benzersor

Bilgi Sistemi Bağımsız Denetim

DERS NOTLARI 2026 BASKISI

SPL BİLGİ SİSTEMLERİ BAĞIMSIZ DENETİM

33 Konuluk Ders Notları

SPL Bilgi Sistemleri Bağımsız Denetim konularının tamamı için benzersor'un hazırladığı özgün konu anlatımı notları.

KİTAPÇIK	
Ders / bölüm	5
Konu anlatımı	33
Kelime	12.374

KAPSAM
Sınav konu listesinin tamamı
Özgün benzersor anlatımı
Resmî kurum yayını değildir

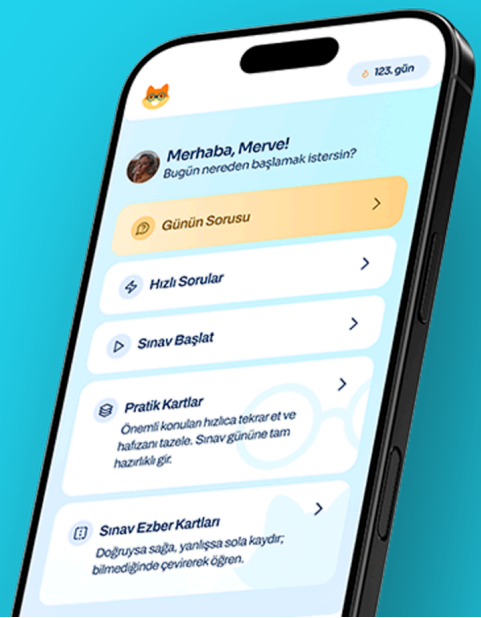
Konu Anlatımı ve Soru

Cebinde!

benzersor uygulamasında bu konuların anlatımını dinleyebilir, her konudan soru çözebilir ve gerçek sınav simülasyonuna girebilirsin.

App Store'dan İndirin

İNDİRİN Google Play



Bu kitapçık hakkında

SPL Bilgi Sistemleri Bağımsız Denetim ders notları · 2026 baskısı · 33 konu

Bu kitapçık nedir?

Bu kitapçık benzersor'un hazırladığı **özgün çalışma notudur**. Konu anlatımlarının tamamı benzersor tarafından yazılmıştır; hiçbir kaynaktan olduğu gibi alınmamıştır. Amacı sınava hazırlanan adaya konuyu bütünlüklü bir anlatımla aktarmaktır.

Resmî bir yayın değildir

Bu belge ÖSYM, SPL (Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu), Diyanet İşleri Başkanlığı, TÜRMOB/TESMER veya sınavı düzenleyen başka bir kurumun yayını değildir; hiçbir resmî geçerliliği yoktur. Kitapçıkta yer alan hiçbir ifade, ilgili kurumların resmî görüşü olarak okunamaz.

Hangi kaynaklara dayanılarak yazıldı?

Anlatımlar aşağıdaki kaynaklara dayanılarak, özgün metin olarak yazılmıştır. Bir çelişki durumunda bağlayıcı olan bu kitapçık değil, aşağıdaki resmî kaynakların güncel metinleridir:

- SPL (Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.) lisanslama sınavı çalışma notları

Kapsam ve mevzuat değişir

Bu baskı **29 Temmuz 2026** tarihinde üretilmiştir ve içeriği o tarihteki sınav konu listesine ve mevzuata dayanır. Sınav kapsamı, konu ağırlıkları ve mevzuat değişebilir; çalışmadan önce sınavı düzenleyen kurumun yürürlükteki kılavuzunu ve ilgili mevzuatın güncel metnini mutlaka kontrol et.

Hata bildirimi

Kitapçıkta bir hata gördüysen **destek@benzersor.com** adresine yazarak bildirebilirsin; düzeltilen içerik bir sonraki baskıya işlenir.

Kapsam

#	DERS / BÖLÜM	YAZILAN / TOPLAM KONU
1	Dar Kapsamlı Sermaye Piyasası Mevzuatı ve Meslek Kuralları	6/6
2	Bilgi Sistemleri Yönetimi ve Denetimi	9/9
3	Bilgi Sistemleri Geliştirilmesi ve Uygulanması	5/5
4	Bilgi Sistemleri İşletimi	6/6
5	Bilgi Sistemleri Güvenliği	7/7

Bu kitapçık, sınav konu listesindeki tüm başlıkları kapsar.

İçindekiler

1.1 · Sermaye Piyasası Kanunu

6362 Sayılı Kanunun Sermaye Piyasası Düzenindeki Yeri

> **KISACA**
> 6362 sayılı Sermaye Piyasası Kanunu, tasarrufların sermaye piyasası araçları yoluyla fon ihtiyacı olan kesimlere aktarılmasını düzenleyen ana çerçevedir. Kanun; ihraççı, yatırımcı, sermaye piyasası aracı, sermaye piyasası kurumu, borsa, merkezi saklama, merkezi takas, kamuyu aydınlatma, Kurul denetimi ve yaptırımlar gibi piyasanın temel yapı taşlarını bir bütün halinde ele alır. Sermaye piyasasında yatırımcı koruması çoğunlukla tam, doğru ve zamanında bilgilendirme üzerine kurulur. Bu nedenle Kanun, bir yandan araçların ihracı ve işlem görmesini düzenlerken diğer yandan SPK'ya ikincil düzenleme, gözetim, tedbir ve yaptırım yetkileri verir.

6362 sayılı Sermaye Piyasası Kanunu, sermaye piyasasının hangi aktörlerle, hangi araçlarla ve hangi denetim düzeni içinde çalışacağını belirleyen temel kanundur. Sermaye piyasası, orta ve uzun vadeli fonların sermaye piyasası araçlarının alım satımı yoluyla tasarruf sahiplerinden fon talep edenlere aktarılmasını sağlar. Bu ilişki, bankacılık aracılığına göre daha doğrudan bir finansman bağlantısı kurar; ihraççı kaynak toplar, yatırımcı getiri beklentisiyle aracı satın alır ve ortaya ortaklık ya da borç-alacak niteliğinde bir hukuki ilişki çıkar.

Kanun sermaye piyasasını birincil ve ikincil piyasa ayrımıyla anlamlandırır. Birincil piyasa, sermaye piyasası araçlarının ihraççı tarafından ilk kez satıldığı alandır ve reel kesime kaynak aktarımı burada gerçekleşir. İkincil piyasa ise daha önce ihraç edilmiş araçların yatırımcılar arasında el değiştirdiği alandır. İkincil piyasa ihraççıya doğrudan yeni fon sağlamasa da likidite yaratır, fiyat oluşumuna yardımcı olur ve birincil piyasadaki ihraç koşullarını etkiler. Bu nedenle sermaye piyasasının sağlıklı işleyişi yalnız ihraç anına değil, araçların sonradan güvenli ve şeffaf biçimde işlem görebilmesine de bağlıdır.

Kanunun merkezindeki unsurlar ihraççılar, yatırımcılar, sermaye piyasası araçları, yardımcı kuruluşlar ve borsalardır. İhraççı, sermaye piyasası aracı ihraç eden, ihraç için Kurula başvuran veya araçları halka arz edilen tüzel kişiler ile yatırım fonlarını kapsar. Yatırımcılar tasarruflarını sermaye piyasası araçlarında değerlendiren gerçek veya tüzel kişilerdir; bireysel, kurumsal ya da nitelikli yatırımcı gibi farklı gruplara ayrılmaları, korunma düzeylerinin farklılaşmasına hizmet eder. Sermaye piyasası araçları ise menkul kıymetler, türev araçlar ve Kurulca bu kapsamda kabul edilen diğer araçları içine alan üst kavramdır.

Kanun çerçeve kanun niteliği taşır. Ana ilkeleri ve yetki sınırlarını belirler, ayrıntılı düzenlemeyi uzman otorite olan Sermaye Piyasası Kuruluna bırakır. Bu yapı Kurula yönetmelik, tebliğ ve ilke kararı çıkarma; başvuruları değerlendirme; piyasa düzenini bozabilecek fiillerde tedbir alma, idari yaptırım uygulama ve suç oluşturan hallerde ilgili mercilere başvurma yetkisi verir. Sermaye piyasası mevzuatı bu nedenle yalnız özel hukuk ilişkilerini düzenlemez; aynı zamanda kamusal gözetim ve düzenleme boyutu da taşır.

Kamuyu aydınlatma Kanunun yatırımcı koruma anlayışının temelidir. Halka arzda izahname, halka arz edilmeksizin ihraçta ihraç belgesi, sürekli ve özel durum açıklamaları, finansal raporlama ve bağımsız

denetim yükümlülükleri yatırımcının bilgiye dayalı karar verebilmesi için kurulur. Bu sistem yatırımcıya sonucu garanti etmez; fakat kararın eksik, yanlış veya gecikmiş bilgiyle verilmesini önlemeyi amaçlar. Kanunun bütününe bakıldığında düzen, piyasa araçlarını tanımlayan, ihraç sürecini kurala bağlayan, aracı kurumları ve altyapı kuruluşlarını yetkilendiren, borsaları düzenleyen ve Kurulu gözetim merkezi haline getiren bir piyasa mimarisi olarak okunmalıdır.

1.2.1 · Özel Durumlar Tebliği II-15.1

Özel Durum Açıklamalarında İçsel Bilgi, Sürekli Bilgi ve Kamuyu Aydınlatma

KISACA

Özel Durumlar Tebliği II-15.1, yatırımcıların zamanında, tam ve doğru bilgilendirilmesini sağlayarak sermaye piyasasının güvenilir, şeffaf, etkin, istikrarlı, adil ve rekabetçi biçimde işlemesini hedefler. Tebliğ, sermaye piyasası araçlarının değerini, fiyatını veya yatırım kararlarını etkileyebilecek bilgi, olay ve gelişmelerin kamuya açıklanmasına ilişkin usul ve esasları düzenler. Özel durumlar içsel bilgi ve sürekli bilgi olarak ikiye ayrılır. İçsel bilgi henüz kamuya açıklanmamış ve yatırım kararını etkileyebilecek nitelikte bilgidir; sürekli bilgi ise içsel bilgi dışında kalan açıklama konularını kapsar. Açıklamalar hızlı, eşit erişilebilir, yanıltıcı olmayan ve güncel olmalıdır.

Özel Durumlar Tebliği II-15.1, sermaye piyasasında kamuyu aydınlatma düzeninin günlük işleyişini kuran ana metinlerden biridir. Tebliğin amacı, yatırımcıların zamanında, tam ve doğru bilgilendirilmesi yoluyla piyasanın güvenilir, şeffaf, etkin, istikrarlı, adil ve rekabetçi ortamda çalışmasını sağlamaktır. Bu amaç, sermaye piyasası araçlarının değerini, fiyatını veya yatırımcıların yatırım kararlarını etkileyebilecek bilgi, olay ve gelişmelerin kamuya açıklanmasını gerektirir. Böylece yatırımcılar yalnız finansal rapor dönemlerinde değil, fiyatı ve kararı etkileyebilecek önemli gelişmeler ortaya çıktığında da bilgilendirilir.

Tebliğ özel durumları içsel bilgi ve sürekli bilgi ayrımıyla ele alır. İçsel bilgi, kamuya henüz duyurulmamış olmasına rağmen aracın değeri, piyasa fiyatı veya yatırımcının alım satım kararı üzerinde anlamlı etki yaratabilecek bilgi ve gelişmeleri ifade eder. Sürekli bilgi ise içsel bilgi tanımının dışında kalan fakat kamuyu aydınlatma düzeni içinde açıklanması gereken bilgi, olay ve gelişmeleri ifade eder. Bu ayrım önemlidir, çünkü içsel bilgi zamanında açıklanmadığında yatırımcılar arasında bilgi eşitsizliği doğabilir ve piyasa fiyatı sağlıklı oluşmayabilir.

Açıklama yükümlülüğünün yerine getirilmesinde hız ve eşit erişim esastır. Açıklamalar yatırımcılar arasında eşit işlem ilkesini zedelemeyecek şekilde yapılmalı; yanlış, yanıltıcı, temelsiz, abartılı veya eksik olmamalıdır. İhraççının mevcut koşulları hakkında yatırımcıların yanlış fikir edinmesine yol açabilecek ifadelerden kaçınılır. Özel durum hakkında bilgi sahibi olan kişiler, bilgi kamuya duyurulana kadar gizliliği korumakla yükümlüdür. Kurul, açıklamalar için rehber hazırlayabilir ve gerekli gördüğünde ihraççıdan ya da ilgili taraflardan açıklama yapılmasını isteyebilir.

İçsel bilgilerin açıklanması bazı durumlarda ertelenebilir. İhraççı, sorumluluğu kendisine ait olmak üzere, meşru çıkarlarının zarar görmemesi, yatırımcıların yanıltılmaması ve bilginin gizli tutulabilmesi koşulları birlikte sağlanıyorsa açıklamayı erteleyebilir. Erteleme sebebi ortadan kalktığında bilgi açıklanır ve açıklamada erteleme kararı ile bunun dayanakları belirtilir. Kurul, erteleme gerekçesinin yerinde olup olmadığını inceleyebilir. Gizlilik sağlanamazsa veya ertelenen bilgi haber ya da söylenti yoluyla piyasaya yansırsa açıklama yükümlülüğü yeniden gündeme gelir.

Tebliğ içsel bilgilere erişimi olan kişilerin izlenmesini de düzenler. İhraççılar, iş akdiyle veya başka biçimde kendilerine bağlı çalışan ve içsel bilgilere düzenli erişimi olan kişileri Merkezi Kayıt Kuruluşuna bildirir; değişiklikleri süresi içinde günceller. Ayrıca olağan piyasa koşullarıyla açıklanamayan fiyat veya işlem hacmi hareketleri, haber ve söylentiler, idari sorumluluğu bulunan kişilerin ya da ana ortakların belirli işlemleri ve önceden yapılmış açıklamalardaki gelişmeler kamuyu aydınlatma sorumluluğunu doğurabilir. Bu düzen, özel durum açıklamasını yalnız şekli bir bildirim değil, piyasa bütünlüğünü ve yatırımcıların bilgi eşitliğini koruyan dinamik bir şeffaflık mekanizması haline getirir.

1.2.2 · Kurumsal Yönetim Tebliği II-17.1

Kurumsal Yönetim İlkeleri, Uyum Raporlaması ve SPK Gözetimi

KISACA

Kurumsal Yönetim Tebliği II-17.1, halka açık ortaklıklarda yönetim yapısının şeffaf, adil, sorumlu ve hesap verebilir biçimde kurulmasına yönelik kurumsal yönetim çerçevesini düzenler. Tebliğ; ortaklıkların gruplandırılmasını, zorunlu ilkelere uyumu, istisnaları, bağımsız yönetim kurulu üyeliğini, yatırımcı ilişkileri bölümünü, ilişkili taraf işlemlerini ve kurumsal yönetim raporlamasını birlikte ele alır. Gönüllü ilkelerde uygula-uygulamıyorsan açıkla yaklaşımı kullanılır; Kurumsal Yönetim Uyum Raporu ve Kurumsal Yönetim Bilgi Formu aracılığıyla uyum durumu KAP üzerinden görünür hale gelir. SPK, zorunlu ilkelere uyumu sağlamak için gözetim ve müdahale yetkilerine sahiptir.

Kurumsal Yönetim Tebliği II-17.1, sermaye piyasasında işlem gören halka açık ortaklıkların yönetim yapısını, pay sahipleriyle ilişkisini, kamuyu aydınlatma davranışını ve menfaat sahiplerine karşı hesap verebilirliğini güçlendirmek için kullanılan temel düzenlemelerden biridir. Tebliğ, kurumsal yönetim ilkelerinin hangi ortaklıklara nasıl uygulanacağını, hangi ilkelerin zorunlu olduğunu, hangi durumlarda istisna tanınabileceğini ve uyum durumunun nasıl raporlanacağını açıklar. Amaç, şirket yönetiminin şeffaf, adil, sorumlu ve hesap verebilir şekilde yürütülmesidir.

Tebliğ kapsamındaki ortaklıklar sistemik önemlerine göre gruplara ayrılır. Bu gruplandırmada piyasa değeri ve fiili dolaşımdaki payların piyasa değeri dikkate alınır. Ortaklığın grubu, hangi kurumsal yönetim ilkelerine zorunlu olarak tabi olacağını etkiler. Tüm gruplar için geçerli zorunlu ilkeler bulunur; birinci grup ortaklıklar bazı ek yükümlülüklere tabi olabilir. Payları ilk defa halka arz edilen veya borsada işlem görmeye başlayan ortaklıklar, Kurul tarafından grupları ilan edilene kadar üçüncü grup yükümlülükleriyle değerlendirilir ve ilk genel kurul tarihi itibarıyla gerekli uyumu sağlamalıdır.

Kurumsal yönetim raporlamasında gönüllü ilkeler bakımından uygula-uygulamıyorsan açıkla yaklaşımı kullanılır. Şirketler Kurumsal Yönetim Uyum Raporu ile gönüllü ilkelere uyum durumunu; Kurumsal Yönetim Bilgi Formu ile mevcut uygulamalarına ilişkin verileri KAP üzerinden açıklar. Uyum yoksa ya da kısmi uyum varsa bunun gerekçesi, riskleri azaltan alternatifler, zamanla sınırlı olup olmadığı ve gelecekte uyum niyeti açıklanmalıdır. Yıllık faaliyet raporunda kurumsal yönetime ilişkin anlatı bölümü ve gerekli beyanlar yer almaya devam eder.

