kullanılan yazılım ve tasarım araçları ile takip 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: ***4.7 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



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		+	+	+							

Denetim Testleri

K1 - Üzerinde önceden anlaşılmış yazılım geliştirme tekniklerine ve kurum BT stratejisine uygun, üst seviye tasarım dokümanları oluşturulur				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K1.T1	Kurum bünyesinde BT altyapı ve yazılım edinimi, kurulumu ve bakımı ile ilgili olarak hazırlanmış politika, prosedür ve iş akışlarının varlığı kontrol edilir.	T	Z	1
K1.T2	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	2
K1.T3	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	3
K1.T4	Örnek olarak seçilen projelerin tasarım yaklaşımının kurum tasarım standartlarına uygun şekilde gerçekleştirildiği hazırlanmış dokümanlar incelenerek ve BT ekipleri ile görüşülerek değerlendirilir.	İ	O	2
K1.T5	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	2
K1.T6	Örnek projelerin üst seviye tasarımlarının kalite gözden geçirmesine tabi tutulduğu ve paydaşların onayından geçtiği gözlemlenir.	İ	O	1

K2 - Detaylı tasarım ve teknik yazılım geliştirme ihtiyaçları belirlenir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K2.T1	Örnek projeler için yazılım kodu üzerinden geçme ve belge inceleme yöntemleri ile veri sözlüğü (veritabanlarındaki tüm veri öğelerin isimlerinin, cinslerinin, değer aralıklarının, kaynaklarının ve varsa erişim yetkilerinin tutulduğu veritabanı) standartlarına uyulduğu gözlemlenir.	İ	Z	3
K2.T2	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	2
K2.T3	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 gözlemlenir.	T	O	3
K2.T4	Örnek projeler için detay tasarım dokümanları incelenerek veri güvenliği, bütünlüğü ve erişilebilirliği ile ilgili ihtiyaçların ve yapılacakların tanımlandığı gözlemlenir.	İ	Z	2
K2.T5	Örnek projelerin tasarım dokümanlarında denetlenebilirlik ve ağ ihtiyaçları konularına değinildiği ve en iyi uygulamaların dikkate alındığı gözlemlenir.	İ	O	3
K2.T6	Örnek projeler için detay tasarım dokümanları incelenerek var olan sistemler ile entegrasyonun nasıl sağlanacağının dokümanlarda belirtildiği gözlemlenir.	İ	O	3
K2.T7	Örnek projeler için detay tasarım dokümanları incelenir ve kullanıcıların çalışacakları önyüzlerin tasarımları hakkında detaylara yer verildiği gözlemlenir.	İ	O	3
K2.T8	Yazılım süreci başlamadan önce detaylı tasarım standartlarının üzerinden gidilerek kontrolünün yapıldığı teyit edilir.	İ	O	3

K3 - Oluşturulmuş detaylı tasarımlara bağlı olarak ilgili çözümün bileşenleri, mevcut yazılım geliştirme, kalite ve dokümantasyon standartlarına uygun olarak geliştirilmeye başlanır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K3.T1	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	2
K3.T2	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	2
K3.T3	Proje sonunda ilgili paydaşlarla beraber değişiklik taleplerine uygun olarak tasarım, kalite ve performans değerlendirmelerinin yapıldığı kontrol edilir.	İ	O	3
K3.T4	Uygulanacak çözüm ile ilgili tüm bileşenlerin belirlenmiş standartlara uygun şekilde belgelendirildiği ve yenilik ve değişiklikler üzerinde sürüm kontrolünün sağlandığı kontrol edilir.	İ	Z	3
K3.T5	Temin edilen çözümler üzerinde yapılan tüm özelleştirme veya kişiselleştirme çalışmalarının etkinliğe, performansa ve diğer sistemlerle entegrasyona olan etkisinin değerlendirildiği gözlemlenir.	İ	Z	3
K3.T6	Kurum bünyesinde kod geliştirme konusunda bir standart bulunup bulunmadığı değerlendirilir.	T	O	2
K3.T7	Örnek projeler seçilerek kurumdaki mevcut kod standartlarının dikkate alındığı kontrol edilir. Bununla ilgili olarak projelerinin kodlarının nerede saklandığına, kullanılan fonksiyonların özelliklerine ve isimleme standartlarına bakılır	İ	O	3
K3.T8	Kaynak kodların bulunduğu ortamlara sadece yetkili insanlar tarafından erişilebiliyor olduğu, bu erişimlerin kaydedilerek saklandığı kontrol edilir.	İ	O	2
K3.T9	Kaynak kodların yazılımcı veya diğer kullanıcı bilgisayarlarına indirilemediği kontrol edilir. Eğer kodlar indirilebiliyorsa (check-out) bunların sistem tarafından kaydının tutulduğu, bir yazılımcı tarafından indirilen bir kodun başka bir yazılımcı tarafından (yazılım bütünlüğünün bozulmaması adına) değiştirilemeyeceği, yazılım geliştirilip sisteme yüklemesi yapıldıktan sonra yazılımın son kullanıcı bilgisayarından silindiği kontrol edilir.	İ	O	3
K3.T10	Kurum bünyesinde gerçekleşen yazılım geliştirme faaliyetlerinde güvenli kodlama prensiplerine uyulduğu kontrol edilir. Bu doğrultuda yazılımcıların arabellek aşımı (buffer overflow) ve kod enjeksiyonu gibi konulara dikkat edildiği ve kodların bu açıdan incelendiği teyit edilir.	İ	O	3

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 testleri**	**T/İ**	**Z/O**	**YS**
K4.T1	Kurum bünyesinde BT çözümlerinin teminine dair bir planın bulunduğu gözlemlenir. Planın içerisinde proje boyunca değişebilecek ihtiyaçlarla ilgili olarak yapılması gerekenlerin belirtildiği gözlemlenir.	T	Z	2
K4.T2	Doğrudan temin yöntemiyle tedarik edilen projeler arasından bir örneklem seçilir. Bu projeler için tüm tedarik planlarının, risk, maliyet, getiriler ve teknik uygunluk unsurlarının dikkate alınarak onaylandığı gözlemlenir. İhale yöntemiyle tedarik edilen çözümler için ilgili kanunda belirtilen tüm adımların uygulandığı incelenir.	İ	Z	2
K4.T3	Tedarik edilen çözümlerle ilgili kurum ihtiyaçlarına yönelik olarak, çözümün özelleştirilme ihtiyaçlarının belgelendiği gözlemlenir.	İ	O	2
K4.T4	Tedarik edilen tüm yazılım ve altyapı bileşenlerinin BT varlık envanterine kaydedildiği gözlemlenir.	İ	Z	1

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 testleri**	**T/İ**	**Z/O**	**YS**
K5.T1	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	2
K5.T2	Örnek çözümler için, çözümün kurum süreçlerine göre özelleştirilmesinin söz konusu olduğu durumlarda, süreçlerin ve operasyonel kılavuzların bu özelleştirmelere göre güncellendiği gözlemlenir.	İ	Z	2
K5.T3	Örnek olarak seçilen projeler için iş süreçleri kontrol gereksinimlerine dayalı olarak, otomatik uygulama kontrollerinin tanımlandığı kontrol edilir.	İ	O	2
K5.T4	Örnek olarak seçilen çözümlerin dokümanları incelenerek güvenlik, veri bütünlüğü, denetim izleri, erişim kontrolü ve veritabanı bütünlüğü gibi kontrollerin dikkate alındığı gözlemlenir.	İ	O	2

K6 - Kurum kalite yönetim sistemine uygun bir şekilde bir BT kalite planı oluşturulur ve ihtiyaç duyulan çözümün temini sürecinde bu kalite planı uygulanır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K6.T1	Çözümün temini ile ilgili olarak kalite güvence planı ve uygulamalarının aşağıdaki maddeleri içerecek şekilde tanımlandığı kontrol edilir. • 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	1
K6.T2	Kalite gözden geçirmelerinin yazılım sürecinden bağımsız kişilerce gerçekleştirildiği kontrol edilir.	İ	Z	1
K6.T3	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	1

K7 - Çözüm bileşenleri için bir test planı ve bu doğrultuda iş süreçleri, uygulamalar ve altyapıyı dahil edecek şekilde bir test ortamı oluşturulur.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K7.T1	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	2
K7.T2	Çözümlere uygun test prosedürlerinin ve var olan şartlar altında çözümü en iyi şekilde değerlendirme imkanını sunacak test senaryolarının hazırlanmış olduğu gözlemlenir.	İ	Z	3
K7.T3	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	3
K7.T4	Test prosedürlerinin çözüm üzerindeki kontrollerin yeterliliğini değerlendirmeye imkân verecek şekilde tasarlandığı ve test sonuçlarının proje paydaşları tarafından onaylandığı gözlemlenir.	İ	O	2

K8 - Edinilen çözümler ile ilgili testler, test planına ya da senaryolara uygun şekilde gerçekleştirilir				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K8.T1	Örnek olarak seçilen projelerde testlerin test planına ve senaryolarına uygun şekilde gerçekleştirildiği gözlemlenir.	İ	Z	2
K8.T2	Son kullanıcı kabul testlerinin yazılım ekibinden bağımsız son kullanıcılar veya iş süreç sahipleri tarafından gerçekleştirildiği gözlemlenir.	İ	Z	1
K8.T3	Testlerin sadece test ortamında gerçekleştirildiği, canlı ortamda test yapılmasının engellendiği teyit edilir.	İ	Z	2
K8.T4	Temin edilen çözümler için hem otomatik gerçekleştirilen testlerin hem de kullanıcı testlerinin gerçekleştirildiği gözlemlenir.	İ	O	2
K8.T5	Test sırasında ortaya çıkan hataların belirlendiği ve kaydedildiği gözlemlenir	İ	O	1
K8.T6	Testlerin kullanıcılar tarafından nihai onaylar verilene kadar devam ettiği, kullanıcı onayı olmayan çözümlerin uygulamaya konmadığı gözlemlenir.	İ	Z	1
K8.T7	Test sonuçlarının kayıt altına alınarak muhafaza edildiği ve ilgili paydaşlarla paylaşıldığı gözlemlenir.	İ	Z	1

K9 - Proje yaşam döngüsü boyunca gerçekleşmiş olan tüm yeni ihtiyaçlar ve değişiklikler ilgili birimler tarafından onaylanır ve takip edilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K9.T1	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	2
K9.T3	Değişiklik taleplerinin önceliklendirildiği kontrol edilir.	İ	O	1
K9.T4	Tüm paydaşların gerçekleşen değişikliklerden haberdar olmasını sağlayacak mekanizmaların kurulmuş olduğu ve bu değişikliklerin paydaşları temsil eden birimler tarafından da onaylandığı gözlemlenir.	İ	O	2

K10 - Çözümün ve ilgili altyapı bileşenlerinin bakımı için bir bakım planı geliştirilir ve uygulanır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K10.T1	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	2
K10.T2	Örnek olarak seçilen çözümlere (tedarik edilmiş ya da kurum bünyesinde geliştirilmiş) ait kayıtlar ve belgeler incelenir ve aşağıdaki unsurları içerip içermediği kontrol edilir. • 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	2
K10.T3	Çözümlerin bakımı sürecinde ihtiyaç duyulan tüm değişikliklerin, değişiklik yönetimi sürecine uygun şekilde gerçekleştiği teyit edilir.	İ	Z	2
K10.T4	Önerilen bakım faaliyetlerinin var olan çözüm faaliyetleri üzerindeki etkisinin analiz edildiği gözlemlenir. Bu analiz kapsamında riskin, kullanıcılara olan etkinin ve bakıma ayrılacak kaynakların değerlendirildiği kontrol edilir.	İ	O	2
K10.T5	Süreç sahiplerinin bakım süreçleri ile ilgili bilgilendirildikleri ve yapılacaklardan haberdar oldukları teyit edilir.	İ	O	1
K10.T6	Bakım faaliyetlerinin yoğunluğunun ve eğilimlerinin incelendiği, anormal yoğunluk olan durumların saptandığı ve önlemlerin alındığı kontrol edilir.	İ	O	2

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 testleri**	**T/İ**	**Z/O**	**YS**
K11.T1	Yeni uygulamaya alınan çözümlerin hizmet seviyeleri üzerine getirebileceği değişikliklerin yönetim tarafından değerlendirildiği kontrol edilir.	İ	Z	2
K11.T2	Yeni hizmet seviyelerinin aşağıdaki örnek unsurları barındıracak biçimde şekillendirildiği kontrol edilir. • Hizmet süreleri • Kullanıcı memnuniyeti • Erişilebilirlik • Performans • Kapasite • Güvenlik • Süreklilik • Uyum • Kullanışlılık	İ	O	1

Ek Kaynaklar

- ISACA, (2007). COBIT 4.1 Framework – AI02. Rolling Meadows, Illionis, ABD.
- ISACA, (2012). COBIT 5 Enabling Processes – BAI03. Rolling Meadows, Illinois, ABD.
- UK Cabinet Office, (2011). ITIL V3 2011 Service Transition, 4. Service Transition Processes
- Software Engineering Institute (2010). CMMI® for Development, Version 1.3. Hanscom AFB, MA, ABD.
- Software Engineering Institute (2010). CMMI® for Acquisition, Version 1.3. Hanscom AFB, MA, ABD.

4.7. BT Hizmet Yönetimi

Sürecin Genel Tanımı

BT hizmet yönetimi, BT'nin kuruma ve 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 beklentilere ve ihtiyaçlara uygun bir hizmet sağlamaktan sorumludur. Bundan dolayı BT bölümünün hizmet seviyesi anlaşmasınca (HSA) ortaya konulan hedeflere uyması önemlidir. Kurumlar bir bölüm BT hizmetlerini kurum içerisinden, geri kalanlarını ise dışarıdan da temin edebilir. Her iki durumda da HSA'larına uyumun sağlanması ve takip edilmesi önemlidir.

HSA, BT birimi ile hizmet ettiği birimler (iş birimleri) arasındaki bir anlaşmadır. HSA'lar, BT tarafından sağlanacak hizmetleri teknik olmayan bir dille, iş biriminin bakış açısından açıklar. Anlaşma süresince hizmetlerin ölçümü ve düzenlenmesi HSA'lar ile mümkündür. HSA'ların amacı sağlanacak hizmetlere dair hedeflerin ortaya konması ve bu hedeflerin takip edilmesidir. Bu nedenle HSA'lar farklı biçimlerde hazırlanabilir.

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 ilgili olup, BT denetimlerinde de ele alınan 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, ayrıca kurumun ve BT hizmetlerinden yararlananların memnuniyet düzeylerinin belirlenmesi açısından da önemlidir ve süreçte yaşanabilecek aksaklıklar başka önemli kontrol eksikliklerine işaret edebilir.

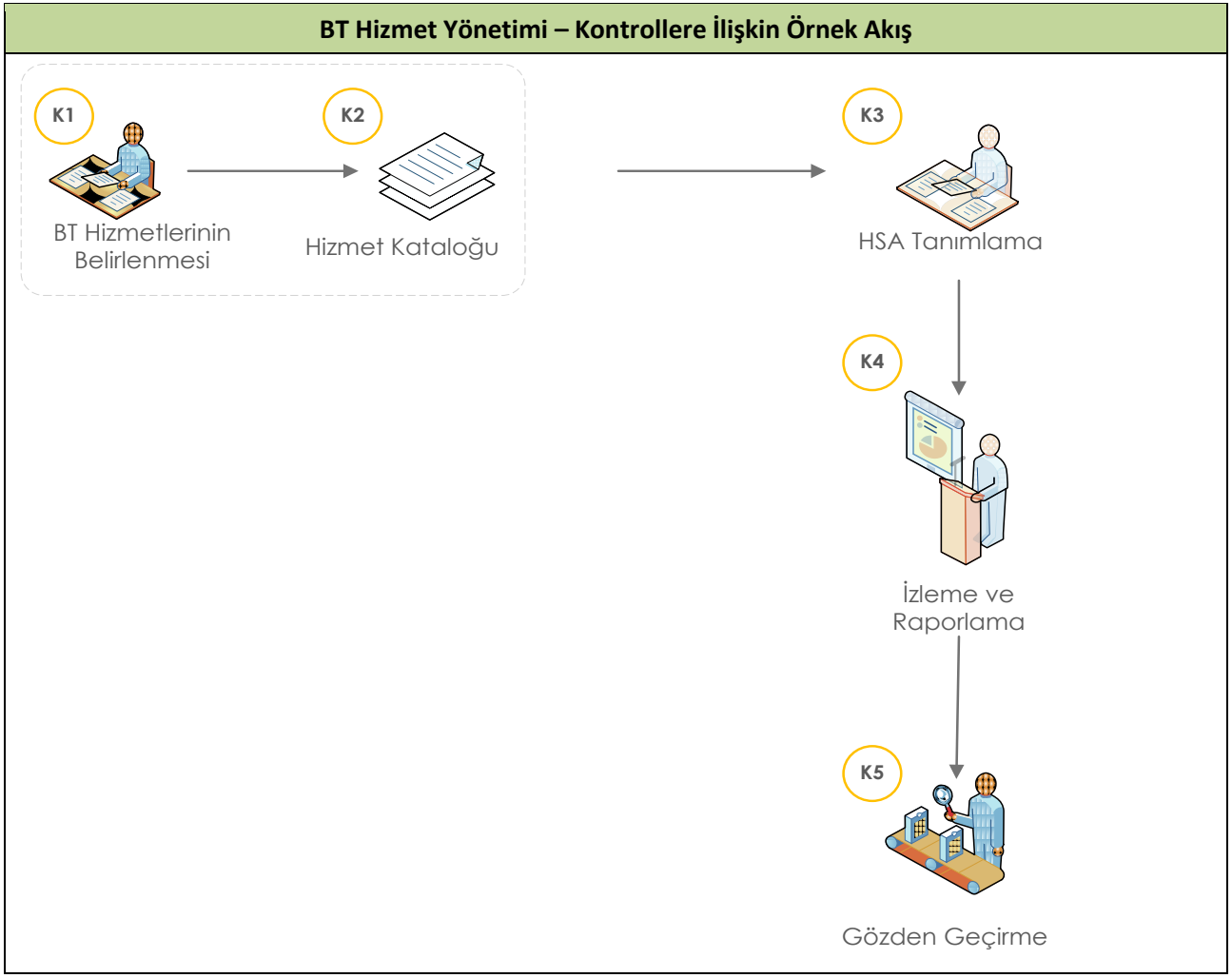
BT hizmet yönetimi süreci, BT denetimi açısından aşağıdaki örnek süreç akışı üzerinden takip edilebilir. Söz konusu akış her kurum için farklı olabileceği gibi, süreç içerisinde ele alınan HSA'ların yapısı, hizmet tipleri, takip ve raporlama mekanizmaları da kurumdan kuruma değişebilmektedir.

Kontrollere İlişkin Örnek Akış

Süreçte yer alan tipik kontrollere aşağıdaki tabloda yer verilmiştir:

BT Hizmet Yönetimi - Kontroller	
K1	İş ihtiyaçlarının ve BT tarafından sağlanan hizmetlerin ve anlaşılmış hizmet seviyelerinin iş süreçlerini nasıl desteklediği incelenir. Hizmet seviyeleri 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, yönetime, performans yönetimi açısından bilgilendirme amacı ile raporlanır.
K5	HSA'lar ve eğer varsa bağlı oldukları sözleşmeler, güncellikleri, ihtiyaçları ne kadar yansıttıkları ve etkinlikleri açısından 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. Hizmet 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 sağlanamaması	+	+	+	+	+
R8. İş birimlerinin ve BT'nin hizmetler ile ilgili olarak kendi sorumluluklarını kavrayamaması	+	+	+		

1.1.1. Denetim Testleri

K1 - İş ihtiyaçlarının ve BT tarafından sağlanan hizmetlerin ve anlaşılmış hizmet seviyelerinin iş süreçlerini nasıl desteklediği incelenir. Hizmet seviyeleri iş birimleri ile değerlendirilir ve bu seviyeler üzerinde anlaşılır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K1.T1	Hizmet yönetimi politika ve prosedürleri incelenir. Bu dokümanların BT tarafından sağlanan hizmetlerin ve bu hizmetlere dair performans göstergelerinin, iş hedefleri ve BT stratejisi ile uyumu olarak tasarlanması ile ilgili yol gösterici olduğu gözlemlenir.	T	Z	2
K1.T2	Kurum bünyesinde BT tarafından iş birimlerine sağlanan hizmetlerin belirlendiği ve bu hizmetler analiz edilerek ileride ihtiyaç duyulabilecek yeni hizmetlerin ve kapasite ihtiyaçlarının da kurum hedeflerine uygun şekilde değerlendirildiği gözlemlenir.	T	Z	2
K1.T3	İş birimlerine sağlanan BT hizmetlerinin düzenli olarak incelendiği ve verilen hizmetlerde gerekebilecek değişikliklerin saptandığı, gerek duyulmayan hizmetlerin sonlandırıldığı gözlemlenir.	İ	O	2

K2 - İlgili hedef gruplar için hizmet katalogları tanımlanır. BT tarafından sağlanan hizmetler bu kataloglarda yayınlanır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K2.T1	İş birimlerine sağlanan ilgili BT hizmetlerinin ve hizmet seviyelerinin bulunduğu katalogların hazırlandığı kontrol edilir.	T	Z	1
K2.T2	Hizmet kataloglarının güncel olduğu ve düzenli olarak güncelliğinin kontrol edildiği gözlemlenir.	İ	Z	1
K2.T3	Hizmet kataloglarında denetim dönemi içerisinde gerçekleşmiş olan güncellemeler temin edilir, bu güncellemeler ile ilgili olarak iş birimlerinin bilgilendirildiği kontrol edilir.	İ	Z	1

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 testleri**	**T/İ**	**Z/O**	**YS**
K3.T1	Sağlanan BT hizmetleri ile ilgili tüm paydaşların HSA'lar ile ilgili bilgilendirilmiş oldukları ve şartları kabul ettikleri gözlemlenir.	İ	Z	1
K3.T2	Örnek olarak seçilen HSA'ların istisnaları, ticari anlaşmaları ve işletim seviyesi anlaşmalarını (İSA) içerdiği kontrol edilir.	İ	Z	2
K3.T3	Kurumdaki HSA yönetimi süreci incelenir ve HSA anlaşmalarında belirlenmiş hedeflerin takip edildiği gözlemlenir.	İ	Z	2
K3.T4	Örnek olarak seçilen HSA'ların uygun BT ve iş birimi temsilcileri tarafından onaylandığı ve imzalandığı kontrol edilir.	İ	Z	1
K3.T5	HSA'ların düzenli olarak gözden geçirildiği ve gerektiği durumlarda uygun değişikliğin gerçekleştirildiği kontrol edilir.	İ	Z	1
K3.T6	Hizmetlerin teknik olarak nasıl sağlanacağını açıklayan İSA'ların oluşturulması, yönetilmesi, gözden geçirilmesi ve düzeltilmesi süreçlerinin kurum bünyesinde mevcut olduğu gözlemlenir.	T	Z	1
K3.T7	Örnek olarak seçilen HSA'lara ait İSA'ların ilgili hizmete dair hizmet ihtiyaçlarını içerdiği kontrol edilir.	İ	Z	2
K3.T8	Örnek olarak şeçilen İSA'ların hizmetin sağlanması ile ilgili uygulanabilir ve uygun tanımları içerdiği kontrol edilir.	İ	Z	2
K3.T9	Örnek olarak seçilen HSA'ların aşağıdaki unsurları içerdiği gözlemlenir. • 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 taahhüdü	İ	Z	1

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 testleri**	**T/İ**	**Z/O**	**YS**
K4.T1	HSA'ların izlenmesi ve izleme sonuçlarının raporlanması ile ilgili sürecin kurum bünyesinde tanımlı olduğu gözlemlenir.	T	Z	1
K4.T2	Sağlanan hizmetlerin performansının değerlendirildiği ve düzenli ve onaylı olarak iş birimlerine ve yönetime raporlandığı kontrol edilir. Raporlananlar arasında önceden üzerinde mutabık kalınmış değerlerden sapmaların bulunup bulunmadığına dikkat edilir.	İ	Z	1
K4.T3	Hizmet seviyesi performansı ile ilgili olarak tahminlerin yapıldığı ve eğilimlerin izlendiği kontrol edilir.	İ	O	1
K4.T4	Performans ile ilgili problemlerin oluştuğu hizmetler öğrenilir. Bu problemlerin çözümü için aksiyon planlarının hazırlandığı gözlemlenir.	İ	Z	1

K5 - HSA'lar ve eğer varsa bağlı oldukları sözleşmeler güncellikleri, ihtiyaçları yansıttıkları ve etkinliklerini kontrol amacı ile düzenli olarak gözden geçirilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K5.T1	Örnek olarak seçilen HSA'lar ve varsa bağlı oldukları sözleşmeler incelenir, güncel oldukları ve gerektiğinde değişiklik gördükleri gözlemlenir.	İ	Z	1
K5.T2	HSA'ların ve eğer varsa bağlı oldukları sözleşmelerin düzenli olarak iş ihtiyaçlarına uygunluk açısından değerlendirildikleri gözlemlenir.	İ	Z	2

Ek Kaynaklar

- ISACA, (2007). COBIT 4.1 Framework – DS1. Rolling Meadows, Illionis, ABD.
- ISACA, (2012). COBIT 5 Enabling Processes – APO09, Rolling Meadows, Illinois, ABD.
- UK Cabinet Office, (2011). 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.

4.8. BT Risk Yönetimi

Sürecin Genel Tanımı

BT 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 kurumun risk yönetimi stratejisi belirlenir. Bilgi teknolojileri 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 mevzuat ile çizilen çerçeveye uygun olarak bilgi teknolojilerine ilişkin risk yönetim süreçlerini geliştirirler.

Sürecin BT Denetimi Açısından Önemi

BT 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. BT risk yönetiminin değerlendirilmesi sayesinde, BT hizmetlerinin karşı karşıya olduğu risklerin kurumca kabul edilmiş düzeylere indirildiğine ve BT'den kaynaklanan risklerin yönetildiğine dair makul güvence sağlanabilir.

BT 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.

