SPL
Sermaye Piyasası
Lisanslama Sicil ve
Eğitim Kuruluşu

Lisanslama Sınavları
Çalışma Notları

Bilgi Sistemleri Yönetimi ve Denetimi

2021

Hazırlayanlar:
Sermaye Piyasası Kurulu Uzmanları


SPL
Sermaye Piyasası
Lisanslama Sicil ve
Eğitim Kuruluşu

Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu

Bilgi Sistemleri Yönetimi ve Denetimi

Ders Kodu: 1020

- Bilgi Sistemleri Bağımsız Denetim Sınavı

31 Aralık 2024

Bu Çalışma Notu, Sermaye Piyasası Kurulu uzmanları tarafından hazırlanmıştır.

SINAV ALT KONU BAŞLIKLARI
BİLGİ SİSTEMLERİ YÖNETİMİ VE DENETİMİ

1. Bilgi Sistemleri Yönetimi
- **1.1.** Bilgi Sistemleri Stratejisinin Geliştirilmesi
- **1.2.** Bilgi Sistemleri Yönetiminin Unsurları

2. Bilgi Sistemleri Denetimi
- **2.1.** Bilgi Sistemleri Denetimi Kavramları
- **2.2.** Bilgi Sistemleri Denetim Faaliyeti

3. Bilgi Sistemleri Yönetimi ve Denetimine İlişkin Mevzuat
- **3.1.** Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ Seri:X; No:22
- **3.2.** Bilgi Sistemleri Yönetim Tebliği VII-128.9
- **3.3.** Bilgi Sistemleri Bağımsız Denetim Tebliği III-62.2
- **3.4.** İlgili Diğer Mevzuat ve Uluslararası Düzenlemeler
- **3.5.** Etik İlke ve Kurallar (Bağımsız Denetçiler İçin Etik Kurallar ve ISACA'nın Etik Kuralları)

İÇİNDEKİLER

KISALTMALAR

BDDK	: Bankacılık Düzenleme ve Denetleme Kurumu
BDDT	: Bilgisayar Destekli Denetim Teknikleri
BDS	: Türkiye Denetim Standartları/Bağımsız Denetim Standartları
BİAŞ veya Borsa	: Borsa İstanbul A.Ş.
BSBDL	: Bilgi Sistemleri Bağımsız Denetim Lisansı
BSBD Tebliği	: III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği
BSI	: İngiltere Standartları Enstitüsü
BSY Tebliği	: VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği
CISA	: Bilgi Sistemleri Denetçisi Sertifikası
COBIT	: Bilgi Teknolojilerine İlişkin Kontrol Hedefleri
Etik Kurallar	: Bağımsız Denetçiler İçin Etik Kurallar
GİB	: Gelir İdaresi Başkanlığı
IAASB	: Uluslararası Denetim ve Güvence Standartları Kurulu
IESBA	: Uluslararası Etik Standartları Kurulu (Muhasebeciler İçin)
ISACA	: Bilgi Sistemleri Denetim ve Kontrol Birliği
ISACF	: Bilgi Sistemleri Denetim ve Kontrol Vakfı
ISO	: Uluslararası Standardizasyon Kuruluşu
IOSCO	: Uluslararası Menkul Kıymetler Komisyonları Örgütü
IT	: Bilgi Teknolojileri
ITAF	: Bilgi Teknolojileri Güvence Çerçevesi
ITGI	: Bilgi Teknolojileri Yönetişim Enstitüsü
ITIL	: Bilgi Teknolojisi Altyapı Kütüphanesi
TSE	: Türk Standartları Enstitüsü
KAP	: Kamuyu Aydınlatma Platformu
KGK	: Kamu Gözetimi Muhasebe ve Denetim Standartları Kurumu
KPI	: Anahtar Başarı Göstergesi-Key Performance Indicator
SEDDK	: Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumu
Seri:X, No:22 Tebliği	: Seri:X, No:22 sayılı Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ
SPKn, Kanun	: Sermaye Piyasası Kanunu
SPK, Kurul	: Sermaye Piyasası Kurulu
SPL	: Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.
PÖİP	: Piyasa Öncesi İşlem Platformu
UDS, ISA	: Uluslararası Denetim Standartları
TCMB	: Türkiye Cumhuriyet Merkez Bankası
TDUB	: Türkiye Değerleme Uzmanları Birliği
TSE	: Türk Standartları Enstitüsü
TSPB	: Türkiye Sermaye Piyasaları Birliği
TTK	: 610 sayılı Türk Ticaret Kanunu
TÜBİTAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
660 sayılı KHK	: 660 sayılı Kamu Gözetimi Muhasebe ve Denetim Standartları Kurumunun Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname

1.1. BİLGİ SİSTEMLERİ YÖNETİMİ

Bu Çalışma Notu, Sermaye Piyasası Kurulu'nun (SPK, Kurul) Bilgi Sistemleri Bağımsız Denetim Lisansı (BSBDL) sınav konularının birincisine yönelik olarak hazırlanmıştır. Bu konuya ve ilgili lisansın takip eden diğer konularına devam etmeden önce bilgi sistemleri ifadesi ile anlatılmaya çalışılan kavramın, çok bilinen bir kavram olmasına karşın, bir kere daha tanımlanması uygun olacaktır.

Bilgi sistemleri, en genel tanımı ile işletmelerde planlama, kontrol, analiz ve karar vermede kullanılmak üzere bilgi toplama, bilgiyi işleme, bilgiyi saklama, bilgiyi kullanma ve bilgiyi yayma amacıyla birlikte çalışan ilişkili unsurlar olarak tanımlanabilir. Bilgi sistemleri, bilgi teknolojileri ile kullanıcılarının etkileşimde bulunduğu yönetsel ve karar destek sistemleridir. Bilgi sistemlerinin temel işlevi planlama, kontrol, analiz ve karar verme için veri ve bilgileri toplamak, işlemek, kaydetmek, dönüştürmek ve yaymaktır. Bilgi sistemlerinin amacı ise işletmelerde ihtiyaç duyulan bilgiyi güvenilir bir şekilde gerektiği zamanda ve yerde sunabilmektir. Bilgi sistemleri, işletmelerde içsel olarak oluşturulan ve üretilen bilgiler ile dışsal olarak elde edilen bilgileri kapsar ve bünyesinde bunların yönetimini içeren sistemleri barındırır. Bilgi sistemleri içsel ve dışsal verileri girdi olarak işleyerek anlamlı bilgilere dönüştürüp, işletmelerin bilgi ihtiyaçlarının giderilmesine yardımcı olur.

Bilgi istemleri, bir işletmenin iş süreçlerini gerçekleştirmeye, kolaylaştırmaya ve hızlandırmaya yarayan tüm bilgi teknolojisi unsurları (yazılım, uygulama, donanım, bunları destekleyen altyapı elemanları) ile bunları kullanılabilir hale getiren ve bu durumu sürekli kılan insan gücünün toplamıdır. Bilgi sistemleri, işletmelerde belirli hedefleri karşılamak üzere, verileri karar verici için anlamlı bilgilere çeviren insan gücü, programlar ve yönetsel süreçlerden oluşan bir dizidir.

Günümüzde tüm işletmeler, bilgi sistemlerini kullanmaktadır. Bilgi sistemleri, girdi, çıktı ve işleme faaliyetleri ile karar verme, proseslerin kontrolü, sorunların çözümü ve yeni mal veya hizmet oluşturmada işletmelerin ihtiyaç duyduğu bilgileri sağlar. Ancak bilgi sistemleri kullanımı bazı faktörlere bağlı olarak değişiklik gösterir. İşletmenin büyüklüğü, iş modeli, sunduğu ürün ve hizmetlerin çeşitliliği, faaliyet gösterdiği sektör ile bilgi sistemleri kullanımına bakış açısı bu faktörler arasında sayılabilir. Altmış yıldan uzun süre işletmelerin işlerini hızlandırmak amacıyla destek hizmeti kapsamında değerlendirilen bilgi sistemleri, teknoloji kullanımının artmasıyla birlikte, özellikle son yirmi yılda farklı bir gözle değerlendirilmeye başlanmıştır.

Bilgi sistemlerinin en önemli unsuru insan gücüdür. Bilgi sistemleri tanımından insan gücü kaldırıldığında, geriye bir sürü donanım, depolama ortamları, yazılım, uygulama kodları gibi teknoloji bileşenleri kalır. Bunları bir araya getirip bütüncül anlamı veren insan gücüdür. Bilgi istemlerinin etkin bir şekilde işlemesi insan unsuruna bağladır. Bu kısımda, bilgi teknolojilerini bir sisteme dönüştüren insan gücü ve yönetim konuları ele alınacaktır.

1.1.1. Bilgi Sistemleri Stratejisinin Geliştirilmesi

1.1.1.1. Bilgi Sistemleri Kurumsal Yönetimi/Yönetişimi

Yönetişim ya da daha yaygın kullanımıyla kurumsal yönetim kavramı. aslında sadece bilgi sistemlerine özgü bir kavram değildir. Kurumsal yönetim, literatürde kapsamına göre dar ve geniş açıdan bakılarak farklı tanamlamalar yapılmaktadır. Bu tanımlamalarda kurumsal yönetimin bir veya birkaç özelliği ön plana çıkarılabilmektedir. Kurumsal yönetim, işletmelerin stratejik yönetimi ile görevli ve sorumlu üst yönetimin, bu görev ve sorumluluklarını gerçekleştirirken, işletmenin ilgili tarafları olan hissedarlar, çalışanlar, müşteriler, tedarikçiler ve diğer taraflar ile olan ilişkilerini düzenleyen, uzun dönemde paydaşlara ekenomik değer yaratılmasına olanak tanıyan her türlü kurallar setidir. Kurumsal yönetim, günümüzde işletmelerde şeffaflık, hesap verebilirlik, paydaşların beklentilerini karşılamak, etik ve sosyal değerlere uygun bir yönetim sergilemek için (daha doğrusu bu unsurları güçlendirmek için) kullanılan bir kavramdır. Ülkemizde bizzat Kurul düzenlemeleri içerisinde yer almaktadır. Bu konuda detaylı bilgiye Sermaye Piyasası Lisanslama, Sicil ve Eğitim Kuruluşu A.Ş.'nin (SPL) 1018 numaralı Kurumsal Yönetim çalışma notundan ulaşılabilir.

Bilgi sistemleri kurumsal yönetimi (veya bir diğer adlandırma ile yönetişimi) kurumsal yönetim disiplininin bir alt kümesidir. Bu Çalışma Notu'nda daha kısa bir kullanım olduğu için bilgi sistemleri

kurumsal yönetimi yerine bilgi sistemleri yönetişimi ifadesi kullanılacaktır.

Bilgi sistemleri politikalarının planlanması, uygulanması, izlenmesi ve iyileştirilmesi için işletme bünyesinde tüm ilgili aktörlerin etkin katılım ve sorumluluk almasını gerektiren bilgi sistemleri yönetişim fonksiyonuna ihtiyaç duyulmaktadır. Teknolojinin işletmelerin iş süreçleri ile üretilen bilginin yönetiminde yaygın bir şekilde kullanılması yeni fırsatların yanında bilgi güvenliği, veri bütünlüğü, faaliyetlerde verimlilik, etkinlik ve kalite gibi hususlarda yaşanan sıkıntılar bu fonksiyonun önemini artırmaktadır.

Bilgi sistemleri yönetişimi, bilgi sistemlerini işletmenin iş hedefleri ve stratejisini gerçekleştirmeye katkı sağlayacak şekilde, bilgi sistemleri risklerini gözeterek ve kaynakları (zaman, insan gücü, malzeme, para vb.) etkin ve verimli şekilde kullanarak yönetmek ve performansını ölçmek için işletilen bir dizi süreçtir. Bu süreçte, işletmedeki tüm süreçlerin hatasız işlemesi, kaynakların verimli kullanılarak kayıp ve kaçakların önlenmesi ve verilerin hızlı ve güvenli bir ortamda oluşturulup, değerlendirilmesine olanak sunan sistem oluşturulmalıdır. Burada bahsedilen işletme herhangi bir türde, yapıda, sektörde olabilir; kar amacı güdebilir veya gütmeyebilir. Bilgi sistemleri yönetişiminden amaç, bilgi sistemlerinin işe "*değer*" katmasını sağlamak, iş tarafı ile bilgi sistemleri tarafını "*aynı hizada*" tutabilmektir. Böylece bilgi sistemleri yatırımlarından beklenen kazanımları hayata geçirebilmektir.

Bilgi sistemleri yönetişiminin birden çok tanımı bulunmaktadır. İnternetten basit bir aramayla benzer birçok tanıma ulaşılabilir. Tanımlar biraz farklılık içerse de tümünde aynı olan birkaç unsur bulunmaktadır. Bu unsurlar; iş stratejisi/hedefleri, bilgi sistemleri stratejisi, bilgi sistemleri yatırımları, bilgi sistemleri riskleri, performans ölçümü, iş-bilgi sistemleri uyumu ve işe değer katmak olarak sayılabilir.

Burada dikkat edilmesi gereken nokta bilgi sistemlerini iyi yönetmek değil, bilgi sistemlerini işe değer/katkı sağlayacak ve risklerini kabul edilebilir seviyeye indirgeyecek şekilde iyi yönetmektir. Buradaki vurgu işe değer katmaktır. Bilgi sistemleri yönetişimi ile amaçlanan iş tarafının stratejisini ve hedeflerini gerçekleştirmesini sağlamaktır. Hedefleri bir döngü içerisinde gerçekleştirmeye çalışmaktadır. Ancak, bu yazıldığı gibi düz bir iş değildir. Tanımları yaparken ortaya bir dizi kavram çıkmaktadır:

- İş stratejisi ve hedefleri → İşin hedefleri neler? Bilgi sistemleri neye yardımcı olacak?

- Bilgi sistemleri stratejisi ve hedefleri → Bilgi sistemleri bunları yaparken nasıl bir yol izleyecek?

- İş ve bilgi sistemlerinin uyum → Uyumsuz olma ihtimalleri var mı?

- Bilgi sistemleri yatırımları/kaynakları → Bilgi sistemlerinin elinde neler var? Kullanabileceği kaynaklar, kapasitesi, yetkinlikleri nelerdir?

- Bilgi sistemleri riski → Bilgi sistemlerinin maruz kaldığı riskler neler? İş hedeflerini gerçekleştirmeye yardımcı olurken neler ters gidebilir?

- Performans değerlendirme → Bilgi sistemlerinin faaliyetleri ne kadar işe yarıyor? Gerçekten işe değer katıyor mu?

Bu kavramlar daha detaylı bir şekilde bir sonraki bölümde ele alınmaktadır.

1.1.1.2. Bilgi Sistemleri Yönetişimi Kavramları

1.1.1.2.1. Strateji Kavramı

Strateji kavramını anlayabilmek için öncelikle "*misyon*", "*vizyon*" ve "*değerler*" kavramlarının anlaşılması gerekmektedir. Bu kavramlar, kurumsal kimlik oluşturmada öneme sahip olup, strateji için öncül kavramlardır.

Bir işletmenin öncelikle kendi kimliğini tanımlaması, kuruluş amacını, neden var olduğunu belirlemesi gerekir. İşletmenin varlık sebebi nedir? İşletme tam olarak ne yapmaktadır? Kimlere hizmet vermektedir? Bu tanım işletmenin misyonunu oluşturur. İşletme kendi kimliğini belirledikten sonra

tercihen bunu yazılı hale getirmelidir. İşletmenin tüm çalışanlarının işletme misyonundan haberdar olması gerekir. Bu aşamadan sonra, sıra işletmenin gelecekle ilgili fikrine gelir.

İşletme varlığını sürdürerek neyi hedefliyor? Nereye ulaşmak istiyor? Hiçbir işletme sabit bir şekilde kalmak istemez. İşletmenin iç ve dış faktörleri devamlı bir değişim halinde olup, işletmeyi de değiştirir. Bu değişim ne yönde olacak? İşletme kendini ileride nerede görüyor? İşletmenin kendi gelecek görüşü nedir diye sorulursa, cevap vizyon olacaktır. Vizyon, işletmenin kendini gelecekte gördüğü pozisyon, yer, rol olarak tanımlanır.

İşletme kendi vizyonunu belirledikten sonra misyonda olduğu gibi bunu yazılı hale getirmelidir. İşletmenin tüm çalışanlarının bu vizyondan haberdar olması gerekir. Daha sonra sıra bu vizyonun nasıl gerçekleştirileceğinin planlamasına gelir. Yalnız burada vizyon konusunun zamanlamasıyla ilgili olarak şunu belirtmek doğru olur: İşletme vizyonunu belirlerken sonu belli olmayan bir süreyi değil, ortalama beş yıllık bir zaman dilimini hesaba katmalıdır. Vizyon uzun dönemli geleceğe yönelik hedef olmakla birlikte, ilelebet değişmeyecek bir şey değildir. Vizyon da sık sık olmamakla birlikte işletmenin faaliyetlerini yürüttüğü ekosistemin gereklilikleri kapsamında belirli aralıklarla değiştirilebilir. Burada özellikle de dış çevrenin değişimi bunu zorlayabilir.

İşletmenin etik ilkeleri olarak ifade edilebilen "*değerler*" kavramı, işletmenin belirlediği vizyon doğrultusunda çalışırken bağlı kalacağı ilkeler ve değerlerdir. Bu değerler statik değil dinamik yapıda olup, uzun bir zaman sürecinde örgütsel yapı ihtiyaçlarına bağlı olarak değişimler geçirir. Bu kavram özellikle yönetişim uygulamalarının gelişimiyle önem kazanmıştır. Burada bahsedilen ilkeler ve değerler; bunlarla sınırlı olmamakla birlikte, şeffaf ve güvenilir olmak, adil bir iş ortamı yaratmak, sürekli eğitim ve gelişmeye önem vermek, sosyal sorumluluk almak, çevreye saygı göstermek olabilir. Son zamanlarda çok sık karşılaşılan "*Yeşil Bilişim-Green Computing*" kavramı buna güzel bir örnektir. Yeşil bilişim kısaca, bilgi teknolojilerinin her alanında bilgi teknolojileri ve çevre etkileşimi[1] kapsamında çevreye verilen zararın mümkün olan en az seviyede olmasını sağlamak için kullanılan bir terimdir. Bu amaçla hayata geçirilen uygulamalardır.

İşletmenin kurumsal başarısının sürdürülebilirliği bakımından çalışanların temel değerlere sadık kalması büyük önem taşır. Bir işletmenin oluşturulup faaliyetlerini etkin ve verimli bir şekilde sürdürmesi, değerlerin üretilip yüceltilmesiyle; işletmenin faaliyetlerinin kötüleşmesi ve sonlandırılması ise değerlerin yıpratılıp tüketilmesiyle gerçekleştirilir. Bu nedenle, işletmenin temel değerleri belirli olmalı ve iç-dış tüm taraflara duyurulmalıdır. Temel değerler, işletmenin dış çevrede tanınması ve marka değerinin yüksek olmasıyla doğrudan ilgilidir. İşletme içinde ise çalışanların motivasyonu üzerinde etkili olur. Temel değerler işletmenin iş yapış tarzını şekillendirir.