Tebliğ yalnızca raporlama metni değildir; SPK'ya uyumun sağlanması için geniş gözetim ve müdahale araçları tanır. Zorunlu ilkelere uyulmaması halinde Kurul uyumu sağlayacak kararlar alabilir, dava veya ihtiyati tedbir yoluna başvurabilir ve belirli koşullarda bağımsız yönetim kurulu üyelerinin atanmasını sağlayabilir. Yatırımcı ilişkileri bölümü, pay sahipleriyle yazışmaların düzenli tutulması, bilgi taleplerinin yanıtlanması, genel kurul hazırlıkları ve sermaye piyasası mevzuatından doğan yükümlülüklerin izlenmesi bakımından önemli bir işleve sahiptir. Denetim açısından bu konu, şirket yönetimi ile kamuyu aydınlatma sorumluluklarının somut kayıt ve süreçlerle desteklenip desteklenmediğini gösterir.

1.2.3 · Yatırım Fonlarına İlişkin Esaslar Tebliği III-52.1

Yatırım Fonlarının Kuruluşu, Malvarlığı ve Şemsiye Fon Yapısı

KISACA

Yatırım Fonlarına İlişkin Esaslar Tebliği III-52.1, yatırım fonunun kuruluşunu, şemsiye fon yapısını, fon malvarlığının ayrılığını, portföy yönetimi ve saklama esaslarını, fon türlerini, bilgilendirme dokümanlarını ve yatırımcıyı koruyan temel sınırları düzenler. Yatırım fonu, katılma payı karşılığında toplanan varlıkların yatırımcılar hesabına portföy yönetim şirketi tarafından yönetildiği ayrı bir malvarlığıdır. Fonun tüzel kişiliği yoktur; buna rağmen fon malvarlığı kurucu, yönetici ve saklayıcı malvarlığından ayrıdır. Bu ayrım, haciz, rehin, teminat, iflas masasına dahil olma ve mahsup gibi risklere karşı yatırımcı korumasının merkezinde yer alır.

Yatırım fonu, tasarruf sahiplerinden katılma payı karşılığında toplanan para veya diğer varlıklarla, yatırımcılar hesabına portföy işletmek üzere portföy yönetim şirketi tarafından içtüzükle kurulan malvarlığıdır. Fonun tüzel kişiliği yoktur; buna rağmen fon malvarlığı kurucu ve portföy saklayıcısının malvarlığından ayrıdır. Bu ayrılık yatırımcıların korunması açısından temel ilkedir. Fon izahnamesi ve yatırımcı bilgi formu, fonun özellikleri, hakları, riskleri, stratejisi ve maliyetleri hakkında yatırımcının bilinçli karar vermesini sağlayacak bilgileri içerir.

Şemsiye fon, katılma payları tek içtüzük kapsamında ihraç edilen fonları kapsayan üst yapıdır. Şemsiye fona bağlı her fon için ayrı izahname ve yatırımcı bilgi formu düzenlenir. Her fonun varlık ve yükümlülükleri birbirinden ayrıdır; bir fonun giderleri veya yükümlülükleri diğer fonlarla karıştırılmamalıdır. Şemsiye fonun tasfiye edilmesi veya devredilmesi halinde bağlı fonların durumu da ilgili kurallara göre değerlendirilir. Tebliğde aksi belirtilmedikçe hükümler her fon için ayrı uygulanır.

Fon malvarlığı yatırımcı lehine ve yatırımcının çıkarı gözetilerek yönetilmelidir. Portföy yöneticilerinin fonun yatırım yapabileceği varlıklar konusunda bilgi ve tecrübeye sahip olması gerekir. Fon portföyündeki varlıklar yetkili portföy saklayıcısı nezdinde saklanır. Fon malvarlığı, belirli işlemler dışında teminat gösterilemez, rehnedilemez, haczedilemez, ihtiyati tedbire konu edilemez ve iflas masasına dahil edilemez. Kurucunun üçüncü kişilere borçları ile fonların aynı kişilerden alacakları mahsup edilemez. Bu yapı, fon malvarlığının kurucu riskinden ayrıştırılmasını sağlar.

Tebliğ şemsiye fon türlerini yatırım stratejilerine göre ayırır. Borçlanma araçları, hisse senedi, kıymetli madenler, fon sepeti, para piyasası, katılım, değişken, serbest, garantili ve koruma amaçlı şemsiye fonlar bu kapsamda değerlendirilebilir. Bazı türlerde portföyün belirli oranının devamlı olarak ilgili varlık grubunda tutulması gerekir. Fon unvanı yatırım stratejisine uygun olmalı ve yatırımcıyı yanıltmamalıdır. Denetim ve uyum açısından önemli olan, fonun içtüzük, izahname, portföy sınırlamaları, saklama düzeni ve yatırımcıyı bilgilendirme yükümlülükleriyle fiili uygulamanın uyumlu olmasıdır.

1.3.1 · TSPB Üyelerinin Sermaye Piyasası Faaliyetlerini Yürütürken Uyacakları Meslek Kuralları

TSPB Meslek Kurallarında Üye Davranışı, Müşteri Koruması ve Piyasa Güveni

KISACA

TSPB üyelerinin meslek kuralları, sermaye piyasası faaliyetlerinde dürüstlük, adillik, mesleki özen, saydamlık, müşteri menfaatinin korunması, haksız rekabetten kaçınma ve piyasa güveninin sürdürülmesi için ortak davranış çerçevesi kurar. TSPB; yatırım hizmet ve faaliyetlerinde bulunan yetkili kuruluşlar ile Kurulca uygun görülen sermaye piyasası kurumlarının üye olduğu kamu kurumu niteliğinde meslek kuruluşudur. Üyeler, yasal düzenlemelere ve Birlik kararlarına uymakla; müşteriyi tanımak, talimatlara uygun hareket etmek, doğru bilgilendirme yapmak, çıkar çatışmalarını yönetmek, sır saklamak ve ilan-reklam faaliyetlerinde yanıltıcı ifadelerden kaçınmakla yükümlüdür.

TSPB üyelerinin sermaye piyasası faaliyetlerini yürütürken uyacakları meslek kuralları, piyasa aktörlerinin yalnız kanuna şeklen uymasını değil, mesleğin güven ve özen gerektiren niteliğine uygun davranmasını hedefler. Türkiye Sermaye Piyasaları Birliği, Sermaye Piyasası Kanunu uyarınca yatırım hizmet ve faaliyetinde bulunmaya yetkili kuruluşlar ile sermaye piyasalarında faaliyet gösteren ve Kurulca uygun görülen kurumların üye olduğu kamu kurumu niteliğinde bir meslek kuruluşudur. Aracı kurumlar, bankalar, menkul kıymet yatırım ortaklıkları, girişim sermayesi ve gayrimenkul yatırım ortaklıkları ile portföy yönetim şirketleri bu üyelik çevresinde yer alabilir.

Birliğin amacı, üyelerin ortak ihtiyaçlarını karşılamak, çalışanların mesleki faaliyetlerini kolaylaştırmak, sermaye piyasasının gelişmesine katkı sağlamak ve üyelerin birbirleriyle, yatırımcılarla ve çalışanlarıyla ilişkilerinde dürüstlük ile güveni hâkim kılmaktır. Meslek kuralları bu amacın davranış düzeyindeki karşılığıdır. Üyelerin saygın meslek mensupları olarak hareket etmesi, yatırımcıya kaliteli hizmet sunması, haksız rekabetten kaçınması, meslek disiplini ve ahlakını koruması beklenir. Birlikçe belirlenen meslek ilke ve kurallarına aykırı fiillerde uyarıdan üyelikten çıkarılmaya kadar farklı disiplin yaptırımları gündeme gelebilir.

Genel ilkeler, üyenin piyasa ile kurduğu ilişkinin temelini oluşturur. Üyeler faaliyetlerini yürütürken yasal ve idari düzenlemeleri bilmek ve bunlara bağlı kalmak zorundadır. Dürüst ve adil davranma ilkesi, müşteri çıkarlarını ve piyasa bütünlüğünü gözetmeyi gerektirir. Bağımsızlık ve tarafsızlık ilkesi, üyenin kendi ilişkileri veya başka üyelerle bağlantıları nedeniyle kararlarının gölgelenmemesini ister. Mesleki özen ve titizlik, faaliyet için gerekli teknik bilgi birikimini oluşturmayı ve gelişmeleri izlemeyi kapsar. Saydamlık ise ilgili tarafların tam, doğru, hızlı ve eşit şekilde bilgilendirilmesi anlamına gelir.

Müşteri ilişkileri meslek kurallarının en görünür alanıdır. Üye, müşteriyle iş ilişkisi kurmadan önce kimlik bilgilerini alır, hizmeti yazılı sözleşme çerçevesinde yürütür ve müşterinin mali durumu, yatırım amacı, yatırım süresi, risk ve getiri tercihleri hakkında gerekli bilgileri edinir. Müşteriye sunulan ürün veya hizmet uygun değilse uyarı yapılır; müşteri bilgi vermiyorsa uygunluk tespitinin yapılamayacağı açıklanır.

Müşteri talimatları açık ve anlaşılır olmalı, çerçeve sözleşmenin sınırları içinde yerine getirilmelidir. Müşteriye ait nakit veya sermaye piyasası araçları üzerinde yetkisiz tasarrufta bulunulamaz.

Bilgilendirme, çıkar çatışmaları ve sır saklama kuralları yatırımcı güvenini tamamlar. Üyeler sundukları hizmetler, ücretler, komisyonlar, masraflar, yükümlülükler ve riskler hakkında doğru, eksiksiz ve zamanında bilgi verir. Bilgiler güvenilir belge, rapor ve analizlere dayanmalı; kesin bilgi ile yoruma dayalı değerlendirme ayırt edilebilmelidir. Abartılı, yanıltıcı veya garanti izlenimi veren ifadeler kullanılmaz. Çıkar çatışması önlenemiyorsa müşteri menfaati öncelenir ve durum açıklanır. Müşteriye ait kimlik ve işlem bilgileri kanunen yetkili merciler dışında açıklanamaz. Bu bütün, meslek kurallarını piyasanın itibarını koruyan pratik davranış rejimi haline getirir.

Sermaye Piyasası Çalışanları İçin Etik İlke ve Davranış Standartları

KISACA

Sermaye piyasası çalışanları etik ilkeleri ve davranış kuralları, piyasada görev yapan kişilerin mesleki faaliyetlerini güven, dürüstlük, tarafsızlık, özen, yetkinlik, gizlilik ve çıkar çatışmalarından kaçınma anlayışıyla yürütmesini amaçlar. Etik ilkeler genel değer çerçevesini kurarken davranış kuralları bu değerlerin günlük iş ilişkilerinde nasıl uygulanacağını somutlaştırır. Çalışanın mevzuata uygun hareket etmesi, gerekli lisans ve mesleki yeterliği koruması, müşteri ve kurum bilgilerini kötüye kullanmaması, piyasa güvenini zedeleyici davranışlardan kaçınması, görevini kişisel çıkar sağlama aracına dönüştürmemesi ve mesleğin saygınlığını koruması beklenir.

Sermaye piyasası çalışanları etik ilkeleri ve davranış kuralları, piyasanın güvene dayalı yapısını kişi düzeyinde koruyan mesleki çerçevedir. Sermaye piyasası kurumları kurumsal sorumluluk taşısa da yatırımcıyla temas eden, bilgiye erişen, işlem süreçlerinde rol alan ve kurum adına davranan kişiler çalışanlardır. Bu nedenle etik kurallar yalnız iyi niyet beyanı değildir; çalışanların bilgi, yetki ve temsil gücünü nasıl kullanacağını belirleyen mesleki sınırlar oluşturur. Etik ilke, mesleğin bağlı kaldığı değeri gösterir; davranış kuralı ise bu değerin somut olayda hangi hareket tarzını gerektirdiğini açıklar.

Etik yaklaşımın merkezinde dürüstlük, güvenilirlik, tarafsızlık ve mesleki özen bulunur. Çalışanın yaptığı işte doğru bilgiye dayanması, müşteriyi veya kurumu yanıltacak ifadelerden kaçınması, kişisel çıkarını görev sorumluluğunun önüne koymaması ve mesleki bilgi düzeyini görevine uygun biçimde sürdürmesi gerekir. Sermaye piyasasında verilen kararlar çoğu zaman yatırımcının malvarlığı, kurumun itibarı ve piyasa fiyatlarının güvenilirliği üzerinde sonuç doğurduğu için, özensiz davranış yalnız bireysel hata olarak kalmaz; piyasa düzenine zarar verebilir.

Davranış kuralları, çıkar çatışmalarını yönetmeyi ve bilgiyi korumayı özellikle önemser. Çalışan, müşteriyle, kurumla, başka çalışanlarla veya üçüncü kişilerle ilişkilerinde bağımsızlığını ve tarafsızlığını zedeleyebilecek durumları fark etmeli, gizlememeli ve kurum içi düzenlemelere uygun biçimde yönetmelidir. Görevi nedeniyle öğrendiği müşteri bilgilerini, işlem bilgilerini veya henüz kamuya açıklanmamış bilgileri kendi ya da başkası yararına kullanamaz. Gizlilik yükümlülüğü yalnız müşteri mahremiyeti için değil, içsel bilginin kötüye kullanılmasını ve yatırımcılar arasında bilgi eşitsizliği oluşmasını önlemek için de önemlidir.

Mesleki yeterlik ve lisans yükümlülüğü etik düzenin teknik boyutunu oluşturur. Çalışanın mevzuatın öngördüğü alanlarda gerekli lisansa sahip olması, görevini bilgi ve yetkinliğiyle uyumlu biçimde yürütmesi, gelişmeleri izlemesi ve kurumun eğitim süreçlerine katılması beklenir. Bilmediği veya yetkisi dışında kalan konularda yanıltıcı güven vermek, yatırımcıyı hatalı yönlendirmek veya kurum adına bağlayıcı izlenim yaratmak etik çerçeveyle bağdaşmaz. Bu nedenle mesleki yeterlik, yalnız sınav veya belge şartı değil, yatırımcıya verilen hizmetin güvenilirliğinin parçasıdır.

Etik ilkeler aynı zamanda kurum kültürüyle ilişkilidir. Çalışanın kuruma, müşteriye, diğer piyasa profesyonellerine ve düzenleyici otoritelere karşı saygılı, açık ve iş birliğine yatkın olması beklenir. Mesleki yükselmelerde yalnız teknik bilgi değil, etik ilkelere ve meslek kurallarına uyum da dikkate alınmalıdır. Etik ihlallerin görmezden gelinmesi, kurum içinde yanlış davranışların normalleşmesine yol açar. Bu yüzden sermaye piyasası çalışanları için etik düzen, bireysel erdem listesi değil; piyasa güvenini, kurum itibarını ve yatırımcı eşitliğini birlikte koruyan mesleki davranış standardıdır.

2.1.1 · Bilgi Sistemleri Stratejisinin Geliştirilmesi

İş Hedefleriyle Uyumlu Bilgi Sistemleri Stratejisi

KISACA

Bilgi sistemleri stratejisinin geliştirilmesi, işletmenin misyonu, vizyonu, değerleri ve kurumsal hedefleriyle bilgi sistemleri önceliklerini aynı hizaya getirme sürecidir. Bilgi sistemleri yalnız yazılım, donanım ve altyapıdan oluşmaz; veriyi anlamlı bilgiye dönüştüren insan gücü, süreçler, uygulamalar ve yönetsel karar yapılarıyla birlikte çalışır. Strateji, bilgi sistemlerinin işletme hedeflerine nasıl katkı sağlayacağını, hangi yatırımların öncelik kazanacağını, hangi risklerin yönetileceğini ve performansın nasıl ölçüleceğini belirler. Etkili bir bilgi sistemleri stratejisi, iş tarafı ile teknoloji tarafı arasında değer üretme, riskleri azaltma ve kaynakları verimli kullanma bağlantısı kurar.

Bilgi sistemleri stratejisinin geliştirilmesi, işletmenin genel amaçları ile bilgi sistemleri yatırımları ve faaliyetleri arasında bilinçli bir bağ kurulmasıdır. Bilgi sistemleri, planlama, kontrol, analiz ve karar verme için gerekli verileri toplayan, işleyen, saklayan, kullanan ve yayan ilişkili unsurlar bütünüdür. Bu yapı yalnız teknik bileşenlerden oluşmaz; yazılım, uygulama, donanım ve altyapı unsurlarını anlamlı hale getiren insan gücü, yönetim süreçleri ve karar mekanizmaları da sistemin parçasıdır. Bu nedenle bilgi sistemleri stratejisi, teknolojinin ne alınacağı sorusundan çok, teknolojinin işletmenin hedeflerine hangi değerle katkı sağlayacağı sorusuna yanıt verir.

Strateji kavramını anlamak için misyon, vizyon ve değerler birlikte düşünülmelidir. Misyon işletmenin neden var olduğunu, ne yaptığını ve kime hizmet verdiğini açıklar. Vizyon, işletmenin orta ve uzun vadede ulaşmak istediği konumu gösterir. Değerler ise bu hedeflere giderken bağlı kalınacak etik ve kurumsal ilkeleri ifade eder. Bilgi sistemleri stratejisi bu üç zeminden kopuk olamaz. İşletme nereye gitmek istediğini tanımlamadan bilgi sistemleri yatırımlarını doğru önceliklendiremez. Aynı şekilde bilgi sistemleri birimi de kendi stratejisini kurumsal hedeflere hizmet edecek bir fonksiyon stratejisi olarak tasarlamak zorundadır.

Bilgi sistemleri yönetişimi, stratejinin geliştirilmesi ve işletilmesi için gereken çerçeveyi sağlar. Amaç bilgi sistemlerini sadece iyi yönetmek değil, iş hedeflerine değer katacak ve bilgi sistemleri risklerini kabul edilebilir seviyede tutacak biçimde yönetmektir. Bu çerçevede iş stratejisi, bilgi sistemleri stratejisi, bilgi sistemleri yatırımları, bilgi sistemleri riskleri, performans ölçümü, iş-teknoloji uyumu ve işe değer katma unsurları birlikte ele alınır. İş tarafı hangi hedefleri gerçekleştirmek istiyor, bilgi sistemleri bu hedeflere nasıl destek olacak, eldeki kaynaklar ne kadar yeterli, hangi riskler hedefi aksatabilir ve faaliyetler gerçekten değer üretiyor mu soruları stratejinin ana eksenini oluşturur.