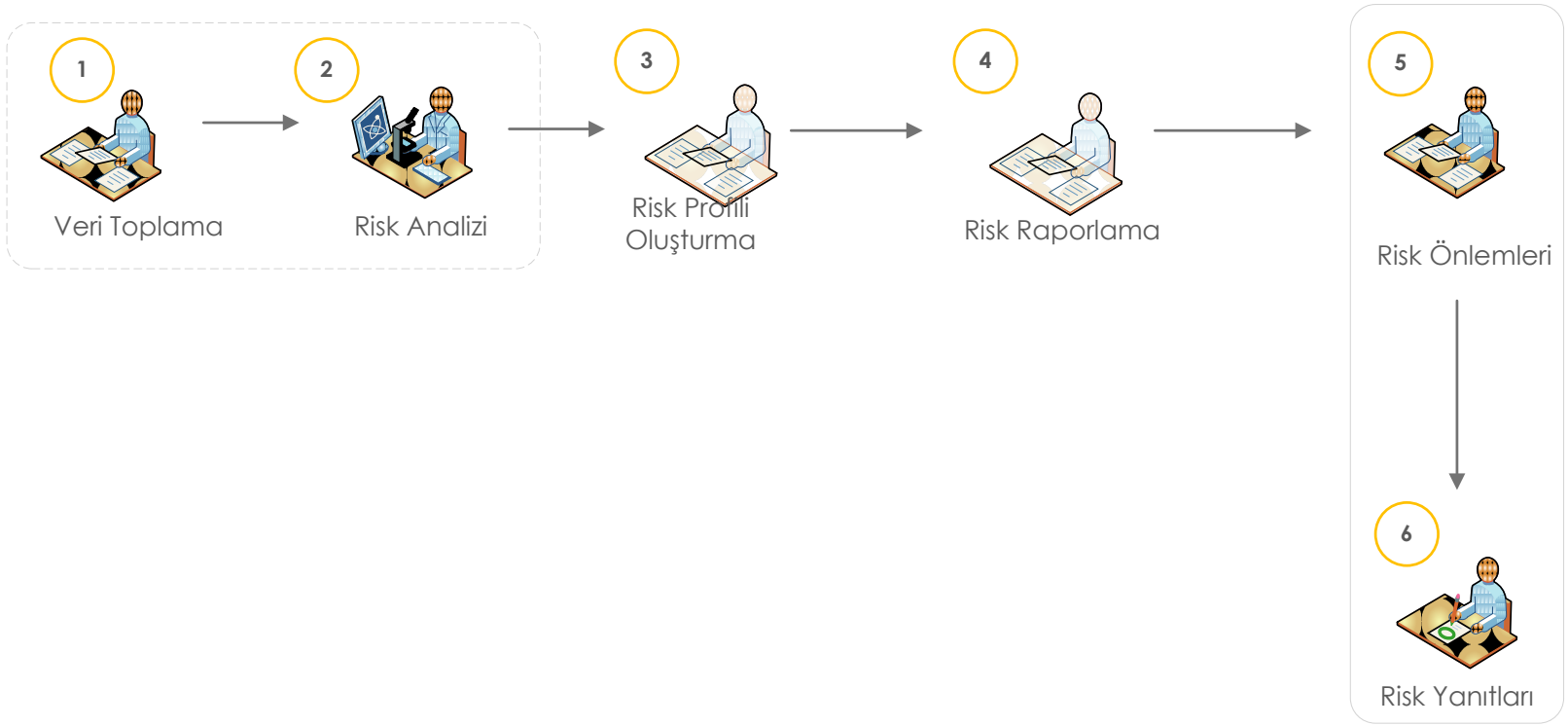
Kontrollere İlişkin Örnek Akış

Süreçte yer alan tipik kontrollere aşağıdaki tabloda yer verilmiştir:

BT 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 ve analiz edilir. 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, etkilenen 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 süreci geliştirilir.

Bahsi geçen kontrollere ilişkin örnek akış şeması aşağıda yer almaktadır:

BT Risk Yönetimi – Kontrollere İlişkin Örnek Akış



Kontrol numaraları

Risk – Kontrol Eşleşmeleri

BT Risk Yönetimi Risk – Kontrol Eşleşmeleri						
Riskler	**K1**	**K2**	**K3**	**K4**	**K5**	**K6**
R1. Önlem alınmamış risklerin gerçekleşmesi sonucu kurum itibarının zarar görmesi, mali ve operasyonel kayıpların oluşması	+	+	+	+	+	+
R2. BT'nin iş süreçleri üzerindeki etkisinin değerlendirilememesi		+	+	+		
R3. Risk azaltıcı kontrollerin beklenen etkiyi sağlamaması		+			+	
R4. Risklerin yanlış nitelik ve nicelik analizlerine göre değerlendirilmesi		+	+			+
R5. Risk envanterinin yetersiz, kurum ve iş ihtiyaçlarına uymayan riskleri içermesi.	+	+	+			
R6. BT'ye ilişkin fonksiyonel ve teknik nitelikteki risklerin yeteri kadar dikkate alınmaması.	+	+	+			
R7. Kurum içerisinde BT'den kaynaklanan risklerin doğru algılanmasına ve takibine ilişkin bilinç düzeyinin yeterli olmaması.				+		

Denetim Testleri

K1 - Etkin bir BT risk tanımlama, analiz ve raporlama mekanizmasının kurulması için risk verileri tanımlanır ve toplanır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K1.T1	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	2
K1.T2	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	2
K1.T3	Kurum tarafından incelenen risk verileri ve tespit edilen eğilimler değerlendirilirken benzer kurum ve kuruluşlardaki en iyi örneklerden faydalanıldığı gözlemlenir.	İ	O	2
K1.T4	BT hizmetlerine, projelerine ve operasyonlarına etkisi olabilecek risk olaylarının kayıt altına alındığı ve incelendiği kontrol edilir.	İ	Z	1
K1.T5	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	1
K1.T6	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	Z	1
K1.T7	Yeni veya ortaya çıkmak üzere olan risk konularının tespit edilmesi için, olay ve risk etmenlerinin periyodik olarak kurum tarafından analiz edildiği denetlenir.	İ	O	1

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 testleri**	**T/İ**	**Z/O**	**YS**
K2.T1	Tüm risk faktörleri ve varlıkların iş süreçleri açısından kritikliği değerlendirilerek risk analizi için harcanacak çabanın kapsamının ve derinliğinin tanımlanmış olduğu kontrol edilir. Risk değerlendirmesi kapsamının maliyet-fayda analizine dayandırılmış olduğu değerlendirilir.	T	Z	2
K2.T2	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	2
K2.T3	Risk senaryolarının gerçekleşme olasılıklarının hesaplandığı, risklerin sebep olacağı etkilerin istatistiksel olarak değerlendirildiği ve artık risk seviyelerinin tahminlendiği gözlemlenir.	İ	Z	2
K2.T4	Artık risklerin kurumun risk toleransı ile karşılaştırıldığı ve aksiyon alınması gereken risklerin belirlendiği gözlemlenir.	İ	Z	2
K2.T5	BT risk senaryoları ile ilgili olası kayıp ya da kazançların ve tahmin edilen gerçekleşme olasılığının tanımlandığı kontrol edilir.	İ	O	2
K2.T6	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	2
K2.T7	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	2
K2.T8	Risk analizi sonuçlarının kurumsal gereksinimler ile uyumlu olduğu ve kararlar alınmadan önce onaylandığı kontrol edilir.	İ	Z	2

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 testleri**	**T/İ**	**Z/O**	**YS**
K3.T1	Kurum bünyesinde personel, uygulamalar, altyapı, 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.	T	Z	2
K3.T2	BT hizmetlerinin ve BT altyapı kaynaklarının hangi iş süreçleri operasyonlarının sürdürülmesi için kritik olduğunun tanımlanmış olduğu kontrol edilir. Bu bağımlılıkların analiz edildiği ve risklerin belirlendiği gözlemlenir.	T	Z	2
K3.T3	Risk profil bilgilerinin düzenli olarak tutulduğu ve risk profili kapsamında kurum risklerine entegre bir şekilde ele alındığı kontrol edilir.	İ	O	2
K3.T4	Risk profillerine göre, risk göstergelerinin tanımlandığı ve mevcut risk ve risk trendlerinin belirlendiği ve izlendiği kontrol edilir.	İ	Z	2
K3.T5	Gerçekleşen riskler ile ilgili bilgilerin tutulduğu ve kurumun BT risk profiline dahil edildiği kontrol edilir.	İ	Z	2
K3.T6	Risk aksiyon planının belgelendiği ve kurum BT risk profiline dahil edildiği kontrol edilir.	İ	Z	2

K4 - Maruz kalınan BT risklerinin mevcut durumu ve fırsatlar ile ilgili bilgiler, paydaşlar ile zamanında paylaşılır.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K4.T1	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	2
K4.T2	Yasal ve düzenleyici hususlar, zorunluluklar, itibar, durum tespitleri ve en kötü ve en olası senaryolar da göz önünde bulundurularak karar alındığı gözlemlenir.	İ	Z	2
K4.T3	Risk yönetim sürecinin etkinliği, kontrollerin etkinliği, eksikler, uyumsuzluklar, fazlalıklar, iyileştirme durumu ve bunların risk profiline etkisi de dâhil olmak üzere mevcut risk profilinin tüm paydaşlara iletilmiş olduğu kontrol edilir.	İ	Z	2
K4.T4	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	2
K4.T5	Risk içeren alanlar için düzenli olarak, daha büyük risk kabulünü sağlayacak ve daha çok getiri getirecek BT ile ilgili fırsatların belirlendiği gözlemlenir.	İ	O	2

K5 - Kurum tarafından riskleri kabul edilebilir bir seviyeye indirebilmek için olanaklar etkin bir şekilde yönetilir.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K5.T1	Kurum bünyesinde risklere karşı belirlenmiş kontrol aktivitelerinin ve bu riskler karşısındaki risk toleransının belirtildiği bir risk-kontrol envanterinin tutulduğu kontrol edilir.	T	Z	2
K5.T2	Riskleri yönetmek için uygulanan kontrol aktivitelerinin sınıflandırıldığı ve BT risk bileşenlerine eşlendiği gözlemlenir.	İ	Z	2
K5.T3	Her bir birimin risklerini izlediği ve bu risklerin ve olası etkilerinin farkında olarak faaliyetlerini sürdürme sorumluluğunu kabul etmiş oldukları gözlemlenir.	İ	O	2

K6 - Uygun maliyetli kontroller ile risklerin etkilerini azaltmak üzere tasarlanmış bir risk tedavi süreci oluşturulur.				
#	**Denetim testleri**	**T/İ**	**Z/O**	**YS**
K6.T1	Bir riskin, ciddi bir iş etkisi ile birlikte önemli bir operasyonel olaya neden olduğunda atılması gereken belirli adımların dokümante edildiği ve test planlarının hazırlanmış olduğu kontrol edilir.	T	Z	2
K6.T2	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	2
K6.T3	Denetim döneminde gerçekleşmiş olan tanımlı riskler temin edilir. Olaylar meydana geldiğinde, etkiyi en aza indirmek için uygun müdahale planının uygulandığı denetlenir.	İ	Z	2
K6.T4	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 yönetişim süreçlerine dahil edildiği kontrol edilir.	T	Z	2

Ek Kaynaklar

- ISACA, (2007). COBIT 4.1 Framework – PO9. Rolling Meadows, Illionis, ABD.
- ISACA, (2012). COBIT 5 Enabling Processes – APO12, Rolling Meadows, Illinois, ABD.
- ISO/IEC (2005). ISO/IEC 27001, Information Security Management Systems – Requirements, Section.
- ISO/IEC (2005). ISO/IEC 27002, 4 Risk Assessment and Treatment.

5. UYGULAMA KONTROLLERİNİN DENETİMİ

Bu bölümde uygulama kontrolleri denetiminde uygulama kontrollerine ilişkin kontrol kategorileri ve BT denetimlerinde karşılaşılabilecek temel kontrol örnekleri yer almaktadır.

- 5.1. Uygulama Kontrolleri
- 5.2. Uygulama Kontrolleri - BT Genel Kontrolleri İlişkisi

5.1. Uygulama kontrolleri

Rehber'in bu bölümünde uygulama kontrollerine ilişkin kontrol kategorilerine ve BT denetimlerinde karşılaşılabilecek temel kontrol örneklerine yer verilmektedir. Uygulama kontrollerine ilişkin tanım, diğer kontrol türleriyle olan ilişkisi ve diğer önemli hususlar Rehber'in ikinci bölümünde açıklanmıştır.

Temel itibariyle süreçler üzerinde bilgi sistemleri tarafından desteklenen uygulama kontrollerinin belirlenen kapsam ve gerçekleştirilen risk değerlendirmelerine istinaden denetlenmesi gerekebilir. Burada özellikle gerçekleşen denetim türü uyarınca ortaya çıkan denetim ihtiyaçları belirli olmaktadır. 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. Dolayısıyla başta mali ve sistem denetimleri olmak üzere, tüm bütünleşik denetimlerde uygulama kontrollerinin incelenmesi değerlendirilmelidir.

Uygulama kontrolleri, BT tarafından sağlanması beklenen "kritik BT işlevselliklerini" içerir. Denetim açısından bu işlevselliklerin yerine getirilmesi, denetlenen verilerin tamlığı ve doğruluğu açısından önem arz eder. Verilerin sistemlere girilmesi, yetkilendirme, bütünlük ve tutarlılık kontrolleri, veri işleme, hesaplama, raporlama, ortaya çıkan hataların tespiti ve raporlanması, mutabakatlar ve çıktıların kontrolü gibi birçok kritik işlev, uygulama kontrolleri tarafından yerine getirilir.

Uygulama kontrolleri özellikle süreç içerisindeki yeri ve özellikleri açısından çeşitli kategoriler halinde ele alınabilmekle birlikte, her BT uygulamasının çalışma yapısı birbirinden farklı olacağı için, standart test adımlarının önerilmesi kolay ve çoğu kez uygulanabilir değildir. Burada denetçi, özellikle denetlenen süreç ve süreci destekleyen BT uygulamaları hakkında detaylı araştırma yapmalı ve çeşitli uygulama kontrolü kategorilerini de dikkate alarak anahtar kontrolleri tespit etmelidir. Bu amaçla BT uygulamalarına ait sistem dokümantasyonunun, son kullanıcı kılavuzlarının ve ilgili kontrol prosedürlerinin gözden geçirilmesi yararlı olabilir. Öte yandan denetçinin bizzat BT uygulaması üzerinde incelemeler yapması da kanıtların güvenilirliğini arttıran bir unsurdur.

Uygulama kontrolleri aşağıdaki ana kategoriler kapsamında incelenmektedir:

Tablo 6 -Uygulama Kontrolleri

Uygulama kontrolü kategorileri	**Örnek uygulama kontrolleri**
1. Kaynak veri hazırlığı ve yetkilendirme	
1.1	Kaynak belgelerin tasarımı, verilerin doğru bir şekilde kaydedilmesine, akışın kontrol edilebilmesine ve referans kontrollerine izin verecek şekilde yapılır.
1.2	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

Tablo 6 -Uygulama Kontrolleri	
	olarak kaynak verilerin hangi medya ortamında kabul edilebileceği belirtilir.
1.3	Uygulamalara kaynak veri girişinden sorumlu personelin güncel bir listesi tutulur, gerekli yönetim kademeleri tarafından onaylanır ve personel değişiklikleri oldukça güncellenir.
1.4	Tüm kaynak belge tipleri standart bir içerikte ve formatta hazırlanır, onaylanır ve değişiklik gerektiğinde güncellenir.
1.5	Uygulama üzerinde gerçekleşen tüm işlemlere otomatik olarak eşsiz ve ardışık işlem numaraları atanır.
1.6	Eksik, hatalı ya da onaylanmamış kaynak belgelerin sisteme girişi yapılmaz ve düzeltme için iade edilir.
2. Kaynak Verilerin Toplanması ve Girilmesi	
2.1	Kaynak belgelerin zamanlılığı (ör: doğru döneme ait olmaları), tamlığı ve doğruluğunun tespit edilebilmesi adına kriterler belirlenir ve veri girişleri bu doğrultuda yapılır.
2.2	Uygulamalara girdi olacak verilerin tanımlı ve bilinen uygulamalar ya da bilgi sistemlerinden geldiğinden emin olunacak önlemler uygulanır.
2.3	Uygulamalara kaynak veri girişinden sorumlu personelin, tedarikçi ya da hizmet sağlayıcı personel dahil, güncel bir listesi tutulur, gerekli yönetim kademeleri tarafından onaylanır ve personel değişiklikleri oldukça güncellenir.
2.4	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.
2.5	Kaynak verileri içeren belgeler gerekli yasal gereksinimler de göz önünde bulundurularak ve uygun güvenlik önlemleriyle korunarak saklanır.
2.6	Muhasebe bilgi sistemi olarak kullanılan uygulamalar üzerinde muhasebe hesapları ile ilgili işlemlerin (ana ve alt hesap tanımlama, değiştirme, silme) ve işlemler sırasında hangi hesapların birbiri ile çalışması gerektiğine dair kurguların eklenmesi, değiştirilmesi ya da silinmesi ile ilgili çalışmalar gerekli personelden alınan onaylara istinaden gerçekleştirilir, söz konusu işlemlere ilişkin denetim izleri oluşturulur ve saklanır. Söz konusu çalışmalar sırasında görevler ayrılığı ilkesine riayet edilir. Saklanan denetim izleri, işlemler

Tablo 6 -Uygulama Kontrolleri	
	sırasında hata olup olmadığının anlaşılması ve görevler ayrılığına riayet edilip edilmediğinin tespiti amacıyla düzenli olarak gözden geçirilir.
3. Doğruluk, Tamlık ve Orijinallik Kontrolleri	
3.1	Kaynak veri girişi sırasında verinin doğruluğu, tamlığı (ilgili tüm kayıtları eksiksiz içerdiği) ve orijinalliği 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.
3.2	Uygulamalara kaynak veri girişinden sorumlu personelin, tedarikçi ya da hizmet sağlayıcı personel dahil, güncel bir listesi tutulur, gerekli yönetim kademeleri tarafından onaylanır ve personel değişiklikleri oldukça güncellenir.
3.3	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 sistemsel olarak sağlanamadığı durumlarda risk azaltıcı ek izleme ve gözden geçirme çalışmaları gerçekleştirilir.
3.4	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. Veri girişi sırasında alınan hatalar sonucu ilgili bilgi sistemine aktarılamayan veri parçaları olursa bunların sisteme tekrar girilmesi sağlanır.
4. Veri İşleme Bütünlüğü ve Doğrulaması	
4.1	Veri işlemenin yalnız onaylanmış uygulama ve araçlar üzerinde yapılabildiğinden emin olunması için gerekli önlemler tesis edilir ve uygulanır.
4.2	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.
4.3	Veri işleme sırasında karşılaşılan hatalara ilişkin uygulama tarafından anlamlı mesajlar üretilmesi için gerekli önlemler alınır, hatalar zamanında takip edilir, çözülür ve raporlanır.
4.4	Kurum tarafından özellikle kritik olarak belirlenmiş tüm işlemlerin başlangıç saati, kim tarafından başlatıldığı, ne kadar sürdüğü vb. gibi detayları kayıt

Tablo 6 -Uygulama Kontrolleri	
	altına alınır ve güvenli bir şekilde saklanır.
4.5	İşlemlerin doğruluğu ve tamlığının kontrol edilebilmesi adına, işlemin başlangıcı ve tamamlanması ile ilgili kayıtlar ya da işlemin başladığı ve tamamlandığı sistemler arasında mutabakat kontrolleri tasarlanır ve uygulanır. Mutabakat kontrollerinin otomatik olmadığı durumlarda yürütülen manüel çalışmalar incelenir.
4.6	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	
5.1	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.
5.2	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.
5.3	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.
5.4	Uygulamalar üzerinde belirlenmiş sistematik kontrollerin ya da bunlara ilişkin onayların belirli ihtiyaçlar doğrultusunda atlanması ya da işlevsiz kılınması olasılıklarına karşı ilgili izleme, tespit ve raporlama mekanizmaları kurulur.
5.5	Uygulamalar üzerinde gerçekleştirilen işlemler arasında, muhasebe kaydı oluşturması gerekenlerin ilgili alt hesaplara doğru ve tam şekilde kaydedilmesi için gerekli kurgular tanımlanır. Söz konusu kayıtların oluşmadığı durumlar için hata kayıtlarının üretilmesi sağlanır ve ilgili hata kayıtları gözden geçirilerek hataların giderilmesine ilişkin gerekli aksiyonlar alınır.
5.6	Uygulamalar üzerinde gerçekleştirilen işlemler sonucunda alt hesaplarda oluşan muhasebe kayıtlarının belirli zamanlarda (ör: her işlemden sonra, ya da gün sonlarında) ana hesaplara kaydedilmesine yönelik kurgular tanımlanır. Söz konusu kayıtların oluşmadığı durumlar için hata kayıtlarının üretilmesi sağlanır

Tablo 6 -Uygulama Kontrolleri	
	ve ilgili hata kayıtları gözden geçirilerek hataların giderilmesine ilişkin gerekli aksiyonlar alınır.

Uygulama kontrolleri doğası gereği her kurumda 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 testi oluşturmak mümkün olmayabilir. Uygulanacak en iyi yaklaşımlardan biri, bu tür bir denetim faaliyeti gereken durumlarda, daha önce bu tür çalışmalarda bulunmuş tecrübeli bir denetçi eşliğinde çalışmaların yürütülmesi olacaktır. Denetim yapılacak uygulama ve sistemlerin daha önceden tanınıyor olması da bu konuda denetçiye önemli bir avantaj sağlayabilir.

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
- Bilgi sistemleri 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.

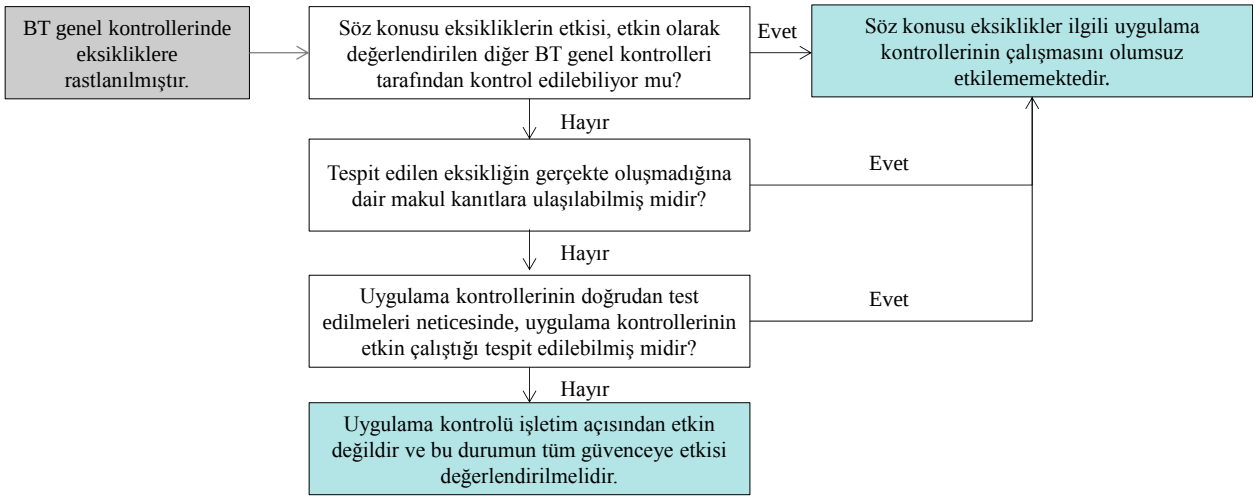
BT genel kontrolleri, ilgili uygulamalar üzerinde tanımlı ve ayarlanmış olan uygulama kontrollerinin tasarlandığı şekilde ve etkin bir biçimde çalışması için kritik bir rol oynamaktadır. Buna örnek olarak BT genel kontrollerinin değerlendirilmesi sırasında bir iş uygulaması üzerinde etkin olmayan yetkilendirme 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 doğası, zamanlaması ve kapsamı 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 aşağıdakilerle sınırlı olmamakla birlikte şunları içerebilir:

- 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 manüel birer kontrolmüş gibi denetim testlerine tabi tutulması (bu yönteme uygulama kontrolünün doğrudan test edilmesi de denir).
- 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.) ve maddi doğruluk testleri.
- 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 görevlerinin belirlenmesi amacıyla aşağıdaki karar ağacı oluşturulmuş olup, denetçi bu karar ağacındaki yönlendirmeler uyarınca denetim görevlerini revize etmelidir.

Şekil 7 – Genel BT Kontrollerindeki Eksikliklerin Uygulama Kontrollerine Etkisinin Değerlendirmesi



Ek Kaynaklar

- ISACA. (2009). COBIT an Application Controls. Rolling Meadows, Illionis, ABD.
- The IIA. (2007). Global Technology Audit Guide 8: Auditing Application Controls. Altamonte Springs, Florida, ABD
- Bankacılık Düzenleme ve Denetleme Kurumu (2010). Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik.
- Bankacılık Düzenleme ve Denetleme Kurumu (2007). Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ.

6. BT ALTYAPI GENEL KONTROLLERİ DENETİMİ

- 6.1. BT Altyapı Genel Kontrollerine Dair Bilgilendirme
- 6.2. İşletim Sistemleri
- 6.3. Veritabanı Sistemleri
- 6.4. Ağ Sistemleri
- 6.5. Uzaktan erişim

6.1. BT Altyapı Genel Kontrollerine Dair Bilgilendirme

Bu bölümde BT altyapı bileşenleri (işletim sistemleri, veritabanı sistemleri, ağ cihazları) üzerinde gerçekleştirilebilecek denetim görevleri sırasında kullanılabilecek ve örnek seçilmiş belirli teknolojilere ait denetim testleri verilmiştir.

BT altyapı bileşenlerinin genel BT denetimi içindeki rolü ve etkisi genel olarak Rehber'in ikinci bölümü içerisinde tartışılmış olup, hangi BT altyapı bileşeninin hangi durumlarda denetim kapsamına alınabileceğine dair gerekli bilgiler 2.2.4 Kapsam Belirleme bölümünde her bir denetim alanı için ayrı ayrı olmak üzere verilmiştir.

6.2. İşletim Sistemleri

6.2.1. Solaris 10 ve Redhat Enterprise Linux 6 İşletim Sistemleri

Risk – Kontrol Eşleşmeleri

Riskler	K1	K2	K3	K4
R1. Bilgi sistemleri üzerinde otomatik olarak tanımlanan varsayılan kullanıcılar kullanılarak diğer kullanıcıların yetkilerinin arttırılması	+			
R2. Bilgi sistemleri üzerinde kritik veri, bilgi ve cihazlara yetkisiz erişimlerin gözlemlenmesi	+	+	+	+
R3. Güvenlik ve parola parametrelerinin, yetkisiz erişimleri önleyecek şekilde atanmaması	+		+	
R4. Yetkisiz 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 arttırma işlemlerinin gerçekleştirilmesi	+	+		

Kontroller

K1 - Kullanıcı Hesap Yönetimi ve Parolalar

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 parolası gibi güvenlik parametreleri de başlangıçta sabit değerlere tanımlanmıştır. Bu gibi kullanıcı hesaplarına varsayılan (default) kullanıcı hesapları denir.

Bilgi sistemleri üzerindeki varsayılan kullanıcı hesap parolaları 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.