İşletme, misyon ve vizyonu ile kim olduğunu ve nereye gitmek istediğini tanımlar. İstenen yere ulaşmak için geçmek zorunda olduğu noktalar (hedefler) ve bu noktalara giderken geçeceği yollar nedir? İki coğrafi lokasyonun arasındaki farklı rotalar gibi, işletmenin de bulunduğu yerden varmak istediği yere giderken seçebileceği farklı yollar olabilir. İşte bu yolların belirlenmesi, stratejinin belirlenmesi aşamasıdır.

Strateji ilk olarak askeri alanda[2] ortaya çıkmasına karşın zaman içerisinde bir çok alanda olduğu gibi modern yönetim olgusunun vazgeçilmez bir kavram olmuştur. Sözlük anlamıyla strateji, belli bir amacın gerçekleştirilmesi için hazırlanan bir plandır. Kurumsal anlamda bir işletmenin, kar amacı gütsün gütmesin, nihai amacına, gelecekte olmak istediği yere ulaşması için izlemesi gereken adeta bir yol haritasıdır. Bir başka deyişle, strateji işletmelerin varoluş amaçlarının ortaya konması, bu amaçlara ulaşılmasına yönelik planlar oluşturulması ve bu sayede varlığını geliştirip sürdürmesine ilişkin takip edilecek yolun oluşturulmasıdır. Tarifi bu şekilde yapılınca akla hemen amacı olmayan işletme var mıdır, amacını nasıl gerçekleştireceğini bilmeyen işletme var mıdır soruları gelebilir. Teorik olarak her işletmenin bir amacı vardır. Ama buna uygun çalışmayı sistematik olarak yap(a)mayan işletmeler de bulunmaktadır. "*En iyi kurum olmalıyım*" ya da "*En iyisi olacağım*" gibi bir ifade ancak bir niyet olabilir, bir amaç olamaz. Çünkü en basitinden ölçülebilir değildir. Hedefe ulaşılıp ulaşılmadığı belirlenemez.

---

[1] *Bu etkileşim, küresel ısınma, iklim değişikliği, toksin ve plastik atıklar, enerji tüketimi, enerji dışındaki doğal kaynakların tüketimi, toprak kullanımı, su kullanımı, ozon tabakasının incelmesi ve biyolojik çeşitlilik gibi başlıklar altında incelenebilir.*

[2] *Savaşı kazanmak için muharebeleri kullanma sanatı olarak tanımlanmıştır.*

Stratejiyi, vizyona (nihai amaç da denilebilir) ulaşmak için belirlenen yol, hareket tarzı diye tanımladıktan sonra, kavramı daha iyi anlayabilmek için aşağıda belirtilen genel özelliklere bakılabilir:

- İşletmeye özgü olması (genel geçer, formülü olan bir şey değil),

- İşletmenin üst yönetimi tarafından geliştirilmesi (astlara yüklenecek angarya bir iş değil),

- Kurum kültürü ve işletme kaynakları (iş gücü dahil) dikkate alınarak geliştirilmesi (aynı sektördeki iki işletmenin bile stratejisi aynı olmayabilir, nihai amaçları aynı olabilir ancak bunu gerçekleştirme tarzı farklılık gösterebilir),

- Dinamik olması (strateji sabit değildir, çünkü işletmenin içinde bulunduğu ortam, ekonomik koşullar, teknolojik gelişmeler, hukuki çerçeve, müşteriler, kendi iş gücü devamlı bir değişim içindedir. Strateji devamlı güncel duruma göre uyarlanmalıdır, esnek olmalıdır),

- Uzun vadeli olması (ortalama 3 ila 5 yıllık bir süreyi kapsamalı),

- "*ne*" ve "*ne zaman*" sorusuna odaklanması, gerçekleştirim detaylarını içermemesi.

Yönetimsel bakımdan startejinin temel öğeleri özet olarak aşağıdaki şekilde sıralanabilir (Özdemir, 1999):

- Strateji, işletmenin faaliyet gösterdiği çevredeki çeşitli koşullar arasındaki ilişkiyi ortaya koyan bir analiz etme ve analiz sonucuna göre de karar verme aracıdır.

- Strateji amaçlara bağlı bir öğedir. Eldeki sınırlı kaynakların en verimli şekilde değerlendirilerek işletme amaçlarına ulaşılması stratejinin varoluş nedenlerindendir.

- Strateji işletmenin dış çevresi ile iç çevresi arasındaki ilişkileri düzenler.

- Strateji uzun vadelidir ve bu özelliği ile rutin karar ve işlemlerden ayrılır.

- İşletmenin kıt kaynaklarının uyum içerisinde yönetilmesini sağlayan strateji, alınacak kararlarda rehber özelliği taşır.

- Her alanında sürekli değişimin yaşanan iş hayatında strateji, işletmelere yön verir.

- Strateji, gelecekle ilgili çevresel belirsizliğin ve dinamizmin çalışanlar üzerinde yarattığı olumsuz etkiyi azaltır, çalışanları motive eder ve cesaretlendirir.

- Strateji, geleceğe, belirsizliğe ve bilinmeyenlerin çözümüne yönelik olduğundan işletmede yeniliklerin yaratılmasını sağlar.

Temel yetkinlik, gelişme vektörü, dış çevre ve sinerji strateji kavramı içerisinde yer alan öğelerdendir. Temel yetkinlik, etkinlik sahası ve rekabet avantajı unsurlarını içeren bir kavramdır. İşletmenin kendisine rekabetçi üstünlük sağlayan ve müşteriye özel değer olarak yansıyan beceriler bütününü içerir. Örgütteki bir becerinin temel yetenek sayılabilmesi için müşteri yararı, rakiplerden farklılaşma ve farklı alanlarda uygulanabilirlik özelliklerine sahip olması gerekir. Gelişme vektörü ise, işletmenin etkinlik alanını belirledikten sonra, onun hangi sahaya yöneleceğini yönetime açıklar. Bu yönelme işletmenin ürettiği ya da üreteceği ürün ve hizmetler konusunda, pazarların durumu değerlendirilerek alınacak kararlarla ilgilidir. Dış çevre faktörü, işletmenin faaliyet gösterdiği çevre koşullarını iyi analiz etme yeteneğine sahip olması ve gelişmeleri yakından takip etmesini gerektirir. Ancak bu şekilde işletme karşısına çıkabilecek fırsat ve tehditleri etkin bir şekilde analiz edebilir. Son öğe sinerji, işletmenin sahip olduğu araçların hangi alanlarda başarılı hangi alanlarda başarısız olacağını belirleyen bir göstergedir.

Bilgi sistemleri veya işletme stratejisi olması bir yana, stratejiye neden ihtiyaç var? Strateji, işletmenin mevcut durumun ve gelecekteki durumun tespitine yardımcı olarak, nihai hedeflere ulaşması için gerekli politikaları içerir. Strateji işletme kaynaklarının fırsatlara göre dağıtılmasını planlayarak sürdürülebilir rekabet gücünün artırılmasını sağlar. İşletmenin bütününü kapsayacak şekilde çeşitli iş ve faaliyetlerin bileşimini, eşgüdümünü ve yönetimini kapsar. Bir işletmeyi yönetenler devamlı gündelik işlere göre karar alırsa, geleceğe hazır olamaz ve geleceğin getireceği risklere (ve maalesef fırsatlara da) hazırlıksız yakalanır. Günümüzde çok başarılı bazı işletmeler, özellikle teknoloji şirketleri, kuruldukları zamandaki faaliyetlerini terketmiş, değişen zamana göre yeni faaliyet alanlarına yönelmiştir. Orijinal

faaliyetlerine bağlı kalsalardı (veya bunların yanına yenilerini eklemeselerdi) çoktan iş dünyasından silinmiş olabilirlerdi. Bu işletmeler geleceği analiz ederek fırsatları görmüşler ve stratejilerini buna göre uyarlamışlardır. İşletme, hem bugünü, hem de geleceği planlamalı ve tüm kaynaklar buna göre harekete geçirilmelidir. İşletmedeki tüm enerji, üzerinde düşünülüp taşınılmış/analiz edilmiş hedeflere yönlendirilmelidir. Bu da sürdürülebilir bir gelişme sağlar. Bu paragraftaki "*işletme*" ifadesi "*bilgi sistemleri birimi*" olarak da okunabilir.

1.1.1.2.2. Bilgi Sistemleri Stratejisi

İşletmelerde bilgi sistemlerinin sratejik rolü, işletmenin rakipleri karşısında üstünlük sağlayacak ürün, hizmet ve yeterliliklerin oluşturulup geliştirilmesinde bilgi teknolojilerinin kullanımını kapsamaktadır. Bu rol bilginin oluşumu, bilginin dönüşümü ve bilginin iletişiminin etkin bir şekilde işletme içerisinde gerçekleştirilmesini sağlar. Bilgi sistemleri yönetişimi kavramlarından biri olan bilgi sistemleri stratejisi, bilgi sistemlerinin işletme hedeflerinin gerçekleştirilmesine nasıl yardımcı olacağının planlanması, tarif edilmesidir. Bu strateji, işletmenin yakın ve orta vadede bilgi sistemleri önceliklerini/hedeflerini belirler ve bilgi sistemleri yatırımlarının buna göre şekillenmesini sağlar.

Bilgi sistemleri stratejisi aslında bir tür fonksiyon stratejisidir. Bir işletmede en geniş anlamda stratejiden söz edilirse, işletmeyi oluşturan birimler için de fonksiyon/birim stratejisinden söz edilir. Fonksiyon stratejisinin amacı aslında kurumsal stratejinin gerçekleşmesine belli bir birimde nasıl destek verileceği sorusunu cevaplamaktır. İşletme stratejisinden belki de en önemli farkı, işletme stratejisinin belirlenmesinde bir ön koşul yokken ve bağımsız belirlenebilirken (işletme içinde uyulması gereken öncül bir doküman olmaması); fonksiyon/birim stratejilerinin ise doğrudan işletme stratejisine bağlı olması ve buna göre şekillenmesidir. İşletme stratejisi bağlayıcıdır.

Bilgi sistemleri stratejisinin bazı özellikleri arasında aşağıdakiler sayılabilir:

- Yönetim kurulu ve üst yönetimin sorumlu olması (işletmenin genelinden bilgi sistemleri birimine inilmesine rağmen sorumluluk halen üst yönetimindir),

- Tüm paydaşlarca üstünde anlaşmaya varılması,

- Performansının ölçülebilmesi,

- Rollerin ve sorumlulukların belirlenmesi,

- Bilgi sistemleri yatırımlarının ve çalışmalarının işe değer katması için işletme stratejisi ile arasında mutlaka uyum olması ve bilgi sistemleri stratejisinde bunun açıkça anlaşılması (burası en sorunlu alanlardan biridir, genelde ya bilgi sistemleri stratejisi hiç düşünülmez ya da sadece bilgi sistemleri birimi içinde ele alınır),

- Bilgi sistemleri stratejisinin gerçekleştirilmesi için bilgi sistemleri yönetimi tarafından kısa, orta ve uzun vadeli planların hazırlanması,

- Bilgi sistemleri riskinin ölçülmesi,

- Bilgi sistemleri yatırımlarının yönlendirilmesi,

- Güncellenebilmesi, esnek olması.

1.1.1.2.3. Bilgi Sistemleri Stratejisi Geliştirme

İşletmeler strateji geliştirirken farklı modeller ve yöntemler kullanabilir. Üzerinde geniş çapta anlaşmaya varılan belirli bir yöntem bulunmamaktadır. Ancak, bilgi sistemleri stratejisinin geliştirme sürecinde genel bir yaklaşım, bunlarla sınırlı olmamak üzere, aşağıdaki gibi olabilir:

- Geliştirilecek sistemin yapısı ve ne amaçla çalışacağı belirlenmelidir.

- Her şeyden önce, işletmenin amaçları, değerleri ve ulaşmak istediği yer anlaşılmalıdır. Diğer bir ifadeyle, işletmenin misyonu ve vizyonu öğrenilmeli; elbette öncesinde de işletmenin misyonu ve vizyonu tanımlanmış olmalıdır.

- Bilgi sistemleri stratejisinin geliştirilmesine ilk önce işletme stratejisinin incelenmesiyle başlanır. İşletme stratejisinin olması, bilgi sistemleri stratejisinin geliştirilmesi için bir ön koşuldur. Bilgi sistemleri stratejisindeki hedefler belirlenirken, işletme stratejisindeki hedefler bir sınır oluşturur. Bu nedenle, işletme stratejisi incelenmeli, burada yer alan hedefler öğrenilmelidir. Bilgi sistemleri stratejisinin geliştirilmesi sırasında işletme stratejisinin dışına çıkılamaz.

- İşletmenin her bir stratejik hedefini gerçekleştirmek için işlettiği/işleteceği iş süreçleri anlaşılmalıdır.

- Bir sonraki aşamada işletmenin veri ihtiyaçları belirlenmelidir. Günümüzde her işletmede belirli bir veri dolaşımı vardır. Bunu ortaya çıkarmak için işletmenin fonksiyonları (yaptığı işler) ve bu fonksiyonları yerine getirirken işlettiği süreçler incelenerek sürecin hangi veriyi kullandığı, bu veriyi nereden elde ettiği, sonuçta nasıl bir veri oluşturduğu ve nereye ilettiği açıkça tanımlanmalıdır.

- İşletmenin her bir iş hedefi için bilgi sistemlerinin neler yapabileceği araştırılmalıdır.

- Bilgi sistemleri stratejisinin kapsamı, süresi, paydaşları, kısıtları (yasal, kurumsal vb) belirlenmelidir. Burada işletmenin değerleri de sınırlayıcı bir faktör olarak dikkate alınmalıdır.

- Mevcut durumun analizi yapılmalıdır. İşletmede hali hazırda hangi sistemler var? İşletmedeki bilgi sistemleri uygulama ve hizmetlerinin envanteri çıkarılmalı ve bunların kullanımı incelenmelidir. Bir anlamda mevcut, işleyen sistemin fotoğrafı çekilmelidir. Bu sayede darboğazlar, eksiklikler, tekrarlar, işleyen ve işlemeyen süreçler ortaya çıkar.

- İşletme stratejisindeki hedefleri gerçekleştirmeye yarayacak; ancak henüz mevcut olmayan bilgi sistemleri çözümleri belirlenmelidir.

- Boşluk analizi yapılmalı ve bulunulan yer ile varılmak istenen yer arasındaki farklılıklar bilgi sistemleri bazında belirlenmelidir.

- Gerekli kaynaklar/yetkinlikler belirlenmeli ve mevcut olmayanların edinimi konusunda planlama yapılmalıdır.

- Yapılacaklar arasında bir önceliklendirme (yine iş hedeflerine bağlı olarak) ve zaman planı yapılmalıdır.

- Gerçekleşmelerin ölçümü için yöntem ve metrikler belirlenmelidir.

1.1.1.2.4. Bilgi Sistemleri Stratejisinin Değerlendirilmesi

Bilgi sistemleri denetimleri esnasında, özellikle bilgi sistemleri strateji geliştirme süreci değerlendirilmelidir. Yukarıda belirtildiği üzere, işletmeler strateji belirleme sürecinde belli bir modele bağlı kalmak zorunda değildir. Ancak kurumsal strateji ve bilgi sistemleri stratejisi için aynı yöntemin kullanılması önemlidir. Bunun yanında, seçilen/kabul edilen yöntem ne olursa olsun mutlaka yazılı ve üst yönetimce onaylanmış olmalıdır. Bilgi sistemleri stratejisinden önce işletme stratejisinin varlığı sorgulanmalıdır. İşletme stratejisi yoksa bilgi sistemleri stratejisinin varlığı bir kazanım sağlamaz.

İşletme stratejisi geliştirilirken kimlerin görev aldığına dikkat edilmelidir. Eğer bilgi sistemlerinin üst yönetimi işletme stratejisinin belirlendiği masada yer almıyorsa, bu durum en başta yapının yanlış kurulduğuna işaret eder. İşletme stratejisi geliştirilirken bilgi sistemleri yönetiminin ekipte yer almaması doğrudan bilgi sistemleri-iş uyumu konusunda risk yaratır.

Benzer şekilde bilgi sistemleri stratejisi geliştirilirken de, masada bu sefer iş birimlerini temsilen üst yönetimin hazır olması gerekir. Aksi durum işletmenin, bilgi sistemlerinin "*gerçekleştirici-enabler*" rolünü kabul etmediği veya işletmede bu farkındalığın henüz sağlanmadığına işaret eder. Tıpkı işletme stratejisinde bilgi sistemleri tarafının olmaması gibi, bu da bilgi sistemleri-iş uyumu konusunda risk barındırır.

Denetim esnasında, işletme stratejisi ile bilgi sistemleri stratejisi beraber değerlendirilmelidir. Strateji içerikleri işletmeye özel ve yoğun alan bilgisi içerdiğinden burada nesnel olarak değerlendirilebilecek husus, bu iki doküman arasındaki ilişkinin görülebilir, anlaşılabilir ve takip edilebilir olup olmadığıdır. Bilgi sistemleri stratejisindeki her bir hedef, bir işletme stratejisine/hedefine

bağlanmalıdır. Bilgi sistemleri stratejisindeki öncelikler işletme stratejisindeki önceliklerle uyum içinde olmalıdır.

Bilgi sistemleri stratejisinin gözetimi ve güncellenmesini gerektiren durumlar belirli olmalı, güncelleme sürecinin nasıl işleyeceği ve kimlerin bu süreci başlatacağı açık olmalıdır.

Bilgi sistemleri stratejisinin, onaylandıktan sonra bilgi sistemleri çalışanlarına duyurulması ve ilgili tüm personel tarafından anlaşılması sağlanmalıdır. Her çalışan, bilgi sistemleri (ve dolayısıyla işletme) stratejisine yapacağı katkıdan haberdar olmalıdır.

Bilgi sistemleri stratejisinin gözetim süreci açıkça belirlenmelidir. Bilgi sistemleri stratejisinin gerçekleşmelerinin nasıl ölçüleceği, ölçümde kullanılacak metrikler, ölçüm sorumluları ve sonuçların nasıl değerlendirileceği belirli olmalıdır.

En nihayetinde strateji geliştirilmesi ve bunun yönetilmesiyle ilgili tüm aşamalar belirli, yazılı, onaylı, ilgililere duyurulmuş ve işler olmalıdır.

1.1.1.2.5. Bilgi Sistemleri Yönetişimi

Bilgi sistemleri yönetişimine geri dönülecek olursa, ilk önce yönetişim ile yönetim kavramının farkının ortaya konulması faydalı olacaktır. Ancak, önce sıkça kullanılacak bir kavram olan "*paydaş*"ın tanımının yapılmasında fayda vardır.