Etkili strateji işletmeye özgüdür, üst yönetim sorumluluğunda geliştirilir, kurum kültürü ve kaynakları dikkate alınarak kurulur, dinamik ve uzun vadeli bir yol haritası niteliği taşır. Strateji günlük operasyon ayrıntılarını değil, hangi hedeflere ne zaman ve hangi önceliklerle gidileceğini gösterir. Teknoloji ortamı, hukuki çerçeve, müşteri beklentileri, siber riskler ve iş süreçleri sürekli değiştiği için bilgi sistemleri stratejisinin de düzenli olarak gözden geçirilmesi gerekir. Bu yaklaşım işletmenin hem

bugünkü faaliyetlerini güvenilir biçimde yürütmesine hem de gelecekte doğabilecek fırsat ve tehditlere hazırlıklı olmasına katkı sağlar.

Bilgi sistemleri stratejisi hazırlanırken temel yetkinlikler, gelişme yönü, dış çevre ve sinerji de dikkate alınır. İşletmenin rekabet avantajı sağlayan becerileri, hangi hizmet veya pazarlara yöneleceği, çevredeki fırsat ve tehditler ile birimler arası uyum bilgi sistemleri kararlarını etkiler. Örneğin yeni bir dijital hizmet hedefleniyorsa altyapı kapasitesi, güvenlik mimarisi, veri yönetimi, personel yetkinliği ve dış hizmet bağımlılığı aynı anda planlanmalıdır. Böylece bilgi sistemleri stratejisi soyut niyet olmaktan çıkar, kaynak dağılımını ve risk önceliklerini yöneten uygulanabilir bir plan haline gelir.

Bilgi Sistemleri Yönetiminde İnsan, Süreç, Teknoloji ve Kontrol Unsurları

KISACA
Bilgi sistemleri yönetiminin unsurları, işletmenin bilgi ihtiyacını karşılayan teknolojik ve yönetsel bileşenlerin birlikte nasıl işletileceğini açıklar. Bilgi sistemleri yazılım, donanım, uygulama, veri, altyapı ve bunları çalıştıran insan gücünden oluşur; ancak bu unsurlar yönetim süreçleriyle bütünleşmedikçe işletmeye değer katamaz. Yönetim; kaynakların planlanması, risklerin belirlenmesi, kontrollerin kurulması, performansın ölçülmesi, veri bütünlüğünün korunması, güvenlik ihtiyaçlarının karşılanması ve hizmetlerin sürekliliğinin sağlanmasını kapsar. Bilgi sistemleri yönetimi, teknoloji tarafını iş hedefleriyle uyumlu çalıştırarak etkinlik, verimlilik, güvenilirlik ve kalite üretmeyi amaçlar.

Bilgi sistemleri yönetiminin unsurları, işletmenin bilgi üretme ve kullanma kapasitesini oluşturan teknik, insani ve yönetsel parçaların birlikte nasıl çalışacağını açıklar. Bilgi sistemleri, verileri karar vericiler için anlamlı bilgiye dönüştüren insan gücü, programlar, donanım, uygulamalar, altyapı ve yönetim süreçlerinden oluşur. Teknoloji bileşenleri tek başına sistem yaratmaz; bu bileşenlerin hangi amaçla kullanılacağını belirleyen yönetim, kullanıcı ihtiyaçlarını anlayan insan gücü ve süreçleri sürekli işleten kontrol yapısı gerekir. Bu yüzden bilgi sistemleri yönetimi, teknik operasyon ile kurumsal hedefler arasında köprü kuran bir yönetim alanıdır.

Bilgi sistemleri yönetiminin ilk unsuru iş hedefleriyle uyumdur. İşletmenin bilgi sistemlerinden beklediği katkı açık değilse kaynaklar yanlış projelere yönlendirilebilir. Yönetim, bilgi sistemleri yatırımlarını işletmenin stratejisine, risk iştahına, hizmet ihtiyaçlarına ve mevzuat yükümlülüklerine göre planlar. Zaman, insan gücü, bütçe, donanım, yazılım ve dış hizmet kaynakları sınırlı olduğu için önceliklendirme zorunludur. Bu önceliklendirme yalnız maliyet hesabı değildir; bilgi güvenliği, veri bütünlüğü, faaliyetlerde verimlilik, hizmet kalitesi ve iş sürekliliği gibi etkiler birlikte değerlendirilir.

İkinci unsur risk ve kontrol yönetimidir. Bilgi sistemleri işletmeye hız ve esneklik sağlarken, veri kaybı, yetkisiz erişim, hizmet kesintisi, hatalı işlem, mevzuata uyumsuzluk ve dış hizmet bağımlılığı gibi riskler doğurabilir. Bu risklerin kabul edilebilir seviyede tutulması için politika, prosedür, görev ayrılığı, erişim yetkilendirmesi, iz kayıtları, değişiklik yönetimi, yedekleme, süreklilik planları ve performans izleme mekanizmaları kullanılır. Kontrollerin amacı yalnız hatayı yakalamak değildir; istenmeyen olayları önlemek, gerçekleşen olayları tespit etmek, etkisini sınırlamak ve normal işleyişe dönüşü desteklemektir.

Üçüncü unsur performans ve sürekli iyileştirmedir. Bilgi sistemleri yönetimi kurulan sistemlerin gerçekten işe değer katıp katmadığını ölçmek zorundadır. Hizmet seviyeleri, kapasite kullanımı, olay çözüm süreleri, kullanıcı memnuniyeti, güvenlik olayları, proje gerçekleşmeleri ve maliyet göstergeleri bu değerlendirmeye katkı sağlar. Ölçülmeyen faaliyetlerin yönetilmesi güçleşir; bu nedenle anahtar performans göstergeleri ve düzenli raporlama bilgi sistemleri yönetiminin ayrılmaz parçasıdır.

İşletmenin faaliyet gösterdiği çevre, teknoloji ve hukuki düzenlemeler değiştikçe bilgi sistemleri yönetiminin de politika, süreç ve kaynaklarını güncellemesi gerekir. Böylece bilgi sistemleri yalnız destek birimi olarak kalmaz, işletmenin güvenilir ve sürdürülebilir biçimde çalışmasını sağlayan stratejik unsur haline gelir.

Yönetimin unsurları organizasyon yapısıyla da ilişkilidir. Görev ve sorumlulukların açık tanımlanması, bilgi sistemleri personelinin yeterliliği, kullanıcıların eğitim düzeyi, politika ve prosedürlerin güncelliği, üçüncü taraf hizmet sağlayıcılarla kurulan ilişkiler ve üst yönetimin gözetimi bilgi sistemleri ortamının olgunluğunu belirler. Bir unsur zayıf kaldığında diğer kontrollerin etkinliği de düşebilir. Örneğin güçlü bir teknik güvenlik ürünü, yetki gözden geçirmesi yapılmıyorsa veya değişiklikler belgelenmiyorsa beklenen korumayı sağlayamayabilir. Bu nedenle bilgi sistemleri yönetimi bütüncül, izlenebilir ve sorumluluk temelli yürütülmelidir. Yönetsel kararların belgelenmesi ve düzenli gözden geçirilmesi, denetimde kanıtlanabilir bir yönetim izi oluşturur.

2.2.1 · Bilgi Sistemleri Denetimi Kavramları

Bilgi Sistemleri Denetiminde Güvence, Kontrol, Risk ve Kanıt Mantığı

KISACA

Bilgi sistemleri denetimi, bir kurumun bilgi sistemleri ortamında kurulan kontrollerin tasarımını ve işleyişini inceleyerek sistemlerin varlıkları koruma, veri bütünlüğünü sürdürme, hedeflere etkili ve verimli biçimde hizmet etme yeterliliği hakkında görüş oluşturur. Bu kavram yalnız teknik altyapı denetimi değildir; uygulamalar, operasyonlar, süreçler, politika ve prosedürler, iç kontroller, riskler, önemlilik ve kanıt toplama birlikte değerlendirilir. Denetim yaklaşımı, hangi risklerin hangi kontrollerle karşılandığını, kontrollerin önleyici, tespit edici veya düzeltici işlev görüp görmediğini ve görüşe dayanak olacak yeterli uygun kanıtın elde edilip edilmediğini anlamaya dayanır.

Bilgi sistemleri denetimi, bilgi sistemleri ortamındaki kontrollerin yalnız var olup olmadığını değil, tasarım ve işleyiş olarak ne kadar güvence sağladığını değerlendiren bir denetim alanıdır. İnceleme konusu yazılım, donanım, uygulama, veri, operasyon ve süreçlerden oluşan bilgi sistemi unsurlarıdır; fakat amaç teknik envanter çıkarmakla sınırlı değildir. Denetçi, bu unsurlar üzerinde kurulan kontrollerin bilgi sistemleri yönetim ilkelerine uygunluğunu, etkinliğini ve yeterliliğini değerlendirerek rapora bağlanabilir bir görüşe ulaşmaya çalışır. Bu nedenle bilgi sistemleri denetimi, varlıkların korunması, veri bütünlüğü, süreçlerin sürekliliği, iş hedeflerine katkı ve kaynakların verimli kullanımı gibi sonuçlara odaklanır.

Denetim kavramı, finansal denetim, operasyonel denetim, uyum denetimi, bütünleşik denetim, üçüncü taraf hizmet denetimi, adli bilişim denetimi ve fonksiyonel denetim gibi farklı türlerle ilişkilidir. Bilgi sistemleri denetimi bu türlerin bazılarıyla birlikte yürütülebilir, bazı durumlarda ise bağımsız bir güvence faaliyeti olarak ele alınır. Örneğin finansal tabloların güvenilirliği, muhasebe kayıtlarını üreten ve saklayan bilgi sistemlerinin güvenilirliğinden etkilenir. Benzer biçimde dış hizmet sağlayıcılar, bulut servisleri veya yazılım hizmeti modelleri kullanıldığında, kurumun kontrol ortamı yalnız kendi binası ve personeliyle sınırlı kalmaz; üçüncü tarafların süreçleri de denetim bakışına dahil olur.

Kontrol, bilgi sistemleri denetiminin merkezindeki kavramdır. Kontrol; riskleri yönetmek için oluşturulan politika, prosedür, kılavuz, uygulama, teknik önlem veya organizasyon yapısı olabilir. Etkili bir kontrol, istenmeyen bir olayın gerçekleşmesini önleyebilir, gerçekleşen olayı tespit edebilir, etkisini sınırlayabilir veya düzeltici bir toparlanma sağlayabilir. Kontroller alanına göre genel kontroller ve uygulama kontrolleri biçiminde; uygulanma biçimine göre önleyici, tespit edici ve düzeltici biçimde; işlevsel özelliklerine göre teknik, fiziksel veya idari nitelikte sınıflandırılabilir. Bu sınıflandırmalar denetçinin hangi kontrolün hangi riske karşı çalıştığını anlamasına yardım eder.

Risk ve önemlilik, denetim kapsamının belirlenmesinde birlikte değerlendirilir. Denetim kaynakları sınırsız olmadığı için denetçi her kontrolü aynı derinlikte incelemek yerine, iş hedeflerini daha fazla etkileyebilecek risklere ve önemli alanlara odaklanır. Doğal risk, kontrol riski ve tespit riski birlikte

düşünülür; kontrol hedeflerine ulaşmayı engelleyebilecek olaylar belirlenir ve bu olayların olasılık ile etkisi değerlendirilir. Bu değerlendirme, hangi sistemlerin, süreçlerin, alt faaliyetlerin ve kontrollerin denetim planında öncelik kazanacağını belirler.

Kanıt, denetim görüşünün dayanağıdır. Denetçi, bir iddianın doğruluğunu makul güvence düzeyinde destekleyen yeterli ve uygun bilgileri toplamalıdır. Bilgi sistemleri denetiminde kanıt; belge inceleme, görüşme, gözlem, yeniden çalıştırma, sistem günlüklerinin incelenmesi, denetim izlerinin değerlendirilmesi, fiziksel inceleme, politika ve prosedürlerin gözden geçirilmesi ya da bilgisayar destekli denetim teknikleriyle elde edilebilir. Kanıtın güvenilirliği kaynağına, elde edilme biçimine, bütünlüğüne ve denetim amacına uygunluğuna bağlıdır. Böylece bilgi sistemleri denetimi kavramları, kontrol ortamını risk temelli biçimde okumayı ve sonuçta savunulabilir bir denetim görüşü üretmeyi sağlayan ortak bir dil oluşturur.

2.2.2 · Bilgi Sistemleri Denetim Faaliyeti

Bilgi Sistemleri Denetiminde Planlama, Uygulama ve Raporlama Akışı

KISACA

Bilgi sistemleri denetim faaliyeti, işin kabulünden denetim raporunun sunulmasına kadar planlama, denetimi gerçekleştirme ve raporlama aşamalarıyla yürütülen risk tabanlı bir süreçtir. Planlama aşamasında amaç, kapsam, denetim evreni, risk değerlendirmesi, ekip, kaynak, zamanlama ve denetim programı belirlenir. Gerçekleştirme aşamasında denetçi, risk olarak değerlendirilen alanlara karşı yeterli ve uygun kanıt toplar; kontrollerin tasarımını ve işleyişini test eder. Raporlama aşamasında ise ulaşılan görüş, kapsam, değerlendirilen kontroller, bulgular ve iyileştirme önerileri tam, güvenilir, objektif, kanıta dayalı, açık ve anlaşılır biçimde ilgili taraflara sunulur.

Bilgi sistemleri denetim faaliyeti, bilgi sistemleri yönetimi ve işletimi kapsamındaki unsurlar ile bu sistemlerde kurulan kontrollerin değerlendirilmesi sonucunda bir görüş oluşturma ve bu görüşü rapora bağlama sürecidir. Faaliyet, denetim işinin kabul edilmesiyle başlar; denetimin planlanması, denetimin gerçekleştirilmesi ve raporlamayla tamamlanır. Bu akışın risk tabanlı yürütülmesi gerekir, çünkü denetim zamanı, insan kaynağı ve teknik kapasite sınırlıdır. Risk tabanlı yaklaşımda önce bilgi sisteminden doğabilecek riskler belirlenir, bu riskleri azaltacak kontroller anlaşılır, kontrollerin kurum yapısına uygun kurulup kurulmadığı ve çalışıp çalışmadığı incelenir, zayıflıklar değerlendirilir ve bulgular belirli bir raporlama düzeni içinde sunulur.

Planlama aşaması, denetimin yol haritasını oluşturur. Denetçi bu aşamada denetim amaç ve kapsamını, denetim evrenini, risk değerlendirmesini, ekip yapısını, kaynak ve zaman gereksinimini, uygulanacak prosedürlerin niteliğini ve denetim programını belirler. Genel denetim stratejisi daha üst düzey çerçeveyi, denetim planı ise uygulanacak işlerin ayrıntısını gösterir. Bilgi sistemleri denetiminde amaçlar çoğu zaman veri akışını anlamak, bilgi sistemleri hedeflerine ulaşılıp ulaşılmadığını değerlendirmek, kontrol etkinliğini belirlemek ve denetim görüşünü destekleyecek kanıtları planlamakla ilgilidir. Teknoloji burada tek başına amaç değil, iş hedeflerini destekleyen ve riskleri taşıyan bir kolaylaştırıcıdır.

Risk değerlendirmesi planlamanın ana belirleyicisidir. Dış çevre, teknolojik değişim, rekabet koşulları ve düzenleyici yükümlülükler ile personel niteliği, süreç yapısı, sistem karmaşıklığı ve organizasyon düzeni gibi iç faktörler birlikte ele alınır. Risklerin olasılığı ve etkisi değerlendirildikten sonra stratejik etki, hizmet ve faaliyetler, düzenlemelere uyum, bilgi sistemleri kaynakları, organizasyon yapısı, finansal etki, sosyal etki ve itibar etkisi gibi başlıklar üzerinden öncelikler kurulur. Bu değerlendirme, denetlenecek alt süreçleri, prosedürlerin zamanlamasını, kapsamını ve ayrılacak kaynağı doğrudan etkiler.

Denetimin gerçekleştirilmesi aşamasında planlanan prosedürler uygulanır ve görüşe dayanak olacak yeterli uygun kanıt aranır. Denetçi belgeleri inceler, personelle görüşür, süreçleri gözlemler, işlem veya

kontrol adımlarını yeniden çalıştırabilir, sistem günlüklerini ve denetim izlerini analiz edebilir, politika ve prosedürleri kontrol edebilir. Bilgi sistemleri denetiminde işletme seviyesi kontroller, yönetişim kontrolleri, bilgi sistemleri yönetim süreçleri, uygulama kontrolleri ve bilgi güvenliği teknik kontrolleri birlikte ele alınır. Anahtar kontrollerin tasarlandığı gibi çalışıp çalışmadığı, ilgili riskin olasılığını veya etkisini azaltıp azaltmadığı, doğru süreç adımında yer alıp almadığı ve yeterli sıklıkta uygulanıp uygulanmadığı değerlendirilir.

Bilgisayar destekli denetim teknikleri, bilgi sistemleri ortamında kanıt toplama kapasitesini artırır. Büyük veri kümelerinin analiz edilmesi, işlemlerin doğrulanması, kontrollere uygunluğun test edilmesi, yapılandırma ayarlarının incelenmesi, güvenlik açıklıklarının belirlenmesi veya kaynak kodu güvenlik analizlerinin yapılması bu kapsama girebilir. Sürekli denetim yaklaşımı, denetim testlerinin gerçek zamanlıya yakın biçimde uygulanmasına imkân vererek istisnai işlemlerin, şüpheli hareketlerin veya önceden tanımlanmış eşiklerin daha düzenli izlenmesini sağlar. Ancak hangi aracın kullanılacağı, denetim amacına ve güvenilir kanıt üretme kapasitesine göre belirlenmelidir.