Unix/Linux 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 diğer sistem dosyaları üzerinde sahiplik oluşturmak için kullanılmaktadır. Varsayılan normal kullanıcılar ise Unix ve Linux işletim sistemi kurulumunu takiben sisteme erişimlerin gerçekleştirilebilmesi amacıyla otomatik olarak tanımlanmaktadır. Unix ve Linux sistemlerde kullanıcı hesap yönetiminde sistem dizini olan etc dizini altındaki passwd and shadow olmak üzere iki tip dosya kullanılmaktadır.

- passwd dosyası sistem/kullanıcı hesaplarının bir listesini tutmaktadır. Kullanıcı kimliği, grup kimliği, ev dizini, kabuk (shell) ve benzeri bilgileri göstermektedir.
- shadow dosyası sistem/kullanıcı hesaplarının şifreli (kriptolu) parola bilgilerini ve isteğe bağlı 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 parolası – 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 (isim, soyad, çalıştığı birim vb.)
/home/users/myilmaz: kullanıcının sistem girişi sonrasında bağlandığı kök dizin
/usr/bin/ksh: kullanıcı komut satırı (shell) programı tipi

Aşağıdaki örnek, bir Redhat Enterprise Linux sisteminde cat /etc/passwd komutu çıktısını göstermektedir.

```
gdm:x:42:42::/var/gdm:/sbin/nologin
distcache:x:94:94:Distcache:/:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
sabayon:x:86:86:Sabayon user:/home/sabayon:/sbin/nologin
admin:x:500:500:Admin:/home/admin:/bin/bash
avahi-autoipd:x:100:101:avahi-autoipd:/var/lib/avahi-autoipd:/sbin/nologin
bmkitche:x:501:501::/home/bmkitche:/bin/bash
nazgrel:x:502:502::/home/nazgrel:/bin/bash
nazgrel1:x:503:503::/home/nazgrel1:/bin/bash
nazgrel2:x:504:504::/home/nazgrel2:/bin/bash
itra:x:506:507::/home/itra:/bin/bash
morgama:x:507:508::/home/morgama:/bin/bash
jobi:x:508:509::/home/jobi:/bin/bash
EYTest:x:509:510::/home/EYTest:/bin/bash
EYTestn:x:510:511::/home/EYTestn:/bin/bash
vineet:x:511:512::/home/vineet:/bin/bash
test:x:512:10::/home/test:/bin/bash
tobias.pereira:x:513:515::/home/tobias.pereira:/bin/bash
root1:x:514:516::/home/root1:/bin/bash
sakiv:x:0:0::/home/sakiv:/bin/bash
```

`/etc/shadow` dosyasının içeriğindeki kayıtlar aşağıdaki formatta gösterildiği şekilde saklanır. Bu dosya içerisinde kullanıcı parolası belli kriptolama algoritmalarıyla (MD5, DES, DES3 vb.) işlenerek kriptolu *(hashed)* şekilde saklanır.

Örnek kayıt:

```
myilmaz:5lX3vWqgK0BDw:15453:0:99999:3:x:y:z
```

myilmaz: kullanıcı adı
5lX3vWqgK0BDw: kriptolu kullanıcı parolası *(hashed password*)
15453: kullanıcı parolasının en son değiştirildiği gün değeri (1 Ocak 1970 tarihinden itibaren gün sayısı)
0: parolanın değiştirilmeden önce kullanılması gereken minimum gün sayısı
99999: parolanın kullanılabileceği maksimum gün sayısı
3: geçerliliğini doldurmak üzere olan parola için ne kadar gün öncesinden uyarı verileceğini gösteren değer
x: parolanın geçerliliği dolduktan sonra kaç gün içerisinde kullanıcı hesabının pasif hale getirileceğini gösterir değer
y: kullanıcı hesabının pasif hale gelmesi için kalan gün sayısı
z: bu parametre alanı kullanılmaz, özel kullanım amaçlarına karşı rezerve edilmiştir

Aşağıdaki örnek, bir Redhat Enterprise Linux sisteminde `cat /etc/shadow` komutu çıktısını göstermektedir.

```
distcache:!!:14454:0:99999:7:::
apache:!!:14454:0:99999:7:::
webalizer:!!:14454:0:99999:7:::
squid:!!:14454:0:99999:7:::
xfs:!!:14454:0:99999:7:::
sabayon:!!:14454:0:99999:7:::
admin:$1$O3Ecto1z$pcmg69hH1zvomdm0YJ/6//:14456:0:99999:7:::
avahi-autoipd:!!:14456::::::
bmkitche:$1$fLIialTF$GbJVvPQAymKHbUwV4UkiR.:14705:0:99999:7:::
nazgrel:$1$pgDnCmpJ$dgM8rSeVTg10XiVbU/yUh/:14798:0:99999:7:::
nazgrel1:$1$R/bFCWFZ$.hyVmLBNNXMh3dVm4J1De0:14798:0:99999:7:::
nazgrel2:$1$vlgOxqQC$OlBDXUpnEMEcYSqxVafTT/:14798:0:99999:7:::
itra:$1$PNWHzIg/$skFLMNkj4pC9bd2n6Xpve0:14813:0:99999:7:::
morgama:$1$PWnfuYpw$9RHFGKbMU5B8fioJDDihd/:14840:0:99999:7:::
jobi:$1$K5ME0WxV$W2BMtnEDWAOMXX2300bYN.:14903:0:99999:7:::
EYTest:$1$/Hc2Akwd$8AdLr18wa3IcSMa3i8lov.:14917:0:99999:7:::
EYTestn:$1$fFze0IpO$Mk6188qQf5nZE7xu0aisb1:14917:0:99999:7:::
vineet:$1$i4/h33Wn$dy6ZpUKqPTs1kR0QVDnHd/:15008:0:99999:7:::
test:$1$qJb8zB3c$3V0xnn2g3/rUzdi7BP5Cv1:15049:0:99999:7:::
tobias.pereira:!!:15898:0:99999:7:::
root1:!!:15966:0:99999:7:::
sakiv:$1$7THXbNHe$KHIp1AIXLAcsqrMHJC1gR0:15966:0:99999:7:::
testitra:$1$ALJYjPjZ$h3XeCZjqFVXhJuncgp92N/:16048:0:99999:7:::
```

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K1.T1	BT güvenliğine ilişkin prosedür temin edilerek prosedürde yayımlanan Unix ve Linux sistem güvenliğine ilişkin standartların, sektörde kabul gören en iyi uygulamalara yönelik yapılandırıldığı gözlemlenir.	T	Z	3
K1.T2	`/etc/passwd` dosyası temin edilerek içeriğindeki kullanıcı adlarından sonra gelen alanda "`x`" işaretinin varlığı gözlemlenir. Bu bağlamda tüm kullanıcı parolalarının şifreli (kriptolu) bir şekilde saklandığı teyit edilir.	İ	Z	3

K1.T3	/etc/passwd ve /etc/shadow dosyaları temin edilip içeriğindeki aktif kullanıcı hesapları tespit edilir*. Aktif kullanıcı hesapları arasından denetim dönemi içerisinde yaratılan kullanıcı hesapları içerisinden örneklem yöntemiyle seçilen kullanıcılar için kullanıcı yetki talep ve onay dokümanları sorgulanarak onaylı prosedürün uygulandığı teyit edilir. ** Aktif olmayan kullanıcı hesapları, kullanıcı ismini takiben "LK" (locked)), "!" (ünlem) ya da "NP" (No Password) parametrelerine sahiptir. (Ör: "listen:*LK*:::::::" ya da "nobody:NP:6445::::::")*	İ	Z	3
K1.T4	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 parolalarının, kurumun bilgi güvenliği politikalarına uygun olarak değiştirildiğinden emin olunmalıdır.	İ	Z	3
K1.T5	Kullanıcı kayıtlarında, Unix ve Linux sistemlerde en yüksek yetkili kullanıcı olan "root" kullanıcısı hariç diğer kullanıcıların kimlik ve grup numaralarının 0 (sıfır) olarak atanmadığı teyit edilir.	İ	Z	3

K2 - Kritik Dosyalara Erişim

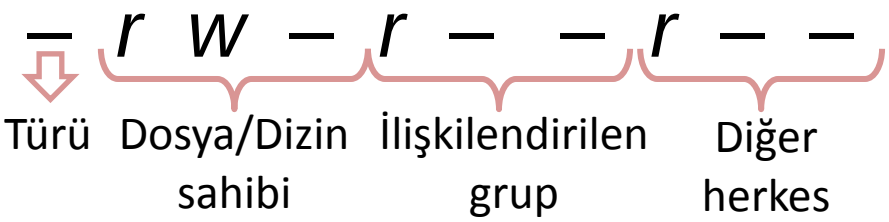
Unix/Linux işletim sistemlerinde kullanıcı hesap yönetimi amacıyla `/etc/passwd`, `/etc/shadow` ve `/etc/group` olmak üzere üç tip dosya kullanılmaktadır. Sırasıyla sistem üzerinde tanımlı kullanıcı adları, kullanıcı parolaları ve kullanıcıların dahil olduğu grupların saklandığı bu dosyalara sadece yetkili kullanıcılar erişmelidir.

UNIX/LINUX tabanlı sistemlerin dosya erişim yetkileri "`r, w, x`" gibi harfler kullanılarak ifade edilir. (Ör: *"*`-rw-r- -r- -`*")* Burada kullanılan harflerin temsil ettiği yetkiler şu şekildedir:

r: okuma (read)
w: yazma (write)
x: çalıştırma (execute)

İlk basamak yandaki tabloda görülen değerleri alabilir.
Sonraki basamaklar üçer hanelik gruplar şeklinde dosya üzerindeki yetkileri aşağıdaki şekilde gösterir:

Türü	Açıklama
-	sıradan dosya
d	dizin
l	başka bir dosyanın kısa yolu
p	işlemler arası bağlantı
s	soket (işlemler arası bağlantı)
b/c	blok ve karakter cihazlar
D	kapı (sunucu ve istemci arasındaki bağlantı) (Sadece Solaris için)



Dosya erişim yetkileri

Yukarıdaki gruplarda görülen erişim yetkileri, yandaki tabloda görüldüğü üzere, her üç haneye karşılık gelen rakamlarla gözlemlenebilir. Bu rakamlar, aşağıdaki değerlerin toplamı esasına göre hesaplanır.

r:4, w:2, x:1

Değer	Açıklama	Unix/Linux kodlaması
777	okuma, yazma, çalıştırma	`-rwxrwxrwx`
666	okuma, yazma	`-rw-rw-rw-`
555	okuma, çalıştırma	`-r-xr-xr-x`
444	okuma	`-r--r--r--`
333	yazma, çalıştırma	`--wx-wx-wx`
222	yazma	`--w--w--w-`
111	çalıştırma	`---x--x--x`
000	erişim izni mevcut değil	`---------`

Tablodaki açıklamalara göre, yukarıdaki örneğin erişim yetkileri kısaca 644 olarak ifade edilebilir.

Bu yetkilerin dışında, Unix/Linux dosya erişim izinlerinde sticky bit ve SUID/SGID bit gibi yetkiler de vardır. Bu yetkiler aşağıdaki şekilde görüldüğü gibi kullanılır. Sticky bit "t" ile ifade edilirken SUID/SGID biti, "s" ile ifade edilir. Sticky bit özelliği, dosya ya da klasörün sahibi ve root kullanıcısı dışında hiçbir kullanıcı tarafından silinememesini sağlar. SUID ve SGID özelliği, bir kullanıcının, bir çalıştırılabilir dosyayı kendisine tanınmış haklardan daha fazla izne sahip olarak çalıştırması gerektiği durumlarda kullanılmaktadır.

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 ilişkilendirilen gruptaki kullanıcıların, son değer ise önceki iki tanıma uymayan tüm kullanıcıların yetkilerini belirlemek için kullanılır. Genel Unix veya Linux 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 veya Linux sistem üzerinde varsayılan olarak bir kullanıcının yarattığı dizinlere ilişkin;

- kullanıcının kendisinin *okuma, yazma* ve *çalıştırma* (7),

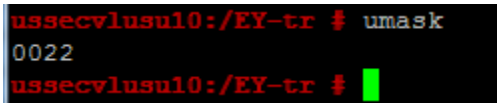
- kullanıcının ait olduğu grubun *okuma* (4),

- diğer bütün kullanıcıların ise sadece *okuma* (4) yetkisinin olması isteniyor.

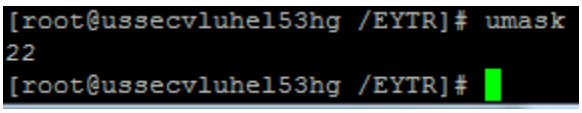
Bu durumda sistem üzerinde atanması gereken "Umask" değeri 777 değerinden 744 değeri çıkartılarak elde edilen 033 değeridir.

Unix/Linux sistemlerde bu izin 033, 0033 veya 33 olarak gözlemlenebilir

SUSE işletim sisteminden örnek ekran görüntüsü:



Linux tabanlı Redhat Enterprise işletim sisteminden örnek ekran görüntüsü:



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/LINUX kodlaması
000	okuma, yazma, çalıştırma	`-rwxrwxrwx`
111	okuma, yazma	`-rw-rw-rw-`
222	okuma, çalıştırma	`-r-xr-xr-x`
333	okuma	`-r--r--r--`
444	yazma, çalıştırma	`--wx-wx-wx`
555	yazma	`--w--w--w-`
666	çalıştırma	`---x--x--x`
777	erişim izni mevcut değil	`---------`

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K2.T1	BT güvenliğine ilişkin prosedür temin edilerek prosedürde yayımlanan Unix/Linux sistem güvenliğine ilişkin standartlar incelenir.	T	Z	3

K2.T2	Komut satırı (shell) aracılığı ile `/etc` dizininde "`ls -l`" komutu çalıştırılarak dizin içerisinde yer alan `passwd`, `group` ve `shadow` dosyalarına ait erişim yetkileri incelenir.
	
	Örnek erişim görüntüleri aşağıdaki gibidir:
	`[root@ussecvluhel53hg ~]# ls -l /etc/ |grep passwd`
	`-rw-r--r--  1 root root  2373 Dec  9 10:15 passwd`
	`-rw-r--r--  1 root root  2373 Sep 18 07:46 passwd-`
	`-rw-r--r--  1 root root  2206 Dec  3  2010 passwd.OLD`
	`[root@ussecvluhel53hg ~]#`
	`[root@ussecvluhel53hg ~]# ls -l /etc/ | grep shadow`
	`-r--------  1 root root   775 Dec  9 10:10 gshadow`
	`-r--------  1 root root   762 Sep 18 07:45 gshadow-`
	`-r--------  1 root root  2040 Dec  9 10:11 shadow`
	`-r--------  1 root root  1977 Sep 18 07:45 shadow-`
	`[root@ussecvluhel53hg ~]#`
	`[root@ussecvluhel53hg ~]# ls -l /etc/ | grep group`
	`-rw-r--r--  1 root root   938 Dec  9 10:10 group`
	`-rw-r--r--  1 root root   922 Sep 18 07:45 group-`
	`[root@ussecvluhel53hg ~]#`
		İ	Z	3

K2.T3	`passwd` ve `group` dosyası için erişimlerin '`-rw r-- r--`' şeklinde; "root" kullanıcısının yazma ve okuma yetkisi, diğer kullanıcıların ise yalnızca okuma yetkisi olacak şekilde atandığı gözlemlenir.	İ	Z	3
K2.T4	shadow dosyası için erişimlerin '`-rw- --- ---`' ya da '`-r-- --- ---`' root kullanıcısının okuma ve/veya yazma yetkisi, diğer kullanıcıların ise hiçbir yetkisinin olmadığı gözlemlenir.	İ	Z	3
K2.T5	Solaris işletim sistemlerinde `/etc/default/login` dosyası temin edilerek içeriğinde '`CONSOLE = /dev/console`' parametresinin aktif durumda olduğu teyit edilir. Linux sistemlerde ise `/etc/security/access.conf` dosyası temin edilerek içeriğinde '`-:wheel:ALL EXCEPT LOCAL`' 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 ile ilgili kayıtlar solaris işletim sistemlerinde `/var/adm/sulog`, Linux sistemlerde `ise /var/log/secure` doyasında saklanır.	İ	Z	3

K3 - Parola ve Güvenlik Parametreleri

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

Unix/Linux sistemlerde oturum açma aşamasında veya oturumlar arası bir kullanıcıdan başka bir kullanıcıya geçilirken, ilgili kullanıcının kullanıcı adı ve parolası girilerek kimlik doğrulaması yapılabilir. Buna paralel olarak, kullanıcılar, parolalarını belli kısıtlamalar çerçevesinde yaratabilir ya da değiştirebilirler. Bu kısıtları, sistem üzerinde tanımlanan güvenlik politikaları ve parola parametreleri belirler.

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K3.T1	Solaris işletim sistemi üzerinde `/etc/default/login` dosyası içeriği temin edilir. Temin edilen dosya içeriğinde `PASSREQ` parametresinin `YES` değerine atandığı `(PASSREQ = YES)` teyit edilir.* * Bu parametre, başında *"#"* imleci olmadığı sürece etkindir. Parametrenin başında *"#"* imleci mevcut ise, sisteme girişte kullanıcılar *kullanıcı adı* ya da *parola* girmeleri için sistem tarafından zorlanmazlar. Bu parametre etkin değil ise, diğer test adımları da geçerliliğini kaybedebilir.	İ	Z	3
K3.T2	Sistem üzerinde `/etc/shadow` dosyası içeriği temin edilir. Temin edilen dosya içeriğindeki kullanıcılara ait dizindeki 3'üncü parametre gözlemlenir. İlgili parametre 1 Ocak 1970 tarihinden itibaren gün cinsinden, kullanıcı hesabına ait parolanın hangi tarihte değiştiğini gösterir.	İ	Z	3

K3.T3	Solaris işletimsistemleri için sistem üzerinde `/etc/default/login` dosyasının içeriği temin edilir. Temin edilen dosya içeriğinde; • Aktif olmayan oturumların kaç saniye sonra kilitlenmesi gerektiğini belirleyen `TIMEOUT` parametresin `3600` (60 dakika) değerinden daha düşük bir değere atandığı teyit edilir. • Sistem üzerinde bir kullanıcı hesabının kaç hatalı giriş denemesi sonrası kilitleneceğini belirleyen `RETRIES` 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 parola girişleri sonrası kullanıcı hesaplarının sistem tarafından kilitlendikten sonra sistemin bu kilidi kaldırma süresini belirleyen `DISABLETIME` parametresinin uygun değere atandığı teyit edilir. Etkinleştirildiği takdirde varsayılan olarak `20` değerine atanmıştır. • Linux tabanlı işletim sistemleri için `/etc/profile` dosyasının içeriği temin edilir. Temin edilen dosya içeriğinde; • Aktif olmayan oturumların kaç saniye sonra kilitlenmesi gerektiğini belirleyen `TMOUT` parametresin `3600` (60 dakika) değerinden daha düşük bir değere atandığı teyit edilir. Linux için `/etc/pam.d/login` dosyasının içeriği temin edilir. Temin edilen dosya içeriğinde; • Sistem üzerinde bir kullanıcı hesabının kaç hatalı giriş denemesi sonrası kilitleneceğini belirleyen `account required /lib/security/pam_tally.so deny=5` 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.	İ	Z	3
K3.T4	Solaris işletim sistemi üzerinde `/etc/default/passwd` dosyası içeriği temin edilir. Temin edilen dosya içeriğinde; • Parola uzunluğu değerinin saklandığı `PASSLENGTH` parametresinin, • Parolada kullanılması gereken en az harf sayısını gösteren	İ	Z	3

	MINALPHA parametresinin*, • Parola içerisinde aynı karakterin en fazla kaç defa yan yana kullanılabileceğini belirten MAXREPEATS parametresinin**, • Kullanıcının eski ve yeni parolası arasındaki olması gereken minimum karakter farkı sayısının atandığı MINDIFF parametresinin***, • Parola içerinde bulunması gereken en az rakam sayısını gösteren MINDIGIT**** parametresinin**, • Parola içerisinde bulunması gereken en az küçük harf sayısını belirten MINLOWER** parametresinin, • Parola içerisinde bulunması gereken en az büyük harf sayısı MINUPPER parametresinin**, • Parola içerisinde bulunması gereken en az özel karakter (%, !, +, vb.) sayısını belirten MINSPECIAL**** parametresinin**, • Parola içerisinde bulunması gereken en az alfa-nümerik karakter (%, !, +, vb.) sayısını belirten MINNONALPHA***** parametresinin******, • Kullanıcı parolasının kullanıcı adı ile aynı olmasını önleyen NAMECHECK parametresinin uygun olarak atandığı gözlemlenir. * MINALPHA parametresi herhangi bir değere atanmamış ise varsayılan olarak 2 değeri alır. ** parametre herhangi bir değere atanmamış ise varsayılan olarak 0 değeri alır. *** MINDIFF parametresi herhangi bir değere atanmamış ise varsayılan olarak 3 değeri alır. **** MINNONALPHA parametresi ile aynı anda kullanılamaz. ***** MINNONALPHA parametresi belirtilmediği durumlarda, varsayılan değer olarak atanan 1 değeri etkindir. Ek olarak, MINDIGIT veya MINSPECIAL parametresi ile beraber kullanılamaz. ****** MINNONALPHA parametresi herhangi bir değere atanmamış ise varsayılan olarak 1 değeri alır. Linux sistem üzerinde RedHat için /etc/pam.d/system-auth dosyası içeriği temin edilir. Temin edilen dosya içeriğinde;			

	• Parola uzunluğu değerinin saklandığı `minlen` parametresinin, • Kullanıcının eski ve yeni parolası arasındaki olması gereken minimum karakter farkı sayısının atandığı `difok` parametresinin, • Parola içerinde bulunması gereken en az rakam sayısını gösteren `dcredit` parametresinin, • Parola içerisinde bulunması gereken en az küçük harf sayısını belirten `lcredit` parametresinin, • Parola içerisinde bulunması gereken en az büyük harf sayısı `ucredit` parametresinin, • Parola içerisinde bulunması gereken en az özel karakter (%, !, +, vb.) sayısını belirten `ocredit` parametresinin,			

K4 - Kullanıcı Oturum Açma Girişimlerinin Gözden Geçirilmesi

Bilgi sistemleri üzerindeki güvenlik önlemleri, yetkisiz erişimleri önleyecek şekilde minimum standartları karşılamalıdır.

Unix/Linux sistemlerde herhangi bir kullanıcı oturumu açık iken; farklı bir kullanıcı hesabı ile oturum açmak için "su" (switch user-kullanıcı değiştir) komutu kullanılır. Kullanıcı geçişlerini gösteren denetim izleri "sulog" dosyasında; tarih, kullanıcı adı ve kullanıcı geçiş girişim sonuçlarının detaylarını içerecek şekilde kayıt altına alınır.

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K4.T1	Solaris işletim sistemlerinde /etc/default/su dosyası içerisindeki SULOG parametresinin /var/adm/sulog değerine atandığı (SULOG = var/adm/sulog) incelenir.* Linux işletim sistemlerinde ise kullanıcı oturum açma kayıtları /var/log/secure dosyası incelenerek gözlemlenebilir. Solaris işletim sistemlerinde cat /var/adm/sulog komutu ile sulog dosyası temin edilerek "su" (switch user) komutu ile hesaplar arası gerçekleştirilen oturum geçişlerinin, kullanıcıların yetki seviyelerine uygun olarak yapıldığı kontrol edilir. * Bu parametre, başında *"#"* imleci olmadığı sürece etkindir. Parametrenin başında *"#"* imleci mevcut ise, "su" komutu ile yapılan kullanıcı oturum	İ	O	3

	değişikliklerinin denetim izleri kayıt altına alınmaz. Bu parametre etkin değil ise, diğer test adımları da geçerliliğini kaybedebilir.			
K4.T2	Aşağıdaki örnek kayıtta görüldüğü gibi, `sulog` dosyası içerisinde kayıt altına alınan kullanıcı oturumu geçişleri incelenir: `SU 02/03 11:40 + pts/10 guestuser-root` Bu örnekte `guestuser` kullanıcısı `pts/10` terminalinden "`su`" komutunu kullanarak 02/03 tarihinde saat 11:40'ta sistem üzerinde root hesabına başarılı bir şekilde (+) geçiş yaptığı görülmektedir.	İ	O	3
K4.T3	Denetim dönemine ait kayıtlar içerisinde *"*`root`*"* gibi yüksek yetkili hesaplara şüpheli ya da yetkisiz geçişlerin varlığı kontrol edilir.	İ	O	3
K4.T4	Solaris işletim sistemi üzerinde aşağıdaki komutlar çalıştırılarak sistem üzerindeki denetim olaylarına ilişkin konfigürasyonların tutulduğu dosyalara sadece "root" kullanıcısının erişebildiği teyit edilir: 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	İ	O	3
K4.T5	Solaris işletim sistemi üzerinde aşağıdaki komut çalıştırılarak "loginlog" dosyasını içeriği temin edilir: cat /var/adm/loginlog Dosya içeriğinde sistem üzerinde oturum açma işlemine ilişkin başarısız kullanıcı girişimlerinin kaydedildiği gözlemlenir. İlgili personel ile görüşülerek bu olayların gözden geçirildiğine ilişkin kanıtlar temin edilir.	İ	O	3

6.2.2. MS Windows Server 2008 İşletim Sistemleri

Riskler	K1	K2	K3	K4
R1. Bilgi sistemleri üzerinde kritik veri, bilgi ve cihazlara yetkisiz erişimlerin ortaya çıkması	+	+	+	+
R2. Bilgi sistemleri üzerinde otomatik olarak tanımlanan varsayılan kullanıcılar kullanılarak diğer kullanıcıların yetkilerinin arttırılması	+		+	
R3. Güvenlik ve parola 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 arttırma işlemlerinin gerçekleştirilmesi	+	+		

Kontroller

K1 - Kullanıcı Hesap Yönetimi ve Parolalar

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 parolası gibi güvenlik parametreleri de başlangıçta sabit değerlere tanımlanmıştır. Bu gibi kullanıcı hesaplarına varsayılan *(default)* kullanıcı hesapları denir.

Bilgi sistemleri üzerindeki varsayılan kullanıcı hesap parolaları 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 parola politikaları ve bu sistemler üzerinde tanımlı kullanıcı hesapları, bu kullanıcı hesaplarının sahip olduğu yetkiler ve ilgili diğer cihazlar (ör: yazıcılar) tek kaynaktan kontrol edilebilir.

Aktif Dizin'de (Active Directory) kullanıcı ve bilgisayar yapılandırmaları politikalar (policy) ile yönetilir. Politikalar, Grup Politika Yönetimi (Group Policy Management) üzerinden ilgili OU (Organizational Unit – Organizasyonel Birim)'e tanımlanarak uygulanır. Organizational Unit'lere kullanıcılar, gruplar, bilgisayarlar ve diğer OU'lar dahil olabilir. 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 OU'lara atanır. "Group Policy Management", OU yapısını direk olarak Aktif Dizin'den temin eder. Dolayısıyla Aktif Dizin'de yapılacak değişiklikler politikaların uygulanacakları alanları etkiler.