Paydaş, bir işletmenin (birimin) işlerinden etkilenen ve bunların işlerini etkileyen tüm taraflar olarak tanımlanabilir. İşletmenin yatırımcıları, müşterileri, her seviyede çalışanları, tedarikçileri, iş ortakları, kamu otoriteleri paydaş kavramının parçasıdır. Görüldüğü üzere paydaşlar işletmenin içinden olabileceği gibi dışından da olabilir.

Yönetişim (governance), yönetimden farklı ve daha kapsamlı bir kavramdır. Yönetim, günlük işleyiş ile ilgilenirken; yönetişim tüm iş süreçlerinin mevcut ve gelecektiki durumları ile ilgilenir. Yönetişim, iyi bir yönetim ve paydaşların güvenini kazanmak için uygun kültürün ve iklimin oluşturulması olarak tanımlanabilir. Yönetişim, işin içinde üst yönetim ve diğer paydaşların olduğu, işletmenin sadece bugünüyle değil, geleceği ile de ilgilenen, sorumluluğu üstlenen ve hesap verebilen bir yapı veya mekanizmaların bütünüdür. Bu bütünde, ilişkiler, etkileşimler ve kurallar vardır. İşletme stratejisinin geliştirilmesi yönetim kurulunun görevidir ve yönetişim uygulamalarının bir parçasıdır. Yönetim ise, yönetim kurulu ve paydaşlarca belirlenen stratejiden kaynaklanan görevlerin yerine getirilmesiyle ilgilenir.

Bilgi sistemleri yönetişimi kavramı birden bire değil, kurumsal yönetim uygulamalarının bilgi sistemleri alanında gelişmesiyle ortaya çıkmıştır. Bilgi sistemlerinin yönetişiminden söz edebilmek için önce bilgi sistemlerinin destek birimi olarak değil, işin bir parçası olarak değerlendirilmesi gerekir.

Bilgi sistemleri yönetişiminin farklı tanımları bulunmakla birlikte, Bilgi Teknolojileri Yönetişim Enstitüsü (Information Technology Governance Institute) tarafından bilgi sistemleri yönetişimi, kurumsal yönetişimin ayrılmaz bir parçası olan ve bilgi sistemleri kaynaklarının, kurumsal strateji ve hedefleri desteklemesini sağlayacak örgütsel yapıları, süreçleri ve liderlik unsurlarının tamamını içeren bütüncül bir anlayış olarak tanımlanmıştır. Bilgi sistemleri yönetişimi, işletmelerin sahip oldukları bilgi sistemlerine ilişkin kaynaklarının en etkin ve verimli bir şekilde işletme nihai amaçlarını gerçekleştirmek için, bilgi sistemlerine ilişkin karar ve uygulama süreçlerinin yürütülmesine ilişkin tüm faaliyetleri kapsar. Bilgi sistemleri faaliyetlerinin yönetilme şekilleridir. Bilgi istemleri yönetişimine ilişkin tanımlar kapsamında ön plana çıkan hususlar:

- Kurumsal yönetişiminin ayrılmaz bir parçasıdır.
- Üst yönetimin sorumluluğundadır.
- Çaşılanlar, bilgi sistemleri yönetişimi kapsamında görev ve sorumluluklar alır.
- Bilgi sistemleri yönetişimi, bilgi sistemleri yönetiminden daha kapsamlıdır.
- İşletmenin nihai amaçlarına ulaşılmasında ihtiyaç vardır.
- Kendine has yapısı, süreçleri ve liderlik fonksiyonu gerektirir.

- Verimlilik, etkinlikve tutumluluk kıstaslarına vurgu yapar.

Günümüzde, bilgi sistemleri yönetişimi farklı paydaşlar tarafından farklı şekillerde tanımlanabilir; fakat sonuç olarak iş hedeflerinin gerçekleştirilmesi veya iyileştirilmesi için stratejik bir araçtır. Bilgi sistemleri yönetişimi, genel yönetimi iyileştirmeyi ve bilgi sistemlerine yapılan yatırımların işletmeye daha yüksek değer katmasını hedefleyen bir kurumsal yönetim unsurudur. Bilgi sistemleri yönetişimi, bilgi sistemlerinin işletmenin iş hedeflerinin gerçekleştirilmesine nasıl bir katkı sağlayabileceği sorusuyla ilgilenir. Bilgi sistemleri operasyonları işletmenin iş hedefleri ve stratejilerine uymalıdır. Her bilgi sistemi projesi ya da önemli değişiklik/karar, bir iş hedefine faydalı olmak zorundadır.

Önemli bilgi sistemleri kararları sadece bilgi sistemleri yönetimi tarafından değil, üst yönetim tarafından sahiplenilmeli ve takibi yapılmalıdır. Bilgi sistemleri yönetişimi, bilgi sistemleri için bir yol ve hedef belirler. Bilgi sistemleri yönetimi ise, belirlenen yolda hedefe ulaşmak için gerekli çalışmaları hayata geçirir.

Bilgi sistemleri yönetişimi sürecinin girdileri; bilgi sistemleri varlıkları, insan ve zaman olup çıktıları ise iş hedeflerine katılan değerdir. Diğer bir ifadeyle, iş gereksinimlerine uygun performans ve süreklilik düzeyinde işletilen bilgi sistemleri hizmetleri ve iş hedeflerinin gerçekleştirilmesine katkı sağlayan uygulamalardır.

Bilgi sistemleri yönetişiminin önemi aşağıdaki gibi sıralanabilir (ISACA, 2019):

- Bilgi sistemleri yatırımlarının artması, üst yönetimin bunun karşılığını daha ölçülebilir şekilde görmek istemesi,

- Yasal düzenlemelere uyum konusunun artan düzenlemelerle birlikte daha karmaşık hale gelmesi, bu konuda sorumluluğun üst yönetimde olması,

- Gelişen iş modelleri ile dış kaynaktan tedarik işleminin cazibesini artırması; ancak çeşitli riskleri de beraberinde getirmesi,

- Bilgi sistemleri risklerinin ve yasal sorumlulukların artması,

- En nihayetinde işletmelerin tüm bu işleri ne kadar iyi yaptıklarını (veya yapamadıklarını) görmek istemesi.

1.1.1.2.6. Bilgi Güvenliği Yönetişimi

Bilgi sistemleri yönetişimi ile beraber değinilmesi gereken bir diğer kavram bilgi güvenliği yönetişimidir (information security governance). Nasıl bilgi sistemleri yönetişiminde, işletmenin bilgi sistemlerine bakış açısı üst yönetim düzeyine çıkarılmışsa ve bilgi sistemlerinin yönlendirilmesi ve gözetimi üst yönetim tarafından yapılıyorsa, bilgi güvenliği yönetişiminde de benzer mantıkla, işletmenin bilgi güvenliğine ilişkin yönlendirme, gözetim ve değerlendirme faaliyetleri üst yönetim tarafından sahiplenilmelidir.

Her tür işletmenin bilgi ile yönetilmesi, dolaşımda olan bilginin çok büyük boyutlara gelmesi, bilgi güvenliği/korunması konusunda gerek ülkeler, gerekse de bölgeler bazında birçok yasal düzenlemenin yürürlüğe girmesi ve işletmelerin bunlara uyum yükümlülüğü bilgi güvenliğinin de üst yönetim düzeyinde sahiplenilmesini ve gözetimini gerekli kılmıştır. Bilgi güvenliği ihlalleri artık işletmelerin iş yapma kapasitelerini doğrudan etkileyebilir seviyededir. Dolayısıyla bilginin korunması, iş operasyonlarının korunması anlamına gelmektedir.

Bilgi güvenliği yönetişimi, bilgi sistemleri yönetişiminin altında değerlendirilebilir veya özellikle büyük işletmelerde ve yüksek riskli işletmelerde bilgi sistemleri yönetişimi doğrultusunda; ancak ayrı bir pratik olarak ele alınabilir. Bilgi güvenliği yönetişimi altında aşağıdaki süreçler sayılabilir:

- Bilgi güvenliği politikasının geliştirilmesi, iş hedefleriyle uyumunun sağlanması, onaylanması ve işletiminin gözetimi,

- Bilgi sistemleri yönetişiminde aşina olunan bilgi sistemleri-iş uyumu, bilgi güvenliği-iş uyumu olarak burada da görülür. Bu durum iş hedeflerinin güvenliği ve iş operasyonlarının güvenliği olarak okunabilir,

- Bilgi güvenliği risk yönetimi,

- Bilgi güvenliği kontrollerinin oluşturulması,

- Bilgi güvenliği ihlallerinin gözetimi,

- Bilgi güvenliğine ilişkin rollerin ve sorumlulukların belirlenmesi,

- Farkındalık ve eğitim,

- Yasa, düzenleme ve standartlara uyumun sağlanması,

- Gerekli kaynakların tahsisi.

Tüm bu konularda gerekli yönlendirme, görevlendirme, gözetim ve değerlendirme süreçleri bilgi güvenliği yönetişimi altında olup, işletme yönetiminin sorumluluğundadır. Bilgi güvenliği yönetişimi, bilgilerin güvenliğinin sağlanmasına yönelik bilgi güvenliği politikalarının oluşturulmasını sağlar. Bilgi güvenliği politikaları, işletmenin bilgiyi nasıl yönettiği, koruduğu ve dağıttığını gösteren kural ve uygulamaları içerir.

1.1.1.2.7. Bilgi Sistemleri Yönlendirme Komitesi

Bilgi sistemleri yönlendirme komitesi (IT steering commitee), yönetim kurulu tarafından işletmenin bilgi sistemleri önceliklerini belirlemek ve bu kapsamda bilgi sistemleri yatırım ve projelerinin yönetimini sağlamak amacıyla kurulur ve yönetim kuruluna rapor verir. Komitenin görevi, bilgi sistemleri yatırımları, bütçesi, önemli projeleri, bilgi sistemleri riski ve bilgi sistemleri performansının gözetimidir. Bu komite, bilgi sistemleri yatırımlarının ve bilgi sistemleri projelerinin öncelik sırasını belirler. Bilgi sistemleri mimarisi ve projelerinin mevzuata uyumu için gerekli yönlendirmeleri yapar. Teknoloji odaklı bir komite değildir. Komitede bilgi sistemleri ve diğer iş birimlerinin üst yönetimi görev alır. Komitenin temel sorumlulukları:

- Bilgi sitemleri-iş uyumunu sağlamak için kısa ve uzun vadeli bilgi sistemleri planlarının gözden geçirilmesi,

- Önemli bilgi sistemleri projelerinin onaylanması ve gözetimi,

- Bilgi sistemleri kaynaklarının gözetimi,

- Bilgi güvenliği faaliyetlerinin gözetimi,

- Dış kaynak kullanımını konusunda gözetim ve onaylama işlevleri,

- Bilgi sistemleri performans ve risk yönetimi (ISACA, 2019).

Komitenin görev ve yetkileri, çalışma biçimi ve hedefleri yazılı olmalıdır. Çok küçük işletmelerde müstakil bir komite olmayabilir; sorumluluklar üst düzey yöneticiler tarafından yerine getiriliyor olabilir. Ama komitenin görev ve yetkileri, çalışma biçimi ve hedeflerinin yazılı olmaması ve özellikle böyle bir farkındalığın olmaması işletme açısından risktir.

Çok büyük işletmelerde, bu komitenin üstünde bilgi sistemleri strateji komitesi yer alabilir. Bu komite genelde yönetim kurulu üyeleri ve uzmanlardan oluşur. Bu komite, bilgi teknolojileri inisiyatifleri hakkında yönetim kuruluna öneri sunar, yönetim kurulu kararı alır ve bilgi sistemleri yönlendirme komitesine gerçekleştirme ve gözetim görevini verir. Yine çok büyük işletmelerde, bizzat bilgi sistemleri projelerinin gözetimiyle ilgili proje gözetim komitesi de olabilir. Proje gözetimiyle ilgili ayrı bir komite olmadığında bilgi sistemleri yönlendirme komitesi bu görevleri de yerine getirir.

1.1.1.2.8. Bilgi Sistemleri ve İş Uyumu

Bilgi sistemleri yönetişimi tanımlarının hepsinde görülen kavramlardan biri, bilgi sistemleri ve iş tarafının uyumudur. Bu kavramla kastedilen çok kısaca, bilgi sistemleri faaliyetlerinin iş hedeflerine

katkı sağlaması ve onları desteklemesidir. İş tarafı ile bilgi sistemlerinin birlikte haraket edebilme yeteneğine sahip olabilmesidir. Bu kavram, söylemesi kolay ancak gerçekleştirmesi zor bir kavramdır. Akla ilk önce iş tarafı ile bilgi sistemleri neden farklı hedefler peşinde olsun, neden birlikte hareket edemesin soruları gelebilir; ama tecrübeler göstermiştir ki, iş ve bilgi sistemleri birimleri arasında birtakım odak kaymaları hep olagelmiştir. Teknolojinin bu kadar yoğun kullanıldığı/kullanılabildiği bir ortamda, bu uyumu garantiye almak için "*bilgi sistemleri ve iş uyumu*" kavramı geliştirilmiştir.

Daha önce belirtildiği üzere, bilgi sistemleri ve iş birimleri arasında uyum hedeflenir, daha doğrusu zaten olduğu kabul edilir; ancak her zaman yakalanamayabilir. Bu durumun sebepleri ve göstergeleri araştırılmış ve aşağıdaki gibi sonuçlara ulaşılmıştır:

- İş tarafının önemli toplantılarında (özellikle yeni ürün/hizmet geliştirilmesi, mevcut faaliyetlerde önemli değişiklikler yapılması gibi) bilgi sistemleri temsilcilerinin yer almaması.

- Bilgi sistemleri-iş uyumu kavramının bilinmemesi (farkındalık eksikliği).

- Bilgi sistemleri tarafında devamlı en yeni teknolojilere yönelme. İşe katacağı değeri göz ardı etme.

- Bilgi sistemleri hedeflerinin kişilere, bilgi sistemleri yönetimine çok bağlı olması (kişiler değiştikçe odağın değişmesi).

- Bilgi sistemlerinin gerekli kaynaklara sahip olmaması (işgücü, zaman, teknoloji gibi).

- Özellikle bilgi sistemleri ve iş tarafı arasında iletişim noksanlığının bulunması.

- Değişime direnç (sanıldığı gibi sadece iş tarafında değil, bilgi sistemleri tarafında da olabilir).

- Birçok işletmede, iş tarafının yeniliklere ve teknolojinin potansiyeline ikna edilmesinin zorluğu.

- İş tarafının bilgi sistemlerini sadece destek noktası olarak görmesi.

- Bilgi sistemlerinin mutlaka gerekli iş süreçlerinin daima bir kaynak israfı olarak görülmesi. Özellikle iş gücüne yatırımın eksik olması. Tüm işlerin/projelerin hep acil olması. Günlük bilgi sistemleri çözümlerine yönelme.

- Bilgi sistemleri-iş uyumu için gerek şart ortada bir iş stratejisinin olmasıdır. Eğer bu yoksa bilgi sistemleri mecburen günlük işlere koşturmaya devam eder. Ya da böyle bir strateji olsa bile bunun iyi tanımlanmamış olması veya iş stratejisinin değiştirilip (hızlı değişen ortamlarda çok olası), bilgi sistemleri stratejisinin değiştirilmemesi hatta bilgi sistemleri stratejisinin hiç olmaması.

- Bilgi sistemleri çalışanlarının işe hep bilgi sistemlerinden başlaması ve son teknoloji, performans, hız gibi konuların hep öncelikli olması (müşteri (iş tarafı) merkezli olmamak).

a. Bilgi Sistemleri-İş Uyumu En İyi Uygulama Örnekleri

Bilgi sistemleri ve iş arasındaki boşluğu, uzaklığı kapatmak için teknolojiden önce insan unsuru önem taşımaktadır. İş odaklı diye tarif edebilen bilgi sistemleri çalışanları (işin dilinden anlayan, işi öğrenen, bu konuya odaklanan) ile bilgi sistemlerine yatkın iş tarafı çalışanları arada köprü görevi görebilir. Aşağıda yer verilen bazı noktalara özellikle dikkat etmek bu uyumun yakalanmasına zemin hazırlayabilir:

- Dil birliği. İş ve bilgi sistemleri tarafı aynı dili konuşabilmeli. "*iş/kurum dili*", "*iş/kurum jargonu*" öğrenilmeli.

- Ölçemezsen iyileştiremezsin. ("*if you can't measure it, you can't improve it"*, Peter Drucker) Stratejik hedefler mutlaka ölçülebilir olmalı. "*En iyi*", "*En hızlı*", "*En ucuz*", "*Azaltmalıyız*" gibi hedefler ölçülemez. Dolayısıyla iyileştirilemez.

- Anlaşılır olmak. Bilgi sistemleri tarafındaki ölçümler (en azından makro düzeyde olanlar) iş tarafının da anlayacağı şekilde yapılmalı. Bilgi sistemleri teknoloji ölçümleri bilgi sistemleri birimi içinde anlamlıdır, birimin dışında değil. Bilgi sistemleri iş tarafına yaptığı katkıyı açıklarken "*işe katılan değer*" bazında açıklama yapmalı. Çok kullanılan bir ölçümden örnek verilecek olursa, sistemin %99,5

ayakta olması bilgi sistemleri birimi için anlamlı. Ama bunu iş tarafına açıklarken bu ölçümün iş için anlamını açıklamak gerekli.

- Üçüncü göz. Teknolojinin iş konusundaki/iş geliştirme konusundaki potansiyeli hakkında gerekiyorsa işletme dışından yardım almak işe yarayabilir. Bazen üçüncü taraflar daha "*dinlenebilir*"dir.

- Proaktif yaklaşım. Bilgi sistemleri biriminin, özellikle de yönetim kademesinin görevi genişlemiş, bilgi sistemlerinden fazlası olmuştur. Artık bu kişiler çalıştıkları işletmelerin işinden de anlamak durumundadır. Diğer bir deyişle, eskiden olduğu gibi "*bizim işimiz teknik*", "*siz ne istediğinizi söyleyin yapalım*" gibi yaklaşımlardan kaçınılmalıdır. Proaktif olarak, işi anlamak ve buna uygun çözümleri kullanıcıya anlatmak gerekir. İşletme içinde bir nevi "*iş geliştirme*" ekibi gibi çalışılmalıdır.

- Yapmadıklarına odaklan. Teknoloji trendleri iyi takip edilmeli. Mevcut durumun sorunsuz işlemesi, işletmenin teknolojinin potansiyelinden gerektiği gibi faydalandığını göstermeyebilir.

- Rolünü öğren. Bilgi sistemlerinde her çalışanın bilgi sistemleri stratejisinden haberinin olması ve kendi üzerine düşen payı bilmesi gerekmektedir.