Raporlama aşaması, denetim çalışmasının görünür çıktısıdır. Rapor; denetim hedeflerini, kapsamı, değerlendirilen kontrolleri, bulguları, kontrollerin etkinliğine ilişkin görüşü ve iyileştirme önerilerini içermelidir. İyi bir denetim raporu tam, güvenilir, objektif, yeterli kanıta dayalı, açık, öz ve anlaşılır olur. Raporda tarafsızlığı zedeleyebilecek savunucu veya suçlayıcı ifadelerden kaçınılır; teknik terimler gerekli olduğunda açıklanır. Böylece denetim faaliyeti yalnız hata arayan bir inceleme değil, yönetimin bilgi sistemleri risklerini anlamasını ve kontrol ortamını güçlendirmesini sağlayan sistematik bir güvence süreci haline gelir.

2.3.1 · Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ Seri: X, No: 22

Seri X No 22 Kapsamında Bağımsız Denetimin Güvence Çerçevesi

> **KISACA**
> Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ Seri: X, No: 22, sermaye piyasasında bağımsız denetimin amacını, kapsamını, genel ilkelerini, denetim kuruluşlarının yetkilendirilme şartlarını, denetim sözleşmelerini ve denetçilerin niteliklerini düzenleyen temel çerçevedir. Bağımsız denetimin amacı, finansal tabloların geçerli finansal raporlama standartları doğrultusunda işletmenin durumunu ve faaliyet sonuçlarını önemli yönleriyle gerçeğe uygun gösterip göstermediği hakkında görüş bildirmektir. Bu görüş; mesleki şüphecilik, mesleki muhakeme, makul güvence, önemlilik, denetim riski, yeterli uygun kanıt, yetkili denetim kuruluşu ve yazılı sözleşme düzeni üzerine kurulur.

Seri: X, No: 22 Tebliği, sermaye piyasasında bağımsız denetimi yalnız teknik bir finansal tablo kontrolü olarak değil, belirli ilkelere, yetkilendirme şartlarına ve sözleşme düzenine bağlanmış bir güvence faaliyeti olarak ele alır. Bağımsız denetimin temel amacı, finansal tabloların finansal raporlama standartlarına göre işletmenin finansal durumunu ve faaliyet sonuçlarını tüm önemli yönleriyle gerçeğe uygun ve doğru biçimde gösterip göstermediği hakkında bağımsız denetçinin görüş bildirmesidir. Denetim kapsamı ise bu görüşe ulaşmak için uygulanacak yöntem ve tekniklerin bütünüdür. Kapsam belirlenirken tebliğ hükümleri, bağımsız denetim standartları, Kurul düzenlemeleri, denetim sözleşmesi ve raporlama gereklilikleri birlikte dikkate alınır.

Tebliğin genel ilkelerinden biri mesleki şüpheciliktir. Denetçi, yönetimi peşinen dürüst ya da dürüst olmayan kabul etmeden, kanıtları sorgulayıcı bir bakışla değerlendirir. Yönetim açıklamaları tek başına yeterli ve uygun denetim kanıtı sayılmaz; açıklamaların diğer bilgi ve belgelerle uyumu incelenir. Mesleki şüphecilik, şüpheli olayların yüzeysel geçilmesini, kanıtlardan gereğinden fazla genelleme yapılmasını ve denetim planı ile prosedürlerinin hatalı varsayımlara dayanmasını azaltır. Bu tutum, işin kabulünden raporlamaya kadar denetimin tüm aşamalarında sürdürülmelidir.

Mesleki muhakeme, denetçinin mevzuat, denetim standartları, finansal raporlama standartları, etik kurallar, eğitim ve deneyim birikimini kullanarak koşullara uygun kararlar vermesidir. Önemlilik düzeyinin ve denetim riskinin belirlenmesi, denetim tekniklerinin zamanlama ve kapsamının seçilmesi, yeterli uygun kanıt toplanıp toplanmadığının değerlendirilmesi ve nihai görüşe ulaşılması mesleki muhakeme gerektirir. Bu muhakeme keyfi değildir; bilinen durum ve gerçeklere, elde edilen kanıtlara ve çalışmayı inceleyecek deneyimli bir denetçinin anlayabileceği çalışma kağıtlarına dayanmalıdır.

Makul güvence, bağımsız denetimin yüksek fakat mutlak olmayan güvence düzeyidir. Denetim, finansal tabloların önemli yanlışlık içermediği konusunda makul güvence sağlayacak şekilde tasarlanır; ancak örnekleme, iç kontrol sistemlerinin doğal sınırlamaları, yönetimin kontrolleri devre dışı bırakma olasılığı, kanıtların çoğu zaman kesin değil ikna edici nitelikte olması ve denetçinin mesleki kanaat

kullanması nedeniyle mutlak güvence beklenmez. Bu nedenle denetim riski sıfıra indirilemez; denetçi denetim riskini kabul edilebilir düşük seviyeye indirecek prosedürleri tasarlayıp uygulamakla yükümlüdür.

Önemlilik, kullanıcıların finansal tablolara dayanarak alacağı ekonomik kararları etkileyebilecek yanlışlıkların değerlendirilmesidir. Denetçi finansal tabloların bütünü için bir önemlilik düzeyi belirler ve bu düzeyi denetim boyunca yeni bilgiler ışığında gözden geçirebilir. Denetim riski ise önemli yanlışlık riski ile tespit edememe riskinin birleşiminden oluşur. Yapısal risk ve kontrol riski işletmenin kendi koşullarından doğarken, tespit edememe riski denetçinin uyguladığı prosedürlerin önemli yanlışlığı ortaya çıkaramama ihtimalidir. Yeterli planlama, doğru ekip seçimi, gözetim, çalışma kontrolü ve mesleki şüphecilik bu riskin azaltılmasına katkı sağlar.

Tebliğ ayrıca sermaye piyasasında bağımsız denetim yapacak kuruluşların ve denetçilerin taşıması gereken şartları düzenler. Denetim faaliyeti Kurulca yetkilendirilen bağımsız denetim kuruluşları tarafından yürütülür; kuruluşun organizasyon, teknik donanım, belge ve kayıt düzeni, kalite kontrol güvence yapısı ve mesleki sorumluluk sigortası gibi şartları sağlaması gerekir. Denetim sözleşmeleri yazılı olarak yapılır; anonim ortaklıklarda denetçi seçimi ilgili şirket organları ve mevzuat çerçevesinde yürütülür. Denetçi unvanları, mesleki deneyim ve yeterlik şartları da bu düzenin parçasıdır. Böylece Seri: X, No: 22, bağımsız denetim görüşünün hem mesleki ilkelere hem de kurumsal yetkinliğe dayanmasını sağlar.

2.3.2 · Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği VII-128.10

VII-128.10 Tebliğinde Bilgi Sistemleri Yönetimi, Güvenlik ve Kontrol Sorumluluğu

KISACA

Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği VII-128.10, sermaye piyasası kapsamındaki işletmelerin bilgi sistemlerini kurma, işletme, yönetme, kullanma ve güvence altında tutma yükümlülüklerini düzenler. Tebliğ, bilgi güvenliği politikasının üst yönetim tarafından hazırlanmasını, yönetim kurulu tarafından onaylanmasını, bilgi sistemleri stratejisinin iş hedefleriyle uyumlu olmasını, risk yönetimi süreçlerinin kurulmasını ve kontrollerin etkin, yeterli ve uyumlu biçimde gözetilmesini öngörür. Kapsam; bilgi varlıkları, kimlik ve erişim, veri bütünlüğü, dış hizmet, denetim izi, güvenlik ihlali yönetimi, sistem geliştirme, süreklilik, değişiklik yönetimi ve iç denetime kadar uzanır.

Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği VII-128.10, sermaye piyasasında bilgi sistemlerinin yönetimini kurumsal yönetim, risk yönetimi ve bilgi güvenliği sorumluluğu içinde ele alan temel düzenlemedir. Tebliğ, sermaye piyasası kurumları, borsalar, piyasa işleticileri, merkezi altyapı kuruluşları, halka açık ortaklıklar, öz düzenleyici kuruluşlar ve kripto varlık hizmet sağlayıcılar gibi geniş bir işletme grubunun bilgi sistemlerine ilişkin usul ve esaslarını belirler. Amaç, bilgi sistemlerinden doğan risklerin yönetilmesi, iş hedeflerinin desteklenmesi, bilginin gizliliği, bütünlüğü ve gerektiğinde erişilebilirliğinin korunmasıdır.

Tebliğin yaklaşımı, bilgi sistemlerini yalnız teknoloji biriminin teknik alanı olarak görmez. Bilgi sistemleri yönetimi, işletmenin kurumsal yönetim uygulamalarının parçasıdır. Bu nedenle bilgi sistemleri stratejisinin iş hedefleriyle uyumlu olması, gerekli finansman ve insan kaynağının sağlanması, politika ve prosedürlerin yazılı hale getirilmesi, rol ve sorumlulukların açıkça belirlenmesi gerekir. Üst yönetim bilgi güvenliği politikasının ve bilgi sistemleri stratejisinin uygulanmasını gözetir; bilgi sistemleri kontrollerinin etkin, yeterli ve uyumlu kurulması, değerlendirilmesi ve gözetimi yönetim kurulunun sorumluluk alanına girer.

Bilgi güvenliği politikası, tebliğin merkezindeki yönetim aracıdır. Bu politika üst yönetim tarafından hazırlanır, yönetim kurulu tarafından onaylanır ve personele ile ilgili taraflara duyurulur. Politika; bilgi güvenliği süreçlerinin işletilmesi için rollerin ve görev tanımlarının belirlenmesini, hedeflerin kurulmasını, bilgi sistemleri risklerinin yönetilmesine ilişkin süreçlerin oluşturulmasını, kontrollerin tesis edilmesini, değerlendirilmesini ve gözetimini kapsar. Politikanın yılda en az bir kez gözden geçirilmesi ve iş ihtiyaçları, yeni tehditler ve değişen risklere göre güncellenmesi beklenir.

Risk yönetimi, bilgi sistemleri faaliyetlerinin sürekliliği için düzenli işletilmesi gereken bir süreçtir. İşletmeler bilgi sistemlerine ilişkin riskleri belirlemek, ölçmek, izlemek, işlemek ve raporlamak üzere prosedürler kurar. Hızlı teknolojik gelişmelere uyum sağlayamama, bilgi sistemleri kullanımından doğan hata ve hile olasılığı, dış hizmet sağlayıcılara bağımlılık, iş ve hizmetlerin bilgi sistemlerine yüksek düzeyde bağlı hale gelmesi, işlem ve denetim izi kayıtlarının güvenliğinin zorlaşması bu risk alanları

arasında değerlendirilir. Risk analizi yılda en az bir kez yapılır; önemli sistem değişikliklerinde tekrarlanır ve iyileştirici faaliyetler üst yönetim onayıyla izlenir.

Kontrol esasları, bilgi sistemlerinin günlük işletiminden güvenlik ihlali yönetimine kadar geniş bir alanı kapsar. Varlık yönetimi, görevler ayrılığı, fiziksel ve çevresel güvenlik, ağ güvenliği, kimlik doğrulama, yetkilendirme, erişim yönetimi, işlemlerin ve kayıtların bütünlüğü, veri gizliliği, dış kaynak hizmetlerinin yönetimi, müşteri bilgilendirmesi, üçüncü taraflarla bilgi değişimi, denetim izi kayıt mekanizması, zaman senkronizasyonu, bilgi güvenliği ihlali müdahalesi, bilgi sistemleri edinimi, geliştirilmesi ve bakımı, uygulama güvenliği, süreklilik, değişiklik yönetimi ve iç denetim bu çerçevenin ana başlıklarıdır. Her başlıkta asıl mantık, riskin sahiplenilmesi, kontrolün yazılı ve izlenebilir kurulması, sorumlulukların ayrıştırılması ve kanıtlanabilir kayıt üretilmesidir.

Tebliğ iç denetim ve gözetimi de bilgi sistemleri yönetiminin ayrılmaz parçası olarak düzenler. Bilgi sistemleri iç denetimi yılda en az bir kez gerçekleştirilir; denetimin bilgi sistemlerinin tasarımı ve işleyişinden sorumlu kişilerce yürütülmemesi esastır. İç denetim sonucunda ulaşılan tespitler rapora bağlanır, bilgi güvenliği sorumlusu bu tespitleri tarihli aksiyon planına dönüştürür ve üst yönetim bu plana uyumu takip eder. Bu yapı, VII-128.10'un bilgi sistemleri yönetimini tek seferlik uyum çalışması değil, politika, risk, kontrol, kayıt, süreklilik ve denetim döngüsü olarak kurguladığını gösterir.

2.3.3 · Bilgi Sistemleri Bağımsız Denetim Tebliği III-62.2

Bilgi Sistemleri Bağımsız Denetiminin Kapsamı ve Raporlama Mantığı

> **KISACA**
> Bilgi Sistemleri Bağımsız Denetim Tebliği, sermaye piyasası kurumlarının bilgi sistemleri yönetimi ve işletimi kapsamındaki faaliyet, yazılım, donanım ve kontrollerinin bağımsız denetimini düzenler. Denetimin amacı; bilgi sistemlerinin yönetim ilkelerine uyumluluğu, etkinliği ve yeterliliği hakkında görüş oluşturmaktır. Tebliğ; denetime tabi kurumlar, denetçi ve kuruluş nitelikleri, denetim sözleşmesi, çalışma, kanıt, raporlama, bildirim ve sorumluluk esaslarıyla bağımsız denetim sürecine kurumsal disiplin kazandırır.

III-62.2 sayılı düzenleme, bilgi sistemleri bağımsız denetimini sermaye piyasası kurumları için özel bir güvence faaliyeti olarak konumlandırır. Bilgi sistemleri bağımsız denetimi, kurumun bilgi sistemleri yönetimi ve işletimi kapsamındaki faaliyetlerini, yazılım ve donanım bileşenlerini ve bu sistemler üzerinde tesis edilen kontrolleri bilgi sistemleri yönetim ilkeleri doğrultusunda değerlendirir. Sonuçta denetlenen kurumun kontrollerinin uyumluluğu, etkinliği ve yeterliliği hakkında görüş oluşturulur ve bu görüş rapora bağlanır.

Tebliğin getirdiği çerçevede denetim, yalnız teknik güvenlik testi değildir. Denetçi yönetişim, risk yönetimi, süreç kontrolleri, erişim, değişiklik yönetimi, süreklilik, veri bütünlüğü, dış kaynak kullanımı ve raporlama altyapısı gibi alanları birlikte değerlendirir. Denetimin kapsamı, denetlenen kurumun faaliyet modeli ve bilgi sistemlerinin önemliliğiyle bağlantılıdır. Finansal ve operasyonel süreçlerin bilgi sistemlerine bağımlılığı arttıkça denetim bulgularının kurumun genel kontrol ortamı üzerindeki etkisi de artar.

Bağımsızlık, yetkinlik ve kanıt toplama denetimin güvenilirliğini belirler. Denetim kuruluşu ve denetçiler yeterli mesleki niteliklere sahip olmalı, bağımsızlığı zedeleyen ilişkilerden kaçınmalı ve çalışmayı planlı biçimde yürütmelidir. Denetim kanıtı, görüşü destekleyecek yeterlilik ve uygunlukta olmalıdır. Bulguların önem derecesi, risk etkisi ve kurumun kontrol ortamındaki karşılığı değerlendirilir. Raporlama aşamasında görüş, kapsam, sınırlamalar, bulgular ve sonuçlar açık biçimde sunulur.

Bu Tebliğ, bilgi sistemleri denetçisine mesleki çalışmanın mevzuat dayanağını verir. Denetçi, teknik açıkları tek tek listelemekle yetinmez; kurumun bilgi sistemleri yönetim ilkelerine ne ölçüde uyduğunu ve bu uyumun faaliyet güvenliği açısından ne ifade ettiğini değerlendirir. Sermaye piyasası kurumlarında sistem kesintisi, veri kaybı, yetkisiz erişim veya kontrol zafiyeti yatırımcıları ve piyasa düzenini etkileyebilir. Bu nedenle bilgi sistemleri bağımsız denetimi, teknoloji kontrolünü sermaye piyasası güvenliğiyle birleştiren özel bir denetim alanıdır.

2.3.4 · İlgili Diğer Mevzuat ve Uluslararası Düzenlemeler

Uluslararası Çerçeveler ve Bilgi Sistemleri Denetim Referansları

> **KISACA**
> Bilgi sistemleri yönetimi ve denetimi, yalnız yerel sermaye piyasası düzenlemeleriyle değil, uluslararası standartlar ve iyi uygulama çerçeveleriyle de şekillenir. COBIT, ITIL, ISO standartları, ISACA çerçeveleri, uluslararası denetim ve etik standartları; yönetişim, kontrol, hizmet yönetimi, bilgi güvenliği, risk ve güvence çalışmalarında ortak dil sağlar. Denetçi bu düzenlemeleri yerel mevzuatın yerine geçirmek için değil, kontrol tasarımını, kanıt kalitesini ve iyi uygulama beklentisini yorumlamak için kullanır.

Bilgi sistemleri denetimi, teknoloji, süreç, insan ve kontrol yapılarının birlikte değerlendirildiği disiplinler arası bir alandır. Bu nedenle denetçi yalnız yerel mevzuatı bilmekle yetinemez; uluslararası standartlar ve iyi uygulama çerçeveleri de denetim muhakemesine yön verir. COBIT, bilgi teknolojileri yönetişimi ve kontrol hedefleri bakımından; ITIL, hizmet yönetimi süreçleri bakımından; ISO standartları, bilgi güvenliği ve yönetim sistemi yaklaşımı bakımından önemli referanslar sunar. ISACA tarafından geliştirilen çerçeveler de bilgi sistemleri denetimi ve güvence çalışmalarının mesleki dilini güçlendirir.