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.

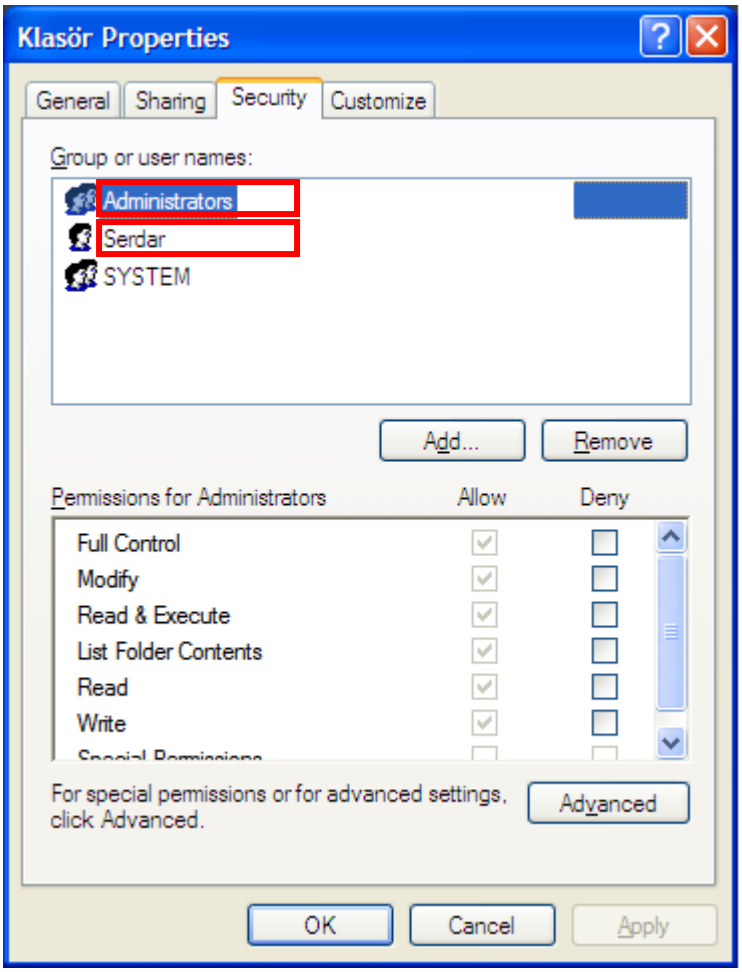
Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K1.T1	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	3
K1.T2	Kullanıcı ve grup listeleri temin edilerek içeriğindeki aktif kullanıcı hesapları tespit edilir. • Kullanıcı ikonu üzerindeki "pasif" simgesi olan aktif olmayan kullanıcı hesapları tespit edilir. • Varsayılan "Konuk" *(Guest)* hesabının erişime kapalı (pasif) olduğu gözlemlenir. • Genel isimlendirmeye sahip (ör: admin, system_user, kullanıcı1, guest vb.) kullanıcı hesapları erişimlerinin sistem üzerinde kapalı olduğu gözlemlenir.	İ	Z	3
K1.T3	Kullanıcı ve grup listeleri temin edilerek; kötü niyetli kişiler tarafından kolay tahmin edilen ve siber saldırılar sırasında saldırı aracı olarak sıkça kullanılan varsayılan "Yönetici" *(Administrator)* hesabının isminin değiştirildiği teyit edilir.	İ	Z	3
K1.T4	Varsayılan kullanıcı hesapları gözden geçirilir ve kritik yetkilerin sadece olması gereken kullanıcılara atandığı kontrol edilir. • Varsayılan hesaplar aktif halde ise ilgili hesapların varsayılan parolalarının, kurumun bilgi güvenliği politikalarına uygun olarak değiştirildiğinden emin olunmalıdır.	İ	Z	3
K1.T5	Kullanıcı gruplarına ilişkin temin edilen liste üzerinde "Yönetici" (*Administrators*), "Etki Alanı Yöneticisi (*Domain Admins*) ve Forest * Yöneticisi (*Enterprise Admins*) grubuna dahil olan kullanıcıların yetkilerinin uygunluğu teyit edilir. ***Forest:** Aktif dizin yapısında, bir organizasyon için tasarlanan en geniş mantıksal yapı.	İ	Z	3

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 / Değiştirme:** Dizin/dosya üzerinde değiştirme fonksiyonuna sahip olduğunu gösterir.
- **Write / Yazma:** Dizin/dosya üzerinde yazma fonksiyonuna sahip olduğunu gösterir.
- **Read & Execute / Okuma ve Yürütme:** Dizin/dosya üzerinde okuma ve çalıştırma fonksiyonlarına sahip olduğunu gösterir.
- **List Folder Contents / Klasör İçeriğini Listeleme:** Dizine ilişkin alt dosya ve dizin içeriklerini listeleme fonksiyonuna sahip olduğunu gösterir.
- **Full Control / Tam Denetim:** 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 da eriştiği gözlemlenebilir.

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K2.T1	Kurum bünyesinde bilgi sistemleri denetimi kapsamına alınan uygulamaların çalışması için kaynak olarak kullanılan dosya ve klasörlere (exe, dll, lib vb.) erişimlerin uygunluğu gözlemlenir: • Denetim kapsamına alınan uygulamalara ait sunucu listesi temin edilir. • Windows platformu üzerinde çalışan uygulama sunucuları içerisinden 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.T2	Windows üzerindeki sistem kayıt defteri içerisinde (Registry) hiyerarşik bir yapıda genel sistem konfigürasyon seçenekleri ve ayarları tutulur. Aşağıdaki adımlar izlenerek bu kayıt defterine ilişkin kullanıcı erişimlerinin uygunluğu teyit edilir: • [Başlat] -> [Çalıştır] -> "regedit32" (ya da "regedit") yazdıktan sonra "Giriş" (Enter) tuşuna basarak "Registry Editor" (Kayıt Defteri Düzenleyicisi) (Regedit32.exe) çalıştırılır. • HKEY_LOCAL_MACHINE sekmesinin altında -> [SYSTEM] -> [CurrentControlSet] -> [Control] -> [SecurePipeServers] -> [Winreg] anahtarına ulaşılır. • [Winreg] sekmesi üzerinde fare ile sağ tuşa tıkladıktan sonra	İ	O	

	"İzinler" (Permissions) seçeneğine tıklanır. • Bu anahtar üzerinde sadece yüksek yetkili (administrator) kullanıcıların erişimi olduğu gözlemlenir.* **İlgili anahtar üzerindeki kullanıcı yetkilerinin gözlemlenebilmesi için sunucu üzerinde yüksek yetkili (Administrator) bir kullanıcı hesabı ile testin gerçekleştirilmesi gerekmektedir.*			
K2.T3	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 (Hesap İşletmenleri), Administrators (Yöneticiler), Enterprise Admins, Schema Admins ve Domain Admins gibi kritik gruplara ait olan kullanıcılar gözlemlenir. 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.	İ	Z	

K3 - Parola ve Güvenlik Parametreleri

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

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

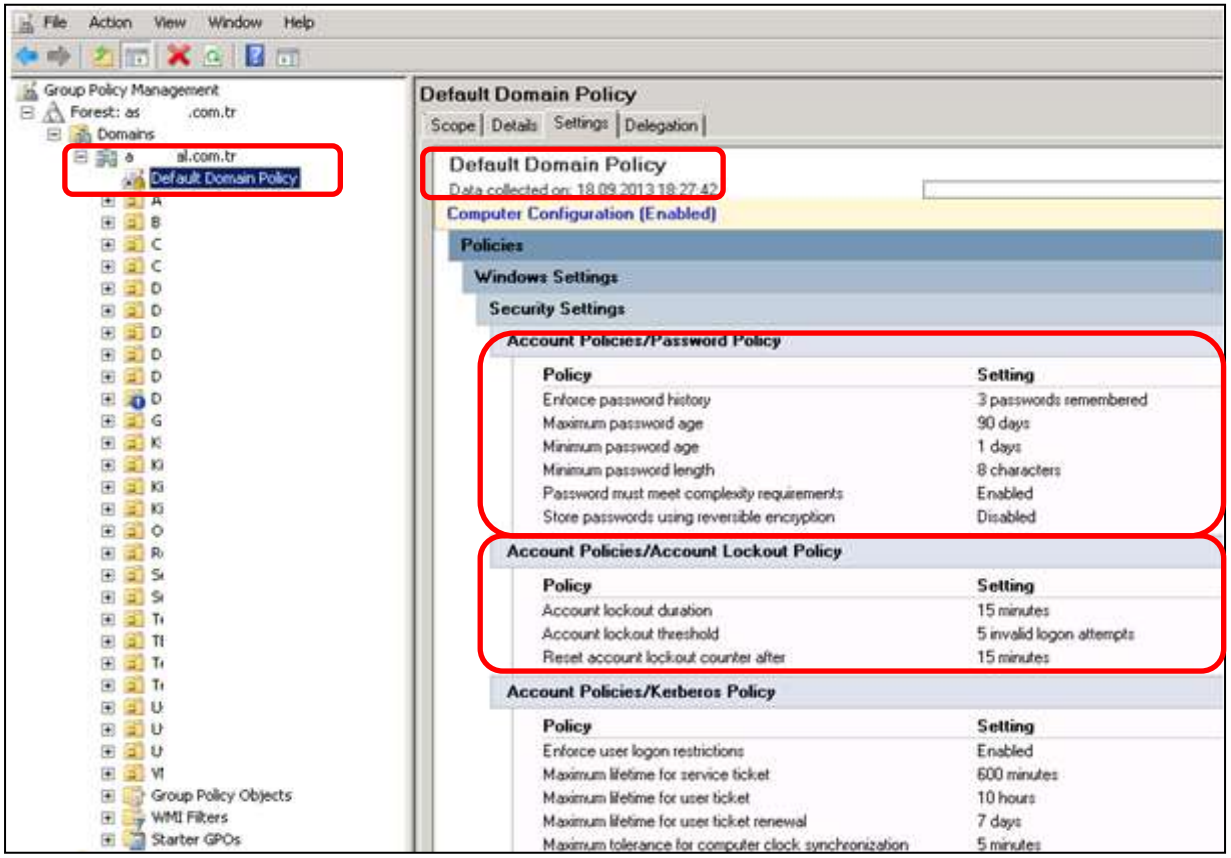
Sistem dili **İngilizce** olan sistemlerde Hesap Kilitleme İlkesi (Account Lockout Policy);

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

Türkçe sistemler için;
[Başlat] -> [Programlar] -> [Yönetim Araçları] -> [Grup İlkesi 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 parola politikasına ilişkin aşağıdaki parametreler tanımlanabilir. Parantez içindeki ifadeler parametrelerin Türkçe Windows İşletim Sistemleri'nde belirtilen halini göstermektedir.

Parametre	Tanım
Enforce password history (Parola geçmişini uygula)	Yeni parola tanımlanırken, tanımlanan sayı kadar geriye dönük parola sayısını tutar ve değiştirilen parolanın bu parolalardan farklı olması beklenir.
Maximum password age (En uzun parola geçerlilik süresi)	parolanın azami kullanma süresini gün bazında belirtir.
Minimum password age (En kısa parola geçerlilik süresi)	parolanın en az kaç gün kullanılması gerektiğini belirler.
Minimum password length (En kısa parola uzunluğu)	İzin verilen en kısa parola uzunluğunu belirtir.
Password must meet complexity requirements (Parolalar karmaşıklık gereklerine uymalıdır)	Parola içerisinde rakam, küçük harf, büyük harf ve özel karakterlerin (+, %, ! vb.) kullanılmasını zorunlu kılar.
Store passwords using reversible encryption (Parolaları geri döndürülebilir şifreleme kullanarak saklama)	Bu parametre kullanıcı parolalarının geri döndürülebilir şekilde kriptolanmasını (encrypted) belirler. Kullanıcı güvenliğini riske atmamak için etkinleştirilmemelidir.

Benzer şekilde hesap kilitleme politikasına ilişkin aşağıdaki parametreler atanabilir:

Parametre	Tanım
Account lockout duration (Hesap kilitleme süresi)	Sisteme azami başarısız giriş denemesi sonrası kilitlenen kullanıcı hesaplarının ne kadar süre kilitli kalacağını belirler.
Account lockout threshold (Hesap kilitleme eşik değeri)	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 (Hesap kilitleme sayacını sıfırlama süresi)	Sistem üzerindeki bir kullanıcı hesabına ilişkin tutulan yanlış giriş deneme sayısının ne kadar süre sonra sıfırlanacağını belirler.

Windows tabanlı sistemlerde, yukarıda da görüldüğü gibi boşta kalan oturumların yönetilmesine ilişkin aşağıdaki parametreler tanımlanabilir:

Parametre	Tanım
Define this policy setting in the template (Bu ilke ayarını şablonda tanımla)	Bu yapılandırmanın kullanılıp kullanılmayacağının tanımlamak için kullanılır.
Minutes (Dakika)	Sistemin hareketsiz kaldığı durumlarda dakika cinsinden oturumu ne kadar süre sonra boşta (idle) olarak tanımlayacağını belirtir.

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K3.T1	Sistem üzerinde parola ilkeleri (Password Policy) içeriği temin edilir. Parola politikaları üzerinde tanımlanan parametrelerin kurum bilgi güvenliği politikalarına uygun olarak, aşağıdaki önerilen değerler (Ö.D.) doğrultusunda atandığı gözlemlenir: • *Enforce password history*: Ö.D. >= 3-5 • *Maximum password age*: Ö.D. = 60-90 gün • *Minimum password age*: Ö.D. > 1 gün * • *Minimum password length*: Ö.D. >= 8 karakter • *Password must meet complexity requirements*: Ö.D. = "Aktif" (Enabled) • *Store passwords using reversible encryption*: Ö.D. = "Pasif" (Disabled) • Bu yapılandırma çok az tutulduğu taktirde kullanıcıların gün içinde bir çok defa olarak parola değiştirip eski parolalarını yeniden kullanma ihtimal vermektedir. ** Bu değerin "0"değerine atanması; kullanıcıların, parolalarını gün içerisinde birçok defa değiştirip, eski parolalarını yeniden kullanmalarına imkan verebilir. Bir başka deyişle; bu değerin "0" olarak atanması, parola tarihçesinin tutulduğu "Enforce password history" parametresini dolaylı olarak pasif hale gelmesine neden olur.*	İ	Z	3
K3.T2	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: • *Account lockout duration*: Ö.D. >= 30 dakika • *Account lockout threshold*: Ö.D. = 3-5 • *Reset account lockout counter after*: Ö.D. > 30 dakika* ** Bu değer "0" olarak atandığında süresiz olarak kilitlenir ve ancak kullanıcı hesap yöneticileri tarafından tekrar aktif hale getirilebilir. Ancak bu değerin "0" olarak atanması bilgi sistemleri personeli üzerinde ek iş yükü doğuracağından operasyonel açıdan verimli değildir.*	İ	Z	3
K3.T3	Sistem üzerinde yaratılan yeni kullanıcı hesaplarına ilişkin parolaların, ilk oturum açıldığında sistem tarafından otomatik olarak değiştirilmeye zorlandığı gözlemlenir. Bu değer kullanıcı ya da grup bazında atanabilir. • İlgili sunucu üzerinde örnek bir kullanıcı hesabı yaratılarak ilk kez oturum açılır. Kullanıcı adı ve parola girildikten sonra; sistemin, kullanıcıyı yeni parola oluşturmaya zorladığı teyit	İ	Z	3

	edilir.			
K3.T4	Sistem üzerinde boşta kalan oturum zaman aşımı (IDLE Session Timeout) içeriği temin edilir. Politika üzerinde tanımlanan parametrelerin kurum bilgi güvenliği politikalarına uygun olarak, aşağıdaki önerilen değerler (Ö.D.) doğrultusunda atandığı gözlemlenir: • *Define this policy setting in the template* için Ö.D. = kutu seçili; • *Minutes* için Ö.D. = 15;	İ	O	3

K4 - Sistem ve Kullanıcı İşlemlerinin Gözden Geçirilmesi

Bilgi sistemleri üzerinde ilgili sistemler ve kullanıcılar tarafından gerçekleştirilen işlemlerin kayıt altına alınması amacıyla ilgili parametreler aktif olarak yapılandırılmıştır.

Aktif Dizin altyapısına sahip olan kurumların bilgi sistemleri altyapısına ilişkin Denetleme Politikası (Audit Policy) kontrol paneli üzerinden yönetilebilir.

Sistem dili **İngilizce** olan sistemlerde Denetleme Politikası (Audit Policy);

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

Türkçe sistemler için;

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

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

Parametre	Tanım
Audit Account Logon Events (Hesap oturumu açma olaylarını denetleme)	Hesap oturumu açma olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit Account Management (Hesap yönetimini denetleme)	Hesap yönetim olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit Process Tracking (İşlem izlemeyi denetleme)	İşlem takibi olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit System Events (Sistem olaylarını denetle)	Sistem olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit Privilege Use (Ayrıcalık kullanımını denetleme)	Ayrıcalık kullanımı olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit Policy Change (İlke değişikliğini denetleme)	İlke (politika) değişikliği olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit Object Access (Nesne	Obje erişimi olaylarının hangi durumlarda kayıt altına

erişimini denetleme)	alınacağını belirlemek için kullanılır.
Audit Logon Events (Oturum açma olaylarını denetleme)	Oturum açma olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.
Audit Directory Service Access (Dizin hizmet erişimini denetleme)	Dizin erişim servisi olaylarının hangi durumlarda kayıt altına alınacağını belirlemek için kullanılır.

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K4.T1	Sistem üzerinde gerçekleşen olayların kayıt altına alma politikası, Denetleme Politikası (Audit Policy) içeriği temin edilir. Politika üzerinde tanımlanan parametrelerin kurum bilgi güvenliği politikalarına uygun olarak, aşağıdaki önerilen değerler (Ö.D.) doğrultusunda atandığı gözlemlenir: • *Audit Account Logon Events* için Ö.D. = Success and Failure (Başarı ve Hata); • *Audit Account Management* için Ö.D. = Success and Failure (Başarı ve Hata) • *Audit Directory Service Access* için Ö.D. = Failure (Hata); • *Audit Logon Events* için Ö.D. = Success and Failure (Başarı ve Hata); • *Audit Object Access* için Ö.D. = Failure (Hata); • *Audit Policy Change* için Ö.D. = Success and Failure (Başarı ve Hata); • *Audit Privilege Use* için Ö.D. = Failure (Hata); • *Audit Process Tracking* için Ö.D. = None (Hiçbiri); • *Audit System Events* için Ö.D. = Failure (Hata).	İ	O	3
K4.T2	Söz konusu parametreler ışığında, ilgili sistemler üzerinde sistem ve kullanıcı işlemlerinin denetim izlerinin (log) ne şekilde ve nasıl saklandığı öğrenilir ve ilgili personel tarafından düzenli olarak gözden geçirildiğine ilişkin kanıtlar temin edilerek incelenir.	İ	O	3

6.3. Veritabanı Sistemleri

6.3.1. MS SQL Server 2008 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 arttırılması	+		+
R3. Güvenlik ve parola 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 arttırma işlemlerinin gerçekleştirilmesi	+	+	

Kontroller

K1 - Varsayılan Kullanıcı Hesapları ve Parolalar

MS SQL veritabanının fiziksel bileşenleri, MS SQL yazılımından ve işletim sistemleri kontrolleri tarafından korunan sunucu üzerindeki çeşitli veritabanlarına ait 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.

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K1.T1	Veritabanı sisteminin üzerinde çalıştığı işletim sistemi güvenlik ayarlarının MS SQL veritabanı dosyalarına erişimi kısıtlayacak şekilde yapılandırıldığı değerlendirilir: • 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 testi için lütfen ***6.1.2 MS Windows İşletim Sistemleri – K2. Kritik Dosyalara Erişim*** bölümüne bakınız.	İ	Z	3

K1.T2	Veritabanı üzerinde "*select * from sys.syslogins*" komutu çalıştırılarak kullanıcı ve grup listeleri temin edilir. Tablo içeriğindeki aktif kullanıcı hesapları tespit edilir: • Windows Authentication (Windows kimlik doğrulama) yöntemi kullanılıyor olsa dahi "*sa*" hesabına karmaşık bir parolanın atandığı doğrulanır. • Parola alanı boş olsa dahi, MS SQL Server veritabanı sistemlerindeki tüm parolalar karmaşık şekilde (kriptolu) halde görünür. *"sa"* hesabını da içeren tüm ayrıcalıklı hesaplara parola 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	3
K1.T3	*Windows Sunucu/Domain üzerindeki "BUILTIN\Administrators"* grubuna ait sistem girişlerinin kaldırıldığı ve bu girişin veritabanı yöneticileri için özel olarak yaratılmış bir Windows grubu ile değiştirildiği teyit edilir: • *SQL Server Management Studio* başlatılır. • *Microsoft SQL Server -> Güvenlik (Security) -> Logins* sekmesine tıklanır. • *"BUILTIN\Administrators"* girişinin özel olarak yaratılmış farklı bir *Windows* 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	3
K1.T4	Varsayılan kullanıcı hesapları gözden geçirilir ve kritik yetkilerin sadece olması gereken kullanıcılara atandığı kontrol edilir: • Varsayılan hesaplar aktif halde ise ilgili hesapların varsayılan parolalarının, kurumun bilgi güvenliği politikalarına uygun olarak değiştirildiğinden emin olunmalıdır.	İ	Z	3
K1.T5	Kullanıcı gruplarına ilişkin temin edilen liste üzerinde yüksek yetkili yönetici gruplarına dahil olan kullanıcıların yetkilerinin uygunluğu teyit edilir.	İ	Z	3

K2 - Kritik Dosyalara Erişim

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K2.T1	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) • Ayrıcalıklı haklara sahip olan kullanıcı listesi gözden geçirilir ve kullanıcı sayısının uygunluğu 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: ○ *sp_helprolemember 'db_securityadmin'* ○ *sp_helprolemember 'db_owner'* ○ *sp_helprolemember 'db_accessadmin'* ○ *sp_helpsrvrolemember 'sysadmin'* ○ *sp_helpsrvrolemember 'serveradmin'* ○ *sp_helpsrvrolemember 'securityadmin'* • Atanan ayrıcalıklı erişim haklarının uygunluğu gözden geçirilir ve ayrıcalıklı erişim haklarının sadece iş tanımları ile uyumlu kişilere verildiği teyit edilir.	İ	Z	3

K3 - Parola ve Güvenlik Parametreleri

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K3.T1	Sistem üzerinde parola politikaları (*Password Policy*) içeriği temin edilir. Parola politikaları üzerinde tanımlanan parola uzunluğu, hesap kitleme süresi, parola karmaşıklığı, parola ömrü gibi parametrelerin kurum bilgi güvenliği politikalarına uygun olarak atandığı gözlemlenir: • *SQL Server Management Studio* başlatılır. • Uygun sunucu objesine sağ tıklanır. • [*Properties*] seçeneğine tıklanır. • [*Security*] sekmesine tıklanır. • [*Server Autehntication (Sunucu Doğrulama)*] seçeneğinin altında [*Windows Authentication mode*] seçeneğinin işaretli olduğu teyit edilir: ○ Eğer [*Windows Authentication mode*]* seçeneğini aktif ise, Windows seviyesinde hesap kilitleme politikası gözden geçirilir. ***(bkz: 6.1.2 MS Windows İşletim Sistemleri – K3. Güvenlik ve Parola Parametreleri)*** • SQL Server veritabanı üzerinde *select * from sys.sql_logins* komutu çalıştırılır. • [is_policy_checked] =1 durumu doğrulanıyor ise Windows hesap kilitleme ayarları SQL hesapları için geçerlidir. **[Windows Authentication mode] seçeneği işaretli ise ve SQL Server veritabanı sistemi MS Windows Server işletim sistemi üzerinde çalışıyorsa, SQL kullanıcı hesapları üzerinde Windows parola politikası uygulanabilir.*	İ	Z	3
K3.T2	Microsoft SQL Server Analiz Servisleri (*SSAS – Analyses Services)* 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: • SQL Server Management Studio açılır. • Veritabanı motoruna analiz sunucusuna (*Analysis Server*) bir bağlantı açıldığına emin olunur. • *Object Explorer* bölümünde bağlantı kurulan sunucuya sağ tıklanır. • Menüde *Properties* sekmesine tıklanır.	İ	Z	3

	• Varsayılan olarak *General (Genel)* sayfasının seçildiğinden emin olunur. • *Show Advanced (All) Properties* kutusu işaretlenir. • *IdleConnectionTimeout (Aktif Olmayan Oturumların Zaman Aşımına Uğraması)* parametresi gözlemlenir: ○ 32-bit uzunluğunda işaretli (*signed*) sayı değeri, pasif bağlantıların zaman aşımına uğrama süresinin saniye cinsinden değeridir. Bu özellik için varsayılan değer, tüm aktif olmayan bağlantıların zaman aşımına uğramayacağını ifade eden *sıfır (0)* değeridir.			