- Bilgi sistemleri yönetişimi. İşletmede bilgi sistemleri yönetişimi yaklaşımını bir şekilde hayata geçirmelidir. Özellikle küçük işletmelerde böyle bir işe girişmek zahmetli olabilir. Ama bilgi sistemleri yönetişimi her işletmede aynı bürokratik yöntemlerle yapılmak zorunda değil. İşletmenin büyüklüğü ve yapısına uygun, daha çevik yaklaşımlar geliştirilebilir.

- Temsilciler birliği. Özellikle büyük bilgi sistemleri projelerinde takımda mutlaka iş tarafının temsilcileri de olmalıdır.

b. Bilgi Sistemleri-İş Uyumunun Değerlendirilmesi

İşletmede, bilgi sistemleri yönetişiminin temel unsurlarından biri olması nedeniyle bilgi sistemleri-iş uyumu mutlaka değerlendirilmelidir. Değerlendirme yaparken özellikle konu hakkında bilgi sistemleri yöneticilerinin farkındalığı ve yukarıda bahsedilen "*istenmeyen*" belirtilerin varlığı araştırılmalıdır. Ayrıca önerilen en iyi uygulama yaklaşımlarının (veya benzerlerinin) uygulaması değerlendirilmelidir.

Değerlendirme sırasında, bilgi sistemleri biriminin çalışma planları incelenmeli, bu planların doğrudan (süregelen işler dışında) stratejiden kaynaklanıp kaynaklanmadığına bakılmalı (işletme ve bilgi sistemleri stratejileri) ve bu işler için gerekli kaynak planlamasının varlığı sorgulanmalıdır. Stratejiye dayalı planların olmaması veya bu planların sahaya yansımasının hiçbir göstergesinin bulunmaması bilgi sistemleri-iş uyumu açısından risk teşkil etmektedir.

1.1.1.2.9. Bilgi Sistemleri Kaynak, Risk ve Performans Yönetimi

Bilgi sistemleri, iş hedeflerine katkı sağlayacak faaliyetleri gerçekleştirirken birtakım kaynakları kullanmak durumundadır. Bilgi sistemleri hedeflerine ulaşılması için yeterli ve etkin kaynaklara ihtiyaç vardır. Bunların belirlenmesi, finanse edilmesi, edinimi, tahsisi, kullanımı, insan kaynakları da dahil olmak üzere yönetimi, bilgi sistemleri yönetişiminin unsurlarındandır. İlerleyen bölümlerde bununla ilgili detay konulara değinilecektir.

Bilgi sistemleri stratejisi ve bu doğrultuda bilgi sistemlerine dair planların hazırlanmasından sonra faaliyetlerin gerçekleştirilmesi ve iş hedeflerine ulaşılması sürecinde bilgi sistemleri birçok riskle karşı karşıyadır. Bilgi sistemlerinde yüksek maliyetli kaynaklara yatırım yapılması, her geçen gün yeni bilgi güvenliği zafiyetlerinin ve ihlallerinin ortaya çıkması ve bu konuda yasal düzenlemelerin artması bilgi sistemlerine ilişkin risklerin kontrol altında tutulmasını ya da diğer bir ifadeyle risk yönetimi yapılmasını zorunlu tutmaktadır.

İşletmelerde risk yönetimi hali hazırda (özellikle finansal işletmelerde) yasal mevzuatta tanımlanmış bir süreç olmasına karşın, bilgi sistemleri risk yönetimi görece yeni bir kavramdır ve yeni bir gereksinimdir. Bilgi sistemleri risklerinin yönetilmesi, bilgi sistemleri yönetişiminin unsurlarından biridir. İlerleyen bölümlerde bununla ilgili detay konulara değinilecektir.

Bilgi sistemleri yönetişimi kavramlarından sonuncusu, performans yönetimidir. Tüm faaliyetlerin planlandığı şekilde yerine getirilip getirilmediği; kaynakların ne kadar etkili kullanıldığı ve

stratejik hedeflere ne kadar ulaşıldığı bu süreçte ortaya çıkacaktır. İlerleyen bölümlerde bununla ilgili detay konulara değinilecektir.

Kısaca bahsedilen bu üç kavram, bilgi sistemleri yönetimi alanında kendine geniş yer bulduğu için Çalışma Notu'nun "*Bilgi Sistemleri Yönetiminin Unsurları*" bölümünde daha detaylı ele alınacaktır.

Bilgi sistemleri yönetişimi ile ilgili detaylı bilgiye Information Systems Auditing and Control Association (https://www.isaca.org/) ve ISO/IEC 38500 Information Technology-Governance of IT for the Organization (https://www.iso.org/standard/62816.html) kaynaklarından, bunlarla sınırlı olmamakla birlikte, ulaşılabilir.

1.1.1.2.10. Bilgi Sistemleri Yönetişiminin Değerlendirilmesi

Bilgi sistemleri yönetişim kavramlarının işletme düzeyinde farkındalığı (isimlendirmeler farklı olabilir), buna ilişkin nasıl bir süreç tasarımı yapıldığı, ne şekilde işletildiği, rol ve sorumlulukların nasıl tanımlandığı, yetki devri varsa bunun yazılı olup olmadığı, iletişim yöntemlerinin ne olduğu, tüm bunların yazılı ve onaylı olup olmadığı gibi hususlar değerlendirme sürecinde ilk başta ele alınmalıdır. Yalnız işletmenin büyüklüğü ve personel sayısı bu değerlendirmede önemli bir parametredir. Yukarıda anlatıldığı üzere, bilgi sistemleri yönetişimi zahmetli bir süreçtir. Büyük işletmelerde olmasa da özellikle küçük işletmelerde bilgi sistemleri (hatta işletme) yönetişiminin tüm mekanizmalarının görülmesi mümkün olmayabilir.

Burada önemli olan, bir şekilde işletmede bu farkındalığın varlığı, bilgi sistemlerinin iş ortağı olarak görülmesi, kurumsal kararlar alınırken özellikle yeni bir faaliyete başlanacak, yeni bir sektöre girilecek, yeni bir ürün/hizmet geliştirme kararı verilecek ise bilgi sistemlerinin işe katılması, iş hedefleri ile bilgi sistemleri hedefleri ilişkisinin bir şekilde kurulmasıdır.

Bilgi güvenliği yönetişmi farkındalığı, bu amaçla yapılanlar, özellikle bilgi güvenliği konusunun işletmede hangi seviyede ve ne detayda ele alındığı hususu da değerlendirilmelidir.

Diğer taraftan, bilgi sistemleri hedeflerinin ve başarımlarının üst yönetim kademesinde takip edilmesi, özellikle büyük bilgi sistemleri yatırımlarının üst yönetim tarafından onaylanması, bilgi sistemleri risklerinin gözetiminin yapılması, bilgi sistemleri kaynaklarının kullanımının takip edilmesi ve yasal düzenlemelere uyumun izlenmesi hususları değerlendirilmelidir. Başka bir ifadeyle bilgi sistemleri yönetişimi, işletmede üst yönetim veya yönetim kurulu seviyesinde ele alınmalı; sadece bilgi sistemleri birimine bırakılmamalıdır.

1.1.1.2.11. Kurumsal Mimari ve Veri Mimarisi

Bir işletme, hedeflerine ulaşmak için birçok bilgi sistemi yatırımı yapmış, insan kaynağı oluşturmuş, örgüt yapısını kurmuş ve gerekli teknolojik altyapıyı sağlamış olmasına karşın tüm bu elindekiler ile ne yapacağını bilemiyorsa, bilgi sistemleri kaynaklarını etkin ve verimli kullanamıyordur. Nitekim birçok işletmede, bilgi sistemlerine yapılan yatırımlardan yeterince geri dönüş alınamamaktadır. Çoğu zaman kimse bilgi sistemleri birimlerinin ne iş yaptığını bilmez. Şimdi bu öğelerin tümü bir araya geldiğinde ortaya karmakarışık bir yapı değil de, işletmenin işine yarayacak bir çözüm (en az maliyetle en etkili şekilde) çıkması için ne yapılmalı? Bu sorunun cevabı *kurumsal mimariyi tanımlamalı* olarak verilebilir.

Kurumsal mimari çok temel olarak bir işletmede; kişiler, süreçler, uygulamalar, teknolojiler ve veri arasındaki ilişkiyi gösteren, bu öğelerin en doğru şekilde işletmeye yerleştirilmesini ve birbiriyle ilişkilerinin kurulmasını sağlayan, bu yapıyı ortaya çıkaran bir mimari plan veya bir yaklaşımdır. Kurumsal mimari, bir işletmeyi oluşturan yapılar, parçalar, bunların işlevleri, bunlar arası ilişkiler, iş ve veri akışları ile bunları yöneten kuralların bütününe verilen isimdir. Her işletmenin nihai bir hedefi vardır. Ancak günlük koşturmacalar içinde bu nihai hedefler gözden kaçabilir. Bu nedenle, kurumsal mimari işletmenin her çalışanına/paydaşına işletmenin hedefinin ve yönünün ne olduğunu hatırlatarak bunların gözden kaçmasını önler. Kurumsal mimari sayesinde işletmedeki her birim/grup/çalışan işletmenin nihai hedefleri ve stratejileri hakkında bilgi sahibi olur, bunun nasıl sağlanabileceğini-eldeki araçların ve süreçlerin neler olduğunu-anlar, çalışmalarını buna göre şekillendirebilir, ayarlayabilir.

Kurumsal mimari sonuçta bir belgedir. Ancak gerek bu belgeyi ortaya çıkarırken gerekse de bunu yaşatırken işletilen süreçler işletmenin girdisi ve çıktısının anlaşılmasını sağlar. Tıpkı strateji gibi kurumsal mimari de işletmeye özgüdür. Kurumsal mimari değişmez değildir. İşletmenin faaliyet gösterdiği çevredeki değişikliklerin işletmenin yapı ve faaliyetlerine etkisi ölçüsünde yeniden gözden geçirilmesi ve değiştirilmesi gerekir.

Kurumsal mimarinin amacı, iş stratejilerinin gerçekleştirilmesi için bilgi sistemlerinin neler yapabileceğini ortaya koymak ve bunu hayata geçirmektir. Kurumsal mimari, işletmelerin bilgi sistemleri altyapısını iş hedefleriyle uyumlu hale getirmek için standartlaştırdığı süreçtir. Bilgi sistemleri kaynaklarını etkin ve verimli bir şekilde kullanılması amaçlanır. Kurumsal mimari çatısı altında üretilen organizasyonel planlar ile işin kalitesi geliştirilir, verimli ve yönetilebilir bir iş süreci adaptasyonuna imkan sağlar. Kurumsal mimari, işletmenin mevcut yapısından başlar ve onu hedefe yöneltir. Ancak gelecek her zaman bilinmezlikleri de içinde barındırır. Kurumsal mimari, işletmenin değişikliklere karşı esnek ve cevap verebilir olmasına yardımcı olur.

1.1.1.2.11.1. Kurumsal Mimarinin Geliştirilmesi

Kurumsal mimarinin oluşturulması aşamasında işletmeye yukarıdan bakmak gerekir. Bu bakış esnasında görülenler önceliklendirilmelidir. Kurumsal mimariyi oluşturma başlangıç ve bitiş noktaları belli, bir defada gidilecek düz bir yol değildir. Mimarinin döngülerle oluşturulması, her aşamada daha detaya inilmesi ve işletmenin değişen ihtiyaç/strateji/hedeflerine göre de mimarinin değiştirilmesi gerekir. Çünkü çok az işletmede zaman içerisinde hedefler/öncelikler değişmeyebilir. Kurumsal mimari, işletmenin hedeflerine ulaşmasına yardımcı olacaksa, işletmenin hedefleri/stratejileri değiştiğinde mimarinin de değişmesi gerektiği açıktır (Armour, F., Kaisler, S., Liu, S.Y., 1999).

Aslında hiçbir işletme mimarisiz değildir. Bir şekilde bilgi sistemleri kullanan her işletmede bir mimari vardır. Bir yerlerden veri gelip bir yerlerde işleniyor ve birileri bunlara bakıyordur. Sadece adı konmamıştır, kötü bir mimaridir ve ihtiyaçlara cevap veremiyordur. Bir işletmede kurumsal mimari yok demek, o işletmenin içi boş demekle aynıdır. İyi tasarlanmış bir kurumsal mimari, fırsatlara ve değişimlere açık olan piyasaya hızlı adaptasyonu sağlayarak, işletme faaliyetlerinin etkinliğini artırır. Ekonomik ortamdaki değişimleri hızlı cevap verme yeteneği kazanma, bilişim altyapısı yönetim giderlerinin azaltılması, çalışanların iletişimleri ve sistemler arasındaki ilişkilerin geliştirilmesi ve iş süreçlerinin ve bu süreçlerin analizinin desteklenmesi hususlardında katkı sağlar.

Kurumsal mimarinin geliştirilmesinde aşağıdaki adımlar izlenebilir:

- Kapsamı belirle. Kurumsal mimari ifadesindeki kurum, aslında işletmenin kendisi değil, bir bölümü/bir birimi de olabilir. Buradaki kurum ifadesi belli hedefleri olan bir grup insanın oluşturduğu yapıyı temsil etmektedir. Ayrıca, kapsam oluştururken, özellikle çok büyük ölçekli kurumlar ve mimari alanında tecrübesi olmayan ekipler söz konusu ise, mutlaka görece az karmaşık/küçük olandan başlamak en iyisidir.

- Ekip oluştur. Ekipte mutlaka iş uzmanlarının/temsilcilerinin olması gerekir.

- Hedef oluştur. Doğrudan kurumsal stratejiyle ilişkili olarak işletmenin (hangi kapsamda alındığından bağımsız) gelecekte olmak istediği yerin, almak istediği şeklin ve vermek istediği görüntünün belirlenmesi gerekir. Zaten tüm süreçten beklenti de budur: Neredeyiz ve nereye varmak istiyoruz.

Bununla birlikte, ortak hedef konusunda tüm taraflar anlaşmalıdır. Bu husus, mimarinin gerçeğe/işlerliğe dönüşmesinin ön koşullarından biridir. Bu noktada aşağıdaki sorular sorulmalı:

a. Paydaşlar kim? Bunlar mimariyi/hedefi nasıl kullanacaklar?

b. Hangi problemler çözülecek?

c. Her problemin önceliği ne?

- Mevcut durumu belirle. Nerede olunduğu bilinmiyorsa, hedefe nasıl gidileceği bilinemez. Bu durumda önce mevcut mimariyi oluşturmak gerekir.

Mimari oluştururken işletmeye 4 çeşit gözlükle bakılması gerekir. Bunlar:

1. İş mimarisi: İşletmenin yaptığı esas iş, işletmenin misyonu, işletmenin yaptığı işler ve ürettiği ürünler/hizmetler. İş birimlerinin amaçlarına ulaşması için uygulanacak süreçleri belirler.

2. İşlevsel mimari: İşletmenin bir önceki adımda sayılan işleri yaparken (ürünü/hizmeti üretirken, satarken) kullandığı/yararlandığı uygulamalar ve bunların birbirleriyle ilişkisi. İş süreçleriyle uygulamaların ilişkisini belirler.

3. Veri/Bilgi mimarisi: Yukarıdaki işler yapılırken girdi/çıktı/dolaşımda olan veri. Kurumsal veri kaynaklarının nasıl düzenleneceği ve bunlara nasıl erişilebileceğini belirler.

4. Altyapı mimarisi: İş süreçlerini destekleyen bilgi sistemleri bileşenleri. Uygulamalar ve bunların ilişkilerini destekleyecek donanım, yazılım ve iletişim alt yapısını belirler.

- Mevcut sistemin güçlü ve zayıf yanları belirlenir. Her bir iş süreci için kullanılan uygulamalar, kullanılan veri, birbiriyle ilişkisi ve arayüzleri.

- Hedef durum belirlenir (hedef mimari).

Hedef durum, işletmenin gelecekteki vizyonunu gerçekleştirmek için gerekli bilgi sistemleridir. İşletmenin orta vadede (3-5 yıl) yapmak istediği işlerdir. Hedef mimari, tıpkı mevcut mimarinin geliştirildiği gibi aşamalar takip edilerek oluşturup geliştirilir. Tek fark, hedef mimari geliştirilirken mevcut durum değil, işletmenin vizyonu dikkate alınır. Hedef mimari, tam olarak işletmenin vizyonundaki resmin parçasıdır. Burada mevcut durum mimarisinden farklı olarak, iş stratejilerinin değişmesi riski vardır ki bu da hedef tasarımın yeteri kadar esnek olmasını gerektirir.

Bütün bu adımlar işletilirken unutulmaması gereken husus, iş gereksinimlerinin asla ihmal edilmemesi ve iş tarafının uzlaşısının mutlaka sağlanmasıdır. Ancak, burada yirmi yıllık kurumsal mimari uygulamalarının gösterdiği üzere, bir de kötü tablo vardır. Yapılan araştırmalara göre kurumsal mimari projelerinin %66'sı başarısızlıkla sonuçlanmaktadır. Peki bunu önlemek için neler yapılabilir? Burada öncelikle aşağıdaki hususlar dikkate alınabilir (Andriole, 2020):

- Kurumsal mimari geliştirirken asıl hedefi hiç gözden kaçırmamak gerekir. Burada asıl hedef, çok iyi bir teknolojik altyapı kurmak, bilgi sistemleri kapasite ve performansını yükseltmek değil, iş hedeflerini gerçekleştirmektir (zaten bu hedef teknolojik iyileştirmeyi de gerektirecektir).

- Kurumsal mimari çalışmalarında hedef iş tarafından teknoloji tarafına kayınca, bu artık bir bilgi sistemleri projesi olur. Devamında üst yönetimin, paydaşların ve iş tarafının desteği ve motivasyonu kaybedilir.

- Kurumsal mimarinin ne ile ilgili olduğu sorusunun cevabı (teknolojiden hiç bahsetmeden) şu olabilir: Kurumsal mimari bir işletmenin iş hedefleri ve stratejileri ile ilgilidir. İş tarafı bugün ve gelecekte ne istiyor? Bilgi sistemleri bunu nasıl sağlayacak? Ve bu uyum sürekli tekrarlanacak; çünkü iş tarafının istekleri devamlı değişecektir.

- Kurumsal mimari sadece işletme stratejisinden/bilgi sistemleri stratejisinden kaynaklanıyorsa anlamlıdır.

Kurumsal mimariye ilişkin çalışmalarda aşağıdaki yanlışların yapıldığı gözlenmektedir:

- Kurumsal mimari geliştirmenin amaç haline gelmesi. Kurumsal mimari amaç değil araçtır. Amaç daima işletmenin hedefleri olmalıdır.