Uluslararası düzenlemelerin ortak amacı, kurumların bilgi sistemlerini iş hedefleriyle uyumlu, riskleri yönetilmiş, performansı izlenebilir ve kontrolleri test edilebilir biçimde yönetmesini sağlamaktır. Denetçi, bu çerçevelerden yararlanarak kontrol alanlarını sınıflandırabilir, süreç olgunluğunu değerlendirebilir, risk-kontrol ilişkisini kurabilir ve bulguların önemini daha tutarlı açıklayabilir. Ancak uluslararası çerçeveler yerel mevzuatın yerine geçmez; denetlenen kurumun tabi olduğu zorunlu düzenlemeler öncelikle dikkate alınır.

Uluslararası denetim ve etik standartları da bilgi sistemleri denetiminin güvence niteliğini destekler. Kanıt toplama, örnekleme, önemlilik, risk değerlendirmesi, raporlama, bağımsızlık ve mesleki şüphecilik gibi kavramlar yalnız finansal denetime özgü değildir; bilgi sistemleri denetiminde de karşılık bulur. Denetçinin görüşü yeterli ve uygun kanıta dayanmalı, kullanılan kriterler açık olmalı ve rapor kullanıcıları çalışmanın kapsamını anlayabilmelidir. Etik standartlar ise denetçinin bağımsızlığını, tarafsızlığını ve gizlilik yükümlülüğünü korur.

Bu konu, denetçiye mevzuat ile iyi uygulama arasındaki ilişkiyi kurmayı öğretir. Bir kontrol yasal olarak zorunlu olmasa bile kurumun risk profili açısından gerekli olabilir; bazı iyi uygulamalar da yerel düzenlemelerin yorumlanmasını kolaylaştırır. Denetçi, COBIT, ITIL, ISO ve ISACA gibi referansları mekanik kontrol listesi olarak değil, denetim amacına uygun değerlendirme araçları olarak kullanmalıdır. Sağlam bilgi sistemleri denetimi, yerel düzenlemeyi uluslararası mesleki birikimle birlikte okuyabildiğinde daha güvenilir hale gelir.

2.3.5 · Etik İlke ve Kurallar (Bağımsız Denetçiler İçin Etik Kurallar ve ISACA'nın Etik Kuralları)

Bilgi Sistemleri Denetiminde Etik, Bağımsızlık ve Mesleki Özen

> **KISACA**
> Bilgi sistemleri denetiminde etik kurallar, denetçinin bağımsız, tarafsız, dürüst, yetkin, gizliliğe saygılı ve mesleki özenle çalışmasını gerektirir. Bağımsız denetçiler için etik kurallar ile ISACA'nın etik ilkeleri; çıkar çatışmalarından kaçınma, yeterli kanıta dayanmadan görüş vermeme, gizli bilgiyi koruma, mesleki yeterliliği sürdürme ve rapor kullanıcılarını yanıltmama yükümlülüklerini vurgular. Etik zemin zayıfsa teknik denetim bulguları güvenilirliğini kaybeder.

Bilgi sistemleri bağımsız denetimi, kurumun teknoloji kontrol ortamı hakkında güvence ürettiği için yüksek etik standart gerektirir. Denetçi, sistemlere, kayıtlara, güvenlik zafiyetlerine, müşteri verilerine ve kurumun hassas iş süreçlerine erişebilir. Bu erişim, güçlü gizlilik ve dürüstlük yükümlülüğü doğurur. Bağımsız denetçiler için etik kurallar ve ISACA'nın etik ilkeleri, denetçinin yalnız teknik yeterlilikle değil, bağımsız ve güvenilir mesleki davranışla hareket etmesini hedefler.

Bağımsızlık ve tarafsızlık etik çerçevenin merkezindedir. Denetçi, denetlenen kurumla çıkar ilişkisi içindeyse, önceki danışmanlık çalışmasını denetliyorsa veya bulguları yumuşatması için baskı altındaysa görüş güvenilirliği zedelenir. Çıkar çatışmaları tespit edilmeli, gerektiğinde iş kabul edilmemeli veya uygun koruyucu önlemler alınmalıdır. Dürüstlük ilkesi, denetçinin bulguları saklamamasını, kanıtı çarpıtmamasını ve rapor kullanıcılarını yanıltacak ifadelerden kaçınmasını gerektirir.

Mesleki yeterlilik ve özen, bilgi sistemleri denetiminde özellikle önemlidir. Teknoloji hızlı değiştiği için denetçi güncel riskleri, kontrol yaklaşımlarını, güvenlik tehditlerini, standartları ve mevzuatı izlemelidir. Yeterli ve uygun kanıt toplanmadan görüş oluşturulmamalıdır. Denetçi uzmanlık alanının sınırlarını bilmeli, gerektiğinde özel uzman desteği almalı ve kullandığı yöntemleri işin kapsamına uygun seçmelidir. Gizlilik ilkesi, denetim sırasında edinilen bilgilerin yetkisiz paylaşılmamasını ve kişisel ya da ticari amaçla kullanılmamasını gerektirir.

Etik kurallar denetim kalitesinin görünmeyen taşıyıcısıdır. Teknik olarak doğru testler yapılmış olsa bile denetçi bağımsız değilse veya rapor çıkar baskısıyla yazılmışsa sonuç kullanılamaz hale gelir. Bilgi sistemleri denetiminde bulgular, kurumun güvenliği, yatırımcıların korunması ve piyasa düzeni üzerinde etkili olabilir. Bu nedenle denetçi; dürüstlük, objektiflik, gizlilik, mesleki yeterlilik, özen ve kamu yararı bilinciyle hareket etmelidir. Etik davranış, denetim görüşünün kabul edilebilirliği için teknik kanıt kadar zorunludur.

3.1.1 · Proje Planlaması

Bilgi Sistemleri Projelerinde Planlama ve Kontrol Zemini

KISACA

Proje planlaması, bilgi sistemleri projesinin amacını, kapsamını, çıktısını, zamanını, maliyetini, kaynaklarını, risklerini ve yönetişim düzenini baştan tanımlayan aşamadır. Proje özgün, tekrarlanmayan, belirli kısıtları ve kontrol ihtiyacı olan faaliyetler bütünüdür. Planlama; fizibilite, kapsam belirleme, maliyet tahmini, zaman çizelgesi, Gantt, PERT, kritik yol, kaynak ve risk planı gibi araçlarla projenin yönetilebilir hale gelmesini sağlar. Denetçi için planlama kalitesi, projenin kontrol edilebilirliğinin ilk kanıtıdır.

Proje planlaması, bilgi sistemleri geliştirme veya uygulama çalışmalarında başarının temelini oluşturur. Proje, belirli bir başlangıç ve bitiş zamanı olan, özgün bir ürün, hizmet veya sonuç üretmeyi amaçlayan, kapsam, zaman ve maliyet kısıtları altında yürütülen faaliyettir. Bilgi sistemleri projeleri çoğu zaman iş süreçlerini, veri akışlarını, kullanıcı rollerini ve kontrol ortamını etkilediği için planlama yalnız teknik görev listesi değildir. Projenin neden yapıldığı, hangi sorunu çözeceği, hangi faydayı sağlayacağı ve hangi sınırlar içinde yürütüleceği açıkça belirlenmelidir.

Planlama aşamasında kapsamın tanımlanması kritik önemdedir. Kapsam belirsizse gereksinimler sürekli değişir, maliyet ve zaman tahminleri bozulur, kullanıcı beklentileri yönetilemez. Fizibilite çalışması teknik, ekonomik, operasyonel ve hukuki açıdan projenin yapılabilirliğini değerlendirir. Mevcut durum analizi, paydaş ihtiyaçları, alternatif çözümler, dış kaynak kullanımı, bulut veya hazır ürün seçenekleri ve güvenlik gereksinimleri bu aşamada ele alınabilir. Sağlam fizibilite, projenin yalnız mümkün olup olmadığını değil, risklere rağmen değer yaratıp yaratmayacağını sorgular.

Zaman ve maliyet planlaması, projenin izlenebilir olmasını sağlar. İş kırılım yapısı, görev atamaları, zaman çizelgesi, Gantt şeması, PERT ve kritik yol yöntemi gibi araçlar faaliyetler arasındaki bağımlılıkları ve gecikme etkilerini görünür kılar. Kaynak planı insan gücü, bütçe, donanım, yazılım ve dış hizmet ihtiyacını belirler. Risk planı ise kapsam değişikliği, maliyet aşımı, teknik başarısızlık, güvenlik açığı, kullanıcı kabulü sorunu ve tedarikçi gecikmesi gibi tehditlere karşı önlem üretir. Planlama, kontrolün ön koşuludur.

Bilgi sistemleri denetçisi proje planını incelerken yalnız belge varlığına bakmaz. Proje hedefleri iş ihtiyaçlarıyla uyumlu mu, kapsam ölçülebilir mi, sorumluluklar atanmış mı, değişiklik yönetimi tanımlı mı, riskler gerçekçi mi ve yönetim onayı var mı sorularını değerlendirir. Planlama zayıfsa sonraki aşamalarda yapılan geliştirme ve testlerin başarısı da kuşkulu hale gelir. Bu nedenle proje planlaması, bilgi sistemleri projelerinde yönetişim, kaynak yönetimi ve kontrol kalitesinin ilk göstergesidir.

3.1.2 · Proje İşletimi

Projenin Yürütülmesi, İzlenmesi ve Kapatılması

> **KISACA**
> Proje işletimi, planlanan bilgi sistemleri projesinin açılış, yürütme, izleme, kontrol ve kapatma aşamalarını kapsar. Proje ekibi görevleri yerine getirir, kaynaklar kullanılır, ilerleme raporlanır, kapsam değişiklikleri değerlendirilir, zaman, maliyet, risk ve faydalar izlenir. Kapatma aşamasında çıktılar teslim edilir, kabul alınır, dokümantasyon tamamlanır ve öğrenilen dersler kayda geçirilir. Denetçi açısından proje işletimi, planın fiilen uygulanıp uygulanmadığını ve kontrol mekanizmalarının çalışıp çalışmadığını gösterir.

Proje işletimi, planlama aşamasında tanımlanan hedeflerin uygulamaya dönüştüğü süreçtir. Proje açılışında sponsor, proje yöneticisi, ekip, paydaşlar, görevler, iletişim düzeni ve çalışma kuralları netleştirilir. Bilgi sistemleri projelerinde bu aşama özellikle önemlidir; çünkü iş birimleri, yazılım geliştiriciler, altyapı ekipleri, güvenlik, uyum, dış tedarikçiler ve kullanıcılar aynı hedefe yönlendirilmelidir. Proje planı kağıt üzerinde güçlü görünse bile işletim süreci zayıfsa çıktı zamanında, bütçesinde veya istenen kalitede tamamlanmayabilir.

Yürütme aşamasında ekipler belirlenen görevleri yerine getirir ve proje yöneticisi faaliyetlerin plana uygun ilerlemesini sağlar. Kaynak tahsisi, görev takibi, toplantılar, raporlamalar, sorun kayıtları ve karar mekanizmaları bu dönemde işler. Değişiklik yönetimi, proje işletiminin en kritik kontrol alanlarından biridir. Kapsam değişikliği kontrolsüz yapılırsa maliyet artar, takvim uzar, test kapsamı bozulur ve kullanıcı beklentileri yönetilemez. Bu nedenle değişikliklerin etkisi, onayı ve dokümantasyonu düzenli biçimde izlenmelidir.

Kontrol ve izleme aşaması, zaman, maliyet, kalite, risk, kaynak kullanımı ve beklenen faydaların düzenli olarak takip edilmesini içerir. Risk yönetimi yalnız planlama sırasında yapılan listeleme değildir; proje ilerledikçe yeni riskler ortaya çıkar ve mevcut risklerin etkisi değişebilir. Kaynak kullanımı, ekip kapasitesi, tedarikçi performansı, maliyet gerçekleşmeleri ve kilometre taşları ölçülmelidir. Proje faydalarının izlenmesi de önemlidir; bilgi sistemleri projesi teknik olarak teslim edilse bile iş hedeflerine katkı sağlamıyorsa başarı eksik kalır.

Projenin kapatılması, çıktının teslim edilmesi, kullanıcı kabulünün alınması, kalan sorunların belgelenmesi, sözleşme ve mali kapanışın yapılması, erişimlerin ve ortamların düzenlenmesi ve öğrenilen derslerin kaydedilmesini kapsar. Denetçi proje işletimini değerlendirirken karar kayıtları, değişiklik onayları, ilerleme raporları, risk izleme belgeleri, test ve kabul kayıtları gibi kanıtları inceler. İşletim süreci disiplinli yürütülmüşse proje sonucu daha denetlenebilir ve sürdürülebilir olur.

3.2.1 · Sistem Geliştirme Süreçleri

SDLC, Gereksinimden Üretim Ortamına Kontrollü Geliştirme

KISACA
Sistem geliştirme süreçleri, bilgi sistemlerinin fikir aşamasından üretim ortamına alınmasına kadar izlenen kontrollü yaşam döngüsünü ifade eder. SDLC; fizibilite, gereksinim analizi, tasarım, geliştirme, test, kullanıcı kabulü, üretime geçiş ve uygulama sonrası değerlendirme aşamalarını içerir. Metodoloji seçimi, dokümantasyon, değişiklik yönetimi, güvenlik, kalite, veri geçişi ve test kontrolleri sürecin başarısını belirler. Denetçi için SDLC, sistemin güvenilir ve kontrol edilebilir biçimde geliştirilip geliştirilmediğini değerlendirme çerçevesidir.

Sistem geliştirme süreçleri, bir bilgi sisteminin ihtiyaçtan çalışan çözüme dönüşmesini sağlayan düzenli faaliyetler bütünüdür. Sistem geliştirme yaşam döngüsü yaklaşımı, her aşamada amaç, sorumluluk, çıktı ve kontrol noktaları belirleyerek projeyi yönetilebilir hale getirir. Bu yaklaşım kurum içi yazılım geliştirmede kullanılabildiği gibi hazır ürün veya üçüncü taraf sistem ediniminde de uygulanabilir. Amaç, iş gereksinimlerini karşılayan, güvenli, kaliteli, sürdürülebilir ve kontrol edilebilir bir sistem ortaya çıkarmaktır.

Süreç genellikle fizibilite çalışması ve gereksinimlerin belirlenmesiyle başlar. İş hedefleri, mevcut sorun, kapsam, paydaş beklentileri, maliyet-fayda dengesi, teknik seçenekler, güvenlik ve uyum gereksinimleri değerlendirilir. Ardından tasarım aşamasında sistem mimarisi, veri yapısı, arayüzler, iş kuralları, kontroller ve entegrasyonlar belirlenir. Geliştirme aşamasında kodlama veya yapılandırma yapılır; bu süreçte versiyon kontrolü, görevler ayrılığı, kod gözden geçirme ve güvenli geliştirme ilkeleri önem taşır.

Test süreçleri sistem geliştirme kalitesinin ana kanıtıdır. Birim, entegrasyon, sistem, güvenlik, performans ve kullanıcı kabul testleri farklı riskleri ölçer. Test ortamının üretimden ayrılması, test verisinin güvenliği, hata kayıtlarının izlenmesi ve düzeltmelerin yeniden test edilmesi gerekir. Üretim ortamına aktarım aşamasında geçiş planı, geri dönüş planı, veri migrasyonu, kullanıcı eğitimi, erişim yetkileri ve operasyonel hazırlıklar kontrol edilmelidir. Kontrolsüz geçiş, sistem kesintisi veya veri bütünlüğü sorunu yaratabilir.

Denetçi sistem geliştirme süreçlerini değerlendirirken kullanılan metodolojiyi, dokümantasyonu, onayları, değişiklik kayıtlarını, test kanıtlarını ve üretime geçiş kontrollerini inceler. Agile, şelale, hızlı uygulama geliştirme veya başka bir yöntem kullanılması tek başına yeterli değildir; yöntemin kuruma uygun uygulanması gerekir. Geliştirme süreci kontrolsüzse uygulama kontrolleri zayıf kalabilir, yetkisiz değişiklik yapılabilir veya kullanıcı gereksinimleri karşılanmayabilir. Bu nedenle SDLC, bilgi sistemleri güvenilirliğinin temel denetim alanıdır.

3.2.2 · Sistem Bakım ve Destek Süreçleri

Canlı Sistemlerde Bakım, Destek ve Değişiklik Kontrolü

> **KISACA**
> Sistem bakım ve destek süreçleri, üretime alınmış uygulama ve altyapıların güvenli, kesintisiz ve iş ihtiyaçlarına uygun biçimde çalışmasını sürdürür. Hata düzeltme, küçük geliştirme, yama, sürüm yükseltme, kullanıcı desteği, olay ve problem yönetimi, konfigürasyon, değişiklik onayı, test ve üretime aktarım bu sürecin parçalarıdır. Denetçi açısından bakım ve destek, canlı sistemlerde yetkisiz değişiklik, hizmet kesintisi, veri bozulması ve kontrol zafiyeti risklerinin yönetilip yönetilmediğini gösterir.

Sistem geliştirme tamamlandığında bilgi sistemleri riski bitmez; canlı ortamda bakım ve destek süreci başlar. Üretimdeki sistemler iş süreçleriyle bütünleşik çalıştığı için hata düzeltmeleri, yama uygulamaları, sürüm değişiklikleri, kullanıcı talepleri ve performans sorunları kontrollü biçimde yönetilmelidir. Bakım ve destek sürecinin amacı, sistemin güvenli, kullanılabilir, güncel ve iş gereksinimleriyle uyumlu kalmasını sağlamaktır. Bu süreç zayıfsa küçük bir değişiklik bile veri kaybına, kesintiye veya kontrol ihlaline yol açabilir.