K3.T3	SQL Server Management Studio çalıştırılarak denetleme ayarlarının üzerinde başarısız oturum açma girişimlerinin kaydedildiği teyit edilir:
	• Uygun sunucu objesine sağ tıklanır.
	• [*Properties*] seçeneğine tıklanır.
	• [*Security*] sekmesine tıklanır.
	• [*Login Auditing*] alanında [*Both failed and successful logins*] (Başarılı ve başarısız oturum açma girişimleri) seçeneğinin işaretli olduğu teyit edilir.
	• Oturum açma girişimleri denetleniyor ise, aşağıdaki özellikleri değerlendirmek için sistem yöneticisinden konular ile ilgili bilgi alınır:
	  ○ Başarısız oturum açma girişimlerinin denetlenme sıklığı
	  ○ Şüpheli oturum açma girişimlerine ve gerçekten yanlış oturum açma denemelerine yer veren prosedürlerin varlığı
	  ○ Başarısız oturum açma girişim raporlarının 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	3

6.3.2. 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 arttırılması	+		+
R3. Güvenlik ve parola 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 arttırma işlemlerinin gerçekleştirilmesi	+	+	

K1 - Kullanıcı Hesap Yönetimi ve Parolalar

Denetim Testleri

<table>
<tr><th>#</th><th>Denetim testleri</th><th>T/İ</th><th>Z/O</th><th>YS</th></tr>
<tr><td>K1.T1</td><td>Varsayılan kullanıcı hesapları için varsayılan parolaların değiştirildiği teyit edilir:
“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_users_with_defpwd.html
SQL> SELECT * FROM DBA_USERS_WITH_DEFPWD;
SQL> SET MARKUP HTML OFF
SQL> SET ECHO ON
SQL> SPOOL OFF
Oluşturulan 'dba_users_with_defpwd.html' dosyası temin edilir.
'dba_users_with_defpwd.html' dosyası incelenerek aşağıdaki varsayılan kullanıcı hesapları için varsayılan parolaların değiştirildiği teyit edilir:
Varsayılan Oracle veritabanı kullanıcıları<table><tr><td>SYS</td></tr><tr><td>SYSTEM</td></tr><tr><td>OUTLN</td></tr><tr><td>SCOTT
ADAMS
JONES
CLARK
BLAKE</td></tr><tr><td>HR (Human Resources)
OE (Order Entry)
SH (Sales History)</td></tr><tr><td>DEMO</td></tr><tr><td>ANONYMOUS</td></tr></table></td><td>İ</td><td>Z</td><td>3</td></tr>
</table>

	AURORAORBUNAUTHENTICATED AWR_STAGE CSMIG CTXSYS DBSNMP DIP DMSYS DSSYS EXFSYS LBACSYS MDSYS ORACLE_OCM ORDPLUGINS ORDSYS PERFSTAT TRACESVR TSMSYS XDB			
K1.T2	Oracle veritabanı sistemlerinde denetim sürecinde oluşturulmuş hesapların listesi temin edilir. ***"DBA_USERS"*** tablosundaki ***"CREATED"*** sütunu incelenerek kullanıcı hesaplarının oluşturulma tarihleri belirlenir. • "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_users.html SQL> SELECT * FROM DBA_USERS; SQL> SET MARKUP HTML OFF SQL> SET ECHO ON SQL> SPOOL OFF • 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 görev tanımına uygun olduğu teyit edilir.* **Denetim surecinde, "DBA_USERS" tablosundaki "Account Status" alanında "EXPIRED" (zamanı geçmiş) veya "LOCKED" (kilitlenmiş) değeri bulunan hesaplar belirlenip, denetim sürecindeki testlerden muaf tutulabilirler.*	İ	Z	3

K2 - Kritik Dosyalara Erişim

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K2.T1	İşletim sisteminin belirtilen dosyalar gibi Oracle veritabanı dosyalarına da erişimi kısıtlayacak şekilde yapılandırıldığını onaylanır. • İşletim sistemi güvenliği incelenirken, aşağıdaki dosyalara erişimi olan kullanıcı ve gruplar hakkında güvenlik ve erişim bilgileri temin edilir. Eğer güncelleme (okuma-yazma) yetkisi olan kullanıcı hesaplarına ilişkin genel isimlendirmeye tabi hesaplar mevcut ise, bu tür hesapların erişimlerinin sadece gerekli kullanıcılarda bulunduğunun teyidi için ne tür kontrollerin mevcut olduğu tespit edilir: o **Araçlar ve İkili Kodlar (Binaries):** Veritabanına destek olan dosya ve araçlardır. o **Tablo alanı (tablespace) veri dosyaları:** Oracle veritabanı sistemleri çeşitli tablo içeriklerini (örn. tablolar, paketler, prosedürler vb.) tablo alanlarında (tablespace) tutar. Bunlar çoğunlukla ".dbf" uzantılı dosyalardır ve $ORACLE_BASE/oradata/<sid>/ klasöründe tutulur. o **Başlangıç dosyası:** Başlangıç parametrelerinin saklandığı dosyadır. Bu dosya, Oracle veritabanı çalıştırıldığında, varsayılan başlangıç parametrelerini yapılandırmak için kullanılır. ***INIT.ORA*** dosyası olarak belirtilir; genellikle ***INIT<veritabanı ismi>.ORA*** olarak isimlendirilir. Bu dosya üzerindeki parametrelere ilişkin yapılan değişikler, veritabanı yeniden başlatılıncaya kadar veritabanına etki etmez. o **Kontrol dosyaları:** Bu dosyalar veritabanının fiziksel yapısına ilişkin durumun değişiminin takibi için kullanılır. Veritabanı başlangıcı esnasında ve veritabanı kurtarımında kullanılır. Kontrol dosyalarının sayıları ve bulundukları konumlar, Oracle başlangıcı sırasında çalıştırılan ***"INIT.ORA"*** dosyası içerisinde ***"CONTROL_FILES"*** parametresinde listelenir. o **Yapılandırma dosyası:** ***"CONFIG.ORA"*** dosyası ***"INIT.ORA"*** dosyasında bulunmayan ek yapılandırma ayarlarını içerir. Bu dosyanın varlığı isteğe bağlı olduğundan tüm Oracle kurulumlarında bulunmayabilir.	İ	Z	3

	"CONFIG.ORA" dosyası sistem güvenliği ve yapılandırması hakkında önemli bilgiler içermektedir. ○ **Veritabanı dinleyici dosyası*:*** Veritabanına erişim sağlamak için, veritabanı dinleyicisinin parolasının tutulduğu dosyadır. ○ ***orapwd<veritabanı ismi>* dosyası**: Bu dosya yüksek yetkili ***SYS, SYSDBA*** veya ***SYSOPER*** rollerine sahip kullanıcıların parolalarının kriptolanmış ***(hashed)*** halini tutar.			
K2.T2	Veritabanı üzerindeki ***PUBLIC*** rolüne atanmış olan yetkilerin uygunluğu teyit edilir. Varsayılan olarak, tüm kullanıcı hesaplarının ***PUBLIC*** rolüne erişimi vardır ve ***PUBLIC*** rolüne ilişkin tanımlanan güvenlik hakları tüm kullanıcılara uyarlanır. Hassas roller, nesneler ve sistem yetkileri PUBLIC rolüne atanmamış olmalıdır: • "DBA_SYS_PRIVS" tablosu temin edilir: ○ "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	İ	Z	3

	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 o Oluşturulan 'dba_sys_privs_privs.html' dosyası temin edilir. o 'dba_sys_privs_privs.html' dosyası incelenerek, PUBLIC rolüne atanmış olan sistem yetkilerinin uygunluğu teyit edilir. "DBA_TAB_PRIVS" tablosu temin edilir: o "sqlplus" aracı "system" hesabı ile çalıştırılır. o Aşağıdaki komutlar SQL penceresine girilir*: 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'); SQL> SET MARKUP HTML OFF SQL> SET ECHO ON SQL> SPOOL OFF o Oluşturulan 'dba_tab_privs_IUADE.html' dosyası temin edilir. o 'dba_tab_privs_IUADE.html' dosyası incelenerek, PUBLIC rolüne atanmış olan nesne yetkilerinin uygunluğu teyit edilir. **Sorguda geçen <TABLO_ADI> kısmına, kurum için mali önem taşıyan tablo ismi yazılmalıdır. Mali olarak önem taşıyan tabloları kurum yetkilileri ile görüşerek belirleyebilirsiniz.* • "DBA_ROLE_PRIVS" tablosu temin edilir: o "sqlplus" aracı "system" hesabı ile çalıştırılır. o Aşağıdaki komutlar SQL penceresine girilir*: 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 o Oluşturulan 'dba_role_privs.html' dosyası temin edilir. o 'dba_role_privs.html' dosyası incelenerek, PUBLIC rolüne atanmış olan rollerin yetkilerinin uygunluğu teyit edilir.			

K3 - Parola ve Güvenlik Parametreleri

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K3.T1	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 prosedürlerin çoğu zaman değiştirilerek merkezi güvenlik modeline uyum sağlamaları gerekir. • "DBA_USERS" tablosu temin edilir: o "sqlplus" aracı "system" hesabı ile çalıştırılır. o Aşağıdaki komutlar SQL penceresine girilir: 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 o Oluşturulan 'dba_users.html' dosyası temin edilir. o 'dba_users.html' dokümanı incelenir ve kullanıcılardan "PASSWORD" değişkeni 'GLOBAL' değeri almış olanları tespit edilir. Bu yapılandırma global kimlik doğrulama mekanizmasının (*Global Authentication and Authorization)* kullanıldığını gösterir. • 'GLOBAL' değerinin mevcut olduğu tespit edilen durumlarda, kurum çalışanları ile görüşülerek, kimlik tespiti yapılan mekanizmanın detaylarına ulaşılır.	İ	Z	3
K3.T2	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.	İ	O	3

	• "DBA_USERS" tablosu temin edilir: o "sqlplus" aracı "system" hesabı ile çalıştırılır. o Aşağıdaki komutlar SQL penceresine girilir: 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 o Oluşturulan 'dba_users.html' dosyası temin edilir. • ' dba_users.html ' dosyasını incelenir ve "DBA_USERS" tablosundaki kullanıcıların herhangi birinin "PASSWORD" alanına karşılık gelen değerin "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$PARAMETER2) bir kopyasını temin etmek için aşağıdaki komut çalıştırılır: SELECT * FROM V$PARAMETER2 WHERE NAME in ('remote_os_authent','os_authent_prefix'); • *V$PARAMETER2* tablosunun çıktısı aşağıdaki adımları uygulayarak alınır: o "sqlplus" aracı "system" hesabı ile çalıştırılır. o Aşağıdaki komutlar SQL penceresine girilir: SQL> SET ECHO OFF SQL> SET MARKUP HTML ON SPOOL ON SQL> SPOOL v_parameter2_external.html SQL> SELECT * FROM V$PARAMETER2 WHERE NAME in ('remote_os_authent','os_authent_prefix'); SQL> SET MARKUP HTML OFF SQL> SET ECHO ON SQL> SPOOL OFF o 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 değerin "EXTERNAL" olarak 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.T3	Veritabanı sistemi üzerinde tanımlı parola parametre değerleri temin edilir. Parola parametreleri üzerinde tanımlanan değerlerin kurum bilgi güvenliği politikalarına uygun olarak atandığı gözlemlenir: • "DBA_USERS" tablosu temin edilir: o "sqlplus" aracı "system" hesabı ile çalıştırılır. o Aşağıdaki komutlar SQL penceresine girilir: 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 o Oluşturulan 'dba_users.html' dosyası temin edilir. • "DBA_USERS" tablosu temin edilir: o "sqlplus" aracı "system" hesabı ile çalıştırılır.	İ	Z	3

	○ Aşağıdaki komutlar SQL penceresine girilir: 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 ○ Oluşturulan 'dba_profiles.html' dosyası temin edilir. • "DBA_SOURCE" tablosu temin edilir: ○ "sqlplus" aracı "system" hesabı ile çalıştırılır. ○ Aşağıdaki komutlar SQL penceresine girilir: 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 ○ Oluşturulan 'password_verify_function.html' dosyası temin edilir. • Her bir kullanıcı hesabı için belirtilen parametrelerin uygunluğu denetlenir: ○ Oracle veritabanında parola yapılandırmaları profillere atanmıştır. Parola yapılandırmalarına ilişkin parametreler "DBA_PROFILES" tablosu içinde tanımlanmıştır. Her kullanıcı bir profil ile bağdaştırılmıştır. Her parola yapılandırması için: - Her bir profil için güvenlik ve parola parametrelerine ilişkin yapılandırmaların uygunluğu teyit edilir. - Kullanıcı hesaplarının uygun profillere atandıkları ve bu profillerdeki güvenlik ve parola yapılandırmalarının ilgili kullanıcıya uygun olup olmadığı gözlemlenir.			

	• **Kabul edilen en kısa parola uzunluğu** Oracle veritabanı belirli parola yapılandırmalarını kontrol etmek için parola onaylama fonksiyonu (PASSWORD VERIFY FUNCTION) atanır. Kabul edilen en kısa parola uzunluğu da bunlara dâhildir. "DBA_PROFILES" tablosu içinde, "PASSWORD_VERIFY_FUNCTION" parametresinde dosya veya dosyaların tanımlandığı teyit edilir. Parametrede dosya tanımlı ise ilgili dosyaları temin ederek, dosya içeriğinde aşağıda belirtilen kodun varlığı teyit edilir (en kısa parola uzunluğu için tavsiye edilen değer 6-8 veya daha büyük bir değerdir): *IF length(password) < 6 THEN raise_application_error(-20002, 'Password length less than 6')* "DBA_USERS" tablosundaki her kullanıcının, parola onaylama fonksiyonu uygun yapılandırılmış bir profile atandığı teyit edilir. • **İlk oturum açılışı için tek kullanımlık parola** Oracle veritabanlarında "PASSWORD_VERIFY_FUNCTION" içerisinde ilk oturum açılışından sonra kullanıcıların parolalarını değiştirmeleri için bir yapılandırma sunulmaktadır. Kullanıcı hesabı açılırken aşağıdaki SQL komutu çalıştırılırsa, kullanıcıların parolalarını değiştirmeleri zorunlu kılınır: *ALTER USER <kullanıcı_adı> PASSWORD EXPIRE* Hesap açılış sürecini incelerken yukarıdaki kodun kullanıldığı teyit edilir. ** Buradaki <kullanıcı_adı> parametresinin yerine kullanıcı hesabının varlığı gözlemlenmelidir.* • **Parola karmaşıklığı** Oracle veritabanlarında "PASSWORD_VERIFY_FUNCTION" içerisinde aşağıdaki parametreler için gerekli yapılandırmalar tanımlanabilir: o Kullanıcı adı ile parolanın aynı olmaması o Kullanıcı parolasının, basit kelimelerin bulunduğu bir listesi ile karşılaştırılarak, "çok basit" olmamasının sağlanması			

	○ En az bir harf, bir rakam ve bir karakter içermesi ○ parolanın, en son kullanılan son üç (ya da en az üç) paroladan farklı olması Yukarıda listelenen maddeler, parola onaylama fonksiyonu içerisinde özelleştirilerek ilave parola kontrolleri eklenebilir.			
K3.T4	Daha önceki denetim testlerinde temin edilen 'dba_profiles.html' dosyası içeriğindeki aşağıdaki parametrelerin her kullanıcı hesabına karşılık gelecek profiller için tanımlandığı teyit edilir; • **Zorunlu parola değiştirme sıklığı (parola ömrü)** "PASSWORD_LIFE_TIME" değerinin belirlendiği durumlarda, "DBA_USERS" tablosundaki her aktif kullanıcı hesabı için, ilgili kullanıcı hesabının parola ömrü yapılandırması yapılandırılmış bir profile atandığı teyit edilir. (Önerilen değer: 90 gün ya da daha az) • **Hesap kilitlenmeden önce izin verilen yanlış oturum açma denemesi sayısı** "DBA_PROFILES" tablosu içerisinde, "FAILED_LOGIN_ARREMPTS" değerinin 3 ile 5 arasında olduğu teyit edilir. Bu değer kullanıcı hesabı kilitlenmeden önce yapılabilecek yanlış oturum açma deneme sayısını gösterir. • **parolanın kilitli kalacağı süre** "DBA_PROFILES" tablosun içerisinde, "PASSWORD_LOCK_TIME" değerinin en az 1 gün olduğu teyit edilir. Bu değer "FAILED_LOGIN_ATTEMPTS" (izin verilen en fazla yanlış oturum açma denemesi sayısı) değerine ulaşıldıktan sonra hesabın yöneticiler tarafında bir müdahale olmazsa ne kadar kilitli kalacağını tanımlar. • **Aynı parola tekrar kullanılmadan önce kullanılması gereken farklı parola sayısı** "DBA_PROFILES" tablosu içerisinde, "PASSWORD_REUSE_MAX" veya "PASSWORD_REUSE_TIME" değerlerinin belirlenen kullanıcı profilleri için tanımlandığı teyit edilir. "PASSWORD_REUSE_MAX" değeri daha önceden kullanılan bir parolayı kullanmadan önce en az kaç defa farklı parolalar kullanılarak parola değişikliği yapılabileceğini belirler. Tavsiye edilen değer 4 veya daha yüksektir.	İ	Z	3

	"PASSWORD_REUSE_TIME" daha önceden kullanılan bir parolanın en az kaç gün sonra tekrar kullanılabileceğini belirtir. Tavsiye edilen değer 365 (gün) veya daha fazlasıdır. • **Boş Oturum Zaman Aşımı** "DBA_PROFILES" tablosu içerisinde belirlenen kullanıcı profilleri için "IDLE_TIME" değerinin 30 veya daha az bir değere atandığı teyit edilir.* Bu değer kullanıcı hesaplarının, oturum açık iken kaç dakika işlem yapılmaması sonrasında sonlandırılacağını belirtir. **Kurum işleyici için belirli kullanıcı hesaplar ve profiller için zaman aşımı parametresinin atanmaması beklenebilir (Örn. yazılım ara yüzleri, sistem araçları vb.)*			
K3.T5	Oracle veritabanı dinleyicisi (*Oracle database listener*) ağ üzerinden veritabanına gönderilen bağlantıları yönetir. Dinleyici, yapısal olarak veritabanı önünde konumlandırıldığından saldırıya maruz kalma riski artmaktadır. ***Oracle 11g*** versiyonu ile birlikle dinleyicinin varsayılan davranışı güvenliği arttırmak için diğer makinelerden gelen "*lsnrctl*" isteklerini reddetmektedir. Örnek olarak; - En güvenli = parola yok, varsayılan. - Daha az güvenli = parola belirtilmiş. Yerel makinede varsayılan olarak ***DBA*** grubuna ait kullanıcılar için parola kontrolü yapılmaz. • ***"LISTENER.ORA"*** dosyasının bir kopyası temin edilir ve parolaların etkin olup olmadığı ve parola girişinde şifrelenmiş bir değerin olup olmadığı belirlenir. Şifrelenmiş bir parola mevcut ise aşağıdaki gibi bir parametre gözlemlenir: PASSWORDS_LISTENER=(<şifrelenmiş değer>) • ***"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: LISTENER= (DESCRIPTION= (ADDRESS_LIST= (ADDRESS=(PROTOCOL=tcp)(HOST=sale-server)(**PORT=1521**)) (ADDRESS=(PROTOCOL=ipc)(KEY=extproc))))	İ	Z	3

K3.T6	Oracle veritabanları üzerinde denetleme (auditing) ayarları üzerinden başarısız oturum açma girişimlerinin kaydedildiği teyit edilir: • "DBA_STMT_AUDIT_OPTS" tablosu temin edilir: o "sqlplus" aracı "system" hesabı ile çalıştırılır. o Aşağıdaki komutlar SQL penceresine girilir*: 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 o 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: USER_NAME FAILURE ---------- ---------- BY ACCESS Eğer başarısız oturum açma denemeleri kayıt altına alınmakta ise, aşağıdaki maddeler belirlenir: • Oturum açma girişimleri denetleniyor ise, aşağıdaki özellikleri değerlendirmek için sistem yöneticisinden aşağıdaki konular ile ilgili bilgi alınır: o Başarısız oturum açma girişimlerinin denetlenme sıklığı o Şüpheli oturum açma girişimlerine ve gerçekten yanlış oturum açma denemelerine yer veren prosedürlerin varlığı o Başarısız oturum açma girişim raporlarının dosyalanması ve güvenli bir şekilde saklanması • Başarısız oturum açma girişimlerine ilişkin raporlanan	İ	O	3

	dokümanlar gözden geçirilir. Tekrar eden ve şüpheli başarısız oturum açma girişimleri belirlenir ve ne gibi aksiyonlar alındığı değerlendirilir.			

6.4. Ağ Sistemleri

Risk – Kontrol Eşleşmeleri

Riskler	K1	K2	K3
R1. Bilgi sistemleri ağ altyapısı içerisindeki kritik donanımlarda 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 parolalarının yetkisiz kişiler tarafından ele geçirilmesi			+

K1 - Ağ ayrıştırması (segmentasyon)

Ağ ayrıştırması; kurum içerisindeki bilgi sistemlerinin bağlı olduğu ağların organizasyon yapısı, iç ağ yapısı ya da farklı bir koşula göre her biri ayrı bir güvenlik çemberine sahip olacak şekilde birbirlerinden ayrılmasıdır.

Ağ ayrıştırmasının amacı; bilgi sistemleri ağ güvenliğini ve kullanıcı yetki kontrol seviyesini arttırmaktır. Ağ ayrıştırması ile bir ağ içerisinde meydana gelebilecek sorunların diğer ağlara sirayet etmemesinin önüne geçilebilir. Ağ ayrıştırması sayesinde bilgi sistemleri ağı içerisinde kademeli kontroller uygulanabilmektedir. Farklı güvenlik gereksinimleri ve uygun bir risk değerlendirmesi sonucu bilgi sistemleri ağı mantıksal olarak; dışarıdan serbestçe erişilebilen sistemler, iç ağlar ve kritik varlıklar gibi alanlara ayrıştırılabilir. Ağ ayrıştırmasının bulunmadığı kurumlarda, ağ yönetimi ve buna bağlı olarak olay/problem yönetimi etkin bir şekilde yapılmayabilmektedir.

Kurum içerisinde bilgi sistemleri ağ altyapısı; kurumun erişim ve ağ güvenliği politikaları ile uyumlu bir şekilde yapılandırılmalıdır. Ağ yönetim sistem ve cihazları üzerinde tanımlı kullanıcı yetkileri güncel ve kurumun yetki ve erişim kurallarına uygun olarak atanmalıdır.

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K1.T1	Kurumun bilgi sistemleri ağ altyapısı yapılandırmasına ilişkin politika ve prosedürler temin edilerek fiziksel ya da sanal ağ ayrıştırmasının varlığı gözlemlenir.	T	Z	3
K1.T2	Kurum içerisinde bir ağ ayrıştırması mevcut ise bilgi sistemleri ağı şemalarında bu durumun gösterildiği teyit edilir.	İ	Z	3
K1.T3	Kurum bilgi sistemleri ağ altyapısı üzerinde ağ ayrıştırmasına ilişkin yapılan kural ve altyapı değişikliklerinin kontrollü gerçekleştirildiği ve düzenli olarak gözden geçirildiği teyit edilir. ***(****bkz:* ***6.2.3 Ağ Sistemleri - K2. Ağ cihazları güvenliği)***	İ	Z	3
K1.T4	Bilgi sistemleri ağ altyapısı sistemleri üzerinde tanımlı kullanıcı yetkileri temin edilip, kullanıcı yetkilendirmelerinin ağ şemasına uygun biçimde yapıldığı teyit edilir. ***(****bkz:* ***4.2 Güvenlik Hizmetleri Yönetimi ve 6.3 Ağ Sistemleri - K2. Ağ cihazları güvenliği)***	İ	Z	3
K1.T5	Bilgi sistemleri ağ altyapısı sistemleri üzerindeki kullanıcı yetkilerinin düzenli aralıklarla gözden geçirildiği teyit edilir. ***(****bkz:* ***4.2 Güvenlik Hizmetleri Yönetimi ve 6.2.3 Ağ Sistemleri - K2. Ağ cihazları güvenliği)***	İ	Z	3

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 ve yönlendirici (*router*) ve anahtarların (*switch*) konumu, 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 Testleri

#	Denetim testleri	T/İ	Z/O	YS
K2.T1	Bilgi sistemleri ağı şemasının temin edilerek tüm ağ cihazlarının konumunun uygun şekilde yapılandırıldığı kontrol edilir.	T	Z	3
K2.T2	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	3
K2.T3	Ağ cihazları yönetim konsolu üzerindeki ağ adreslerini tanımlayan IP (*Internet Protocol*) ve içerik filtreleme ayarlarının ilgili güvenlik politikası ile uyumluluğu gözlemlenir.	T	Z	3
K2.T4	Güvenlik duvarı üzerinde tanımlı güvenlik parametrelerine ilişkin varsayılan değerde her zaman tüm kanalları ve servisleri reddedecek şekilde *(DENY ALL)* yapılandırılmış olduğu; istisnaların *(exception)* ise bu varsayılan değer üzerine tanımlandığı gözlemlenir.	İ	Z	3
K2.T5	Ağ cihazları yapılandırılmasının ve kural değişikliklerinin düzenli olarak gözden geçirildiği gözlemlenir.	İ	Z	3
K2.T6	Ağ cihazları yönetim konsolu üzerindeki parola politikalarının, kurumun parola standartları politikası ile uyumluluğu kontrol edilir.	İ	Z	3
K2.T7	Ağ cihazları üzerinde tanımlı kullanıcıların listesi temin edilir ve örneklemler üzerinden mevcut erişim yetkilerinin ilgili güvenlik politikalarına uygunluğu kontrol edilir.	İ	Z	3
K2.T8	Ağ cihazları üzerindeki sürüm ve yama listesi kayıtları temin edilerek denetim dönemi içerisinde gerçekleşen yapılandırma değişiklikleri ve yamalar arasından rastgele örneklem seçilir. Bu örneklemlere karşılık gelen kural değişikliği talepleri ve onay dokümanları temin edilerek kontrol sürecine uygunluğu incelenir.	İ	Z	3
K2.T9	Güvenlik Duvarı/IPS 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	3
K2.T10	Şüpheli ağ trafiği sonucu üretilen alarm raporlarının ve bildirimlerin kaydedildiği teyit edilerek düzenli aralıklarla gözden geçirildiği gözlemlenir.	İ	Z	3
K2.T11	Güvenlik duvarı/IPS üzerindeki varsayılan güvenlik ayarlarının ve tanımlı varsayılan kullanıcıların uygun şekilde değiştirildiği kontrol edilir.	İ	Z	3

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 parolası gibi bilgiler ağ üzerinde şifreli olarak iletilir.
- Bilgi sistemleri ağı üzerindeki veri trafiği, yalnızca yetkili kullanıcılar tarafından yönetilmektedir.

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K3.T1	Bilgi sistemleri ağı üzerindeki veri haberleşme kanallarının güvenliği ile ilgili politika ve prosedürlerin güncelliği ve onaylı olduğu teyit edilir.	T	Z	3
K3.T2	Bilişim sistemleri ağına dâhil olan tüm donanım ve yazılımların kurum yönetimi tarafından belirlenen BT güvenlik politikalarına uyumluluğu kontrol edilir.	T	Z	3
K3.T3	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	3
K3.T4	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	3
K3.T5	Çevrimiçi işlemler için vatandaş ya da kurum çalışanlarına ait özlük bilgileri gibi gizli veriler; mevcut mevzuatla uyumlu şekilde iletilir.	İ	O	3

K3.T6	Bilgi sistemleri üzerinden kimlik doğrulama amaçlı iletilen kullanıcı adı ve kullanıcı parolası gibi bilgilerin ağ üzerinde şifreli olarak iletildiği teyit edilir.	İ	Z	3
K3.T7	Bilgi sistemleri ağı aracılığı ile aktarılan şifrelenmiş verilerin, AES *(Advanced Encryption Standard)* gibi güçlü algoritmalar aracılığı ile şifrelendiği teyit edilir.	İ	O	3

6.5. 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 varlıklarının ve ağ kaynaklarının güvenliğinin sağlanması, kurum bilgi sistemleri üzerinde tanımlanan uzaktan erişim yetkilerinin 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 parolalarının yetkisiz kişiler tarafından ele geçirilmesi			+

Denetim Testleri

#	Denetim testleri	T/İ	Z/O	YS
K1.T1	Bilgi sistemleri uzaktan erişim politikası ve uzaktan erişim yetkisine sahip kullanıcı listesi temin edilerek, kurum yönetimi tarafından onaylı ve güncel olduğu gözlemlenir.	T	Z	3
K1.T2	Bilgi sistemlerine uzaktan erişimler sırasında kullanılan kullanıcı doğrulama mekanizmalarının, kurumun bilgi güvenliği politikasına uygun yapılandırıldığı kontrol edilir.	T	Z	3
K1.T3	Bilgi sistemleri ağına uzaktan erişimler sırasında kullanıcının bildiği bir parolanın yanı sıra, sahip olduğu değişken parolalar ile (SMS, değişken parola üretici aygıtlar "token" vb araçlar ile) erişim yapabildiği teyit edilir.	İ	O	3
K1.T4	Bilgi sistemleri güvenlik donanımı ve ağ cihazlarının, kurumun bilgi sistemleri ve uzaktan erişim politikalarına uygun yapılandırıldığı gözlemlenir. ***(**bkz: **6.2.3 Ağ Sistemleri - K2. Ağ cihazları güvenliği**)***	T	Z	3
K1.T5	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 içerisinden örnek kullanıcılar seçilerek ilgili kullanıcılara ait yetkilendirmenin kontrollü ve ilgili sürece uygun olarak gerçekleştirildiği gözlemlenir.	İ	Z	3
K1.T6	Denetim dönemi için kurumun bilgi sistemleri üzerinde gerçekleştirilen uzaktan erişimlere ilişkin denetim izleri temin edilerek kullanıcıların uygunluğu test edilir.	İ	Z	3

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, Illionis, ABD.
- ISACA. (2012). COBIT 5 Enabling Processes. Rolling Meadows, Illinois, ABD.
- 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.
- TÜBİTAK Bilgem Kılavuzları. https://www.bilgiguvenligi.gov.tr/kilavuz-dokumanlar/index.php
- 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.