- Kurumsal mimaride terminoloji ve kullanılan yöntemlerin çok teknik ve çok karmaşık olması ve tüm paydaşlar tarafından (tam olarak) anlaşılamaması. Yöntemlerin detayına inildikçe asıl konunun unutulması.

- Kurumsal mimari ekibinde iş biriminin yer almaması, tamamen bir bilgi sistemleri projesi olarak yürütülmesi.

- Teknik olarak çok doğru bir mimari geliştirmeye çalışılması, iş tarafı açısından konuya bakmanın unutulması.

Kurumsal mimaride en nihayetinde, iş süreçleri, bunları destekleyen uygulamalar, bunlarda girdi/çıktı olan veri, süreçlerin birbiriyle ilişkisi ve en altta bunları destekleyen teknolojik altyapı yer almaktadır.

Kurumsal mimarinin faydaları olarak aşağıdakiler sayılabilir:

- Kurumsal yapının mimari bileşenlerinin tek bir modelde görüntülenmesi,

- Yapılan değişikliklerin mimariye olan etkilerinin ortaya konulması,

- Stratejik karar mekanizmalarının desteklenmesi,

- Uluslararası standartlarda dokümantasyon yapılabilmesi,

- İş süreçlerinin hangi sistemler üzerinde çalıştığının görselleştirilmesi ve yönetiminin kolaylaşması,

- Daha fazla uygulama kapasitesi ve daha fazla uygulama ile çalışabilme,

- Bilgi sistemleri geliştirmede, bakım ve destek maliyetlerinde azalma,

- Risk yönetimi ve iş sürekliliği planlamalarının yapılabilmesi,

- Teknoloji alanında yapılacak güncellemelerin yönünün tespit edilmesi,

- Sürdürülebilir büyümeyi desteklemesi,

- Genele yayılan sorunları daha kolay ele alma,

- Bilgi sistemleri bileşenlerini daha kolay güncelleme ve değiştirme,

- Bilgi sistemleri geliştirme, satın alma veya dış kaynak kullanma esnekliği,

- Daha düşük yatırım riski ve daha yüksek yatırım getirisi (maksimum yatırım getirisi),

- Yeni yatırımlarda risk ve maliyetleri azaltma,

- Bilgi sistemleri altyapısındaki karmaşıklığı ortadan kaldırma,

- Etkin ve verimli tedarik süreci.

Kurumsal mimari ile ilgili detaylı bilgiye, Zachman Framework (https://www.zachman.com/) ve The Open Group Architecture Framework (https://www.opengroup.org/togaf) kaynaklarından, bunlarla sınırlı olmamakla birlikte, ulaşılabilir.

1.1.1.2.11.2. Veri Mimarisi

Veri mimarisi, kurumsal mimarinin bir alt dalı olarak düşünebilir. Yukarıda yer verildiği üzere, mimari oluşturulurken kullanılan dört bakış açısından biri de veri/bilgi mimarisidir. Kurumsal mimari, iş hedeflerinin bilgi sistemleri kaynak ve uygulamalarıyla nasıl gerçekleştirileceğinin bir modeliyse; veri mimarisi de iş hedeflerinin gerçekleştirilmesi sırasında işletmede ihtiyaç duyulacak veri, mevcut veri, veri kaynakları, verinin toplanması, saklanması, kullanılması, dolaşımı, aralarındaki ilişkiler ve tabii olduğu kurallar/standartlar ile ilgili teknolojinin sunduğu çözümlerin bir modellemesidir. İşletmede üretilen, dışardan alınan, kullanılan, dolaşan, dışarıya sunulan verinin planı ya da dokümantasyonudur (Olavsrud, 2022). İşletmenin stratejik veri gereksinimleri ve veri varlıkları ile veri yönetimi kaynaklarının yapısını tanımlar.

Veri mimarisinin prensipleri:

- Veri işletmede ortak bir kaynaktır. İşletmenin bölümleri ayrı ayrı yerlerde veri depoları olmamalıdır.

- Veri kullanımını kolaylaştıran araç ve arayüzler olmalıdır. Çalışanlar kendinlerine verilen erişim yetkileri kapsamında ihtiyaç duydukları verilere kolay erişebilmelidir.

- Verinin güvenliği gözetilmeli ve erişim kuralları/hakları belirlenmelidir. Veri ortak kaynaktır; ancak herkes her veriye aynı şekilde erişememelidir.

- Veri uygun bir şekilde düzenlenmelidir. Veriler arası önemli ilişkiler modelleme, verilerin boyutlarını ayarlama gibi işlemler bir düzen içerisinde yapılmalıdır.

- Veriye ait ortak bir dil geliştirilmeli, birimler arası farklı kavramlar ve adlandırmalar ortadan kalkmalıdır. Verilerde ortak isimlendirme kullanılmalıdır.

- Veri akışı optimize edilmelidir. Verinin sistem içerisindeki hareket sayısının azaltılması maliyetleri azaltır ve kurumsal çevikliği artırır.

Kurumsal veri mimarisi üç farklı katmanı vardır. Bunlar:

1) Kavramsal/iş modeli: Tüm veri varlıklarını içerir ve kavramsal bir veri modeli sağlar.

2) Mantıksal/sistem modeli: Veri varlıklarının ilişkilerini tanımlar ve mantıksal bir veri modeli sağlar.

3) Fiziksel/teknoloji modeli: Veri mimarisinin, teknoloji altyapısına nasıl uygulandığını sağlar.

Veri mimarisinin geliştirilmesi, her büyüklükte işletmeye fayda sağlar. İşletmenin veri akışının belirgin olmasını sağlayarak eksiklikler ve tekrarları da ortaya çıkarır. Veri entegrasyonu ve veri kalitesinin iyileştirilmesi faaliyetlerini destekler. Etkin bir veri yönetimi ve içsel veri standartlarının geliştirilmesini sağlayarak, verilerin doğru ve tutarlı olmasına yardımcı olur. Ancak veri mimarisi, özellikle büyük ve faaliyetleri karmaşık işletmelerde veri analizi/iş zekası uygulamaları için bir gereksinimdir (Stedman, 2021).

Veri mimarisi, kurumsal mimari gibi bir belgedir. Bu belge de işletmeye özgüdür ve detayı işletmenin büyüklüğüne ve faaliyetlerinin çeşitliliğine göre değişir. Küçük işletmelerde, nispeten küçük ve basit bir veri mimari belgesi olacaktır. Veri mimarisi geliştirmekteki amaç, kullanılmayan teknolojik dokümanlar yığınına yeni bir doküman eklemek değil; işletmenin veri ihtiyaçlarını, işlediği/kullandığı/ürettiği verinin anlamını, özelliklerini, kullanım kurallarını ve veri akışını belgelemek, veriden daha fazla anlam üretmek, verinin potansiyelini daha iyi görebilmek ve bu sayede işlerin daha verimli ve etkin yapılmasını sağlamaktır. Veri mimarisi, veri modellemeden farklı olup, iş akışı ve işlenecek veri türleri arasındaki ilişkiler gibi daha makro seviyedeki görünümle ilgilidir.

Kurumsal mimari gibi veri mimarisi de iş tarafındaki/teknolojideki gelişmelere göre güncellenmelidir. Benzer şekilde kurumsal mimari gibi, işletmedeki her birim tarafından kabul görmesi ve "*kullanılması*" için, veri mimarisinin de basit, anlaşılır, teknik araç ve detaylardan arınmış olması gerekir. Birimler tarafından "*kullanılabilir*" olması için çok önemli bir nokta da verinin iş anlamının/değerinin mutlaka belirtilmesinin gerektiğidir. Teknolojik gereksinimler ve çözümler ise daha çok bilgi sistemleri birimini ilgilendirir.

Tıpkı kurumsal mimarinin geliştirilmesinde olduğu gibi, veri mimarisi geliştirilirken de işin içinde iş birimlerinin yöneticileri (desteklerini göstermek için) ve iş birimlerinin çalışanları olmalıdır. Sonuçta oluşacak belge, iş hedefleri ile uyum içinde olmalıdır.

Veri mimarisi ile ilgili detaylı bilgiye Zachman Architecture for Enterprise Framework (https://www.zachman.com/), The Open Group Architecture Framework (https://www.opengroup.org/togaf) ve Data Management Body of Knowledge (https://www.dama.org/cpages/body-of-knowledge) kaynaklarından, bunlarla sınırlı olmamakla birlikte, ulaşılabilir.

1.1.1.2.11.3. Kurumsal Mimarinin Değerlendirilmesi

Kurumsal mimarinin değerlendirme sürecinde, ilk önce kavramın bilinirliği değerlendirilmelidir. Belki de resmi olarak bu isim kullanılmıyor olabilir. Öncelikle kavramın farkındalığına, sonra da kullanılıp kullanılmadığına bakılmalıdır. Daha önce belirtildiği üzere çok küçük işletmelerde ayrıntılı bir mimari beklenmemekle birlikte, bu konunun bir şekilde gündeme gelmiş olması iyiye işarettir.

Bazı işletmelerde, aktif olarak kullanılan uygulamalar ve dolaşımda olan verinin tümüyle kayda geçirilmediği görülmektedir. Daha da önemlisi, işletmelerde kullanılmayan ancak halen aktif olan iş uygulamaları ve kullanılmayan ancak veri taşımaya devam eden kanallar da mevcut olabilir. Bunların

hepsi hem bilgi sistemleri-iş uyumuna ilişkin, hem de kaynak ve performans yönetimine ilişkin sorunların habercisidir. Ayrıca kullanılmayan ancak açık tutulan her kaynak, bilgi güvenliği için de ilave risk unsurudur.

Bilgi sistemlerinde, tıpkı ağ (network) topolojisinin çıkarılması gibi, uygulama (application) topolojisinin çıkarılması (desteklediği iş süreçleri ve kullanım amaçları ile beraber) işletmeye çok faydalı olacaktır. Veri kullanımı çok yoğun olan bir işletmede ise özellikle veri mimarisine (veri kaynakları, dışarıdan gelen veri, dışarı gönderilen veri, iş süreçlerinde veri kaynaklarının kullanımı) ilişkin hiçbir dokümantasyonun olmaması riske işaret eder.

İşletmede mimariye ilişkin bir sürecin bulunması durumunda değerlendirilmesi gereken hususlar, mimarinin nasıl ve kimler tarafından geliştirildiği (farklı birimlerden çalışanlar olmalı), mimarinin başlangıç noktasının işletme/bilgi sistemleri stratejisi olup olmadığı, mimarinin geliştirildikten sonra nasıl kullanıldığı (doğrudan iş uygulamaları/hizmetlerinin geliştirilmesinde kullanılmalı), mimarinin güncelliği ve güncelliğinin nasıl sağlandığı olmalıdır. Kurumsal mimari gereksinimleri doğrultusunda tasarlanan mimarinin bu gereksinimleri karşılayıp karşılamadığı gözden geçirilmelidir. Gözden geçirme sırasında, mimarinin potansiyel riskleri, ödünleri ve duyarlılık noktaları tespit edilerek gerekli değerlendirmeler yapılmalıdır.

1.1.1.2.12. Kontrol Ortamı

Amerika'da 5 bağımsız meslek kuruluşundan oluşan COSO (Committee of Sponsoring Organizations), iç kontrolün işletlemelerde standartlaşan bir yapıya kavuşmasına öncülük ederek COSO iç kontrol modelini geliştirmiştir. COSO modeline göre iç kontrolün birbiri ile ilişkili 5 bileşeni vardır:

1) Kontrol ortamı
2) Risk değerlendirme
3) Kontrol faaliyetleri
4) Bilgi ve iletişim
5) İzleme ve değerlendirme

Burada, kontrol ortamı ele alınacaktır.

1.1.1.2.12.1. Kavramlar

Kontrol, maruz kalınan riskleri azaltmaya yarayan her türlü süreç ve mekanizmadır. Kontrol; doğruluğu, güvenliği ve en nihayetinde amaçlara ulaşılmasını sağlar. Kontroller, sürdürülebilirlik, iyi tanımlanmış ve tekrar edilebilir süreçler ve tutarlı sonuçlar sağlar. Somutlaştırabilmek adına kontrol, her türlü politika, prosedür, talimat, kural, yazılım, donanım olabilir.

İç kontrol, bir işletmenin maruz kaldığı risklerin azaltılması, iş hedeflerinin başarılması, hataların ve hilelerin önlenmesi ve yasal düzenlemelere uyumun sağlanması için oluşturulan tüm mekanizma, politika ve prosedürlerden oluşan yapı olarak tanımlanabilir. İşletmenin iç mevzuatı gibi düşünülebilir. COSO modeli iç kontrolü, işletmelerin yönetimi ve çalışanlarından etkilenen ve hedeflerine (faaliyetlerde etkinlik ve verimlilik, finansal raporlamada güvenilirlik, mevzuata uyum) ulaşması için oluşturulmuş geniş bir yapı (süreç) olarak tanımlamıştır. İç kontrol mekanizmaları işletmenin asıl faaliyetlerinin içine yedirilmiş olup, ayrı bir sistem değildir. Finansal kontrollerin yanında yönetsel kontrolleri de kapsar. İç kontrol, işletmedeki her çalışanı etkiler, her çalışan iç kontrol sisteminin içindedir (Bursa Uludağ Üniversitesi, 2019). Bu sistemin merkezinde insan vardır.

Doğru bir şekilde oluşturulan iç kontrol sistemi, işletmenin varlıklarının korunmasının yanında, faaliyetlerde etkinlik ve verimlilik sağlayarak stratejik hedeflerin gerçekleşmesine yardımcı olur. Güçlü bir iç kontrol sistemi, işletmenin performansının kapasitesinin üst sınırlarına taşımada, sektördeki en iyi uygulamaların hayata geçirilmesinde, kaynakların etkin ve verimli bir şekilde kullanılmasında ve rakiplerine kıyasla daha iyi hizmet sunarak sürdürülebilirliğin sağlanmasında önemli katkılar sağlar. Benzer şekilde, güvenilir bir iç kontrol sistemi, denetçinin denetim faaliyetlerini kolaylaştırır, daha az denetim testini gerektirir.

Kontrol ortamı ise, işletmede üst yönetim tarafından oluşturulan kontrollere yaklaşım, bağlılık, ve kontrollerin kapsayıcılığı ile kurum kültürü, etik değerleri ve üst yönetimin bunlara desteğini gösteren

tüm mekanizmalardır. Burada bağlılık, önem ve kararlılık diye belirtilen nitelikler doğrudan üst yönetimden beklenir. Üst yönetim kontrol ortamının "*havasını*"(*tone at the top*) belirler. Kontrol ortamının oluşturulması ve sürdürülebilirliği personele değil, üst yönetime bağlıdır.

Kontrol ortamı, işletme çalışanlarının görev ve sorumluluklarını yerine getirdiği ortam olup, onların kontrol bilincini etkiler, geliştirerek ve bir düzene oturtmaya temel oluşturur. İşletmenin geçmişi, kültürü ve iş yapış şekli kontrol ortamını şekillendirir ve iç kontrol sürecinin verimli bir şekilde yürütülmesini doğrudan etkiler.

İşletmede etkin ve yeterli kontrollerin varlığı, üst yönetimin sorumluluğudur. Kontrollerin ilk sahibi yönetimdir. Kontroller, içerik olarak işletmeye özgün olmakla birlikte; faaliyet türü, sahası ve işletmenin boyutlarından bağımsız olarak her işletmede kontrol vardır, olmalıdır.

Kontrollerin belirli bir maliyeti vardır. Kontroller tasarlanırken en önemli noktalardan biri maliyetinin olası faydasını aşmasını önlemektir. Ancak, yasal mevzuattan kaynaklanan kontroller için böyle bir kriter yoktur ve bunlar uygulanması mecburi kontrollerdir. Kontroller bir kere tanımlandıktan sonra sonsuza kadar düzgün bir şekilde ve %100 etkinlikte işleyecek diye bir şey de yoktur. Periyodik gözetime ve güncellemeye gerek duyulur. Ayrıca kontrollerin tüm ilgililere uygun şekilde duyurulması ve herkesin kendi görev alanındaki kontrollerin güncel hallerine ulaşabilmesi sağlanmalıdır.

Kontrollerin her birinin bir hedefi vardır. Bilgi Sistemleri Denetim ve Kontrol Birliği'ne (ISACA) göre kontrol hedefi, bir kontrolün uygulanmasıyla amaçlanan sonuçtur. Kontroller çeşitli bakış açılarına göre sınıflandırılabilir: Yönetimsel, teknik, mantıksal, tespit edici, telafi edici, genel ve uygulama kontrolleri gibi.

Yeni bir kontrol tasarlandıktan veya mevcut bir kontrol iyileştirildikten sonra, risklerin gerçekleşme olasılığı veya yapacağı etki değişebileceğinden, risk analizi tekrarlanmalıdır.

Politika, bir işletmenin amaçlarını gerçekleştirmek için çalışırken uyması gereken ilkeler bütünüdür. Kurum kültürüne, yönetim kurulu ve üst yönetim bakış açısına doğrudan bağlıdır. Bir başka deyişle, politika, yönetimin beklentilerini, niyetini ve yönünü ifade eden üst seviye dokümandır (ISACA, 2019).

Politika doğal olarak bir kısıtlama getirir, sınırlayıcı bir dokümandır. İşletmedeki herkesten politikadaki ilkelere uyması beklenir. İşletmelerde karar alma tarzı politika ile sınırlandırılarak kayıt altına alınır. Ancak politika karar alıcıya ve uygulayıcıya bir miktar takdir yetkisi de verir. Çünkü, politikada işlere dair detay yoktur, genel çerçeve vardır. Politika işletmeye özgüdür. İşletmeden işletmeye değişir. Politika, hem işletme düzeyinde, hem de işletmenin birimleri düzeyinde hazırlanabilir. Ancak birim politikaları, aynı stratejide olduğu gibi, işletme politikaları ile sınırlıdır.

Politika karar alma süreçlerinde çalışana rehberlik sağlar. Ancak bir işletmede sadece politikaya bakarak işlerin "*nasıl*" yapılacağı anlaşılmaz. Politika ilkeleri, hareket planını belirler, bunun yardımıyla kararlar alınır. Alınan kararların nasıl uygulanacağı, diğer bir ifadeyle işlerin nasıl yapılacağı ise prosedür ile belirlenir.

Burada "*süreç*" kavramını da açıklamak gerekir. Süreç, birbiriyle ilişkili bir grup aktivitedir. Bir amacı, girdileri, çıktıları, sorumluları vardır. Bir işin adım adım tarifidir, işin gerçekleştirilmesi için alınacak aksiyonlardır. Süreçler kontrol değildir;a ama kontroller genellikle süreçlerin içine yedirilir. Örneğin, bilgi sistemleri üzerinde yetkilendirme bir "*süreç*"tir. Yetki talebine olumlu cevap vermeden önce talep sahibinin amirinden onay almak/onayı olup olmadığına bakmak ise yetkilendirme sürecinin içinde yer alan bir kontroldür. Bazen kontrol ve süreçler birbirine karıştırılabilir. Ancak genellikle şunu söyleyebiliriz: Eğer iş sürecindeki adım risk azaltıcı bir faaliyet ise bu aslında bir kontroldür.