Bakım faaliyetleri düzeltici, uyarlayıcı, iyileştirici veya önleyici nitelikte olabilir. Düzeltici bakım hataların giderilmesini, uyarlayıcı bakım mevzuat veya altyapı değişikliklerine uyumu, iyileştirici bakım performans ve kullanılabilirlik artışını, önleyici bakım ise gelecekteki sorunları azaltmayı hedefler. Kullanıcı destek süreçleri olay kayıtlarının alınması, önceliklendirilmesi, çözülmesi ve kapanışının belgelenmesini gerektirir. Problem yönetimi tekrarlayan olayların kök nedenini bulmaya çalışır. Hizmet masası, izleme ve eskalasyon yapısı bu sürecin görünür yüzüdür.

Değişiklik yönetimi bakım ve destek süreçlerinin en kritik kontrol alanıdır. Canlı sistemde yapılan değişiklikler talep, etki analizi, onay, geliştirme, test, kullanıcı kabulü, üretime aktarım ve geri dönüş planı gibi adımlarla yürütülmelidir. Acil değişiklikler bile sonradan gözden geçirilmeli ve belgelenmelidir. Konfigürasyon yönetimi, hangi bileşenin hangi sürümde olduğunu ve değişikliklerin hangi varlıkları etkilediğini izlemeyi sağlar. Yetersiz konfigürasyon bilgisi, hata çözümünü ve denetim izini zorlaştırır.

Denetçi bakım ve destek süreçlerini incelerken olay kayıtları, değişiklik talepleri, onaylar, test kanıtları, sürüm geçiş kayıtları, erişim yetkileri, yama yönetimi ve hizmet seviyesi raporlarını değerlendirir. Amaç, canlı sistemlerde değişikliklerin yetkili, test edilmiş, izlenebilir ve geri alınabilir biçimde yapıldığını görmektir. Bakım süreci disiplinli yürütülmezse geliştirme aşamasında kurulan kontroller zamanla aşınır. Bu nedenle bakım ve destek, bilgi sistemleri kontrol ortamının sürekliliğini sağlayan ana süreçtir.

3.2.3 · Uygulama Kontrolleri

Girdi, İşleme ve Çıktı Kontrolleriyle Uygulama Güvenilirliği

KISACA

Uygulama kontrolleri, belirli bir bilgi sisteminde işlemlerin yetkili, tam, doğru, geçerli ve izlenebilir biçimde yürütülmesini sağlayan kontrollerdir. Giriş veya kaynak kontrolleri veri alınırken doğruluk ve yetkiyi; işleme kontrolleri hesaplama, sınıflandırma, bütünlük ve hata yönetimini; çıktı kontrolleri rapor ve sonuçların doğru kişilere doğru biçimde ulaştırılmasını güvence altına alır. Denetçi için uygulama kontrolleri, iş sürecinin bilgi sistemi üzerinde güvenilir sonuç üretip üretmediğini test etmenin ana alanıdır.

Uygulama kontrolleri, belirli bir uygulama veya iş süreci içinde verinin doğru alınmasını, doğru işlenmesini ve doğru çıktıya dönüşmesini sağlayan mekanizmalardır. Genel bilgi sistemleri kontrolleri altyapı, erişim ve değişiklik yönetimi gibi geniş alanları kapsarken, uygulama kontrolleri doğrudan işlem düzeyine iner. Bir sermaye piyasası kurumunda müşteri emri, hesap hareketi, raporlama, ücret hesaplama veya portföy kaydı gibi işlemler uygulama kontrollerine dayanır. Bu kontroller zayıfsa sistem çalışıyor görünse bile hatalı veya yetkisiz sonuç üretebilir.

Giriş veya kaynak kontrolleri, verinin sisteme alınma anındaki doğruluğunu ve geçerliliğini hedefler. Zorunlu alan kontrolleri, format kontrolleri, limit kontrolleri, yetki kontrolleri, çift kayıt önleme, sıra numarası, mutabakat ve kaynak belge eşleştirme gibi araçlar bu gruba girer. Amaç, yanlış, eksik, yetkisiz veya mükerrer verinin sisteme girmesini önlemektir. Denetçi, giriş kontrollerinin yalnız tanımlı olup olmadığını değil, istisnaları nasıl ele aldığını ve kullanıcıların kontrolü aşıp aşamadığını da değerlendirir.

İşleme kontrolleri, sisteme alınan verinin doğru hesaplanmasını, sınıflandırılmasını, aktarılmasını ve saklanmasını sağlar. Toplam kontrolleri, işlem günlükleri, hata raporları, otomatik hesaplama kuralları, dosya bütünlük kontrolleri ve ara mutabakatlar bu kapsamda kullanılabilir. Çıktı kontrolleri ise raporların tam, doğru, zamanında ve yetkili kişilere ulaştırılmasına odaklanır. Çıktıların dağıtım listeleri, rapor erişimleri, istisna raporları, kullanıcı incelemeleri ve arşiv kayıtları kontrol ortamının parçasıdır. Girdi, işleme ve çıktı kontrolleri birlikte çalışmadığında uçtan uca güvence sağlanamaz.

Bilgi sistemleri denetçisi uygulama kontrollerini test ederken iş sürecini anlamalı, kritik işlem noktalarını belirlemeli ve kontrollerin tasarım ile işletim etkinliğini kanıtlarla değerlendirmelidir. Test verisi, yeniden hesaplama, örnekleme, log incelemesi, kullanıcı yetki analizi ve istisna raporları bu çalışmada kullanılabilir. Uygulama kontrollerinin kalitesi, finansal bilgi, müşteri verisi ve operasyonel sonuçların güvenilirliğini doğrudan etkiler. Bu nedenle uygulama kontrolleri, teknik sistem denetimi ile iş süreci denetiminin kesiştiği ana güvence alanıdır.

4.1.1 · Bilgi Sistemleri Altyapısı Elemanları

Donanım, Yazılım, Veri ve Arayüzlerin İşletim Temeli

> **KISACA**
> Bilgi sistemleri altyapısı elemanları, kurumun bilgi sistemlerini çalıştıran donanım, yazılım, depolama, ağ, sunucu, işletim sistemi, veri tabanı, arayüz ve kullanıcı bileşenlerinden oluşur. Kullanıcı cihazları, sunucular, ağ ekipmanları, sistem yazılımları, veri yönetişimi, ara katmanlar ve son kullanıcı bilgi işlemi iş süreçlerinin teknik zeminini sağlar. Denetçi açısından altyapı elemanları, varlık envanteri, konfigürasyon, bakım, performans, erişim ve güvenlik kontrollerinin kurulacağı temel kapsamı belirler.

Bilgi sistemleri altyapısı, kurumun iş süreçlerini çalıştıran teknik bileşenlerin bütünüdür. Donanım ve yazılım bu altyapının en görünür parçalarıdır; ancak altyapı yalnız bilgisayar veya sunucudan ibaret değildir. Kullanıcı cihazları, sunucu donanımları, depolama ortamları, ağ ekipmanları, işletim sistemleri, veri tabanları, ara katman yazılımları, uygulamalar, arayüzler ve bunları yöneten insan süreçleri birlikte çalışır. Bir iş sürecinin güvenilirliği, çoğu zaman bu bileşenlerin doğru yapılandırılmasına ve izlenmesine bağlıdır.

Donanım bileşenleri merkezi işlem birimi, bellek, depolama, çevre birimleri, sunucular, kullanıcı cihazları ve ağ cihazları gibi unsurları kapsar. Sunucu bilgisayarlar, ana iş uygulamalarını, veri tabanlarını, dosya hizmetlerini veya kimlik doğrulama servislerini çalıştırabilir. Ağ cihazları ise sistemler arasındaki iletişimi sağlar. Donanım yönetiminde envanter, bakım programları, performans izleme, kapasite takibi ve tedarik süreci önemlidir. Kayıt dışı veya izlenmeyen donanım, hem operasyonel hem güvenlik riski doğurur.

Yazılım bileşenleri işletim sistemleri, sistem yardımcı programları, veri tabanı yönetim sistemleri, uygulamalar, ağ yazılımları ve güvenlik araçlarından oluşur. İşletim sistemi bütünlüğü, sıkılaştırılmış baz konfigürasyonlar, yama yönetimi ve sanallaştırma kontrolleri altyapı güvenilirliğini etkiler. Veri yönetişimi de altyapının ayrılmaz parçasıdır; verinin yaşam döngüsü, veri modelleri, veri tabanı güvenliği ve veri ambarı yapısı kontrol edilmelidir. Ara katmanlar ve sistem arayüzleri, farklı uygulamalar arasında veri akışını sağladığı için hata ve yetkisiz erişim riski taşıyabilir.

Denetçi altyapı elemanlarını değerlendirirken varlıkların tam ve güncel envanterini, sahipliklerini, konfigürasyon standartlarını, erişim kontrollerini, bakım kayıtlarını, kapasite durumunu ve güvenlik önlemlerini inceler. Altyapı unsurlarının görünürlüğü yoksa riskleri ölçmek de güçleşir. Son kullanıcı bilgi işlemi gibi merkezi kontrol dışındaki araçlar da finansal veya operasyonel kararları etkileyebilir. Bu nedenle altyapı elemanları, bilgi sistemleri işletiminin kapsamını ve denetimin başlangıç noktasını oluşturur.

4.1.2 · Bilgi Sistemleri Altyapısı Teknolojileri

Bulut, Büyük Veri, Yapay Zekâ, RPA ve Blok Zincir Teknolojileri

KISACA

Bilgi sistemleri altyapısı teknolojileri; bulut bilişim, büyük veri, nesnelerin interneti, yapay zekâ, robotik süreç otomasyonu ve blok zincir gibi modern çözümleri kapsar. Bu teknolojiler ölçeklenebilirlik, otomasyon, veri işleme ve yeni hizmet modelleri sağlarken güvenlik, mahremiyet, üçüncü taraf bağımlılığı, veri bütünlüğü, model riski ve denetlenebilirlik gibi yeni riskler doğurur. Denetçi bu teknolojileri yalnız teknik yenilik olarak değil, kontrol ortamını değiştiren altyapı tercihleri olarak değerlendirmelidir.

Bilgi sistemleri altyapısı teknolojileri, kurumların iş süreçlerini daha hızlı, esnek ve veri odaklı hale getiren modern araçları içerir. Bulut bilişim, kurumlara altyapı, platform veya yazılım hizmetlerini ihtiyaç oldukça kullanma imkânı sunar. Büyük veri, yüksek hacim, hız ve çeşitlilikteki verilerin işlenmesini sağlar. Nesnelerin interneti fiziksel cihazları veri üreten uç noktalara dönüştürür. Yapay zekâ, otomasyon ve karar destek kabiliyeti getirir. Robotik süreç otomasyonu tekrarlı iş adımlarını yazılım robotlarıyla yürütür. Blok zincir ise dağıtık kayıt ve kriptografik doğrulama yaklaşımıyla farklı güven modeli sunar.

Bu teknolojilerin ortak faydası, iş süreçlerine esneklik ve hız kazandırmasıdır; ancak her fayda yeni kontrol ihtiyacı doğurur. Bulut kullanımında veri konumu, erişim, şifreleme, hizmet seviyesi, sağlayıcı denetimi ve çıkış stratejisi önemlidir. Büyük veri projelerinde veri kalitesi, kaynak doğruluğu, mahremiyet ve saklama politikaları kritik hale gelir. Nesnelerin interneti cihazlarında kimlik doğrulama, güncelleme ve ağ ayrıştırması zayıfsa saldırı yüzeyi büyür. Yapay zekâ uygulamalarında model doğruluğu, önyargı, açıklanabilirlik ve güvenli kullanım sorgulanmalıdır.

Robotik süreç otomasyonu ve blok zincir de özel riskler taşır. RPA robotları genellikle insan kullanıcı gibi sistemlere bağlanır; bu nedenle yetki, görevler ayrılığı, işlem günlüğü ve değişiklik yönetimi dikkatle kurulmalıdır. Blok zincir uygulamalarında özel anahtar güvenliği, akıllı sözleşme hataları, ağ yapısı, işlem geri alınamazlığı ve entegrasyon kontrolleri denetim alanına girer. Yeni teknolojiler kurumun kontrol sorumluluğunu ortadan kaldırmaz; aksine bazı kontrolleri üçüncü taraf, otomasyon veya algoritma katmanlarına taşır.

Denetçi altyapı teknolojilerini değerlendirirken önce kurumun hangi teknolojiyi hangi iş amacıyla kullandığını anlamalıdır. Sonra veri akışı, sorumluluk paylaşımı, erişim modeli, güvenlik kontrolleri, izleme, yedekleme, süreklilik, sözleşme koşulları ve denetim izleri incelenmelidir. Teknoloji adı tek başına güvence sağlamaz. Bulut, yapay zekâ veya blok zincir kullanımı; doğru yönetişim, risk analizi ve kontrol tasarımı yoksa operasyonel ve düzenleyici riski artırabilir. Bu nedenle modern altyapı teknolojileri, denetimde risk odaklı ve iş süreciyle bağlantılı ele alınmalıdır.

4.2.1 · Hizmet Yönetimi

Bilgi Sistemleri Operasyonlarında Hizmet Masası ve Değişiklik Yönetimi

KISACA

Hizmet yönetimi, bilgi sistemleri hizmetlerinin kullanıcı ve iş birimi ihtiyaçlarına uygun, ölçülebilir ve kontrollü biçimde sunulmasını sağlar. Hizmet masası, talep yönetimi, olay yönetimi, problem yönetimi, değişiklik, sürüm, yama, konfigürasyon, hizmet seviyesi anlaşmaları, kaynak yönetimi ve yığın işler bu alanın ana süreçleridir. Denetçi açısından hizmet yönetimi, operasyonel sorunların kayda alınıp alınmadığını, kök nedenlerin analiz edilip edilmediğini ve değişikliklerin kontrollü yürütülüp yürütülmediğini gösterir.

Bilgi sistemleri hizmet yönetimi, kurumun teknoloji hizmetlerini iş ihtiyaçlarına uygun şekilde sunmasını ve bu hizmetleri ölçülebilir süreçlerle yönetmesini amaçlar. Hizmet masası, kullanıcıların olay, talep ve sorunlarını bildirdiği merkezi temas noktasıdır. Bu yapı, olayların kaybolmasını önler, önceliklendirme sağlar ve çözüm sürelerini izlenebilir hale getirir. Hizmet yönetimi yalnız kullanıcı şikâyetlerini çözmek değildir; kesintileri azaltmak, hizmet kalitesini yükseltmek ve iş sürekliliğini desteklemek için operasyonel kontrol ortamı kurmaktır.

Olay yönetimi, hizmetteki kesinti veya bozulmanın hızlı biçimde giderilmesine odaklanır. Olayın kaydedilmesi, sınıflandırılması, önceliklendirilmesi, atanması, çözülmesi ve kapatılması gerekir. Problem yönetimi ise tekrarlayan veya önemli olayların kök nedenini bulmaya çalışır. Olay yönetimi yangını söndürürken, problem yönetimi yangının neden çıktığını araştırır. Bu ayrım yapılmadığında aynı arızalar tekrar eder ve kullanıcı güveni azalır. Talep yönetimi ise standart kullanıcı isteklerinin kontrollü biçimde karşılanmasını sağlar.

Değişiklik, sürüm ve yama yönetimi hizmet yönetiminin en riskli alanlarından biridir. Canlı sistemlerde yapılan değişiklikler iş süreçlerini doğrudan etkileyebilir. Değişiklik taleplerinin etki analizi, onayı, testi, üretime aktarımı ve geri dönüş planı bulunmalıdır. Sürüm yönetimi, yeni veya güncellenmiş yazılımların kontrollü dağıtımını sağlar. Yama yönetimi güvenlik ve hata düzeltmeleri için önemlidir; ancak test edilmeden uygulanan yamalar kesinti yaratabilir. Konfigürasyon yönetimi, hizmeti oluşturan bileşenlerin ve aralarındaki ilişkilerin izlenmesini destekler.

Denetçi hizmet yönetimini değerlendirirken hizmet masası kayıtlarını, olay çözüm sürelerini, problem raporlarını, değişiklik onaylarını, yama takibini, hizmet seviyesi anlaşmalarını ve yığın iş kontrollerini inceler. Amaç, operasyonların kişisel çabayla değil, tanımlı ve kanıtlanabilir süreçlerle yürütüldüğünü görmektir. Hizmet yönetimi zayıfsa kurum sistem kesintilerini ölçemez, değişiklik riskini kontrol edemez ve kullanıcı taleplerini izleyemez. Bu nedenle hizmet yönetimi, bilgi sistemleri işletiminin günlük kontrol omurgasıdır.

4.2.2 · Gözetim, Kapasite ve Performans Yönetimi

Yedekleme, İzleme, Kapasite ve Kullanılabilirlik Kontrolleri

KISACA

Gözetim, kapasite ve performans yönetimi, bilgi sistemleri hizmetlerinin izlenmesini, yedeklenmesini, geri döndürülebilmesini, yeterli kapasiteyle çalışmasını ve kabul edilebilir performans seviyesinde kalmasını sağlar. Yedekleme teknolojileri, geri dönüş testleri, kapasite planlama, kullanılabilirlik yönetimi, sürekli iyileştirme, izleme, etki analizi ve hizmet seviyesi ölçümü bu alanın ana başlıklarıdır. Denetçi için bu süreçler, sistemlerin yalnız çalışıp çalışmadığını değil, sürdürülebilir ve ölçülebilir şekilde işletilip işletilmediğini gösterir.