7. TERİMLER SÖZLÜĞÜ

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
Acil değişiklik	Mümkün olan en kısa sürede gerçekleştirilmesi gereken değişiklik – örneğin, önemli bir vakayı çözmek veya bir güvenlik yamasını uyarlamak. Değişiklik yönetimi süreci normal olarak acil değişiklikleri ele almak için belirli bir prosedür içerir.
Active Directory	Microsoft ağlarında kullanılan dizin hizmetidir. Bu veritabanı, kullanıcılar, bilgisayarlar, mekanlar, yazıcılar gibi organizasyonun tüm bilgilerini saklar.
Açılış toplantısı	İç denetçilerin ön araştırmalar sonrasında denetlenen alan ile ilgili yeterli düzeyde bilgiye sahip olduktan sonra denetlenecek birim yöneticileri ile yaptıkları toplantıdır.
Algoritma	Sisteme sağlanan bir girdiden farklı bir çıktı elde edilmesi için o girdi üzerinde yapılan hesaplamalar ve / veya düzenlemeler.
Ana kütle (Popülasyon)	İç denetçinin denetlenen alanın tamamı hakkında bir sonuca ulaşmak için örnek seçmek istediği veri setidir. Bu nedenle, örnekleme yapılacak olan ana kütlenin denetimin amaçlarına uygun olması ve denetim hedefi için tam ve eksiksiz olduğunun doğrulanması gerekir.
Anahtar performans göstergesi	Bir BT hizmeti, süreç, plan, proje veya diğer aktivitenin yönetilmesine yardımcı olmak için kullanılan metrik. Anahtar performans göstergeleri, kritik başarı faktörlerinin kazanımını ölçmek için kullanılır. Birçok metrik ölçülebilir, fakat bunların sadece en önemlileri anahtar performans göstergesi olarak tanımlanır ve sürecin, BT hizmetinin veya aktivitenin etkin olarak yönetiminde ve raporlanmasında kullanılır. Anahtar performans göstergeleri, verimliliğin, etkinliğin ve maliyet etkinliğinin hepsinin yönetildiğinin güvencesini sağlayacak şekilde seçilmelidir.
Bağımsızlık	İç denetim faaliyeti, iç denetimin kapsamının belirlenmesi, yürütülmesi ve sonuçlarının paylaşılması ve raporlanması hususunda her türlü müdahaleden uzak ve serbest olmak zorundadır.
Batch job (Yığın iş)	Bilgisayar bilimlerinde, belirli bir zamanda yapılması planlanan çoğunlukla kullanıcı etkileşimi gerektirmeyen işlerin biriktirilmesidir. Ör: farklı bilgisayarlardan verinin bir sunucuda toplanarak yedeklerin alınması
Bilgi güvenliği yönetim sistemi	Organizasyonun bilgi güvenliği yönetimi amaçlarını gerçekleştirmesini garanti eden politikalar, süreçler, standartlar, kılavuzlar ve araçlar çerçevesi.

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
Bilgi teknolojisi	Bilginin üretilmesi, toplanması, biriktirilmesi, işlenmesi, yeniden elde edilmesi, yayılması ve korunmasını sağlayan ve bunlara yardımcı olan araçlardır. Bilgi teknolojisi; bilginin toplanması, işlenmesi, depolanması, iletişim ağları aracılığıyla bir yerden bir yere iletilmesi, kullanıcıların hizmetine sunulması, yönetilmesi, saklanması ve güvenliğinin sağlanması ile söz konusu sistemlerde saklanan bilgiye erişim kurallarının belirlenmesinde yararlanılan yazılım ve donanım teknolojilerini kapsayan bir bütündür.
Bilgisayar Destekli Denetim Teknikleri (Computer Assisted Audit Techniques)	Denetimin verimliliğini arttırmak üzere, manüel olarak yapılan denetim prosedürlerinin, bilgisayar yardımıyla yapılmasına imkân veren araçlardır. Pratikte manüel olarak çok sayıda verinin incelenmesinin mümkün olmadığı durumlarda bu amaçla geliştirilen yazılım programları sayesinde denetim kapsamındaki veri seti içerisindeki aykırılıkların, farklılıkların ve eksikliklerin ortaya çıkarılmasıdır. Bilgisayar destekli denetim tekniklerinin etkin bir şekilde kullanılabilmesi, ilgili veri setinin kalitesine ve ne kadarının bilgisayar ortamında muhafaza edildiğine bağlıdır
Bilinen hata kaydı	Bilinen hatanın ayrıntılarını içeren kayıt. Her bilinen hata kaydı, durum, kök neden ve geçici çözümü içeren bilinen hatanın yaşam döngüsünü dokümante eder. Bazı uyarlamalarda, bilinen hatanın problem kaydında ilave alanlar kullanılarak dokümante edilir.
BT altyapısı	Uygulamaları ve BT hizmetlerini geliştirmek, test etmek, sunmak, izlemek, kontrol etmek ve desteklemek için gereken tüm donanım, yazılım, ağ, tesisler vb. BT altyapısı terimi, ilişkili kişiler, süreçler ve dokümantasyon hariç bilgi teknolojilerinin tümünü içerir.
BT operasyonları	Konsol yönetimi, iş çizelgeleme, yedekleme ve geri yükleme ve yazdırma ve çıktı yönetimi dahil BT operasyon kontrol tarafından yürütülen aktiviteler. BT operasyonları, hizmet operasyonu ile eş anlamlı olarak da kullanılır.
BT yöneticisi	Kurumda Bilgi Teknolojileri alanında yönetim sorumluluğu olan personel. (Ör. Bilgi İşlem Dairesi Başkanlığı Yazılım Geliştirme Müdürü)
Bulgu formu	İç denetçinin, denetim sırasında tespit ettiği hususları önem derecesine göre sınıflandırarak oluşturduğu bir çalışma kâğıdı türüdür. Bulgu formunda; mevcut durum, mevcut durum ile olması gereken durum arasındaki farklılığın nedeni, mevcut durum nedeniyle kurumun ya da kişilerin maruz kalabileceği riskler ile bu risklerin etkileri, uyulması gereken kriterler ve öneriler yer almalıdır.
Bulgu riski	İç denetçinin, denetim teknik ve prosedürlerini uygulamasına rağmen mevcut hata ve yanlışlıkları tespit edememesi riskidir.
Bütünlük	Verinin ve konfigürasyon birimlerinin sadece yetkili personel ve aktiviteleri tarafından değiştirildiğini garanti eden güvenlik ilkesi. Bütünlük, donanım ve yazılım arızası, çevresel olaylar ve insan müdahalesi dahil tüm olası değişiklik nedenlerini değerlendirir.
Canlı ortam	BT hizmetlerini sunmak için kullanılan canlı konfigürasyon birimlerini bulunduran kontrollü ortam.

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
Çağrı	Kullanıcıdan hizmet masasına gelen telefon çağrısı. Bir çağrı, vaka veya hizmet isteminin kaydı ile sonuçlanabilir.
Çalışma kâğıdı	Denetime hazırlık, risk ve kontrol değerlendirmeleri, yapılan testler, bunların sonucunda elde edilen bilgi ve kanıtlar ile raporlama ve izleme faaliyetleri gibi denetim süresince yapılan tüm çalışmaların belgelendirildiği kâğıtlardır. Çalışma kâğıtları, denetimin yürütülmesinde iç denetçiye yardımcı olmaya ve iç denetçinin ulaştığı bulguları desteklemeye hizmet eder.
Değişiklik	BT hizmetlerini etkileyebilen herhangi bir şeyi ekleme, değiştirme veya ortadan kaldırma. Kapsam, tüm BT hizmetleri, konfigürasyon birimleri, süreçler, dokümantasyon vb. olabilir.
Değişiklik değerlendirmesi	Önerilen değişikliklerin etkisini öngörmek için kullanılan teknik. Değişiklik senaryoları, önerilen değişikliklerin kapsamına açıklık getirmek ve maliyet fayda analizine yardımcı olmak için belirli senaryolar kullanır.
Değişiklik tarihçesi	Konfigürasyon biriminin yaşamı boyunca tüm değişiklikleri hakkında tutulan bilgi.
Denetim görüşü	Denetim görevi sırasında toplanan bilgi ve kanıtlar doğrultusunda denetim konusu hususlarla ilgili olarak görevin amaç ve kapsamına uygun bir şekilde genel bir kanaate ulaşılmasıdır. Bu görüş ile denetlenen birim yöneticisine ve üst yöneticiye, denetim alanına ilişkin genel durumu hakkında bilgi sunulur.
Denetim izi (log)	İlgili olduğu sistem üzerinde gerçekleştirilen işlemleri kaydeden mekanizmanın sakladığı kayıtlar.
Denetim kanıtı	Denetim bulgularını ve denetim sonucunda iç denetçinin ulaştığı kanaati desteklemek veya ispat etmek üzere toplanan ve kullanılan bilgi ve belgelerdir. İç denetçi, denetim amacına ulaşabilmek için topladığı kanıtları uygunluk, güvenilirlik ve yeterlilik olmak üzere üç açıdan değerlendirir. Denetim kanıtının uygunluğu, kanıtlar ile denetim amaçları ve kriterleri arasında net ve mantıksal bir bağlantı bulunmasını gerektirir. Güvenilirliğinin tespiti için denetim kanıtının; kaynağı (kurum içi, kurum dışı gibi), doğası (yazılı, sözlü, görsel ya da elektronik gibi) ve gerçekliği (asıl olma, imza, mühür gibi) açılarından değerlendirilmesi gerekir. Denetimin amaç ve kapsamına ilişkin önemli soruları cevaplıyor ise denetim kanıtlarının yeterliliğinden bahsedilebilir.
Denetim testi	Denetim kapsamına alınmasına karar verilen hususlarla ilgili olarak ilgili denetlenen birimde var olduğu belirtilen kurumsal yönetim, risk yönetimi ve kontrol süreçlerinin gerektiği gibi çalışıp çalışmadığının süreçler, kayıtlar ve belgeler üzerinden incelenmesidir.
Dış hizmet sağlayıcı	Belli bir alanda uzman seviyesinde bilgi, beceri ve tecrübe sahibi olan kurum dışından kişi veya şirketlerdir.
Dip Toplam	Bir tabloda veya listede yer alan verilerin toplanması ile elde edilen değer
Dosya uzantısı	Bir dosyanın kodlanma veya kullanılma şeklini gösteren dosyanın sonuna konulan nokta işaretinden sonra gelen uzantı. (ör: .exe, .jpg, .png)

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
En iyi uygulama	Birçok organizasyon tarafından başarılı şekilde kullanılmakta olan kendini ispat etmiş aktiviteler veya süreçler.
Entegrasyon testi	Değişikliklerin testinin parça parça yerine bütün olarak beraber yapılmasıdır. Bu şekilde değişiklikler arasındaki ilişkiler de test edilir.
Etik kurallar	Uluslararası genel kabul görmüş etik kurallarla uyumlu olarak İDKK tarafından belirlenen ve iç denetçilerin uyacakları Meslek Ahlak Kurallarıdır.
Etki	Mevcut durumun belirlenen kriterlerle aynı olmaması sebebiyle denetlenen birim ve/veya diğer ilgililerin karşılaşabileceği risk veya bu riske maruz kalma halidir.
Etki alanı (Windows domain)	Tüm kullanıcı hesaplarının, bilgisayarların, yazıcı ve diğer bileşenlerin bir ya da bir grup bilgisayar üzerinde bulunan merkezi bir veritabanına (etki alanı denetçisi) kayıtlı oldukları bilgisayar ağı.
Etkililik	Bir faaliyetin, planlanan ve gerçekleşen etkisi arasındaki ilişkiyi; hedefe ulaşma derecesini ve yerindeliğini ifade eder.
Fayda-maliyet analizi	Kamu ekonomisinde yatırım projelerini etkinlik yönünden değerlendirmeye yarayan, topluma en yüksek faydayı sağlayacak olan projelerin seçiminde veya öncelik sırasının tespit edilmesinde yararlanılan bir tekniktir.
Firewall	Güvenlik duvarı. Bilgisayar ağına dışarıdan erişimlerin ve iç trafiğin kontrol altında tutulması amacıyla kullanılan güvenlik sistemlerinin genel adıdır.
Geri yükleme	Bir vaka sonrası onarımı ve kurtarmayı takip eden aşamada BT hizmetinin kullanıcıların kullanımına kazandırılması için aksiyon alma.
Gizlilik	Verinin sadece onaylı kişi tarafından erişilebilir olmasını gerektiren güvenlik kuralı.
Görev iş programı	Görev iş programında hangi denetim testlerinin kim tarafından, nerede, hangi tarihler arasında yapılacağı kaydedilir.
Görevler ayrılığı ilkesi	Hata, eksiklik, yanlışlık, usulsüzlük ve yolsuzluk risklerini azaltmak için faaliyetler ile mali karar ve işlemlerin onaylanması, uygulanması, kaydedilmesi ve kontrol edilmesi görevlerinin personel arasında paylaştırılmasıdır. Bu ilkenin uygulanması için her faaliyet, mali karar veya işlemin onaylanması, uygulanması, kaydedilmesi ve kontrolü görevleri farklı kişilere verilmelidir.
Görüşme	Denetlenen birimde işlemlerin veya faaliyetlerin nasıl gerçekleştirildiği hakkında bizzat iç denetçi tarafından ilgili görevlilerle yüz yüze görüşülerek bilgi edinilmesidir.
Gözlem	Denetlenen birimde işlemlerin veya faaliyetlerin nasıl gerçekleştirildiğinin bizzat iç denetçi tarafından izlenerek bilgi edinilmesidir.
Güvence	Kurumsal yönetim, risk yönetimi ve kontrol ve süreçlerine dair bağımsız bir değerlendirme sunabilmek amacıyla kanıtların objektif bir şekilde incelenmesidir.
Güvenirlilik	Bir BT hizmetinin veya diğer bir konfigürasyon biriminin üzerinde anlaşılan işlevini kesintisiz olarak ne kadar süre yerine getirebildiğinin ölçümü.

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
Hizmet kataloğu	Konuşlandırmaya uygun olanlar dahil, bütün canlı BT hizmetlerinin bilgilerini barındıran bir veritabanı veya yapısal dokümandır.
Hizmet seviyesi	Bir veya daha fazla hizmet seviye hedeflerine karşı ölçülen ve raporlanan başarı. Hizmet seviyesi terimi, bazen konuşma dilinde hizmet seviye hedefini ifade etmek için de kullanılır.
Hizmet seviyesi anlaşması	Bir BT hizmet sağlayıcı ile hizmet alan arasındaki anlaşma. Hizmet seviye anlaşması (HSA), BT hizmetini tanımlar, hizmet seviye hedeflerini belgeler ve BT hizmet sağlayıcının ve hizmet alanın sorumluluklarını tanımlar. Tek bir hizmet seviye anlaşması birçok BT hizmetini veya birçok hizmet alanı kapsayabilir.
İç denetim	Kamu idaresinin çalışmalarına değer katmak ve geliştirmek için kaynakların ekonomiklik, etkililik ve verimlilik esaslarına göre yönetilip yönetilmediğini değerlendirmek ve rehberlik yapmak amacıyla yapılan bağımsız, nesnel güvence sağlama ve danışmanlık faaliyetidir. Bu faaliyetler, idarelerin yönetim ve kontrol yapıları ile malî işlemlerinin risk yönetimi, yönetim ve kontrol süreçlerinin etkinliğini değerlendirmek ve geliştirmek yönünde sistematik, sürekli ve disiplinli bir yaklaşımla ve genel kabul görmüş standartlara uygun olarak gerçekleştirilir.
İç denetim birimi başkanı	Üst yönetici tarafından görevlendirilen ve iç denetim faaliyetinin yönetiminden sorumlu olan kişidir.
İç Denetim Koordinasyon Kurulu	İç denetim alanında merkezi uyumlaştırma fonksiyonunu ifa etmek üzere, Maliye Bakanlığına bağlı olarak faaliyet yürüten bir Kuruldur.
İç denetim planı	İç denetimin etkili, ekonomik ve verimli bir şekilde yapılmasını sağlamak amacıyla denetimin alanı ve konuları, ihtiyaç duyulan işgücü ve diğer kaynaklar ile eğitim faaliyetlerini içerecek şekilde hazırlanan 3 yıllık plandır.
İç denetim programı	En riskli alan ve konulara öncelik verilmek ve denetim maliyeti de dikkate alınmak suretiyle, birim yöneticileri ve gerektiğinde çalışanlarla görüşülerek iç denetim planıyla uyumlu olarak hazırlanan programlardır.
İç kontrol	İdarenin amaçlarına, belirlenmiş politikalara ve mevzuata uygun olarak faaliyetlerin etkili, ekonomik ve verimli bir şekilde yürütülmesini, varlık ve kaynakların korunmasını, muhasebe kayıtlarının doğru ve tam olarak tutulmasını, malî bilgi ve yönetim bilgisinin zamanında ve güvenilir olarak üretilmesini sağlamak üzere idare tarafından oluşturulan organizasyon, yöntem ve süreçle iç denetimi kapsayan malî ve diğer kontroller bütününü ifade eder.
İş akış şeması	Denetlenecek birimin iş süreçlerini ve bir faaliyetin başlangıcından sonuçlandırılmasına kadar olan aşama ve işlem adımlarını görsel hale getirmeyi sağlayan ve işlem adımlarını geometrik şekillerle gösteren şemadır. Sistemin tanınmasında, işlem adımları arasındaki olası risklerin belirlenmesi ve değerlendirilmesinde ve sınırların belirlenmesinde de kullanılan iş akış şemaları aynı zamanda sistem içinde tıkanma yaşanan noktaların, görevler ayrılığı ilkesine uyulmayan durumların ve aynı işin birden fazla yerde tekrar edilmesi gibi verimsizliklerin ve kontrol zayıflıklarının belirlenmesine ve süreçlerdeki kritik kontrol faaliyetlerinin ortaya çıkarılmasına yardımcı olur.

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
İş etki analizi	İş etki analizi, iş süreklilik yönetiminde yaşamsal iş fonksiyonlarını ve bağımlılıklarını tanımlayan aktivitedir. Bu bağımlılıklar tedarikçileri, kişileri, diğer iş süreçlerini, BT hizmetlerini vb. İçerebilir. İş etki analizi, BT hizmetleri için kurtarma gereksinimlerini tanımlar. Bu gereksinimler, kurtarma zamanı hedefleri, kurtarma noktası hedefleri ve her bir BT hizmeti için en düşük hizmet seviye hedeflerini içerir.
İş riski	Kurum'un ana faaliyetlerini gerçekleştirdiği konuda oluşabilecek sıklığı ve büyüklüğü belirsiz olan, bir kayıpla veya kazançla sonuçlanabilecek olası durumlar.
İş sürekliliği planı	Kesintiyi takiben iş süreçlerini geri yüklemek için gereken adımları tanımlayan plan. Plan, başlatma için tetikleyicileri, katılması gereken kişileri, iletişim yollarını vb. tanımlar. BT hizmet süreklilik planları, iş süreklilik planlarının önemli bir kısmını oluşturur.
İşlem	Bir BT hizmeti tarafından gerçekleştirilen ayrık fonksiyon. Örneğin, bir banka hesabından diğerine para transferi. Tek bir işlem, birçok verinin eklenmesini, silinmesini ve değiştirilmesini içerebilir.
İşletim seviyesi anlaşması	BT hizmet sağlayıcı ile aynı organizasyonun diğer kısmı arasındaki anlaşma. OLA, BT hizmet sağlayıcının BT hizmetlerinin hizmet alanlara sunumunu destekler ve sunulacak malları ve hizmetleri ve tarafların sorumluluklarını tanımlar. Örneğin, operasyonel seviye anlaşması aşağıdaki şekilde olabilir; • Üzerinde anlaşılan zamanda donanımı edinmek için BT hizmet sağlayıcı ile tedarik bölümü arasında • Vaka çözümlemenin üzerinde anlaşılmış zamanda gerçekleştirilmesi için hizmet masası ile destek grubu arasında.
İşletim sistemi	Bilgisayar donanım kaynaklarını yönetip, yazılımların hizmetine sunmak amacını taşıyan yazılımlar bütünü.
İzleme	Denetim faaliyetleri sonucunda ortaya çıkan bulgular ile danışmanlık faaliyetleri sonucunda denetlenen birim ile mutabık kalınarak izlenmesi kararlaştırılan hususlara ilişkin ilerlemelerin değerlendirilmesini kapsar.
Kabuk (Shell)	İşletim sistemi hizmetlerine erişim için kullanılan kullanıcı arayüzüdür.
Kamu İç Denetim Rehberi	İç denetim faaliyetine ilişkin olarak İDKK tarafından çıkarılan bu Rehber iç denetim sürecine yönelik genel çerçeveyi çizmek ve iç denetim faaliyetine ilişkin ilkeleri anlatmak amacıyla hazırlanmıştır.
Kamu İç Denetim Standartları	İç denetimin planlanması, uygulanması ve raporlanması ile iç denetçilerin yetkin, dürüst, tarafsız ve bağımsız bir şekilde görev yapabilmelerine ilişkin hususları düzenlemek üzere İDKK tarafından belirlenen standartlardır. Bu standartların belirlenmesinde, Uluslararası İç Denetçiler Enstitüsünün (IIA) "Uluslararası İç Denetim Mesleki Uygulama Standartları" esas alınmıştır.
Kapanış toplantısı	Bulgular ve öneriler paylaşıldıktan sonra denetlenen birim ile bulgularda yer alan hususlarla ilgili olarak her iki tarafın birbirini tam olarak anladığından emin olmak amacıyla yapılan toplantıdır.
Kaynak kod	Yazılım kodlarının ve talimatlarının bir insan tarafından okuyup anlaşılabilecek durumdaki halidir.

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
Kilit/anahtar kontroller	Kontrolün çalışmaması halinde yürütülen faaliyetin sekteye uğraması, mali kayıpların ortaya çıkması gibi hususlar yaşanması muhtemel ise bu kontroller kilit kontrollerdir.
Konfigürasyon	BT hizmetini sunmak için birlikte çalışan konfigürasyon birimleri grubunu veya BT Hizmetinin ayıt edilebilen parçasını ifade etmek için kullanılan genel terim.
Konfigürasyon yönetimi	Hizmetin sunulması için gerekli olan varlıkların düzgün kontrol edildiğini ve bu varlıklara ait bilgilerin kesin ve güvenilir bilgilerin gerektiği yerde ve zamanda kullanılabilirliğini güvence altına almaktan sorumlu süreç. Bu bilgi, varlıkların nasıl yapılandırıldığının ve varlıkların arasındaki ilişkilerinin detaylarını içerir.
Kontrol	Üst yönetim ve ilgili diğer taraflarca risk yönetimini güçlendirmek ve idarenin belirlenmiş amaç ve hedeflerine ulaşma ihtimalini artırmak için yapılan her türlü faaliyet, alınan önlem ve karardır.
Kontrol çerçevesi	Bir kurumda olması gereken veya mevcut tüm iç kontrolleri kapsayan ve idarenin iç kontrol sisteminin değerlendirilmesinde temel alınabilecek tanımlanmış ve genel kabul görmüş kontrol kategorileri sistemini ifade eder.
Kontrol ortamı	COSO iç kontrol modelinin kurumdaki kontrol faaliyetlerine ilişkin genel çerçevesini gösterir. Üst yönetimin idare içerisindeki kontrolün önemine ve uygulanmasına ilişkin yaklaşımı ve buna ilişkin faaliyetlerdir. Kontrol ortamı, iç kontrol sisteminin temel amaçlarını gerçekleştirmek için bir yapı ve disiplin sağlar. Kontrol ortamı; dürüstlük ve etik değerler, yönetimin felsefesi ve idare tarzı, organizasyonel yapı, yetki ve sorumlulukların belirlenmesi, insan kaynakları politikaları ve uygulamaları ile personelin yeterliliği unsurlarından oluşur.
Kontrol süreçleri	Riskin, risk yönetim süreçleriyle belirlenen riske ait kabul edilebilir sınırlar içinde kalmasını sağlamak amacıyla tasarlanan ve kontrol çerçevesinin bir parçası olan faaliyet, politika ve prosedürlerdir.
Kontrol süreçlerini değerlendirmek	İdarenin amaçlarına ulaşmasını sağlayacak uygun bir iç kontrol yapısının oluşturulması ve sürdürülmesi için değerlendirmeler yapmak ve önerilerde bulunmaktır.
Kontrol riski	İç kontrol sisteminin iyi tasarlanamaması, kurulamaması veya zamanla etkililiğini yitirmesi nedeniyle, kontrol sistemindeki zayıflıkları önleme veya tespit etmede başarısız olması riskidir.
Kök neden	Bir vakanın veya problemin altında yatan veya asıl neden.
Kriptolama	Bilgilerin güvenli veya gizli bir şekilde iletilmesini veya saklanmasını sağlamak adına belli bir sisteme göre şifrelenmesi.
Kritik BT işlevselliği	Kurum iş süreçlerinin etkin bir şekilde gerçekleştirilebilmesi ve hedeflenen çıktılara ulaşabilmesi için ihtiyaç duyulan ve BT birimi tarafından sağlanan işlevler (ör: uygulamalar, sistemler, altyapı, süreçler, faaliyetler, vb)
Kullanıcı grubu	Aynı güvenlik haklarına sahip kullanıcı hesapları topluluğudur. Güvenlik grupları olarak da adlandırılabilir.