ISACA'ya göre prosedür, belirli bir işi ilgili standart veya düzenlemelere uygun olarak gerçekleştirmek için gerekli adımların tanımlandığı bir dokümandır. Bir sürecin bir bölümü veya tümünü ifade edebilir. Prosedürleri tanımlamak genellikle süreç sahibinin işidir; ancak üst yönetim tarafından izlenir. En nihayetinde üst yönetimin sorumluluğudur; çünkü kontrol ortamının bir parçasıdır. Prosedürler, kontrol aktiviteleri olarak da tanımlanır. Çünkü her prosedür bir kontroldür. Süreçlerin yazılı hale getirilmesi diye tarif edilen durum prosedürlerin oluşturulmasıdır.

Prosedür, yönetimin kontrol işlevini gerçekleştirmesine yardımcı olur. Süreçlerin tekrar edilebilir olmasını, ölçülebilmesini ve iyileştirilebilmesini sağlar. Personele yardımcı olur, tekerleğin yeniden keşfedilmesini engeller. Prosedürler kullanıma alınmadan önce bir süre denenmelidir. Taslak prosedürü aynı işi yapan birden çok kişi (mümkünse) takip edip süreçlerin doğru ve tam olması sağlanmalıdır (bu sayede işin sadece yazılı dokümantasyonu değil, kendisi de olgunlaşır). Prosedürler periyodik güncellenmeli ve duyurulmalıdır.

Burada kontroller için anlatılanlar arasında iş veya bilgi sistemleri kontrolleri diye ayrım yapılmamıştır. Çünkü yazılanlar hepsi için geçerlidir. Sadece birimden birime kontrollerin içerikleri değişir.

Prosedürlere bağlı çalışmak, özellikle bazı alanlarda (teknoloji gibi) çok sevilmeyebilir. Çünkü prosedür inisiyatifi çalışandan alan bir yapıdır. İşleri de bir miktar uzatabilir (kalite, sürdürülebilirlik ve tutarlılık lehine). Bu durumu önlemek için bazı işletmelerde, özellikle iş sahası ve çalışan profiline de bağlı olarak prosedürlerin daha sık gözden geçirilmesi, çalışanlardan geri bildirim alınması gerekebilir.

Talimat ise, adım adım bir işin açıklanmasıdır. Prosedürden çok daha detaylı hazırlanır. Uygulama adımları net biçimde, yorumlamaya gerek kalmayacak şekilde belirlenir. Bir prosedürün içindeki bir işin talimatı olabilir. Özellikle adımları belirli; ancak çok adımlı işlerde gözden kaçan bir durum olmaması için kullanılır. Ortama, kullanılan ekipman ve sisteme çok bağımlı bir dokümandır.

Görüldüğü üzere, kontroller hakkında çok fazla tanım bulunmaktadır. Bunları ilk okuyanın aklına bir yığın doküman gelebilir. İşletmelerin büyüklüğü, personel sayısı, hukuki çerçevesi, faaliyetlerin karmaşıklığı da bu doküman yığınını artırabilir. Ancak, özellikle küçük işletmelerde sayfalarca doküman hazırlayıp bunları bir kenara atmaktansa, nispeten az, basit ama "*yaşayan*" dokümanlar hazırlamak çok önemlidir. Çünkü ne yazık ki bütün bu külliyatı hazırlayıp onaylayıp sonra tozlu bir rafa kaldıran bir çok örnek bulunmaktadır. Önemli olan, işletmenin yapısına uygun, çevik ve kullanılabilir dokümanlar hazırlamaktır. Kontrollerle ilgili detaylı bilgiye bu Çalışma Notu'nun "*Bilgi Sistemleri Denetimi*" bölümünden ulaşılabilir.

Risk yönetimi kontrol ortamının vazgeçilmez bir parçasıdır. Esasen riske cevap olarak kontroller oluşturulur. Bu sebeple bilgi sistemleri kontrolleri geliştirilmeden önce, bilgi sistemlerine ilişkin risk değerlendirmesi yapılmalıdır. Değerlemenin sonucunda belirlenen riskler, kategorileri, seviyesi, ait oldukları iş süreçleri ile geliştirilebilecek olası kontrollerin maliyeti analiz edilerek kontroller seçilmelidir.

Kontrol etkinliği (işe yararlılığı) de denetim ile ölçülür, dolayısıyla denetime tabii tutulmayan kontrollerin etkinliği bilinemez.

Kontrol ortamı ile ilgili, detaylı bilgiye Committee of Sponsoring Organizations of the Treadway Commission-COSO (https://www.coso.org) ve Control Objectives for Information and Related Technologies (COBIT) (https://www.isaca.org/resources/cobit) kaynaklarından, bu kaynaklarla sınırlı olmamak üzere, ulaşılabilir.

1.1.1.2.12.2. Kontrol Ortamının Değerlendirilmesi

Bir işletmede kontrol ortamının sağlıklı bir şekilde değerlendirilebilmesi için öncelikle bileşenleri belirlenmelidir. COSO modelinde bu bileşenler, dürüstlük ve etik değerler, yönetim felsefesi ve tarzı, yetkinliklere bağlılık, örgütsel yapı, yetki ve sorumluluk dağılım ile insan kaynakları yönetimi ve ve uygulamaları olarak tanımlanmıştır. Bu kapsamda, bu bileşenlere ilişkin faaliyet, süreç, uygulama, prosedür gibi düzenlemeler bulunup bulunmadığına bakılmalıdır. Bulunanların ise uygulanma düzeyleri belirlenmelidir. Diğer taraftan, işletmede kontrol ortamına ilişkin bir görüş oluştururken bu konuda işletmedeki farkındalık ve bileşenlere aşinalık değerlendirilmelidir. Bundan sonra işletmede kontrol unsurlarının nasıl bir süreçle geliştirildiği incelenmelidir. Her seviyedeki kontrolün geliştirilmesi, onaylanması, duyurulması, gözden geçirilmesi ve gözden geçirme periyodunun tanımlanmış olup olmadığına bakılmalıdır. İşletme ve bilgi sistemleri genelindeki kontroller incelenip yukarıda belirtilen sürecin işletilip işletilmediği kanıtlarıyla beraber değerlendirilmelidir.

İşletme politikaları sadece işletmenin kendisini değil, üçüncü tarafları da etkiler. Özellikle güvenlik, kişisel verileri koruma gibi bazı özel politikaların üçüncü taraflara da duyurulması ve bu

taraflarca bunlara uyumun takip edilmesi/garanti altına alınması için çeşitli mekanizmaların işletiliyor olması gerekir. Doğal olarak, bir de üçüncü tarafların işletmeyi etkileyen politikaları olabilir, bunlara da uyuluyor ve güncelliği takip ediliyor olmalıdır.

Burada işletme ve üçüncü taraflar olarak belirtilen kavram, yeri geldiğinde bilgi sistemleri-iş birimleri olarak okunmalı ve bilgi sistemleri kontrollerinin değerlendirilmesi bu şekilde ele alınmalıdır. Bilgi sistemleri açısından değerlendirildiğinde, hiçbir kontrolün mevcut olmadığı bir durum kesinlikle riske işaret eder. Ancak sayıca çok fazla, içerik olarak çok yoğun, hiyerarşisi bozuk bir kontrol yığını da akla başka bir riski getirmelidir: Uyum için yazılmış ancak kullanılmayan kontroller. Bilgi sistemleri kontrolleri değerlendirilirken bu durum mutlaka akılda tutulmalı, kontrollerin bilinirliği, güncelliği ve sahadaki karşılığı değerlendirilmelidir.

1.1.2. Bilgi Sistemleri Yönetiminin Unsurları

1.1.2.1. Yönetim Kavramı

Yönetim kelimesi idare ve sevk anlamında kullanılmaktadır. Literatürde çok farklı tanımları olmakla birlikte, yönetim, bir grup insanı bir araya getirip belirli hedef ve amaçlar doğrultusunda, eldeki kısıtlı kaynakları etkin ve verimli kullanarak çalıştırmaktır (LumenLearning, 2021). Bir başka ifadeyle yönetim, başkaları aracılığı ile iş yapmaktır. Toplumlara bakılırsa, her alan ve kademede işlerin aslında birlikte yapıldığı görülmektedir. Toplumdaki her bireyin, her bir ihtiyacını tamamen tek başına, sadece kendi gücüyle sağlaması imkansıza yakındır. Dolayısıyla toplumun her alanında birden çok kişi bir araya gelerek bir iş/ürün/hizmet üretmektedir. Birden çok insanın bir araya gelerek iş yapması ise kişiler arası planlama, iş bölümü, organizasyon ve kontrol süreçlerini beraberinde getirmekte; böylece yönetim kavramı anlam kazanmış olmaktadır. Tanım kurumsal açıdan ele alınırsa, yönetim; işletmenin hedeflerini çeşitli kaynakların kullanımı aracılığı ile gerçekleştirmektir.

Buradan anlaşılacağı üzere, yönetim hem kişilerin hem de kaynakların yönetimini içerir ve tek bir süreç/fonksiyon olarak görülemez. Yönetim, en dar çerçevede; planlama, örgütleme, yönlendirme ve kontrol süreçlerini içerir. Bu süreçlere de yönetim fonksiyonları adı verilir. Yöneticinin işi, yönetim fonksiyonlarını gerçekleştirmektir.

Buraya kadar az çok anlaşıldığı üzere yönetim denince akla;

- Ortak bir amaç,
- Yönetilecek bir grup insan,
- İnsan dışındaki diğer kaynaklar

gelmelidir.

Yönetim fonksiyonu bu üç bileşeni öyle bir şekilde bir araya getirmelidir ki, çıktı olarak ortak amaç üretilsin/amaca erişilsin, bununla da kalmayıp bu amaç minimum kaynakla (işgücü ve diğer kaynaklar) ve sürdürülebilir şekilde elde edilsin.

1.1.2.2. Yönetim Fonksiyonları

Yönetim, bir önceki başlıkta başkaları aracılığı ile iş görme olarak tanımlanmıştı. Ancak bu tanım, yöneticinin hiçbir iş görmeyeceği, tüm işleri başkalarına yaptıracağı anlamına gelmemektedir. Yöneticinin de bir takım işleri vardır; ancak bunlar genelde alandan bağımsız, tüm yöneticiler için ortak olan işlerdir. İşte yönetim fonksiyonları diye tabir edilen olgular aslında yöneticinin işidir. Yönetici, yönetim ile hedeflenen amaca ulaşılabilmek için yönetim fonksiyonlarını icra etmek durumundadır.

Yönetilen birim ister işletmenin tamamı, isterse işletmenin bir birimi olsun, birime bir takım girdiler girer ve çıktı olarak da o işletmenin veya birimin hedefi/amacı gerçekleşir/ortaya çıkar. Yönetim; iş gücü, finansal, teknik, idari gibi kaynaklar üzerinde bir takım dönüştürücü faaliyetler sonrasında birimin amacını gerçekleştirir. Yönetim fonksiyonları denildiğinde akla bu resim gelmelidir (Paşaoğlu, Tokgöz, Şakar, Ergun Özler, Özalp, 2013).

Yönetim fonksiyonları genelde dört gruba ayrılır:

Planlama: Yönetimin ilk fonksiyonudur. Yönetim faaliyeti, planlama ile başlar. Amaca ulaşmak için yapılması gereken aksiyonların tanımlanmasıdır. Ne yapılacak, ne zaman yapılacak, nasıl yapılacak, niçin yapılacak ve kim yapacak? Tüm bu soruların cevapları bu aşamada verilir. Tabii burada aksiyonlara/hareket tarzına karar verirken tüm seçeneklerin masaya yatırılması ve çeşitli kriterlere göre en iyisine karar verilmesi gerekir. Burada kriterlerden kasıt, işletmenin içinde bulunduğu ortam, iç ve dış koşullar, hukuksal çerçeve, sahip olduğu kaynaklar, iş gücü, zaman kısıtları gibi unsurlardır ve planlama aşaması tüm bu unsurların bir potada eritilmesi aşamasıdır.

Planlama, kişiyi geleceği tahmin etmeye zorlar, böylece geleceğin bilinmezliğinin getirdiği belirsizliği azaltmaya yardımcı olur. Planlama, işletmeyi ilgilendiren geleceğe yönelik alternatif hareket biçimleri arasından seçim yapmaktır. Önceden/önden karar verme işlemidir. Amaçlara ulaşmak için ne yapılması gerektiği, bunun ne zaman ve hangi kaynaklarla yapılması gerektiğinin ortaya çıkarılmasıdır. Eylem planının belirlenmesidir.

Önünde üst yönetim tarafından belirlenen hedefler olan yönetici, işe önce bu amaçların başarılması için gereken görevleri/işleri planlayarak başlamalıdır. Neyi, kimin, kimle, ne zaman ve hangi kaynaklarla yapacağı bu aşamada belirlenir.

Planlamanın türü, planın yapıldığı yöneticinin işletmedeki seviyesine/kademesine göre değişir. Üst yönetim stratejik, orta kademe taktik, alt kademe ise operasyonel planlama yapar.

Örgütleme: Planlama fonksiyonunun ardından örgütlenme gelir. Belirlenen planların bir bağlama oturtulması, işler için sorumlulukların ve yetkilerin atanması, görev tanımları, kişiler arası ilişkilerin tesisi, organizasyon yapısının belirlenmesi, alt grupların/takımların oluşturulması ve mekan ve kaynakların hazırlanması örgütlemenin aşamalarını oluşturur. Burada çalışanlar arasındaki iletişimin nasıl olacağı, kimin neyi kime ileteceği, çalışanların yapacakları işe göre gruplara ayrılması, kaynakların ve mekanın kullanılma şartları belirlenir. Kısacası örgütlenme, işletmenin amaçlarını gerçekleştirmek için insan ve diğer kaynakların bir araya getirilmesi, düzene sokulması işidir.

Yöneltme (yürütme): İşletmede işlerin planlanması ve gerekli organizasyonun yapılması, işlerin gerektiği gibi yürümesi için yeterli değildir. Planlama ve örgütleme işlevinden sonra yöneltme fonksiyonu devreye girer. Aslında bu fonksiyon, işlerin kendisinden ziyade çalışanlarla doğru bir iletişimin kurulması, işyerinde iletişim mekanizmalarının tesisi, çalışanların motive edilmesi, pozitif ve barışçıl bir çalışma ortamı oluşturulması, çatışmaların çözümlenmesi ve işlerin yolunda gitmesiyle ilgilidir. Yöneticiler liderlik vasıflarını da en çok bu aşamada gösterirler. Yönetim hem bir bilim, hem de sanatsa, sanat kısmı burasıdır. Motivasyon, sorun çözme, liderlik, iletişim, kültür… Planlama ve örgütleme aşamasında işler sadece kağıt üzerinde gibi görünür. İşte yürütme fonksiyonu, bu yapıya bir hareket kazandırma ve bunu sürekli kılma aşamasıdır. Makinenin çalışmaya başlaması ve çalışır tutulması gibi. Bu fonksiyonun amacı, planlanan ve yapı olarak örgütlenen işlerin gerçekten yapılma aşamasıdır. Bu aşamada çıktıların oluşması beklenir. Emir-komuta zinciri de yürütmenin konusudur. İşlerin doğru ve verimli bir şekilde yapılması, çalışanların görev ve sorumluluklarının bilincinde olması ve emir verme sisteminin doğru işlemesine bağlıdır. Etkin bir yöneltme sisteminin kurulması için;

- Takım ruhunu gerçekleştirme,
- Çalışanları iyi tanıma,
- Görev ve sorumlulukarı ehil olan çalışanlara verme,
- Yönetici olarak örnek olma,
- Çalışanlar ile iyi ilişkiler kurma,
- Çalışanlar ile iyi iletişim kurma,
- Çalışanları sürekli gözetim altında tutma,
- İşletme içerisinde iyi bir raporlama (sözlü veya yazılı) alt yapısı oluşturma,

şartları sağlamak gerekir.

Denetim: Son fonksiyon denetim, kontrol olarak adlandırılır. Planlanan işler yapıldı mı? Amaçlara ulaşıldı mı? Aksayan yer neresi? Kaynaklar yeterli oldu mu? İşler zamanında bitti mi? Bu gibi

soruların karşılığı denetim fonksiyonu ile ortaya çıkacaktır. Daha önce belirlenmiş kriterler ile fiili durum karşılaştırılır ve ortaya çıkan sapmalar karşılaştırılır. Sapmalar belirlendikten sonra düzeltici tedbirler alınır. Her alanda olduğu gibi yönetimde de ölçme yapmadan iyileştirme yapılamaz. Bu nedenle, bu aşamada, yönetim içim ölçüm yaklaşımlarının, metriklerin belirlenmiş olması gerekir.

Denetimin evreleri arasında:

- Denetime konu hususlarda standartların belirlenmesi,

- Mevcut fiili durumun tespit edilmesi,

- Mevcut durum ile standartların karşılaştırılması,

- Sapmaların tespit edilmesi ve yorumlanması,

- Sapmalara yönelik düzeltici tedbirlerin belirlenmesi

sayılabilir.

Yukarıda sayılan bu dört yönetim fonksiyonu devamlı birbirini takip eder. Yönetim fonksiyonları hem doğrusal, hem de karşılıklı birbirini besler. Fonksiyonların işletiminde bir miktar esneklik olmalı ki işletmenin değişen koşullara uyum yeteneği olsun. Örneğin planlar revize edilebilir, organizasyon değişebilir (LumenLearning, 2021).

1.1.2.3. Yönetimsel Roller ve Yetkinlikler

Yönetici, ortak bir amaç için bir araya gelmiş farklı uzmanlıklardaki kişilerin yönlendirilmesi ve idaresinden sorumlu kişidir. Yöneticinin başarması gerekenler temelde:

- Ortak amaca istenen şekilde/belirlenen niteliklere uygun bir şekilde ulaşmak,

- Ortak amaç için kaynakları organize etmek,

- Kaynak kullanımını optimum düzeyde tutmak.

Kaynaklar sonsuz olduğunda ortak amacı gerçekleştirmek çok kolay olabilirken: kaynaklar sınırlandığında (gerçek hayatta) ortaya birçok çatışma çıkması kaçınılmaz olacaktır.