Gözetim, kapasite ve performans yönetimi, bilgi sistemleri hizmetlerinin beklenen seviyede çalışmasını sağlamak için yürütülen operasyonel süreçlerdir. Kurumlar sistemleri yalnız kurmakla yetinemez; işlem hacmi, kullanıcı sayısı, veri büyüklüğü, ağ trafiği, depolama tüketimi, hata oranları ve hizmet kesintileri düzenli izlenmelidir. Gözetim, sorun ortaya çıktıktan sonra fark etmeyi değil, belirtileri erken yakalamayı hedefler. Bu nedenle izleme araçları, uyarı eşikleri, sorumluluklar ve raporlama mekanizması açık olmalıdır.

Yedekleme ve yedekten geri dönme kontrolleri, veri kaybı riskini azaltır. Tam, artımlı veya farklı yedekleme yöntemleri; dâhili veya harici depolama seçenekleri; yedekleme sıklığı, saklama süresi ve şifreleme kararları kurumun risk iştahına göre belirlenmelidir. Ancak yedek almak tek başına yeterli değildir. Yedekten geri dönüş testleri yapılmadığında, felaket anında yedeklerin bozuk, eksik veya kullanılamaz olduğu anlaşılabilir. Denetçi, yedekleme işlerinin başarı kayıtlarını ve geri dönüş testlerini özellikle inceler.

Kapasite yönetimi, mevcut ve gelecekteki iş yükünü karşılamak için kaynakların yeterli olup olmadığını değerlendirir. İşlemci, bellek, depolama, ağ bant genişliği ve uygulama performansı izlenir; büyüme eğilimleri analiz edilir. Kapasite planlaması yapılmazsa sistemler yoğun dönemlerde yavaşlar veya kesintiye uğrar. Kullanılabilirlik yönetimi, hizmetlerin erişilebilir kalmasını ve kesintilerin etkisinin azaltılmasını hedefler. Esneklik, yedeklilik, yük dengeleme ve hata toleransı bu kapsamda değerlendirilebilir.

Denetçi bu süreçlerde izleme kayıtları, kapasite raporları, performans metrikleri, yedekleme sonuçları, geri dönüş testleri, hizmet seviyesi raporları ve sürekli iyileştirme aksiyonlarını inceler. Amaç, operasyonların sezgisel değil ölçülebilir biçimde yönetildiğini görmektir. Kapasite ve performans yönetimi zayıfsa kurum kritik dönemlerde hizmet veremez; yedekleme zayıfsa veri kaybını telafi edemez. Bu yüzden gözetim, kapasite ve performans yönetimi bilgi sistemleri işletiminin dayanıklılığını gösteren ana kanıt alanıdır.

4.3.1 · Bilgi Sistemleri Sürekliliği Kavramları

İş Sürekliliği, Felaket Kurtarma ve Kritik Hizmetlerin Korunması

KISACA

Bilgi sistemleri sürekliliği, kesinti, felaket veya ciddi olay sonrasında kritik bilgi sistemleri hizmetlerinin kabul edilebilir seviyede sürdürülebilmesi ya da hedeflenen sürede geri yüklenebilmesidir. İş sürekliliği, felaket kurtarma, kritik süreç, etki analizi, kurtarma süresi hedefi, kurtarma noktası hedefi, risk azaltma, yedeklilik ve test kavramları bu alanın temelidir. Denetçi açısından süreklilik, kurumun bilgi sistemleri kesintilerine önceden planlanmış ve test edilmiş biçimde yanıt verebilme yetkinliğini gösterir.

Bilgi sistemleri sürekliliği, kurumun kritik iş süreçlerini destekleyen teknoloji hizmetlerinin kesinti anında kabul edilebilir düzeyde devam ettirilmesini veya belirlenen sürede geri yüklenmesini hedefler. Modern kurumlar bilgiye ve bilgi sistemlerine yüksek derecede bağımlıdır. Sistem kesintisi; işlem yapılamaması, müşteri hizmetinin durması, veri kaybı, gelir kaybı, itibar zararı ve düzenleyici sorunlar doğurabilir. Bu nedenle süreklilik, yalnız teknik yedekleme konusu değil, kurumun hayatta kalma ve hizmet sunma kapasitesiyle ilgilidir.

İş sürekliliği, kurumun kritik ürün ve hizmetlerini kesintiden sonra önceden belirlenmiş kabul edilebilir seviyede sürdürebilme yeteneğidir. Bilgi sistemleri sürekliliği bu genel çerçevenin teknoloji boyutudur. Felaket kurtarma ise bilgi sistemleri altyapısının, uygulamaların ve verinin olağanüstü durumdan sonra geri yüklenmesine odaklanır. Kritik süreçlerin belirlenmesi, iş etki analizi, risk değerlendirmesi, kurtarma süresi hedefi ve kurtarma noktası hedefi bu planlamanın temel kavramlarıdır. Hangi sistemin ne kadar sürede ve ne kadar veri kaybıyla geri döneceği önceden bilinmelidir.

Süreklilik yönetimi, kesintileri tamamen yok edeceğini iddia etmez; riskleri azaltır ve olay gerçekleştiğinde kurumun planlı hareket etmesini sağlar. Yedeklilik, alternatif lokasyon, yedek veri merkezi, bulut kurtarma, iletişim planı, acil durum ekipleri, rol ve sorumluluklar, kriz yönetimi ve tedarikçi bağımlılıkları birlikte değerlendirilir. Kritik üçüncü taraf hizmetlerinin süreklilik kapasitesi de kurumun kendi planı kadar önemlidir. Planlar güncel değilse veya test edilmemişse gerçek olayda işe yaramayabilir.

Denetçi bilgi sistemleri sürekliliği kavramlarını değerlendirirken kurumun kritik sistemlerini nasıl belirlediğini, iş etki analizini nasıl yaptığını, RTO ve RPO hedeflerini nasıl tanımladığını, süreklilik stratejisini hangi kanıtlara dayandırdığını ve planlarını test edip etmediğini inceler. Süreklilik, doküman varlığından ibaret değildir; eğitim, tatbikat, test sonuçları, iyileştirme aksiyonları ve yönetim sahipliği gerektirir. Bu nedenle bilgi sistemleri sürekliliği, operasyonel dayanıklılığın en önemli denetim alanlarından biridir.

4.3.2 · Bilgi Sistemleri Süreklilik Planının Yönetimi

Süreklilik Planının Kurulması, Test Edilmesi ve Güncel Tutulması

KISACA

Bilgi sistemleri süreklilik planının yönetimi, planın hazırlanması, uygulanması, test edilmesi, güncellenmesi ve kurumsal kültüre yerleştirilmesini kapsar. İş etki analizi, risk değerlendirmesi, kurtarma stratejisi, acil durum ekipleri, iletişim planı, yedekleme, alternatif altyapı, tatbikatlar, test sonuçları ve iyileştirme aksiyonları plan yönetiminin ana bileşenleridir. Denetçi açısından etkili plan, yalnız yazılmış değil; yönetimce sahiplenilmiş, düzenli test edilmiş ve değişen iş-teknoloji ortamına göre güncellenmiş plandır.

Bilgi sistemleri süreklilik planı, kritik bilgi sistemleri hizmetlerinin kesinti veya felaket sonrasında nasıl sürdürüleceğini ve nasıl geri yükleneceğini açıklayan yönetim aracıdır. Planın hazırlanması tek seferlik proje olarak görülmemelidir; süreklilik yönetimi yaşayan bir süreçtir. Kurumun iş modeli, kritik sistemleri, tedarikçileri, personeli, altyapısı ve riskleri değiştikçe plan da güncellenmelidir. Güncel olmayan bir plan, gerçek olay anında yanlış kişilere, yanlış sistemlere veya geçersiz prosedürlere yönlendirebilir.

Plan yönetiminin başlangıç noktası iş etki analizi ve risk değerlendirmesidir. İş etki analizi, hangi süreçlerin kritik olduğunu, kesintinin finansal, operasyonel, yasal ve itibari etkilerini ve kabul edilebilir kesinti sürelerini belirler. Risk değerlendirmesi ise doğal afet, siber saldırı, donanım arızası, veri kaybı, enerji kesintisi, personel erişimsizliği ve tedarikçi sorunu gibi tehditleri analiz eder. Bu bilgilerden hareketle kurtarma stratejisi seçilir. Strateji; yedekli sistem, alternatif lokasyon, bulut hizmeti, manuel geçici süreç veya üçüncü taraf destek gibi seçenekler içerebilir.

Etkili plan; ekipleri, sorumlulukları, iletişim kanallarını, karar yetkilerini, kurtarma adımlarını, öncelikli sistemleri, yedekleme ve geri dönüş prosedürlerini açıkça tanımlar. Tatbikatlar ve testler planın uygulanabilirliğini gösterir. Masa başı testleri, teknik geri dönüş testleri, kısmi veya tam kapsamlı tatbikatlar farklı güvence seviyeleri sağlar. Test sonucunda eksikler belirlenmeli, aksiyonlar atanmalı ve plan güncellenmelidir. Planın personele duyurulması ve kritik roller için eğitim verilmesi de yönetim sürecinin parçasıdır.

Denetçi süreklilik planının yönetimini incelerken plan dokümanını, onay tarihini, iş etki analizini, RTO ve RPO hedeflerini, test sonuçlarını, iyileştirme kayıtlarını, iletişim listelerini, tedarikçi bağımlılıklarını ve yedekleme geri dönüş kanıtlarını değerlendirir. Amaç, planın yalnız mevzuat uyumu için hazırlanmadığını, gerçek bir kesintide uygulanabilir olduğunu görmektir. Süreklilik planı düzenli test edilmiyor, güncellenmiyor veya yönetim tarafından sahiplenilmiyorsa kurumun kritik hizmetleri ciddi risk altındadır.

Bilgi Güvenliğini Kurumsal Bir Yönetim Sistemi Olarak Kurmak

> **KISACA**
> Bilgi güvenliği yönetimi, bilginin gizlilik, bütünlük ve erişilebilirlik özelliklerini korumak için kurum genelinde politika, rol, risk yönetimi, eğitim, ölçüm ve ihlal yönetimi süreçlerinin kurulmasıdır. Konu yalnızca teknik ekiplerin görevi değildir; üst yönetim sahipliği, onaylı politika, sorumlulukların yazılı tanımı, düzenli farkındalık, risk işleme kararları, sızma testi ve kanıtlanabilir izleme birlikte çalışmalıdır.

Bilgi güvenliği yönetimi, kurumun bilgi varlıklarını kabul edilebilir risk düzeyinde korumasını sağlayan yönetim disiplinidir. Temel amaç bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korumaktır. Gizlilik yetkisiz erişimi engeller, bütünlük bilginin tam ve doğru kalmasını sağlar, erişilebilirlik ise yetkili tarafların ihtiyaç anında bilgiye ulaşabilmesini ifade eder. Siber güvenlik bu çerçevenin dijital altyapı, ağ, cihaz ve siber uzay boyutuna odaklanır; bilgi güvenliği ise hem dijital hem fiziksel ortamdaki bilginin korunmasını kapsar. Bu nedenle güçlü bir kurum yaklaşımı iki kavramı birbirini tamamlayan yapılar olarak ele alır.

Yönetimin başlangıç noktası üst yönetim sahipliğidir. Bilgi güvenliği teknik bir operasyon gibi görülürse kurum genelinde kalıcı sonuç üretmez. Üst yönetim bilgi güvenliği politikasını onaylamalı, sorumluları belirlemeli, risk yönetimini sahiplenmeli, eğitim ve farkındalık faaliyetlerini desteklemeli, ihlal yönetimi için karar mekanizması kurmalıdır. Bilgi güvenliği rolleri organizasyon yapısında görünür olmalı; görev tanımları yazılı, onaylı ve ilgililere duyurulmuş olmalıdır. Büyük yapılarda farklı birimlerden temsilcilerle çalışan bir ekip, kararların iş süreçlerine uygulanmasını kolaylaştırır.

Politika ve risk yönetimi bu yapının çekirdeğidir. Bilgi güvenliği politikası kurumun kapsamını, hedeflerini, rol ve sorumluluklarını, risk yönetimi yaklaşımını, tabi olunan düzenlemeleri, eğitim beklentilerini ve politika ihlallerinin sonuçlarını açıklamalıdır. Risk yönetiminde bilgi sistemleri varlıkları, zafiyetler ve tehditler belirlenir; ardından risk değerlendirmesi yapılarak kabul edilebilir risk seviyesiyle karşılaştırılır. Risk azaltma, engelleme, paylaşma veya kabul etme seçenekleri yazılı şekilde değerlendirilir. Risk kararları periyodik olarak ve bilgi sistemlerinde önemli değişiklik olduğunda yenilenmelidir.

Denetim açısından bilgi güvenliği yönetiminin varlığı kadar işlerliği de önemlidir. Politika ve prosedürlerin güncel, onaylı ve duyurulmuş olması; eğitim kayıtlarının bulunması; risk değerlendirme sonuçlarının yazılı olması; kontrollerin sahiplerinin ve hedef tarihlerinin belirlenmesi gerekir. Gözetim ve ölçüm faaliyetleri iç denetim, dış denetim, sızma testi, kırmızı-mavi takım çalışmaları, performans göstergeleri ve kontrol etkinliği değerlendirmeleriyle desteklenebilir. Bilgi güvenliği ihlal yönetiminde bildirim, sınıflandırma, müdahale, kök neden analizi, düzeltici faaliyet ve iz kayıtlarının saklanması düzenlenmelidir. Denetçi, yalnızca doküman görmekle yetinmez; süreçlerin sahada karşılığı, kanıtları ve iyileştirme döngüsü olup olmadığını değerlendirir.

5.2 · Varlık Yönetimi

Bilgi Sistemleri Varlıklarını Yaşam Döngüsü Boyunca Yönetmek

> **KISACA**
> Varlık yönetimi, donanım, yazılım, lisans, veri ve bilgi sistemleri bileşenlerinin envantere alınması, sahipliklerinin belirlenmesi, sınıflandırılması, etiketlenmesi, uygun kullanılması, dolaşımı ve imhasının kontrol edilmesidir. Güncel envanter, onaylı sahiplik, sınıflandırmaya uygun koruma, taşınabilir varlık kontrolleri ve kayıtlı imha süreci olmazsa kurum hangi varlığı hangi riskten koruduğunu kanıtlayamaz.

Varlık yönetimi, bilgi güvenliğinin pratik zemininin kurulmasını sağlar. Kurum hangi donanımı, yazılımı, lisansı, veri kümesini, cihazı veya hizmeti kullandığını bilmiyorsa bu varlıklara ilişkin riskleri de doğru değerlendiremez. Bu nedenle varlık yönetiminin ilk amacı kapsamı görünür hale getirmek, ikinci amacı her varlığın sahibi, sınıfı, kullanım yeri, korunma ihtiyacı ve yaşam döngüsü durumunu kontrol altında tutmaktır. Varlık sahipliği, varlığın işletmeye kabulüyle başlar ve imha ya da güvenli kullanımdan kaldırma aşamasına kadar devam eder.

Varlık envanteri güncel, tutarlı ve erişilebilir olmalıdır. Envanterde varlığın temel bilgileri yanında sahiplik, sınıf, konum, kullanıcı, lisans durumu ve kullanım amacı gibi bilgiler yer alır. Büyük kurumlarda otomatik keşif araçları envanterin güncelliğini destekleyebilir; küçük kurumlarda daha basit yöntemler kullanılabilir. Ancak bilgi sistemleri envanteri ile diğer kurumsal envanterler arasında tutarsızlık oluşmamalıdır. Aynı varlığın iki farklı kayıt sisteminde farklı görünmesi bakım, erişim, lisans ve sorumluluk kararlarını zayıflatır.

Sınıflandırma ve etiketleme, varlıkların hangi koruma düzeyine tabi olacağını belirler. Bilgi önemine, kritik iş sürecine, yasal gerekliliğe veya risk düzeyine göre sınıflandırılabilir. Bilgiyi işleyen, saklayan veya ileten varlıklar da bu sınıfa uygun şekilde değerlendirilmelidir. En hassas bilginin işlendiği sistem daha düşük sınıfta bırakılırsa kontrol seviyesi yetersiz kalır. Etiketleme, fiziksel varlıklarda envanter etiketi gibi görünür yöntemlerle; elektronik bilgilerde sınıflandırma işaretleri veya erişim politikalarıyla yapılabilir. Yöntem tutarlı ve kurum tarafından anlaşılır olmalıdır.

Uygun kullanım, dolaşım ve imha süreçleri varlık yaşam döngüsünün kontrol noktalarıdır. Taşınabilir cihazlar, çıkarılabilir ortamlar ve kurum dışına çıkan varlıklar kayıp, yetkisiz erişim ve veri sızıntısı riski taşır. Bu varlıklar için yetkilendirme, şifreleme, kayıt, teslim, iade ve izleme kuralları belirlenmelidir. Varlıkların yer değiştirmesi, kullanıcı değişimi, bakım, devreden çıkarma ve imha işlemleri kayıt altına alınmalıdır. İmha aşamasında veri güvenli silinmeli veya fiziksel olarak yok edilmeli; işlem kanıtları saklanmalıdır. Denetçi için iyi varlık yönetimi, envanter ile gerçek kullanımın, sahiplik kararlarının ve koruma kontrollerinin birbirini doğrulamasıdır.

Bilgi İşleme Tesislerini Fiziksel ve Çevresel Risklerden Korumak

> **KISACA**
> Fiziksel ve çevresel güvenlik, bilgi sistemlerini barındıran bina, sistem odası, veri merkezi, cihaz, medya ve altyapının yetkisiz fiziksel erişime, hasara, kesintiye ve çevresel olaylara karşı korunmasıdır. Giriş kontrolü, ziyaretçi kaydı, kamera, güvenlik görevlisi, yangın algılama ve söndürme, enerji, iklimlendirme, su baskını ve doğal afet önlemleri birlikte değerlendirilir.