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
Kullanıcı onayı	Bir geliştirmeden ya da projeden etkilenecek olan kullanıcıların kendilerine verilen sorumluluklar ışığında gerçekleşen değişiklikleri değerlendirerek onaylaması.
Kullanılabilirlik (Erişilebilirlik)	Bir BT hizmetinin veya konfigürasyon biriminin üzerinde anlaşılmış işlevini gerektiğinde gerçekleştirebilmesi. Kullanılabilirlik, güvenirlilik, bakım yapabilme, hizmete elverişlilik, performans ve güvenlikle belirlenir. Kullanılabilirlik genellikle % olarak hesaplanır. Bu hesaplama için anlaşılmış hizmet zamanı ve duruş süresi esas alınır. Bir BT hizmetinin iş çıktı ölçümlerinin kullanılabilirliğini hesaplamak için en iyi pratiktir.
Kurtarma noktaları	Kurumun bir felaket ya da sürekliliği etkileyecek başka bir durumun gerçekleşmesi halinde ne kadar süreli veri kaybına tahammülü olduğunu ifade eder.
Kurtarma zamanı	Kurumun hangi faaliyette ne kadar iş görememeye tahammülü olduğunu ifade eder.
LDAP (Basit dizin erişim protokolü)	Internet protokolü üzerinden dağınık dizin bilgi sistemlerinin erişilmesi ve yönetilmesini sağlayan bir uygulama protokolüdür.
Linux	Linux, açık kaynak kodlu bir işletim sistemidir. Bir UNIX türevidir.
Lisans	Bir yazılımın kullanımını ve yeniden dağıtımını düzenleyen yasal bir araçtır.
Mali denetim	Gelir, gider, varlık ve yükümlülüklere ilişkin hesap ve işlemlerin doğruluğunun ve mali sistem ve tabloların güvenilirliğinin değerlendirilmesidir. Mali denetim kapsamında elde edilen sonuçlar çerçevesinde, denetlenen birim veya sürece ilişkin oluşturulan iç kontrollerin etkinliği ve yeterliliği de değerlendirilir.
Man in the middle attack (Aradaki adam saldırısı)	Bir network üzerinde bulunan bilgisayar (kurban) ile router, switch, server gibi diğer ağ araçları arasına girerek verileri yakalama ve şifrelenmemiş verileri görebilme prensibine dayanan bir saldırı çeşididir.
Manuel kontroller	Süreç içerisinde çalışanlarca manuel olarak gerçekleştirilen kontrollerdir.
Master plan	Belirli bir dönem boyunca gerçekleştirilecek olan projeleri, harcanacak çabanın ve zamanın planı.
Metrik	Bir sürecin, BT hizmetinin veya aktivitenin yönetilmesine yardımcı olmak için ölçülen ve raporlanan birim.
Mimari	Bileşenlerinin birbirleri veya bulundukları ortam ile ilişkilerini içeren bir sistemin veya BT hizmetinin yapısı. Mimari, sistemin tasarımına ve gelişimine rehberlik eden standartları ve kılavuzları da içerir.
Olgunluk	Bir sürecin, fonksiyonun, organizasyonun güvenirlilik, verimlilik ve etkinlik ölçüsü. En olgun süreçler ve fonksiyonlar resmi olarak iş amaçları ve strateji ile uyumludurlar ve sürekli iyileştirme için bir çerçeve ile desteklenirler.

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
Ortam	BT altyapısının belirli bir maksat için kullanılan alt kümesi – örneğin, canlı ortam test ortamı, inşa etme ortamı. Ayrıca, 'fiziksel ortam' teriminin içinde kullanımı, iklimlendirme, güç sistemleri ve bunların bulunduğu yer anlamına gelir. Ortam, ayrıca bir şeyi etkileyen veya tesir eden dış şartları ifade etmek için de kullanılan genel bir terimdir.
Otomatik kontroller	Sistem içerisine yerleştirilen, bilgisayar destekli kontrollerdir.
Örnekleme	Denetlenecek tüm iş ve işlemleri ifade eden ana kütle (popülasyon) hakkında bir sonuca varmak veya bir sonuca varılmasına yardımcı olmak amacıyla seçilen unsurların belirli özellikleri hakkında denetim bulguları ve delillerin değerlendirilebilmesi için, denetim prosedürlerinin o ana kütlenin % 100'ünden daha az bir kısmına uygulanmasıdır.
Örneklem birimi	Saha çalışmasında kullanılacak denetim testlerinin amacına bağlı olarak ana kütle içinden seçilen birim/belge/kişi vs.dir.
Örneklem büyüklüğü	Ana kütle hakkında bir sonuca ulaşmak için kullanılacak ana kütle parçasını ifade eder. Örneklem büyüklüğünü tespit ederken, iç denetçi, örnekleme riskini, kabul edilebilecek hata miktarını ve beklenen hataların kapsamını dikkate almalıdır.
Örnekleme riski	İç denetçinin vardığı sonucun, ilgili ana kütlenin tümü aynı denetim prosedürüne tâbi tutulsaydı, ulaşılacak olan sonuçtan farklı olabileceği ihtimalinden kaynaklanır. İki tip örnekleme riski vardır: • Yanlış kabul riski: Örneklemenin ana kütleyi yeterli düzeyde temsil etmemesi nedeniyle, ana kütle düzeyinde hatalı olan bir durumun yanlış veya eksik örneklem seçimi nedeniyle hatasız kabul edilmesi riskidir. • Yanlış ret riski: Yanlış kabul riskinin tam tersi olup, örneklemenin ana kütleyi yeterli düzeyde temsil etmemesi nedeniyle, popülasyon düzeyinde hatasız olan bir durumun yanlış veya eksik örneklem seçimi nedeniyle hatalı kabul edilmesi riskidir.
Örneklemden kaynaklanmayan risk	İç denetçinin uygun olmayan denetim teknikleri kullanması kanıtları hatalı yorumlaması gibi seçilen örneklemden kaynaklanmayan farklı sonuçlara ulaşılması riskidir.
Parametre	Sisteme ait bir özelliği tanımlamak için kullanılan bir isim, anlam veya ölçü.
Paydaş	Bir kurumda, bir projede, bir BT hizmetinde vb. ilgi sahibi olan tüm kişiler. Paydaşlar, aktiviteler, kaynaklar veya teslim edilecek çıktılar ile ilgilenebilirler.

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
Performans denetimi	Yönetimin bütün kademelerinde gerçekleştirilen faaliyet ve işlemlerin planlanması, uygulanması ve kontrolü aşamalarındaki etkililiğin, ekonomikliğin ve verimliliğin değerlendirilmesidir. Performans denetiminin amacı, tahsis edilen beşeri, mali ve teknolojik kamu kaynaklarının etkili, ekonomik ve verimli bir şekilde parasal değerlerine uygun olarak kullanılıp kullanılmadığının objektif olarak incelenip değerlendirilmesidir. Diğer bir ifadeyle, kullanılan kaynakların denetlenen birimin amaç ve hedeflerine uygunluğunun ve elde edilen çıktılarla orantılı olup olmadığının denetlenmesidir.
Performans testi	Belirli bir yükün altında test edilecek yazılımın performansının test edilmesidir.
Program	Bir ilişkili amaçlar ve diğer nihai çıktılar kümesinin hepsini bir bütün olarak gerçekleştirmek için birlikte planlanan ve yönetilen birçok sayıdaki proje ve aktivite.
Proje	Bir amacı veya diğer nihai çıktıları gerçekleştirmek için gereken, insan ve diğer varlıkların geçici olarak bir araya gelmesiyle oluşan organizasyon. Her bir proje, başlangıç, planlama, yürütme, kapanış aşamalarını içeren bir yaşam döngüsüne sahiptir.
Proje portföyü	Projeleri yaşam döngüleri boyunca yönetmek için kullanılan bir veritabanı veya yapılandırılmış doküman. Proje portföyü projeleri koordine etmek ve amaçlarını maliyet etkin ve zamanında karşıladığını güvence altına almak için kullanılır. Büyük kuruluşlar da proje portföyü genellikle bir proje yönetim ofisi tarafından tanımlanır ve sürdürülür. Proje Portföyü, yeni hizmetler ve önemli değişikliklerin normal olarak projelerle yönetilmesi durumunda, hizmet portföy yönetimi için önemlidir.
Prosedür	Bir aktivitenin nasıl başarılacağını belirten adımları içeren doküman. Prosedürler, süreçlerin bir parçası olarak tanımlanır.
Rassal	Rastgele olarak seçilmiş demektir.
Rastgele örnekleme	Ana kütledeki örneklem birimlerinin bütün kombinasyonlarının seçilme şanslarının eşit olmasını sağlayan istatistiksel örnekleme yöntemidir.
Risk	Kurumların kuruluş amaçları ile hedeflerine ulaşmasına ve görevlerin ifasına engel olabilecek veya beklenmeyen zararlara yol açabilecek durum ya da olaylardır.
Risk değerlendirmesi	Kurumların kuruluş amaçları ile hedeflerine ulaşmasına ve görevlerin ifasına engel olabilecek veya beklenmeyen zararlara yol açabilecek durum ya da olayları tahmin etmek, belirlemek, ortaya çıkarmak ve gidermek amacıyla uygun kontrol önlemlerinin geliştirilmesini de kapsayan çalışmaların bütünüdür.
Risk envanteri / Risk kütüğü	Bir kurumun önemli risklerinin kaydedildiği merkezi bir risk kaydıdır. Burada riskler etkisi, olasılığı, alanı ve türüne göre sınıflandırılarak tanımlanır. Risk kütüğünde riskin yönetim sorumluluğunun kimde olduğu, potansiyel risk faktörleri ve risk göstergeleri de yer alabilir.

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
Risk esaslı denetim	İdarelerin faaliyet alanlarına ilişkin risk faktörlerinin tanımlanmasını, risk seviyelerinin ölçülmesini, bu riskler için uygulanan kontrollerin etkinlik ve yeterliliğinin değerlendirilmesini ve yüksek risk içeren alanlara denetim önceliğinin verilmesini öngören bir denetim yaklaşımıdır.
Risk faktörü	Riskin varlığını veya riske maruz kalmayı ifade eden bir sürecin ölçülebilir veya gözlemlenebilir özelliklerini ifade eder. Diğer bir ifadeyle, risk düzeyinin belirlenmesinde kullanılan kriterlerdir.
Risk iştahı	Bir kurumun misyonu, vizyonu ve ulaşmaya çalıştığı stratejik hedefleri doğrultusunda herhangi bir zaman diliminde, herhangi bir önlem almanın gerekliliğine karar vermeden önce kabul etmeye hazır olduğu risk düzeyidir.
Risk kontrol matrisi	Şekil ve içeriği özel olarak belirlenen ve denetim görevinde kullanılan standart ve önemli bir çalışma kâğıdıdır. Denetim alanı kapsamındaki alt faaliyet/süreçlerin risk düzeylerine göre derecelendirilmesi amacıyla RKM; alt faaliyet veya süreç, bunlara ilişkin yapısal (doğal) riskler, bu risklere karşı mevcut kontroller, uygulanacak testler ve risk düzeylerini içerir.
Risk önceliklendirmesi	Riskleri, idarenin amaç ve hedeflerine ulaşılması bakımından karşılaştırarak önem derecelerine göre sıralamayı ifade eder. Öncelik verilen riskler idare açısından üzerinde en fazla durulması gereken ve giderilmesi veya etkilerinin azaltılması için öncelikli çaba harcanması gereken riskleri ifade eder.
Risk yönetimi	Risklerin tanımlanması, değerlendirilmesi ve etkisinin kabul edilebilir bir seviyede tutulabilmesi için gerekli kontrollerin uygulanması, gözden geçirilmesi ve raporlanmasını sağlayan yönetim sürecidir.
Root	Unix/Linux sistemlerinde yönetim için kullanılan en yetkili kullanıcıdır.
Router (Yönlendirici)	Aynı protokolleri kullanan iki bilgisayar ağı arasında veri iletimini sağlayan ağ donanımıdır.
Saha çalışması	Çalışma planının onaylanmasının ardından başlayan aşama olup, bu aşamada çalışma planı ekinde yer alan görev iş programında yer alan testler gerçekleştirilir. Denetim testlerinin gerçekleştirilmesi risk kontrol matrisinin kontrol uygulamaları sütununda yer alan kontrollerin var olduklarına ve etkin bir şekilde çalışıp çalışmadıklarına dair uygun delillerin elde edilmesini kapsamaktadır.
Script	Belli bir çalışma ortamı (run-time environment) için hazırlanmış bir yazılım kodu içerisinde yer almayan bunun yerine direkt olarak çalıştırılan komutlar.
Sertifikasyon	Bir standarda uyumluluğu onaylamak için sertifika verme. Sertifikasyon, bir bağımsız ve akreditasyon kuruluşunun resmi denetimini içerir. Sertifikasyon terimi, bir kişinin yeterliliğe sahip olduğunu doğrulamak için sertifikalandırılmasını ifade etmek için de kullanılır.

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
Sistem	Amaçlar bütününü gerçekleştirmek için birbiri ile birlikte işleyen birçok şey. Örneğin; • Yazılım, donanım ve uygulamaları içeren bir bilgisayar sistemi • İçinde birlikte planlanan ve yönetilen, politika çerçevesini, süreçleri, fonksiyonları, standartları, kılavuzları ve araçları içeren yönetim sistemi - örneğin, kalite yönetim sistemi. Birbirleri ile ilişkili işlevsellikleri yerine getirmek üzere tasarlanmış birçok yazılım modülünü içeren veritabanı yönetim sistemi veya işletim sistemi.
Sistematik seçim/örnekleme	Örneklem birimlerinin, seçmeler arasında belirli sabit bir aralık bırakılarak ve ilk aralığın bir rasgele başlangıç noktasından başlatılarak seçildiği istatistiksel örnekleme yöntemidir.
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 testi	Bir yazılımın veya donanımın belirlenen tüm gereklilikleri karşılayıp karşılamadığını değerlendirmek için uygulanan testtir.
Son kullanıcı (End user)	Bir sistemi ya da ürünü iş amaçlı olarak kullanan kişi.
Sosyal mühendislik	Bilgi güvenliği kapsamında, insanlar arasındaki iletişimdeki ve insan davranışındaki açıklıkları tanıyıp, bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahalelere verilen isimdir.
Sözlü kanıtlar	Genellikle sorgulama ya da mülakat sonucunda kurumun iç ve dış paydaşlarından elde edilen bilgilerdir. Denetim çalışmaları kapsamında diğer denetim teknikleriyle elde edilemeyecek önemli ipuçlarının elde edilmesine ve konunun çok daha iyi anlaşılmasına imkân sağlamaktadır. Ancak sözlü kanıtların doğrudan kullanımı yerine mümkün olduğunca belgelerle desteklenmesi, yeterli düzeyde güvenilir ve uygun kanıtla denetim amaçlarına ulaşılmasını sağlayacaktır. Sözlü kanıtların güvenilirliği ve uygunluğu değerlendirilirken mülakat yapılan kişinin görevi, bilgisi, uzmanlığı, inanılırlığı ve samimiyeti göz önünde bulundurulmalıdır.
SQL (Yapılandırılmış Sorgu Dili)	Bir veritabanında bulunan verileri yönetmek için kullanılan bir veritabanı yönetim dilidir.
Stres testi	Bir sistemin sağlamlığının normalin çok üzerinde yük ile test edilmesidir.
Suistimal	Hile, sahtekârlık, emniyeti kötüye kullanma ile nitelendirilebilecek hukuk dışı fiillerdir. Bu fiiller, sadece şiddet tehdidi veya fizikî güç kullanımının gerçekleştirilmesine bağlı değildir. Suiistimaller; para, mal veya hizmet sağlamak, hizmet kaybından veya ödeme yapmaktan kaçınmak veya şahsıyla veya işle ilgili bir avantaj elde etmek amaçlarıyla çeşitli taraflar ve kurumlar tarafından gerçekleştirilebilir.
Sunucu	Bir ağa bağlı olarak, yazılım fonksiyonelliğinin diğer bilgisayarlar tarafından kullanımına olanak sağlayan bilgisayar.

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
Süreç	Bir girdiyle başlayan (İnsan gücü, makine, malzeme, teknoloji gibi) ve bu girdiye katma değer katılarak belirli bir çıktı üreten birbiriyle bağlantılı adımlar, işlemler dizisidir. Kaynakları kullanan ve girdilerin çıktılara dönüşümünün sağlanması için yönetilen faaliyet.
Switch (Dağıtıcı)	Bilgisayarların ve diğer ağ öğelerinin birbirlerine bağlanmasına olanak veren ağ donanımıdır.
Tarafsızlık/Nesnellik	Kişisel çıkarların veya başkalarının etkisi altında kalmaksızın, incelenmekte olan faaliyet veya süreçle bağlantılı bütün hususları dikkate alan ve görüşlerin nesnel delillere dayanarak oluşturulmasını ifade eden zihinsel bir durumdur. İç denetçi görüşlerini, değerlendirmelerini ve tavsiyelerini sunarken gereken mesleki tarafsızlığı göstermelidir.
Tedarikçi	BT hizmetlerin sunumu için gereken ürün veya hizmetleri tedarik etmekten sorumlu üçüncü taraf. Tedarikçilere örnek olarak, genel donanım, yazılım satıcıları, ağ hizmeti veren firmalar, telekom firmaları, ve dış kaynak organizasyonları verilebilir.
Telafi edici kontroller	Olmayan ya da maliyeti çok yüksek olabilecek kontrollerin yerini kısmen de olsa doldurabilen, telafi etmeye yönelik kontrollerdir. Genelde işlem sonrası gerçekleştirilmekte olup, ortaya çıkarıcı kontrollere göre daha kısa süreli ve dar kapsamlı kontrollerdir. Kurumlarda bazen, önleyici kontrolleri uygulamak için yeterli maddi veya insan kaynağı bulunmaz. Örneğin, görevler ayrılığı ilkesinin uygulanması için yeterli sayıda personel bulunamayabilir. Böyle bir durumda telafi edici kontroller, yöneticilerin yargısal kararlar çerçevesinde riskli gördükleri bazı alanlarda sondaj usulü ile evrak incelemeleri gibi ani ve rutin olmayan işlemler aracılığıyla aylık bütçe gerçekleşmelerinin takibini sağlamalarına benzer önlemlerden oluşur.
Tespit edici kontroller	İstenmeyen sonuçlar meydana geldikten sonra bu sonuçları tespit etmeye ve düzeltmeye yönelik kontrollerdir.
Token	Yetkili kullanıcılara BT servislerine erişim için otomatik anahtar üreten fiziksel cihazlara verilen isimdir.
UNIX	Açık kaynak kodlu bir işletim sistemidir.
Uygulama	BT hizmeti tarafından istenen fonksiyonları sağlayan yazılım. Her bir uygulama birden fazla BT hizmetinin bir parçası olabilir. Bir uygulama bir veya daha fazla sunucu veya istemci üzerinde çalışır.
Uygulama sonrası gözden geçirme	Bir değişikliğin veya projenin uyarlanması sonrasında gerçekleştirilen gözden geçirme. Uygulama sonrası gözden geçirme, bir değişikliğin veya projenin başarılı olup olmadığını belirler ve iyileştirme fırsatlarını tanımlar.

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
Uygunluk denetimi	Kamu idarelerinin faaliyet ve işlemlerinin ilgili kanun, tüzük, yönetmelik ve diğer mevzuata uygunluğunun incelenmesidir. Uygunluk denetiminde dikkat edilecek husus, sistem yapısının ve kontrollerin tasarımının genel olarak mevzuatta düzenlenmiş olmasıdır. Bu nedenle uygunluk denetimlerinde kontrollerin test edilmesinde iç denetçiler, hazırlamış oldukları kontrol listelerinden yararlanabilir. Uygunluk denetiminde hedef işlemlerin mevzuata uygunluğu olmasından dolayı, kontrolün çalışıp çalışmadığının yanı sıra kontrolle güvence altına alınmış işlemin doğruluğunun da test edilmesi gerektiğidir.
Usulsüzlük	Muhasebe kayıtları, mali tablolar, diğer rapor, belge veya kayıtlarda önemli bilgilerin kasten ihmal edilmesi veya yanlış sunulmasını ifade eder.
Üst yönetici	Milli Savunma Bakanlığında Bakan, bakanlıklarda müsteşar, üniversitelerde rektör, diğer kamu idarelerinde en üst yönetici, il özel idarelerinde vali ve belediyelerde belediye başkanı üst yöneticidir.
Vardiya	Sabit bir zaman dilimi için belirli bir rolü yürüten insan grubu veya takımı. Örneğin, günde 24 saat kullanılan bir BT hizmetine BT operasyon kontrol personeli 4 vardiya olarak destek verebilir.
Varlık	Herhangi bir kaynak veya kabiliyet. Bir Hizmet Sağlayıcının Varlıkları, bir hizmetin sunumuna katkıda bulunabilecek herhangi bir şeyi içerir. Varlıklar aşağıdakilerden biri olabilir: yönetim, organizasyon, süreç, bilgi, insan, enformasyon, uygulamalar, altyapı ve finansal sermaye.
Veri dönüşümü testi	Veri dönüşümü gerektiren değişikliklerin verilerin bütünlüğü açısından doğru olarak gerçekleştiğinin testidir.
Verimlilik	Kullanılan kaynaklarla, bir faaliyetin sonuçlarını ya da çıktılarını azamiye çıkarmayı ifade eder.
Veritabanı	Birbiri ile ilişkili verilerin toplandığı alanlardır.
Versiyon / sürüm	Bir yazılımın her yenilenmiş hali için verilen yeni numaralandırma.
Yama	Bir bilgisayar programı ya da o programın sakladığı verilerle ilgili sorunları çözmek için tasarlanan yazılım. Güvenlik açıklarının kapatılması, hataların düzeltilmesi, kullanışlılığın artırılması veya performans artırımı yazılım yamalarına örnekler olabilir.
Yargısal örnekleme	İç denetçinin örneklem belirlerken belirli bir yanlılık (örneğin, belirli bir değerin üzerindeki bütün örneklem birimleri, bütün eksi değerli olanlar, bütün yeni kullanıcılar vb.) uyguladığı örnekleme yöntemidir. Ancak bir yargısal örneklemin istatistiksel temellere dayanmaması ve sonuçların örneklemin ana kütleyi temsil edici nitelikte olmaması ihtimali nedeniyle, ana kütlenin tamamına teşmil edilmemesi gerektiği not edilmelidir.
Yazılım varlık yönetimi	Tüm yaşam döngüleri boyunca yazılım varlıklarının kullanımının ve sahipliğinin takip edilmesinden ve raporlanmasından sorum süreç. Yazılım varlık yönetimi, tüm bir hizmet varlık ve konfigürasyon yönetimi sürecinin parçasıdır.
Yedekleme	Orijinal olanın bütünlük veya kullanılabilirlik kaybına karşı korumak için veriyi kopyalama.

Tablo 7 - Terimler Sözlüğü	
Terim	**Açıklama**
Yeniden hesaplama/uygulama	Bir hesaplama veya işlemi tekrar yaparak aynı sonuca ulaşılıp ulaşılmadığının test edilmesidir. Bu test, denetlenen birim çalışanları tarafından gerçekleştirilen işlemlere ne kadar güvenilebileceği hakkında iç denetçiye fikir verir.
Yetkinlik	İç denetçiler, kişisel sorumluluklarını yerine getirmek için gereken bilgi, beceri ve diğer niteliklere sahip olmak zorundadır. İç denetçiler, görevin tamamını veya bir kısmını yapmak için gereken bilgi ve becerilerin veya diğer niteliklerin hepsine sahip değilse, İDB başkanı idare içindeki veya dışındaki uzmanlardan denetim görevinin hedeflerine ulaşmasını sağlamak üzere nitelikli tavsiye ve yardım temin etmek zorundadır.
Yönetişim	Kurumun amaçlarının uzlaşma dahilinde belirlenebilmesi için paydaş ihtiyaçlarının, koşulların ve alternatiflerin değerlendirilmesi; önceliklendirme ve karar verme mekanizmaları sayesinde kuruma yön verilmesi ve nihayetinde kararlaştırılan yön ve amaçlara uyumun izlenmesi unsurlarını kapsamaktadır.
Zafiyet	Bir tehdit ile ortaya çıkabilecek zayıflık. Örneğin, açık bir güvenlik duvarı portu, hiç değiştirilmeyen parola veya kolaylıkla alev alabilen bir halı. Noksan bir kontrol de zafiyet olarak değerlendirilir.

8. EKLER

Ek 1 – Bilgi Toplama Formu

1. Lütfen aşağıdaki tabloyu güncel kurum bilgilerini kullanarak doldurunuz

Bilgi	İçerik
Kurumun Adı	
Ana faaliyetler	
Kurum bütçesi	
Yıllık bilgi teknolojileri bütçesi (TL)	

2. Bilgi teknolojileri ile ilişkili olarak son bütçe dönemi içinde yapılan en büyük miktardaki üç sermaye giderini ve faaliyet giderini listeleyiniz

Sermaye Giderleri

No	Harcamanın Niteliği	Tutar (TL)	Tarih
1			
2			
3	Son iki yılın bütçe tahminleri ile harcama miktarlarını ekleyiniz.		

Cari Giderler

No	Harcamanın Niteliği	Tutar (TL)	Tarih
1			
2			
3	Son iki yılın bütçe tahminleri ile harcama miktarlarını ekleyiniz.		

3. Kurum strateji dokümanını ve BT stratejisini ekleyiniz.

4. Bilgi teknolojileri denetimi ile ilgili olarak aşağıdaki bilgileri doldurunuz

Unvan	Açıklama
Genel Yönetim	Bilgi işlem biriminin yönetiminden sorumlu kişi.
İletişim kurulacak kişi	Söz konusu alanla ilgili olarak denetim çalışmalarında iletişim kurulacak kişi

1- Yazılım

1. Kurum iş faaliyetlerini destekleyen uygulamaları ve özelliklerini lütfen aşağıdaki tabloaya ekleyiniz

Uygulama İsmi	Uygulamanın Açıklaması	İlgili Ana İş Süreci	Uygulamanın kaynağı*	Uzaktan / İnternet üzerinden erişim	Uygulama Platformu	Uygulama veritabanı (versiyonu ile)	Uygulamanın kurulu olduğu işletim sistemi (versiyonu ile)

2. Dış firmalardan tedarik edilen BT hizmetlerine ilişkin sözleşmeleri ekleyiniz

3. Planlanan, devam eden ve denetim dönemi içerisinde tamamlanmış BT program ve projelerinin listesini doldurunuz.

Projenin adı	Amacı	Planlanan Başlangıç Tarihi	Planlanan Bitiş Tarihi	Mevcut Durumu (Bulunduğu Aşama)

Uygulama kaynağı alanına aşağıdaki ifadelerden uygun olanına karşılık gelen harf yazılmalıdır:

K Kurum bünyesinde geliştirilmiştir
D Satın alınmış ve değiştirilmiştir
S Satın alınmış, ancak değiştirilmemiştir
Ü Üçüncü partilerin yönetimindedir

2 - Donanım

4. Bilgi sistemleri açıklamalı ağ topolojisini ekleyiniz (ağ mimari yapısı, ağ altyapısında kullanılan teknolojiler, anahtarlama ve yönlendiricilerin konumları vb.)