Yöneticinin Rolleri

Birden çok insanı belli bir amaç etrafında toplamak, birtakım yetkinliklere/becerilere sahip olmayı gerektirir. Ortak bir amacın olması her zaman grubun ahenk içinde, etkin ve verimli çalışmasını garanti etmez. İşte burada yönetimsel yetkinlikler devreye girer. Bir yöneticinin sahip olması gereken özellikler farklı şekillerde kategorize edilebilir. Yöneticinin karakter özellikleri, entelektüel özellikleri, sosyal özellikleri gibi. Yöneticilerin belirli özelliklere sahip olmasının yanında bazı yeteneklere de belirli ölçüde sahip olması gerekir. Bunlar bulunulan yönetim düzeyine göre değişmekle birlikte, temel olarak teknik yetenek, iletişim yeteneği, beşeri ilişkiler yeteneği, kavramsal yetenek, analitik yetenek ve karar verme yeteneği sayılabilir.

Yöneticilik rolü aslında şemsiye bir kavramdır. Yöneticilik tekil bir rol olmayıp, tek bir tanımı da yoktur. Yönetim fonksiyonlarından anlaşıldığı üzere, yöneticinin bu sayılan fonksiyonları yerine getirebilmesi için işletmede oynaması gereken birden çok rol vardır (yöneticinin şapkaları). Rol, bir dizi birbiriyle bağlantılı, organize davranış olarak tanımlanabilir. Bu konuda en çok kabul gören tezlerden biri bir yönetim düşünürü olan Henry Mintzberg'in yaptığı çalışmaların sonucunda ortaya çıkmıştır. Mintzberg'e göre yöneticinin oynaması gereken on değişik rol vardır ve bunlar üç kategoride incelenebilir:

1. Kişiler Arası (Interpersonal) Roller

Kişiler arası ilişkilerle ilgili roller bu grupta toplanır. Bu roller işletmede çalışanların diğer taraflar arasındaki ilişkiyi düzenler. Bu ilişkilerde kural veya yaptırım bulunmamakta olup, yöneticinin kendi gayret ve kişiliğiyle kurulur.

1.1. Temsil (Figurehead): Yöneticinin organizasyonunu ve takımını temsil rolü vardır. Kendi takımını (birimini, bölümünü) dışarıya ve üst yönetime karşı temsil eder. Üst yönetimi de takımına karşı temsil eder.

1.2. Liderlik (Leader): Yöneticilerin çalışanlarıyla olan ilişkisinin niteliğini en çok etkileyen/belirleyen rol budur. Yönetici organizasyonu ve takımı için bir liderdir. Çalışanları motive eder, bir takım ruhu yaratır, işyerinin ruh halini belirler. Hedeflerin başarılması için çalışanları harekete geçirir. İnsanlarda bir işi başarmak için şevk yaratmak liderin görevidir.

1.3. İrtibat (Liaison): Yöneticinin organizasyonu dışında kişi/gruplarla iletişimde olmasıdır. Günümüzün yaygın tabiriyle "*yöneticinin network*"ü olmalıdır. Geniş bir irtibat ağı, organizasyona fayda sağlar.

2. Bilgilendirici (Informational) Roller

Bilgi akışını sağlayan roller bu gruba girer. Yönetcinin işletmedeki işlerde yeterli bilgiye sahip olmasını gerektirir. Bu sayede işletmenin faaliyetlerini hedefleri çerçevesinde gerçekleştirmesini sağlar ve karşılaştığı sorunlara çözümler üretebilir. Yöneticinin sadece bilgili olması değil, bilgiyi toplama, işleme ve kullanma yeteneğinin olması gerekir.**Gözetim (Monitor)**: Yönetici bu rolü ile birimde/işletmede işlerin gidişatı hakkında bilgi toplar.

2.2. Dağıtım (Disseminator): İşletme içinden ve dışından faydalı bilgileri çalışanlara yayar.

2.3. Sözcülük (Spokesperson): Birim/işletme hakkında açıklama yapar, bilgi verir.

3. Karar Verici (Decisional) Roller

Karar alma ile ilgili roller bu gruba girer. Yöneticinin temel görevinin karar verme olması nedeniyle kurulan ilişkiler ve edinilen bilgiler, bu rolün sağlıklı biçimde yerine getirmesine yöneliktir.

3.1. Girişimcilik (Entrepreneur): Yeni fikirlerin geliştirilmesi ve yerleştirilmesi, yeni ürün ve/veya hizmet geliştirme. Yeni teknolojilerin adaptasyonu. Yöneticinin işinin bir yarısı günümüzse, bir yarısı da gelecekle ilgilidir. Girişimcilik rolü, organizasyonun yerinde saymasını/sadece günlük işlere odaklanılmasını engeller.

3.2. Sorun Çözme (Disturbance Handler): Kriz, sorun çözme. Takımdaki çatışmaların çözümü.

3.3. Kaynak Dağıtıcı (Resource Allocator): Sınırlı kaynakların paylaştırılması, önceliklerin belirlenmesi. Görevlerin icrası için gereken kaynakların minimum maliyetle ve doğru zamanda sağlanması.

3.4. Arabulucu (Negotiator): Yöneticinin takımı lehinde pazarlık yapması. İstekler sonsuz ancak kaynaklar sonlu olduğunda yöneticinin hem takım içinde, hem işletme içinde arabulucu rolü devreye girecektir.

Yönetim kademeleri ise aşağıdaki şekilde bir sınıflandırmaya tabi tutulabilir.

Üst Yönetim: İşletmenin tümünü etkileyen kararlar alan, işletmenin uzun dönemli başarısından sorumlu olan/bu konuda hesap veren, özellikle dış etkenleri izleyen (hissedarlar, ekonomi, hukuk, kamu, devlet, tüketici, müşteri) ve işletme/bilgi sistemleri stratejilerini belirleyen yöneticiler. Üst yönetimin çalışmaları tüm işletme düzeyiyle ilgili olup, hedeflerin en iyi şekilde gerçekleştirilmesine yöneliktir. Yönetim kurulu, genel müdür ve genel müdür yardımcıları üst yönetimi oluşturur.

Orta Kademe: Birim/bölüm yöneticileri. Görevleri, stratejik planları sorumlu olduğu birimin aksiyonlarına çevirip bunların gerçekleşmesini sağlamaktır. Orta kademe, üst yönetim tarafından belirlenen hedeflere ulaşmak için gerekli faaliyetlerin koordinasyonundan sorumlu olarak görevler icra eder ve üst yönetime raporlama yapar.

Alt Kademe: Günlük operasyonların yürütülmesiden sorumludurlar. Çalışanlarla doğrudan ilişki içinde olup sahada ortaya çıkan problemleri ilk gören yöneticilerdir. İşlerin yapılmasından, orta kademe tarafından belirlenen hedeflere ulaşılmasından doğrudan sorumludur. Sahadaki tüm

aksaklıklardan haberdar olmalı, gerekli önlemleri almalı ve periyodik olarak orta kademeyi bilgilendirmelidir. Alt kademe yöneticinin görevi neredeyse tamamen sahayla ilgili iç işlerdir.

1.1.2.4. Bilgi Sistemleri Organizasyonu, Roller ve Sorumluluklar

İşletmede bilgi sistemleri biriminin temel fonksiyonu (işlevi), işletmenin amaçlarını gerçekleştirmesi için bilgi teknolojisi tabanlı hizmetleri -çözümleri- sunmak ve bu yapıyı çalışır durumda tutmaktır. Daha önce belirtildiği gibi nihai amaç iş hedeflerinin gerçekleştirilmesidir.

Bilgi teknolojileri kullanılmadan önce, bilgiler elle işlendiğinden dolayı bilgiye erişim sınırlı ve bilgi akışı oldukça yavaştı. Bilgi teknolojilerinin gelişmesi ile birlikte bilgi işleme kapasitesi ve hızı artmıştır. Bilgi sistemleri birimleri, teknolojik sistemlerin başlangıcından itibaren işletmelerde bugün olduğu yerde bulunmuyor. Bilgi teknolojilerinin tarihçesine ve işletmelerde oynadığı role bakılırsa, zaman geçtikçe bilgi sistemlerinin işletmeler içinde müstakil bir birim olarak görülmeye ve yöneticilerine de daha fazla sorumluluk atanmaya başlandığı görülür. Bu değişim doğrudan bilgi sistemlerinin yarattığı değer ile ilgilidir. Bir fonksiyon işe ne kadar çok değer katarsa, işletme için o kadar önemli görülür.

Günümüzde bilgi teknolojisi çözümleri ile elektronik posta ve internet erişiminden çok daha fazlası kastedilmektedir. Çünkü bilgi sistemleri artık sadece bunlardan ibaret değildir. Hatta verilen bu iki örnek özelinde konuşulursa, bu hizmetler için bilgi sistemleri birimine ihtiyaç bile yoktur.

Teknolojinin gelişimi ve işletmenin faaliyet gösterdiği sektöre bağlı olarak, bilgi sistemleri yönetiminin "*destek noktası*" konumundan "*stratejik birim/ortak*" konumuna geçmesi beklenmektedir. Bu konumdaki bir birimden sadece işe destek olması değil, bizzat yeni iş modelleri ve çözümleri geliştirmesi beklenir.

İşletmede bilgi sistemleri organizasyonu, daha önce çokça ifade edildiği gibi, iş hedeflerine ulaşılmasına katkıda bulunmaktadır. Geçmişte genellikle idari işler veya finans gibi birimlerin altında yer alan bilgi sistemleri, özellikle büyük işletmelerde ve sermaye piyasası kurumlarında iş fonksiyonlarının gerçekleştirilmesinde doğrudan rol aldığı için kendi başına bir birim olarak işletmede yer edinmektedir.

Bilgi sistemleri biriminin organizasyonu için verilecek iki büyük karar vardır: İşletmenin içinde nasıl yerleştirilecek, kendi içinde nasıl düzenlenecek?

İdeal olarak bilgi sistemlerinin fonksiyonlarını belirlemeden önce, işletmenin stratejisi ve devamında bilgi sistemlerinin stratejisi belirlenmelidir. Böylece bilgi sistemleri birimi bunlara göre tasarlanıp, bilgi sistemleri-iş uyumu hususunda ilk aşama düzgün kurulur. İşletmede zaten bilgi sistemleri birimi varsa (müstakil veya başka bir birimin altında), ama strateji geliştirme pratikleri işletmede yeni başladıysa ne yapılacak? Bu durum, bilgi sistemleri organizasyonunun gözden geçirilmesi ve stratejiye dayalı olarak düzenlenmesi için bir fırsat olabilir.

İşletmenin ve bilgi sistemlerinin stratejisi çerçevesinde, bilgi sistemleri biriminin fonksiyonları belirlenmelidir. Bu kapsamda bilgi sistemleri, stratejisini gerçekleştirebilmek için hangi fonksiyonlara ihtiyaç duyuyor ve devamında bu fonksiyonların hangilerini kendi yapacak? Hangilerini dış kaynak yoluyla temin edecektir? Bu soruların cevabını bulmak gerekecektir.

1.1.2.4.1. Bilgi Sistemleri Fonksiyonları

Bilgi sistemleri birimi, işletmede donanımlardan başlayıp en soyut düzeyde tüm bilgi teknolojisi işlerinden sorumludur. İşletmenin yapısına, çalıştığı sektöre, faaliyetlerin çeşitliliğine, büyüklüğüne ve almak istediği risk iştahına göre bilgi sistemleri birimlerinin organizasyonu dallanıp budaklanır.

Bilgi sistemleri fonksiyonları, isimlendirme şekilleri, sınırları ve birbirleriyle ilişki biçimleri işletmeden işletmeye değişebilse de genelde tüm işletmelerde görülebilecek fonksiyonlar birbirine benzerdir. Bilgi sistemlerinin beş temel fonksiyonu aşağıdaki şekilde sınıflandırılabilir:

- Altyapı yönetimi,

- Yazılım/Sistem geliştirme,

- Güvenlik,

- Veri,

- Destek hizmetleri.

Bu beş fonksiyonun ayrı ayrı birbirleriyle ilişkisi vardır. Örneğin güvenlik-geliştirme (güvenli geliştirme) veya güvenlik-veri (verinin yaşam döngüsünde güvenliğini sağlama) gibi. Biraz daha detaylı bir sınıflandırma ise aşağıdaki şekilde olabilir:

1) Bilgi Sistemleri Yönetimi

- Bilgi sistemleri biriminin yönetim fonksiyonlarının icra edildiği yerdir.

- Bilgi sistemleri stratejisinin hazırlanmasında rol alınması, eylemlerin, başarı göstergelerinin ve metriklerin belirlenmesi, stratejinin gerçekleştirilmesine yönelik planların ve çözümlerin hayata geçirilmesi, ölçümlerin yapılması ve üst yönetim ve diğer iş birimleriyle iletişim hep bu yapılanma tarafından yerine getirilmektedir.

2) Kurumsal Mimari

- Kurumsal mimari fonksiyonu bilgi sistemleri altında bir alt birim olarak düşünülebileceği gibi, kurumsal düzeyde bir ekip olarak da düşünülebilir. Özellikle küçük işletmelerde böyle bir yapılanma görülmez; ancak büyük işletmelerde görülmesi beklenir.

- Kurumsal mimari doğası gereği bir ekip işidir. Çünkü burada amaç işletme stratejisinin, hedeflerinin, iş süreçlerinin, veri ve bilgi gereksinimlerinin teknolojik çözümlerle ve hizmetlerle hayata geçirilmesini sağlamaktır. Bu yüzden kurumsal mimariyle ilgilenen ekipte sadece bilgi sistemleri birimi çalışanlarının değil, işletmedeki tüm birimlerden çalışanların bulunması gerekir. Ama özellikle küçük ve orta ölçekli işletmelerde bu konuda tam zamanlı çalışan müstakil bir birim beklemek pek gerçekçi olmayabilir. Bunun yerine bilgi sistemleri ve iş tarafının ilgili çalışanlarının bir proje yapılanması gibi diğer görevlerinin yanı sıra, bu iş için çeşitli zamanlarda bir araya gelip çalışmaları, kurumsal mimari konusunun hiç ele alınmamasına nazaran çok daha etkili bir çözümdür.

3) Yardım Masası

- İşletmenin büyüklüğüne göre kişi veya birim şeklinde oluşturulur.

- Her türlü bilgi sistemleri (yazılım/donanım) sorunları için son kullanıcıya destek hizmeti sunulur.

- Gerektiğinde problemlerin uygun birimlere (geliştirme, altyapı) sevk edilmesi sağlanır.

4) Sistem ve Ağ Yönetimi

- Sunucu sistemlerin kurulması, yapılandırılması ve çalışır halde tutulmasını sağlar.

- Ağ kurulumu, yapılandırılması ve çalışır halde tutulmasını sağlar.

- Kullanıcıya yönelik hizmetlerin sağlanması için sunucu sistemlerinin yapılandırılmasını ve gözetimini (uygulamaların çalışır halde tutulması, elektronik posta hizmeti, yedekleme hizmeti, dosya saklama/yazdırma hizmetleri gibi) sağlar.

- İş/Felaket kurtarma planları hazırlar.

5) Uygulama Hizmetleri

- Gerek son kullanıcılar, gerekse de bizzat bilgi sistemleri personeli tarafından kullanılacak her türlü uygulamanın edinilmesi veya geliştirilmesini temin eder.

- Uygulamalar işletme bünyesinde geliştirilebileceği gibi dış kaynak kullanımı yöntemiyle de tedarik edilebilir.

- Uygulamalara yönelik tüm hata ve talepleri cevaplandırır. Bazı büyük işletmelerde uygulama geliştirme ile uygulama bakımı (hata ve yeni talep) fonksiyonları birbirinden ayrı ekiplere verilmiş olabilir.

6) Güvenlik

- Günümüzde bilgi sistemleri birimlerinde, ister diğer fonksiyonların altında, ister ayrı bir fonksiyon olarak (özellikle büyük işletmelerde) oluşturulmuş olsun, bilgi sistemleri ile ilgili tehdit ve riskler ele alan güvenlik fonksiyonu yer almaktadır. Güvenlik birimi çok küçük işletmelerde öncelikli olarak sistem/ağ/altyapı birimlerinin altında bulunurken, işletme ve bilgi sistemleri birimi büyüdükçe diğer fonksiyonel birimlerin (uygulama gibi) altında da güvenlik sorumluları bulunur veya bu birimlerin çalışanları bilgi güvenliği sorumlusu şapkalarını da takarlar. Büyük işletmelerde ise güvenlik yönetiminin genellikle ayrı bir birim olduğu görülür. Çünkü kendi içinde de birçok farklı rol barındırması gerekecektir.

7) Veri Yönetimi

- Verilerin güvenli, verimli ve uygun maliyetle toplanmasını ve saklanmasını sağlar.

- Veri tabanı yönetim sistemlerini oluşturup yönetir.

- Verilerin işletme politika ve tabi düzenlemeleri kapsamında kullanımını optimize eder.

- İşletmeler arası veri alış verişini sağlar.

- Veri mimarisi/yönetimi/yönetişimini sağlar.

- Veri analizi ve veri bilimi işlevlerini yürütür.

8) Uyum

- İşletme büyüdükçe ve sektörüne göre uyulacak düzenleme/standart sayısı da arttıkça, bilgi sistemleri içinde ayrı bir uyum yapılandırılması ihtiyacı ortaya çıkar.

- İşletme çok büyük olmadıkça uyum biriminin bilgi sistemleri altında ayrı bir yapılanma olması beklenmez. Genellikle diğer görevlerinin yanı sıra bu işle de görevlendirilen personel vardır.

- Uyumla görevli kişiler güvenlik birimlerinin altında görev alabilirler.

- Bu kişilerin özellikle işletmenin iç kontrol/uyum birimleriyle koordineli çalıştıklarını görülür.

- Ülkemizde çeşitli sektörlerde ikincil düzenlemeler seviyesinde zorunlu tutulan Kurumsal Siber Olaylara Müdahale Ekipleri (Kurumsal SOME) ya uyum ya da güvenlik birimlerinde (veya iki fonksiyonun da yer aldığı birimde) yer alan personelden oluşmaktadır. Bu durum işletmeye göre değişebilmekle birlikte, bilgi sistemleri dışında özellikle hukuk birimlerinden çalışanlar da SOME ekiplerinde görev alabilir.

- Dış kaynak yönetimi/tedarikçi yönetiminde görev alabilir.

- Birimde dış kaynak kullanımı (ileride detaylı anlatılacak) varsa, gözetimi ve yönetimiyle ilgili mutlaka personel bulunmalıdır. Küçük işletmelerde diğer görevlerin yanında bununla da görevlendirilmiş kişiler olabilir.

- Tam olarak dış kaynak kullanımı olmayan ancak satın alma yoluyla edinilen ürün/hizmetlerde gözetim ve yönetim fonksiyonlarının icrası gerekir.

Bu sınıflandırma listeleri değişebilir, adlandırmalar ve fonksiyonlar farklılık gösterebilir, bazı fonksiyonlar aynı başlık altında yer alabilir veya daha detaylı organizasyonlar oluşturabilir.