Fiziksel ve çevresel güvenlik, bilgi sistemleri güvenliğinin yalnızca mantıksal erişimden ibaret olmadığını gösterir. Sunucular, ağ cihazları, yedekleme ortamları, sistem odaları, veri merkezleri, kablolama altyapısı ve kullanıcı cihazları fiziksel ortamda bulunur. Bu unsurlara yetkisiz fiziksel erişim, hırsızlık, sabotaj, yangın, su baskını, elektrik kesintisi, aşırı ısı, nem veya doğal afet gibi olaylar bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini doğrudan etkileyebilir. Bu nedenle fiziksel ve çevresel kontroller teknik güvenlik kontrollerinin tamamlayıcısıdır.

Fiziksel kontrollerin temel amacı tesislere, odalara, cihazlara ve kayıt ortamlarına yalnızca yetkili kişilerin ulaşmasını sağlamaktır. Personel ve araç giriş çıkışlarının kayıt altına alınması, ziyaretçi prosedürü, kimlik doğrulama, kartlı geçiş, biyometrik kontrol, turnike, kilitli dolap, güvenlik görevlisi, kamera ve alarm sistemleri bu kapsamda değerlendirilir. Kritik alanlarda görev ayrılığı, refakat kuralı ve erişim yetkisinin periyodik gözden geçirilmesi önemlidir. Acil durumlarda can güvenliği gereklilikleri ile fiziksel erişim kontrolleri dengelenmelidir; güvenlik kapıları tahliyeyi engellememelidir.

Çevresel kontroller, bilgi işleme tesisinin kesintisiz ve güvenli çalışmasını hedefler. Elektrik altyapısı, kesintisiz güç kaynağı, jeneratör, topraklama, iklimlendirme, nem kontrolü, yangın algılama, gazlı söndürme, su baskını önleme ve doğal afet hazırlığı bu başlık altında ele alınır. Sistem odası veya veri merkezi konumu seçilirken coğrafi riskler, bina güvenliği, komşu alanların etkisi, erişim kolaylığı ve felaket senaryoları dikkate alınır. Donanımın bakım kayıtları, kapasite gereksinimleri ve çevresel sensörlerin izlenmesi de kontrol ortamının parçasıdır.

Denetçi bu konuda yalnızca fiziksel ekipmanın varlığına bakmaz. Yetki listelerinin güncelliği, giriş çıkış kayıtlarının bütünlüğü, ziyaretçi kayıtlarının tutulması, kamera görüntülerinin saklama süresi, yangın ve enerji sistemlerinin test kayıtları, iklimlendirme izleme raporları ve acil durum tatbikatları incelenir. Kritik alan erişimleri iş rolüyle uyumlu değilse veya çevresel kontroller test edilmiyorsa güvenlik kâğıt üzerinde kalır. Sağlam fiziksel ve çevresel güvenlik, bilgi sistemleri sürekliliği ve bilgi güvenliği kontrollerinin uygulanabilir kalmasını sağlar.

5.4 · Ağ Güvenliği

Ağ Mimarisini Tehditlere Karşı Katmanlı Biçimde Korumak

> **KISACA**
> Ağ güvenliği, kurum ağlarının topoloji, protokol, cihaz, kablosuz erişim, internet bağlantısı, uzak erişim ve saldırı vektörleri bakımından korunmasıdır. Segmentasyon, güvenlik duvarı, ağ erişim denetimi, izleme, saldırı tespit ve engelleme, VPN, güvenli yapılandırma, yama yönetimi ve derinliğine savunma kontrolleri ağ üzerindeki yetkisiz erişim ve kesinti riskini azaltır.

Ağ güvenliği, bilgi sistemlerinin birbirleriyle ve dış dünya ile iletişim kurduğu altyapının korunmasını ifade eder. Ağlar fiziksel iletim ortamı, anahtar, yönlendirici, kablosuz erişim noktası, güvenlik duvarı, sunucu, uç cihaz, protokol ve servislerden oluşur. Yerel ağlar, geniş alan ağları, kablosuz ağlar, internet bağlantıları ve uzak erişim kanalları farklı riskler taşır. Bu nedenle ağ güvenliği yalnızca bir güvenlik duvarı kurmak değil, mimariyi, iletişim kurallarını, erişim noktalarını ve izleme mekanizmalarını bütün olarak yönetmektir.

Ağ mimarisinde segmentasyon kritik bir kontroldür. Farklı güvenlik seviyesine sahip sistemlerin aynı düz ağda bulunması, bir noktadaki zafiyetin tüm ortama yayılmasına neden olabilir. Kullanıcı ağı, sunucu ağı, yönetim ağı, misafir ağı, kablosuz ağ ve kritik sistemler mantıksal olarak ayrılmalıdır. Güvenlik duvarları ve erişim kontrol listeleri yalnızca gerekli trafiğe izin verecek şekilde yapılandırılmalıdır. Varsayılan açık yaklaşım yerine ihtiyaç temelli erişim tercih edilmelidir. Yönetim arayüzleri, kablosuz erişim noktaları ve uzak bağlantılar ayrıca sıkılaştırılmalıdır.

Tehditler farklı kaynaklardan gelebilir. Kötü niyetli dış aktörler, içeriden yetkisiz kullanıcılar, hatalı yapılandırmalar, zararlı yazılımlar, sosyal mühendislik, kablosuz ağ saldırıları, web uygulama zafiyetleri ve hizmet kesintisi saldırıları ağ güvenliği risklerini artırır. Derinliğine savunma yaklaşımı, tek bir kontrolün başarısız olması halinde diğer katmanların koruma sağlamasını amaçlar. Genişliğine savunma ise farklı sistem ve süreçlerde tutarlı güvenlik seviyesinin kurulmasını gerektirir. Ağ cihazlarının yama durumu, konfigürasyon yönetimi ve varsayılan parola kullanımının engellenmesi temel gerekliliklerdir.

Denetçi ağ güvenliğini değerlendirirken ağ diyagramlarının güncel olup olmadığını, varlık envanteriyle tutarlılığını, segmentasyon kurallarını, güvenlik duvarı politika setlerini, kablosuz ağ güvenliğini, VPN ve uzak erişim kontrollerini, saldırı tespit ve engelleme sistemlerini, ağ erişim denetimini ve logların izlenmesini inceler. Erişim kuralları iş gereksinimiyle açıklanamıyorsa, eski kurallar temizlenmiyorsa veya izleme kayıtları olay müdahalesine bağlanmıyorsa kontrol zayıflar. Güvenli ağ mimarisi, iş sürekliliği ve bilgi güvenliği için görünür, yönetilebilir ve kanıtlanabilir bir iletişim zemini oluşturur.

5.5 · Erişim Güvenliği

Kimlik, Yetki ve Erişim Kontrollerini Tutarlı Yönetmek

> **KISACA**
> Erişim güvenliği, kullanıcıların ve sistemlerin yalnızca yetkili oldukları kaynaklara erişmesini sağlayan kimlik tanımlama, kimlik doğrulama, yetkilendirme ve hesap yönetimi kontrolleridir. Parola, çok faktörlü doğrulama, biyometri, rol tabanlı yetki, görev ayrılığı, en az yetki, ayrıcalıklı hesap yönetimi, periyodik gözden geçirme ve erişim kayıtları birlikte değerlendirilir.

Erişim güvenliği, bilgi sistemleri kaynaklarına kimin, hangi koşulda, hangi yetkiyle ulaşabileceğini belirleyen kontrol alanıdır. Temel süreç kimlik tanımlama, kimlik doğrulama ve yetkilendirme adımlarından oluşur. Kimlik tanımlama kullanıcı veya sistemin kim olduğunu iddia etmesidir; kimlik doğrulama bu iddianın parola, token, sertifika, biyometrik veri veya çok faktörlü yöntemlerle doğrulanmasıdır. Yetkilendirme ise doğrulanmış kimliğin hangi veri, uygulama, işlem veya yönetim fonksiyonlarına erişebileceğini belirler.

Erişim kontrolleri teknik ve yönetsel kararların birleşimidir. Rol tabanlı erişim, iş fonksiyonlarına göre yetki setleri tanımlar ve kişilere doğrudan rastgele yetki verilmesini azaltır. En az yetki ilkesi, kullanıcının görevini yapmak için ihtiyaç duyduğu asgari yetkiyle çalışmasını sağlar. Bilmesi gereken ilkesi, özellikle hassas verilerde erişimin görev gereğiyle sınırlanmasını gerektirir. Görev ayrılığı ise kritik bir işlemin tek kişi tarafından başlatılıp onaylanmasını engelleyerek hata ve kötüye kullanım riskini azaltır. Bu ilkeler yoksa kimlik doğrulama güçlü olsa bile yetki riski devam eder.

Hesap yaşam döngüsü erişim güvenliğinin en sık zafiyet üreten alanıdır. Yeni kullanıcı hesabı açma, rol değişikliği, geçici yetki verme, ayrıcalıklı hesap kullanımı, parola sıfırlama, ayrılan çalışan hesabını kapatma ve servis hesaplarını yönetme süreçleri yazılı olmalıdır. Ayrıcalıklı hesaplar daha yüksek risk taşıdığı için onay, izleme, oturum kaydı, çok faktörlü doğrulama ve düzenli gözden geçirme gerektirir. Paylaşılan hesaplar hesap verebilirliği zayıflatır; zorunlu hallerde sorumluluk ve kayıt mekanizması kurulmalıdır.

Denetçi erişim güvenliğini değerlendirirken yetki matrislerini, kullanıcı listelerini, onay kayıtlarını, ayrılan personel hesaplarını, ayrıcalıklı hesapları, başarısız giriş denemelerini, parola ve çok faktörlü doğrulama politikalarını, uzaktan erişim kurallarını ve periyodik erişim gözden geçirmelerini inceler. Kullanıcının fiili yetkisi görev tanımıyla uyumlu değilse, eski yetkiler temizlenmiyorsa veya kritik işlemler görev ayrılığı olmadan yapılabiliyorsa erişim güvenliği zayıftır. Sağlam erişim yönetimi, gizlilik ve bütünlüğü korurken olay sonrası izlenebilirliği de mümkün kılar.

5.6 · Veri ve İz Kayıtlarının Güvenliği

Veriyi ve Logları Yaşam Döngüsü Boyunca Koruma

> **KISACA**
> Veri ve iz kayıtlarının güvenliği, verinin üretim, kullanım, saklama, aktarım, arşivleme ve imha aşamalarında korunması ile sistem loglarının bütün, erişilebilir ve değiştirilemez tutulmasını kapsar. Veri sınıflandırması, saklama süreleri, log kaynaklarının yönetimi, kriptografik özet, simetrik ve asimetrik şifreleme, açık anahtar altyapısı ve anahtar yönetimi temel kontrol alanlarıdır.

Veri güvenliği, bilgi sistemlerinde işlenen bilginin yaşam döngüsü boyunca korunmasını gerektirir. Veri yalnızca veri tabanında duran kayıt değildir; üretildiği, işlendiği, aktarıldığı, yedeklendiği, arşivlendiği ve imha edildiği her aşamada risk taşır. Sınıflandırma, hangi verinin hangi gizlilik ve bütünlük seviyesine sahip olduğunu belirler. Kişisel veri, müşteri verisi, finansal veri, işlem kayıtları veya kritik operasyonel veri aynı kontrol seviyesine tabi olmayabilir. Kontrol seviyesi verinin önemine, yasal gerekliliklere ve iş sürecindeki etkisine göre belirlenmelidir.

İz kayıtları güvenliğin kanıt ve tespit katmanıdır. Sistem, uygulama, veri tabanı, ağ cihazı, güvenlik aracı ve kullanıcı işlemlerinden üretilen loglar olayların anlaşılmasını sağlar. Ancak logların güvenilir olabilmesi için zaman bilgisi doğru olmalı, kayıtlar bütün tutulmalı, yetkisiz değişiklikten korunmalı ve yeterli süre saklanmalıdır. İz kayıtlarının kaynağı, kapsamı, saklama süresi, erişim yetkisi ve merkezi izleme mekanizması tanımlanmalıdır. Gerektiğinde olay yönetimi, denetim ve adli inceleme süreçleri bu kayıtlara dayanır.

Kriptografik kontroller veri güvenliğinin önemli araçlarıdır. Kriptografik özet fonksiyonları verinin değişip değişmediğini kontrol etmek için kullanılır. Simetrik şifreleme aynı anahtarla şifreleme ve çözme yaparken yüksek performans sağlar; asimetrik şifreleme açık ve özel anahtar yapısıyla kimlik doğrulama, güvenli anahtar değişimi ve dijital imza gibi kullanım alanları sunar. Açık anahtar altyapısı sertifika otoriteleri, sertifikalar ve iptal mekanizmalarıyla güven ilişkisini yönetir. Kriptografi tek başına yeterli değildir; algoritma seçimi, anahtar uzunluğu ve anahtar yaşam döngüsü doğru yönetilmelidir.

Denetçi veri ve iz kayıtları güvenliğini değerlendirirken veri sınıflandırmasını, saklama ve imha politikalarını, yedek ve arşiv kontrollerini, log kaynaklarının tamlığını, merkezi log yönetimini, loglara erişim yetkilerini, zaman senkronizasyonunu, kriptografik anahtarların üretim, dağıtım, saklama, kullanım, kurtarma ve imha süreçlerini inceler. Loglar değiştirilebilir durumdaysa veya kritik sistemler log üretmiyorsa olayların kanıtlanması zorlaşır. Veri yaşam döngüsü ve iz kayıtları birlikte yönetildiğinde hem koruma hem hesap verebilirlik güçlenir.

5.7 · Üçüncü Taraflarla İletişim Güvenliği

Üçüncü Taraf İlişkilerinde Güvenliği Yaşam Döngüsüyle Yönetmek

KISACA

Üçüncü taraflarla iletişim güvenliği, kurum dışındaki hizmet sağlayıcı, tedarikçi ve iş ortaklarıyla paylaşılan veri, sistem erişimi ve hizmet süreçlerinin güvenli yönetilmesidir. İlişki başlamadan önce veri gizliliği, fiziksel güvenlik, siber güvenlik, erişim, SLA ve hukuki riskler değerlendirilir; sürdürme ve sonlandırma aşamalarında erişimler, değişiklikler, raporlar ve veri temizliği kontrol edilir.

Üçüncü taraflarla iletişim güvenliği, kurumun doğrudan kendi personeli ve sistemleri dışında kalan taraflarla kurduğu ilişkilerde bilgi güvenliğini korumasıdır. Hizmet sağlayıcılar, dış kaynak kullanımı yapılan firmalar, tedarikçiler, bakım ekipleri, bulut veya barındırma sağlayıcıları ve iş ortakları kurum verisine ya da sistemlerine doğrudan veya dolaylı erişebilir. Bu erişim doğru yönetilmezse kurumun kendi kontrolleri güçlü olsa bile gizlilik, bütünlük ve erişilebilirlik riski üçüncü taraf üzerinden gerçekleşebilir.

İlişkinin başlama aşamasında güvenlik gereksinimleri sözleşme ve teknik kontrollerle netleştirilmelidir. Veri gizliliği kapsamında verinin nasıl işlendiği, depolandığı, aktarıldığı, yedeklendiği ve imha edildiği öğrenilmelidir. Kişisel veri ve sektörel düzenlemeler açısından uyum şartları değerlendirilmelidir. Veri konumu, birincil ve ikincil sistemlerin nerede barındırıldığı, alt yüklenicilere veri aktarımı ve yedekleme düzeni incelenmelidir. Fiziksel güvenlik, siber güvenlik, uzak erişim, şifreleme, iz kayıtları, sertifikasyonlar, sızma testi sonuçları ve olay yönetimi süreçleri de başlangıç değerlendirmesine dahildir.

Sürdürme aşaması, sözleşmenin imzalanmasından sonra kontrolün bırakılmamasını gerektirir. Üçüncü tarafların personel, sahiplik, yönetim, altyapı veya sistem değişiklikleri izlenmelidir. Kurum kaynaklarına hangi üçüncü taraf kullanıcılarının eriştiği düzenli takip edilmeli, bilmesi gereken ilkesi uygulanmalı ve gereğinden fazla yetki verilmemelidir. Varlık yönetimi, açıklık ve yama yönetimi, düzenli raporlar, tarafsız denetim raporları, sızma testleri ve hizmet seviyesi anlaşmaları performansın izlenmesinde kullanılır. SLA içinde kesinti giderme süresi ve veri kaybı hedefleri gibi süreklilik ölçütleri bulunabilir.

Sonlandırma aşaması çoğu zaman yüksek risklidir. Sözleşme bittiğinde kullanıcı hesapları askıya alınmalı veya kapatılmalı, uzak erişim yetkileri kaldırılmalı, sertifika, anahtar, token, kart ve fiziksel erişim araçları geri alınmalıdır. Üçüncü tarafın işlediği veriler için silme, arşivleme, anonimleştirme veya iade süreçleri sözleşme ve mevzuata uygun yürütülmelidir. Erişim ve işlem kayıtlarının saklama süresi belirlenmeli, ilişki sonrası kanıt ihtiyacı göz önünde tutulmalıdır. Denetçi, üçüncü taraf güvenliğini bir defalık tedarik kontrolü değil, başlama, sürdürme ve sonlandırma aşamalarından oluşan izlenebilir bir yaşam döngüsü olarak değerlendirir.

benzersor

Bilgi Sistemi Bağımsız Denetim

DERS NOTLARI 2026 BASKISI

SPL BİLGİ SİSTEMLERİ BAĞIMSIZ DENETİM

İyi çalışmalar

Bu ders notları benzersor tarafından ücretsiz hazırlandı; resmî kurum yayını değildir. Hata bildirimi: destek@benzersor.com

Okudun, sıra pekiştirmede

Şimdi çöz!

Okuduğun konuyu hemen soruyla pekiştir. benzersor uygulamasında konu anlatımı, soru bankası ve gerçek sınav simülasyonu bir arada.

App Store'dan İndirin

İNDİRİN Google Play