5. Kurum bilgi sistemleri altyapısının bulunduğu sistem odalarının konumları, şemaları ve ekipman listelerini ekleyiniz

6. Kurum sistem odaları yetki listelerini ekleyiniz

7. Kurum bünyesinde BT ile ilgili olarak kullanılan araçları lütfen aşağıdaki tabloda listeleyiniz

Kullanılma amacı	Model	Adet
Örn: Checkpoint firewall, Cisco IPS vs.		

3- Politika, prosedür ve raporlar

a. Değişiklik Yönetimi Prosedürü
b. Bilgi güvenliği politikası ve prosedürü
c. Kullanıcı Yetkilendirme Yönetimi Prosedürü
d. Şifre politikalarıyla ilgili prosedür
e. Zamanlanmış ve Toplu İşler Yönetimi Prosedürü (Batch Job)
f. Dosya Yedekleme Ve Geri Yükleme Prosedürü (Backup)
g. Sistem odası kullanımına ilişkin politika ve prosedürler
h. Problem yönetimi konusunda resmi prosedür
i. Elektronik Erişim Prosedürü
j. Zamanlanmış görevlerin tanımlanmasına ilişkin politika ve prosedürler
k. İş sürekliliği ve felaket kurtarma planları
l. Acil durum test değerlendirme raporu
m. Geçmiş dönem denetim raporları (İş sürekliliği, iç ve dış BS denetimleri)

Ek 2 – Risk Değerlendirme Formu

Ek 2.1 - Kurum Seviyesi Risk Değerlendirme Formu

Risk Unsurları	#	Risk Değerlendirme Konusu/Risk Faktörleri	Cevap
1) Stratejik etki	**1**	Kurum BT fonksiyonlarındaki muhtemel bir aksaklığın kamuoyu nezdinde Kurum itibarına etkisi	
	2	Kurum BT fonksiyonlarındaki muhtemel bir aksaklığın diğer kamu kuruluşlarıyla olan entegrasyona etkisi	
	3	Kurum BT fonksiyonlarındaki muhtemel bir aksaklığın kurumun stratejik hedeflerine etkisi	
	4	BT uygulamaları vasıtasıyla üretilen verilerin/raporların stratejik karar alma mekanizmalarındaki etkisi	
2) Hizmet/faaliyet	**5**	BT fonksiyonlarının Kurumun ana faaliyetlerinin yerine getirilebilmesi açısından önemi	
	6	BT hizmet sürekliliğinin Kurumun hizmet ve faaliyetlerinin sürekliliği açısından önemi	
	7	Kurumun BT hizmetlerinin vatandaşa sunulan hizmetlerin kalitesi açısından önemi	
3) Yasal uyum/ mevzuat	**8**	Kurumun ilgili faaliyet alanındaki yasal yükümlülüklerini karşılamada BT fonksiyonları ve altyapısının rolü	
	9	BT fonksiyonları ve altyapısından kaynaklanan mevzuat uyumsuzluklarının sıklığı	
	10	BT faaliyetlerinin daha önce iç ya da dış denetimden geçip geçmediği	
4) BT kaynakları	**11**	Kurum faaliyetlerinin desteklenmesi ve raporlama ihtiyaçlarının karşılanmasında BT otomasyonu kullanımı	
		Düşük: Kurum faaliyetleri ve raporlama ihtiyaçları büyük ölçüde manüel olarak karşılanmaktadır.	
		Orta: Kurum faaliyetleri ve raporlama ihtiyaçlarının bir bölümü BT otomasyonu ile gerçekleştirilmektedir	
		Yüksek: Kurum faaliyetleri ve raporlama ihtiyaçları tamamen BT otomasyonuna dayanmaktadır.	
	12	BT uygulama ve altyapıları üzerinden gerçekleştirilen yıllık işlem hacmi	
	13	BT uygulama ve altyapıları son kullanıcı sayısı	
	14	BT uygulama ve altyapılarının merkezi ya da dağıtık olma durumu (örn. taşra)	
	15	BT uygulama ve altyapılarına uzaktan erişim mevcut olup olmadığı	
	16	BT uygulama ve altyapıları üzerinde denetim dönemi içerisinde teknolojik dönüşüm (örn. ana sunucular) gerçekleşme durumu	
	17	Ana faaliyetleri destekleyen BT uygulama ve altyapıları arasındaki entegrasyonun seviyesi	
	18	BT hizmet ve altyapı yönetiminde üçüncü taraflara bağımlılık seviyesi (uygulama ve altyapı bileşenleri)	
	19	BT hizmetlerinde denetim dönemi içerisinde yaşanan kesintilerin oranı	
	20	BT süreçlerine ilişkin dokümantasyon seviyesi	
	21	BT uygulama ve altyapılarına yönelik kapasite ve performansın izlenme durumu	
	22	BT bütçesinin kurum bütçesi içerisindeki oranı	
	23	BT kaynaklı hataların mali etkisinin Kurum bünyesinde değerlendirilip değerlendirilmediği	
	24	BT kaynaklarının bilgi güvenliği açısından kuruma ifade ettiği değer	
		Gizlilik	
		Bütünlük	

		Erişilebilirlik	
5) Organizasyon yapısı	**25**	BT fonksiyonunun kurumun stratejik ihtiyaçlarına cevap vermek açısından bilgi, birikim, tecrübe seviyesi	
	26	Kritik BT faaliyetlerinin belirli BT personeline bağımlılık seviyesi	
	27	BT personelinin kurum içerisindeki ortalama kıdem seviyesi	
	28	BT hizmet ve altyapı yönetiminde üçüncü partilere bağımlılık seviyesi (faaliyetler açısından)	
	29	BT personelinin iç ve dış eğitim olanaklarından faydalanma düzeyi	
	30	BT personelinin performansının belirli göstergelere göre izlenip izlenmediği	
	31	BT personelinin rol ve sorumluluklarının dokümante edilip edilmediği	

Örnek Kurum Seviyesi Risk Değerlendirme Formu

	Risk Değerlendirme Konusu/Risk Faktörleri	Verilebilecek Cevaplar ve Ağırlıkları*						Soru Katsayısı**		
1)	**Stratejik etki**	**Cevap**	**Ağırlığı**	**Cevap**	**Ağırlığı**	**Cevap**	**Ağırlığı**	**Soru Katsayısı**	**Verilen Cevap (Örnek)**	**Puan (Örnek)**
1	Kurum BT fonksiyonlarındaki muhtemel bir aksaklığın kamuoyu nezdinde Kurum itibarına etkisi	Düşük	20%	Orta	60%	Yüksek	100%	4	Yüksek	4
2	Kurum BT fonksiyonlarındaki muhtemel bir aksaklığın diğer kamu kuruluşlarıyla olan entegrasyona etkisi	Düşük	20%	Orta	60%	Yüksek	100%	4	Yüksek	4
3	Kurum BT fonksiyonlarındaki muhtemel bir aksaklığın kurumun stratejik hedeflerine etkisi	Düşük	20%	Orta	60%	Yüksek	100%	4	Orta	2,4
4	BT uygulamaları vasıtasıyla üretilen verilerin/raporların stratejik karar alma mekanizmalarındaki etkisi	Düşük	20%	Orta	60%	Yüksek	100%	3	Yüksek	3
2)	**Hizmet/faaliyet**									
5	BT fonksiyonlarının Kurumun ana faaliyetlerinin yerine getirilebilmesi açısından önemi	Düşük	20%	Orta	60%	Yüksek	100%	7	Yüksek	7
6	BT hizmet sürekliliğinin Kurumun hizmet ve faaliyetlerinin sürekliliği açısından önemi	Düşük	20%	Orta	60%	Yüksek	100%	7	Yüksek	7
7	Kurumun BT hizmetlerinin vatandaşa sunulan hizmetlerin kalitesi açısından önemi	Düşük	20%	Orta	60%	Yüksek	100%	7	Yüksek	7
3)	**Yasal uyum/mevzuat**									
8	Kurumun ilgili faaliyet alanındaki yasal yükümlülüklerini karşılamada BT fonksiyonları ve altyapısının rolü	Düşük	10%	Orta	50%	Yüksek	100%	7	Yüksek	7
9	BT fonksiyonları ve altyapısından kaynaklanan mevzuat uyumsuzluklarının sıklığı	Düşük	10%	Orta	50%	Yüksek	100%	7	Yüksek	7
10	BT faaliyetlerinin daha önce iç ya da dış denetimden geçip geçmediği	Evet	0%	Hayır	100%			4	Evet	0
4)	**BT kaynakları**									
11	Kurum faaliyetlerinin desteklenmesi ve raporlama ihtiyaçlarının karşılanmasında BT otomasyonu kullanımı Düşük: Kurum faaliyetleri ve raporlama ihtiyaçları büyük ölçüde manüel olarak karşılanmaktadır. Orta: Kurum faaliyetleri ve raporlama ihtiyaçlarının bir bölümü BT otomasyonu ile gerçekleştirilmektedir Yüksek: Kurum faaliyetleri ve raporlama ihtiyaçları tamamen BT otomasyonuna dayanmaktadır.	Yok	20%	Kısmen	60%	Var	100%	3	Kısmen	1,8
12	BT uygulama ve altyapıları üzerinden gerçekleştirilen yıllık işlem hacmi	<1 Milyon	20%	1 Milyon 10 Milyon	60%	>10 Milyon	100%	2	1 Milyon 10 Milyon	1,2
13	BT uygulama ve altyapıları son kullanıcı sayısı	<600	20%	600 - 4750	60%	>4750	100%	2	600 - 4750	1,2
14	BT uygulama ve altyapılarının merkezi ya da dağıtık olma durumu (örn. taşra)	Merkezi	0%	Dağıtık	100%			2	Merkezi	0
15	BT uygulama ve altyapılarına uzaktan erişim mevcut olup olmadığı	Hayır	0%	Evet	100%			1	Evet	1
16	BT uygulama ve altyapıları üzerinde denetim dönemi içerisinde teknolojik dönüşüm (örn. ana sunucular,) gerçekleşme durumu	Hayır	0%	Evet	100%			2	Evet	2
17	Ana faaliyetleri destekleyen BT uygulama ve altyapıları arasındaki entegrasyonun seviyesi	Yok	20%	Kısmen	60%	Var	100%	2	Kısmen	1,2
18	BT hizmet ve altyapı yönetiminde üçüncü taraflara bağımlılık seviyesi (uygulama ve altyapı bileşenleri)	Düşük	20%	Orta	60%	Yüksek	100%	2	Yüksek	2
19	BT hizmetlerinde denetim dönemi içerisinde yaşanan kesintilerin oranı	Düşük	20%	Orta	60%	Yüksek	100%	2	Yüksek	2
20	BT süreçlerine ilişkin dokümantasyon seviyesi	Yok	100%	Kısmen	60%	Var	20%	2	Kısmen	1,2
21	BT uygulama ve altyapılarına yönelik kapasite ve performansının izlenme durumu	Yok	100%	Kısmen	60%	Var	20%	2	Kısmen	1,2
22	BT bütçesinin kurum bütçesi içerisindeki oranı	<%1	20%	%1-%4	60%	>%4	100%	2	<%1	0,4
23	BT kaynaklı hataların mali etkisinin Kurum bünyesinde değerlendirilip değerlendirilmediği	Evet	0%	Hayır	100%			2	Hayır	2
24	BT kaynaklarının bilgi güvenliği açısından kuruma ifade ettiği değer									
	Gizlilik	Düşük	20%	Orta	60%	Yüksek	100%	2	Yüksek	2
	Bütünlük	Düşük	20%	Orta	60%	Yüksek	100%	2	Yüksek	2
	Erişilebilirlik	Düşük	20%	Orta	60%	Yüksek	100%	2	Yüksek	2
5)	**Organizasyon yapısı**									
25	BT fonksiyonunun kurumun stratejik ihtiyaçlarına cevap vermek açısından bilgi, birikim, tecrübe seviyesi	Yeterli	0%	Yetersiz	100%			2	Yeterli	0
26	Kritik BT faaliyetlerinin belirli BT personeline bağımlılık seviyesi	Düşük	20%	Orta	60%	Yüksek	100%	2	Yüksek	2
27	BT personelinin kurum içerisindeki ortalama kıdem seviyesi	<2 yıl	20%	2-6 yıl	60%	>6 yıl	100%	2	>6 yıl	2
28	BT hizmet ve altyapı yönetiminde üçüncü partilere bağımlılık seviyesi (faaliyetler açısından)	Düşük	20%	Orta	60%	Yüksek	100%	2	Yüksek	0,4
29	BT personelinin iç ve dış eğitim olanaklarından faydalanma düzeyi	Düşük	100%	Orta	60%	Yüksek	20%	2	Yüksek	0,4
30	BT personelinin performansının belirli göstergelere göre izlenip izlenmediği	Yok	100%	Kısmen	60%	Var	20%	2	Kısmen	1,2
31	BT personelinin rol ve sorumluluklarının dokümante edilip edilmediği	Yok	100%	Kısmen	60%	Var	20%	2	Kısmen	1,2
								100		

Risk Notu***
19,7

* Bir cevabın ağırlığı 1'i geçemez

** Soru katsayılarının toplamı 100'ü geçmemelidir

*** Ortaya çıkan toplamın 4'e bölünmesi ile elde edilir. Puanlama için bkz. Şekil 3

Ek 2.2 - Uygulama Seviyesi Risk Değerlendirme Formu Soruları

#	Uygulamalar için risk değerlendirme soruları	Cevap
1	Uygulamanın mali hesapların oluşumu, finansal tabloların güncellenmesi ve finansal raporlama açısından önem derecesi	
2	Uygulamanın kurumun ana faaliyet alanlarına ve iş süreçlerine olan destek seviyesi	
3	Uygulamanın kurumun hizmet ve faaliyetlerine olan etkisi	
4	Uygulamanın vatandaşa sunulan hizmetler açısından kritiklik derecesi	
5	Uygulamanın Kurumun faaliyetleri ve raporlamaları açısından sağladığı otomasyon seviyesi	
6	Uygulama üzerinden gerçekleştirilen işlem hacmi	
7	Uygulama üzerinde tanımlı kullanıcı sayısı	
8	Uygulama altyapısının ve yönetiminin merkezi ya da dağınık olma durumu (örn. taşra)	
9	Uygulamaya uzaktan erişim mevcut olup olmadığı	
10	Uygulamaya ilişkin yıllık karşılaşılan hata/problem sayısı	
11	Uygulama üzerinde denetim dönemi içerisinde teknolojik dönüşüm (örn. ana sunucular,) gerçekleşme durumu	
12	Uygulama üzerinde denetim dönemi içerisinde gerçekleşen değişiklik sıklığı	
13	Uygulamanın yönetiminde üçüncü partilere bağımlılık seviyesi	
14	Uygulama üzerinde denetim dönemi içerisinde yaşanan kesintilerin oranı	
15	Uygulamanın programlama dili ve altyapısı (veritabanı vs.) açısından güncel teknolojilerin takip edilip edilmediği	
16	Uygulamanın bilgi güvenliği açısından kuruma ifade ettiği değer	
	Gizlilik	
	Bütünlük	
	Erişilebilirlik	

Uygulama Seviyesi Risk Değerlendirme Formu

#	Uygulamalar için risk değerlendirme soruları	Verilebilecek Cevaplar ve Ağırlıkları*						Soru Katsatyısı*	Uygulama (Örnek)	
		Cevap	Ağırlığı	Cevap	Ağırlığı	Cevap	Ağırlığı		Verilen Cevap (Örnek)	Puan (Örnek)
1	Uygulamanın mali hesapların oluşumu, finansal tabloların güncellenmesi ve finansal raporlama açısından önem derecesi	Düşük	20%	Orta	60%	Yüksek	100%	7	Orta	4,2
2	Uygulamanın kurumun ana faaliyet alanlarına ve iş süreçlerine olan destek seviyesi	Düşük	20%	Orta	60%	Yüksek	100%	7	Orta	4,2
3	Uygulamanın kurumun hizmet ve faaliyetlerine olan etkisi	Düşük	20%	Orta	60%	Yüksek	100%	6	Orta	3,6
4	Uygulamanın vatandaşa sunulan hizmetler açısından kritiklik derecesi	Düşük	20%	Orta	60%	Yüksek	100%	7	Orta	4,2
5	Uygulamanın Kurumun faaliyetleri ve raporlamaları açısından sağladığı otomasyon seviyesi	Düşük	20%	Orta	60%	Yüksek	100%	5	Orta	3
6	Uygulama üzerinden gerçekleştirilen işlem hacmi	Düşük	20%	Orta	60%	Yüksek	100%	5	Orta	3
7	Uygulama üzerinde tanımlı kullanıcı sayısı	Düşük	20%	Orta	60%	Yüksek	100%	5	Orta	3
8	Uygulama altyapısının ve yönetiminin merkezi ya da dağınık olma durumu (örn. taşra)	Merkezi	0%	Dağınık	100%			5	Merkezi	0
9	Uygulamaya uzaktan erişim mevcut olup olmadığı	Hayır	0%	Evet	100%			5	Evet	5
10	Uygulamaya ilişkin yıllık karşılaşılan hata/problem sayısı	Düşük	20%	Orta	60%	Yüksek	100%	5	Orta	3
11	Uygulamaya üzerinde denetim dönemi içerisinde teknolojik dönüşüm (örn. ana sunucular,) gerçekleşme durumu	Hayır	0%	Evet	100%			7	Evet	7
12	Uygulama üzerinde denetim dönemi içerisinde gerçekleşen değişiklik sıklığı	Düşük	20%	Orta	60%	Yüksek	100%	5	Orta	3
13	Uygulamanın yönetiminde üçüncü partilere bağımlılık seviyesi	Düşük	20%	Orta	60%	Yüksek	100%	7	Orta	4,2
14	Uygulama üzerinde denetim dönemi içerisinde yaşanan kesintilerin oranı	Düşük	20%	Orta	60%	Yüksek	100%	7	Orta	4,2
15	Uygulamanın programlama dili ve altyapısı (veritabanı vs.) açısından güncel teknolojilerin takip edilip edilmediği	Evet	0%	Hayır	100%			5	Evet	0
16	Uygulamanın bilgi güvenliği açısından kuruma ifade ettiği değer									0
	Gizlilik	Düşük	20%	Orta	60%	Yüksek	100%	4	Orta	2,4
	Bütünlük	Düşük	20%	Orta	60%	Yüksek	100%	4	Orta	2,4
	Erişilebilirlik	Düşük	20%	Orta	60%	Yüksek	100%	4	Orta	2,4
								100		

Risk Notu***
14,7

* Bir cevabın ağırlığı 1'i geçemez

** Soru katsayılarının toplamı 100'ü geçmemelidir

*** Ortaya çıkan toplamın 4'e bölünmesi ile elde edilir. Puanlama için bkz. Şekil 4

Ek 3 – Örnek Teknoloji Envanteri Formu

Uygulama İsmi	Uygulamanın Açıklaması	İlgili Ana İş Süreci	Bilgi Sistemi Donanımı/Platformu	İşletim sistemi ve versiyonu	Veritabanı ve versiyonu	Uygulamanın kaynağı*	Uzaktan / İnternet üzerinden erişim	Açıklamalar	Sistem Sahibi	Ünvanı	Bölümü/Departmanı	Telefon	E-Posta
CA IDM	Kimlik yönetimi uygulaması	BT	SUN Tesla	Sun Solaris 11.1	Oracle 8.0	P	E		Ahmet Öztürk	Sistem Yöneticisi	Sistem ve Ağ	1111	ahmet.ozturk@abc.gov.tr

Ek 4 – Örnek Çalışma Kâğıdı

Denetlenen süreç	İlgili birim	Süreç kontrolü	Denetim testi	Denetim testi	Kontrol Frekans	Üzerinden gitme (ÜG)	Test	Sonuç	Bulgu	Gözden Geçirme
Değişiklik Yönetimi	BT Değişiklik ve Konfigürasyon Yönetimi	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.	K1.T1	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.	Yıllık	***Gerçekleştiren:*** Ahmet Öztürk ***Tarih:*** 05.06.2014 ***Popülasyon:*** 1 ***Örnek (Yöntem ve Büyüklük):*** 1 ***ÜG açıklama: (ÜG nasıl yapıldı ve ne görüldü?)*** Kurum BT Değişiklik Yönetimi Prosedürü temin edilmiş ve Kurum bünyesinde kullanılmakta olan uygulamalara ilişkin onlarak izlenmesi gereken değişiklik yönetimi sürecini anlattığı gözlemlenmiştir. Ek olarak altyapı değişiklikleri için Altyapı Değişiklik Yönetimi Prosedürü dokümanının hazırlandığı gözlemlenmiş, dokümanda yapılacak altyapı değişiklikleri ile ilgli olarak yapılması gerekenlere yer verildiği görülmüştür. ***ÜG kanıt: (Açıklayıcı şekilde isim verip ilgili dokümanlara referans veriniz)*** BT.001 BT Değişiklik Yönetimi Prosedürü BT.002 Altyapı Değişiklik Yönetimi Prosedürü	Üzerinden gitme çalışması bu kontrol için test yerine de geçmektedir.	ÜG Etkin / Test Etkin	-	***Gerçekleştiren:*** Can Ünver ***Tarih:*** 10.06.2014
Yardım Masası, Olay ve Problem Yönetimi	BT Yardım Masası	Olaylarla ilgili tanımlanmış çözüm ya da geçici çözümler belgelendirilir, uygulanır ve kayıt altına alınır. İlgili BT hizmetinin tekrar devreye alınması için gerekli işlemler yapılır.	K4.T2	Seçilen örnek olayların çözümlenmesinde kullanılan geçici çözümlerin kayıt altına alındığı ve takip edildiği gözlemlenir.	Diğer	***Gerçekleştiren:*** Burhan Topel ***Tarih:*** 06.06.2014 ***Popülasyon:*** 1565 ***Örnek:*** *1* ***ÜG açıklama:*** Denetim dönemi boyunca gerçekleşmiş olaylar arasından örnek olarak seçilen 346872 numaralı çağrı için gerçekleştirilen çözümün kayıt altına alındığı gözlemlenmiştir. ***ÜG kanıt:*** BT.015 Çağrı Listesi BT.016 346872 Numaralı Çağrı Görüntüsü	***Gerçekleştiren:*** Burhan Topel ***Tarih:*** 06.06.2014 ***Popülasyon:*** 1565 ***Örneklem:*** *25* ***Test açıklama:*** *Gerçekleştirilen incelemede rassal olarak seçilen örneklem içerisinde yer alan 3 örnek için (346958, 345416, 345492)olay çözümlerinin kaydedilmediği gözlemlenmiştir.* ***Test kanıt:*** BT.017 Olay Yönetimi Testleri	ÜG Etkin/ Test Etkin Değil	*Kurum bünyesinde Olay Yönetimi sürecinde çözümlenen olayların tümünün çözümlenme şekillerinin kaydedilmediği gözlemlenmiştir.*	***Gerçekleştiren:*** Can Ünver ***Tarih:*** 10.06.2014

REHBERİN HAZIRLANMASINDA ROL ALANLAR (alfabetik sıraya göre)

Adı ve Soyadı	**Kurumu**	**Unvanı**
REHBER HAZIRLAMA EKİBİ		
Can ÜNVER, CISA	EY	BT Denetçisi
Emre BEŞLİ, CISA, CGEIT, CRISC, CRMA, ISO 27001 LA	EY	BT Denetçisi
Serdar MERCAN	EY	BT Denetçisi
Ümit ŞEN, CISA, CISSP, CRMA, ISO 27001 LA	EY	BT Denetçisi
REHBERİN HAZIRLANMASINA KATKIDA BULUNANLAR		
Ateş SÜNBÜL, CISA, ISO 27001 LA	EY	BT Denetçisi
Cüneyt GÜLER	Maliye Bakanlığı	Daire Başkanı
Halis KIRAL, CIA, CCSA, CGAP	Maliye Bakanlığı İDMU Dairesi	Maliye Uzmanı
Hasan ERKEN, CISA	Hazine Müsteşarlığı	İç Denetçi
Nazlı Ebru ÇİÇEKDAĞI	EY	BT Denetçisi
Nilhan FİDAN, CISA, CRISC, ISO 27001 LA	EY	BT Denetçisi
Onur GÜNEŞ	Maliye Bakanlığı İDMU Dairesi	Sözleşmeli Bilişim Uzmanı
Orhan İNCEKARA	EY	BT Denetçisi
Yezdan SALİH	EY	BT Denetçisi
REHBERİ GÖZDEN GEÇİRENLER		
Burak Baysal, CISA, ISO 27001 LA	EY	BT Denetçisi
Sönmez Ateş	EY	BT Denetçisi
GÖRÜŞLERİYLE KATKI YAPANLAR		
Abdullah Erdem İŞBİLİR	İstanbul Büyükşehir Belediyesi	İç Denetçi
Ahmet Bora ÖZTEKİN, CGAP	Milli Savunma Bakanlığı	İç Denetçi
Ahmet KEBELİ, CGAP	Spor Genel Müdürlüğü	İDB Başkanı
Alpaslan MENEVŞE, CISA, CRISC, LT C31000	Şekerbank	Yönetmen
Altan YILMAZ	DSİ Genel Müdürlüğü	İç Denetçi
Bakır GÖKALP	DSİ Genel Müdürlüğü	İç Denetçi
Çağrı CANCANOĞLU	Maliye Bakanlığı İDMU Dairesi	Maliye Uzmanı
Evren Güncel ERMİSKET, CGAP	Aile ve Sosyal Politikalar Bakanlığı	İç Denetçi
Fergün SİPER	Maliye Bakanlığı İDMU Dairesi	Çözümleyici
Gökhan MACİT, CIA	Karayolları Genel Müdürlüğü	İç Denetçi
H.Alpay KARASOY	Aksaray Üniversitesi	Yrd.Doç.Dr.
M. Hulusi GÜNŞEN	İzmir Büyükşehir Belediyesi	İç Denetçi
M. Murat COŞKUN, CGAP	Ege Üniversitesi	İç Denetçi
Murat Sami BAYKIZ	Jandarma Genel Komutanlığı	İç Denetçi
Ozan ALKAN	Maliye Bakanlığı İDMU Dairesi	Maliye Uzmanı
Şerif Olgun ÖZEN, CGAP	Çalışma ve Sosyal Güvenlik Bakanlığı	İDB Başkanı