İşletmelerin bilgi sistemleri birimleri planlanırken, çalışılan sektör, işletmenin büyüklüğü ve iş fonksiyonları dikkate alınmalıdır. Özellikle personel sayısı az olan küçük işletmelerde birçok bilgi sistemleri fonksiyonu birleştirilip tek bir adla anılabilir ve burada personel olarak bir veya birkaç kişi istihdam edilebilir. İşletme büyüdükçe hem ayrı bir bilgi sistemleri birimine ihtiyaç oluşur; hem de istihdam edilecek bilgi sistemleri personel sayısı artar. Büyük işletmelerde bilgi sistemleri birimleri genelde üst yönetim seviyesinde yapılandırılır (C level). Daha küçük işletmelerde ise genelde direktörlük veya müdürlük seviyesinde olur ve özellikle çok küçük işletmelerde operasyon birimlerine bağlı olabilir. Ancak, sonuçta yukarıda sayılan işlerin ya işletmenin kendi personeli tarafından ya da dışarıdan hizmet temini yoluyla bir şekilde yerine getirilmesi gerekmektedir. Bu işler sayesinde işletme, faaliyetlerine yönelik olarak bilgi sistemlerinden gerekli desteği ve katkıyı görür.

Yukarıda kısaca tanımlarına yer verilen bilgi sistemleri fonksiyonları, işletmenin büyüklüğüne göre en az birkaç kişiden başlamak üzere teknik formasyonlu personel tarafından yürütülür. Sistem analisti, geliştirici, test mühendisi, ağ mühendisi, teknisyen… Unvanlar işletmelere göre değişmekle birlikte, belirli bir görevi kaç kişinin yerine getireceği işletmenin büyüklüğüne, bütçesine, işin kritikliğine, mevcut iş gücünün yetkinliğine ve performansına bağlıdır. Diğer taraftan, burada çok önemli bir ölçüt kritik görevlerin bir kişiye bağlı kalmasını engellemektir. Bu durum görevler ayrılığının bir gereğidir ve bu kavram bir sonraki başlıkta detaylı olarak ele alınacaktır.

Rollerle ilgili önemli husus, her rolün/görevin resmi, yazılı bir tanımının olması (üst yönetim/yönetim kurulu tarafından onaylı) ve herkesin kendi görevini bilmesinin sağlanmasıdır. Uygulama geliştirici veya sistem mühendisi ne yapacağını elbette bilir şeklinde bir yaklaşım, hem çalışanlar arasında hem de çalışan-yönetici arasında çatışmalara yol açabilir. Her çalışan kendinden bekleneni tam olarak anlamalı, gerektiğinde bununla ilgili bilgiye rahatça ulaşmalı ve görev tanımında yapılan her tür değişikliği de gecikmeden öğrenmelidir. Görev tanımları yazılı ve onaylı olduğu gibi, aynı zamanda çalışanların kime raporlama yapacağı ve kime karşı sorumlu oldukları da açıkça belirli olmalıdır. Tüm bunları sağlamak ise bizzat yönetimin sorumluluğundadır.

1.1.2.4.2. Görevler Ayrılığı

Görevler ayrılığı kavramı, hem muhasebe, hem denetim hem de bir bilgi teknolojileri terimidir. İngilizcesi "s*egregation of duties*" olup, bazı yerlerde "*seperation of duties*" olarak da geçmekte ve kısaca "*SoD*" olarak adlandırılmaktadır.

İşletmelerin kaynakları kısıtlıdır. İnsan kaynağı da bu kısıtlı kaynaklardan biridir. Kısıtlı iş gücü kaynağıyla işlerin yapılabilmesinin bir yolu görevleri birleştirerek, bir kişinin birden çok rolü üstlenmesidir. Bunu birçok bilgi sistemleri görevlerinde görmek mümkündür. Ancak yapılan işin çeşitli niteliklerinden dolayı, bazı görevlerin/işlerin sağlayacağı olası maddi kazançlara karşın; aynı kişide birleştirilmemesi gerekir. Çünkü öyle görevler vardır ki, birleştirilmesi iş gücü tasarrufu yaparken diğer yandan daha maliyetli bir riskin ortaya çıkmasına sebep olabilir. Bu risk hata, ihmal veya suistimal riskidir. Bu riskleri bertaraf edebilmek için de görevler ayrılığı, bir kontrol olarak tasarlanır.

Günümüzün digital dünyasında iş hedeflerine ulaşmak isteyen işletmeler, iş süreçlerinin değişen koşullara uymasını sağlamak, sürdürülebilir başarı için görevler ayrılığı ilkesini benimseyerek güncel sistemlerini kendi yapısına entegre etmesi gerekir. İç kontrol sisteminin temel unsurlarından biri olan görevler ayrılığı ilkesi, basit bir tanımla, bir işi başlatan, gerçekleştiren ve onaylayan kişilerin farklı olmasıdır veya önemli görev ve sorumlulukların, hata, ihmal ve suistimalleri önlemek amacıyla farklı çalışanlar arasında paylaştırılmasıdır. Böylelikle önemli görevlerin tüm aşamalarının sadece bir kişiye bağlı kalması engellenir (Yost, t.y.). Hiçbir çalışanın bir işlemin başından tamamlanmasına kadar geçen süreçte, birden fazla kritik sorumluluk almamasını sağlar. Ayrıca bu ilke, yetki yönetimi ve yetkilerin paylaştırılmasını hedefler.

Görevler ayrılığı ilkesi, bilgi sistemleri fonksiyonlarının sadece bir veya ikisine ait olmadığı için belli bir konunun altına alınmamıştır (yazılım veya operasyon gibi). Görevler ayrılığı ilkesi, bilgi sistemleri birimlerinde birçok alanda gözlenebilir. Örneğin yazılım geliştiricilerin üretim ortamına erişiminin olmaması, yazılımın son sürümlerinin ancak farklı bir çalışandan onay alındıktan sonra üretim ortamına yüklenmesi, yetki taleplerinin ancak talep edenden farklı ve daha üst bir mevkide çalışan tarafından onaylandıktan sonra karşılanması gibi.

Bilgi sistemleri biriminde görevler ayrılığı kontrolünün yerleştirilebilmesi için ilk olarak işlerin bu bakışla değerlendirilmesi gerekmektedir. Hangi iş/iş adımları birbirinden ayrılmalı ki işle ilgili hata, eksiklik, yanlışlık, ihmal veya suistimal olasılığı en aza indirilebilsin? Hangi iş adımlarını aynı kişinin yapması çıkar çatışmasına sebep olabilir? Veya belli bir iş sürecinde meydana gelecek hatayı (illa ki suistimal olmayabilir ama sonuç itibariyle varlık/iş süreci yine de zarar görebilir) ortaya çıkarabilmek için iş nasıl adımlara bölünmelidir? Bu gibi bir bakış açısıyla tüm işler tespit edilip ayrıştırılmalıdır. Yazılı görev tanımları da belirli olduğuna göre (olmalı) çalışanlara görev atamaları bu tespitlere göre yapılmalıdır. Ayrıca görevler ayrılığına yönelik yazılı politika/prosedür/süreç tanımları gerektiği seviye ve detayda hazırlanmalıdır.

Ayrılması gereken veya alt adımlara bölünmesi gereken iş süreçleri ve karşılık gelen roller tespit edilirken elde edilen bulgular, *"SoD matrisi*" denilen bir şekilde yazılı hale getirilirse; gerek gözetim gerekse yeni görevlendirmelerde faydalı olacaktır. SoD matrisi, aslında basit bir excel dokümanı olarak hazırlanabilir. Bir sütunda kritik iş adımları, bir satırda da ise görev tanımları yer alır. Her iş adımı/görev tanımının birleştiği hücreye, bu iş adımının bu görevi üstlenen kişiyle yapılıp yapılmayacağı belirtilir. Böyle bir doküman hazırlanıp güncel tutulursa birime faydalı olacaktır. SoD matrisi hazırlarken dikkat edilmesi gereken birkaç nokta aşağıda verilmiştir:

- Görev tanımlarının sahadaki duruma uyması,

- Tüm işlerin detaylı incelenmesi ve doğru şekilde bölünmesi,

- Personel sayısı veya personelin görev değişikliğinde bu tablonun güncellenmesi, gerekirse personele atanan işlerin de değişmesi.

SoD matrisi, ister her iş adımını farklı bir çalışana verecek kadar geniş iş gücü kaynağı olsun, ister telafi edici kontrollerle süreç yönetilsin ve isterse de iş rotasyonu yapılsın sonuç olarak işletmeye faydalı olacak bir dokümandır.

Ancak, bu ilke her ne kadar iş süreçlerini hata, eksiklik, yanlışlık, ihmal ve suistimalden korusa da, kendi içinde belli bir maliyeti bulunmaktadır. Burada temel olarak iki tür maliyetten bahsedilebilir. Birinci maliyet, iş süreçlerini alt adımlara bölmek ve farklı kişilere vermek, araya seviyeler konulmasını gerektirmesi nedeniyle işin tamamlanma süresini artırır. İkincisi ise, daha çok çalışana ihtiyaç duyulması nedeniyle katlanılacak ücrettir.

Risk yönetimi ve kontrol tasarlama süreçlerindeki en önemli sorulardan biri şudur: Maruz kalınan risk ile tasarlanan kontrol birbiriyle uyumlu mu? Dengeli mi? Kontrolü çalıştırmak mı daha maliyetli yoksa maruz kalınan risk gerçekleştiğinde ortaya çıkacak durum mu daha maliyetli? İşin riskinden daha maliyetli bir kontrol tasarlanmamalıdır (tabi daha önce belirtildiği üzere yasal zorunluluklardan kaynaklanan kontroller bu ilkenin dışındadır). Çünkü böyle bir durum aslında söz konusu işten vazgeçilmesine yol açabilir. Kontrol tasarlanırken (gerek görevler ayrılığı, gerekse diğer tüm kontroller) bu kriter unutulmamalıdır.

Finans sektöründe çok küçük işletmeler vardır. Bu işletmelerde görevler ayrılığı nasıl sağlanabilir? İşler belirlenip, alt adımlara bölünmesine karşın, personel sayısının çok kısıtlı olması nedeniyle görevler ayrılığı ilkesi nasıl uygulanabilir? Burada bir ara çözüm ve tabi bunun da bir maliyeti vardır. Telafi edici kontrol (compensating control) kontroller tasarlanarak görevler ayrılığı ilkesi ile amaçlanan hedef (hata/suistimal önleme) gerçekleştirilemese bile en azından fark edebilir.

Telafi edici kontroller, olmayan ya da maliyeti çok olabilecek kontrollerin yerini kısmen telafi etmeye yönelik kontrollerdir. İşletmelerde yeterli maddi veya insan kaynağının bulunmadığı durumlarda uygulanır. Bu kontroller, normalde hata, eksiklik, yanlışlık, ihmal veya suistimali önlemek amacıyla farklı kişiler tarafından üstlenilmesi gereken görevler tek çalışan tarafından yerine getiriliyorsa, en azından süreçte yaşanabilecek olumsuzlukları, gerçekleştikten sonra da olsa fark edip buna uygun eylemlerin hayata geçirilmesini sağlayan kontrollerdir. Buna bilgi sistemlerinden en bilinen, en çok görülen örnek verilmek istenirse, kritik iş süreçleri sırasında yapılan işlemlere dair iz kayıtlarının (log) toplanması ve bu kayıtların belirli aralıklarla (çok uzun olmayan) gözden geçirilmesidir. İz kayıtları asgari olarak;

- Kaydı oluşturan sistem,

- Kaydın oluşturulduğu tarih, saat ve zaman dilimi bilgisi,

- Kaydı oluşturan işlemle birlikte, gerçekleştirilen değişikliğin ne olduğunu gösteren bilgi,

- Kaydın ilişkili olduğu tekil kullanıcıyı veya sistemi gösteren bilgiyi

içermelidir.

Bu konuda, çok bilinen ve aslında teknik olmayan, bilgi sistemleri birimlerinin dışında da gereken yerlerde kullanılabilecek bir kontrol, işlerin rotasyonudur. Bu, belli bir işi/iş adımını bir süreliğine normalde yerine getiren kişiden farklı bir kişiye atamaktır. Tercihen esas görevlinin

işletmeden bir süre uzak kaldığı durumlarda yapılır veya bazı işletmelerde kişi "*zorunlu tatil*"e çıkarılır. Büyük işletmelerde, düzenli bir biçimde çalışanların birimleri değiştirilerek rotasyon uygulamaları görülür. Burada amaç, iş süreci farklı bir kişi tarafından yerine getirilirken yolunda gitmeyen hususların, eksikliklerin tespit edilmesidir. Bu yöntem aslında işletmelerde iş süreçleri bazında bir yedeklilik de yaratabilir. Ancak bu uygulama daha çok büyük işletmelerde görülür.

Telafi edici kontrollerin uygulanmasında iki unsuru dikkate almak gerekmektedir:

- Birincisi, bu kontrollerin bir maliyeti vardır. Örneğin iz kaydı tutan sistemlerin geliştirilmesi/edinilmesi/işletilmesi gibi. Telafi edici kontrollerin işletmesini, kritik işi yapan kişiden farklı kişiler yapmalıdır.

- İkincisi ise, gözetim işinin sık periyotlarla yapılması gereklidir. Kritik bir iş sürecinde mecburen tek kişi çalışıyor ve iz kayıtları tutuluyorsa, iz kayıtlarının incelenmesi, iş gerçekleştikten çok sonraya bırakılırsa, hatanın ya da suistimalin gerçekleştiği durumlarda çok geç kalınmış olunabilir. Bu yüzden bu gözetim işinin (elbette ki bu işi kesinlikle kritik işi yapandan farklı bir kişi yapacak, burada görevler ayrılığından kaçış yok) önceden belirli ve işin niteliğine uygun sıklıkta yapılması gerekmektedir.

Son olarak, görevler ayrılığına ilişkin tüm politika, prosedür, süreç dokümanı, SoD matrisi gibi yazılı dokümanların oluşturulup onaylanması (en azından bilgi sistemleri yöneticisi tarafından), güncel halde tutulması ve tüm ilgili personele duyurulması gerekir.

İşletmelerde görevler ayrılığı ilkesini değerlendirirken ilk önce, diğer tüm süreçleri değerlendirirken yapıldığı gibi, konuya ilişkin tüm yazılı dokümantasyonun edinilip kağıt üzerinde bu işin nasıl yapıldığı anlaşılmaya çalışılmalıdır. Daha sonra her seviye çalışanın konu hakkındaki farkındalığı, kendi görev ve yetkileri bazında görevler ayrılığının nasıl sağlandığı hakkında bilgi edinilmelidir. Birim yöneticileriyle de, varsa telafi edici kontrollerin nasıl uygulandığı, gözetiminin nasıl ve ne sıklıkla yapıldığı öğrenilmelidir. Gözetim sonuçları ve gerekmesi halinde alınan aksiyonlar yazılı olmalıdır. Ayrıca yönetimden, SoD matrisinin nasıl güncel tutulduğu (olup olmadığı), nasıl duyurulduğu öğrenilmeli ve çalışanların da güncel durumdan haberlerinin olup olmadığı hususu değerlendirilmelidir. Görevler ayrılığı ilkesinin uygulanmadığı ve telafi edici kontrollerin de mevcut olmadığı durumların ise kesinlikle riski artıran bir durum olduğu akılda tutulmalıdır.

1.1.2.5. Bilgi Sistemleri Birimleri İçin En İyi Uygulama Örnekleri

Bu bölümde yol gösterici olarak bilgi sistemleri için bazı en iyi uygulama örnekleri (best practices) verilmektedir. En iyi uygulama örnekleri; bir iş kolunun veya sürecinin etkinliğini iyileştiren, çok denenmiş ve genel kabul görmüş bir grup uygulama/yöntemdir. Ancak en iyi uygulama örnekleri hiçbir zaman körlemesine uygulanmamalı, duruma göre yorumlanmalı ve neden yapıldığı/ne kazanılacağı iyi hesap edilmelidir (Stangarone, 2018)(Miller, 2021)(Roush, Hertcik, 2020). En iyi örneklere, bunlarla sınırlı olmamak üzere, aşağıda yer verilmektedir:

- Bilgi sistemleri yöneticisinin odağı teknolojik konulardan bilgi sistemleri-iş uyumuna yönelmelidir.

- Bilgi sistemleri yatırımlarının işletmeye nasıl değer katacağına odaklanmalı ve bunu diğer iş birimleri yöneticilerine ve üst yönetime anlatmalıdır.

- Bilgi sistemleri yöneticisi, teknik personel olmaktan vazgeçmeli, takımının/ekibinin yeteneklerini, kaynakların durumunu, işlerin gidişatını takip etmelidir.

- Bilgi sistemleri biriminde yöneticiden en alt personele kadar herkesin kişisel gelişimine kaynak ayrılmalıdır.

- Bilgi sistemlerinde her süreç ve iş ölçülmelidir.

- Bilgi sistemleri biriminden beklenen en önemli özellikler: İşlerin zamanında bitmesi, bütçeyi aşmamak ve beklenen sonuçların kazanılmasıdır.

- Yazılı süreçler ile hızlı aksiyon alma arasında bir denge kurulmalıdır. Aksiyon alma, talebe cevap verme konusunda genelde büyük işletmeler daha bürokratik, küçük işletmeler ise daha çeviktir. Her durumda işletmede dengeyi sağlamak önemlidir.

- Gündelik koşturmacalar ile yenilikçilik arasında dengeyi kurmak gereklidir. Bilgi sistemleri birimlerinin zaman ve emeğinin çok büyük bir yüzdesi mevcut durumu korumaya, sistemin işler durumda tutulmasına harcanmaktadır. Sadece mevcudun korunması aslında bir anlamda geriye gitmek olarak da yorumlanabilir. Bilgi sistemleri birimleri iş tarafını ileriye götürecek teknolojik potansiyele bilinçli olarak zaman ayırmalıdır. Bu iş, boş kalan zamanlarda yapılacak bir şey olarak görülmemelidir.

- İşler mümkün olduğunca otomatikleştirilmelidir.

- Yeniliklere uyum sağlayabilen bir yapıda olunmalıdır. Teknolojik gelişmeler ve iş yapılan sektörde kullanımı konusunda hep güncel kalınmalıdır.

- Kullanıcılara inisiyatif verilmelidir. Günümüzde bilgi sistemleri teknolojileri yıllar önceki gibi sadece teknoloji alanında yetişmiş kişilerin tekelinde değildir. Teknoloji okur-yazarlığı ve son kullanıcılar için geliştirilmiş araçların sayısı artmaktadır. Bu durumda, işletmenin bütün olarak bilgi güvenliğinin ve işlemlerin bütünlüğünü bozmayacak kontrolleri hayata geçirerek son kullanıcıları desteklemek ve onlara alan açmak gerekir. Bu şekilde bilgi sistemleri birimleri de işletmeyi dönüştürücü yeniliklere daha fazla zaman ayırabilir.

- İş ve bilgi sistemleri birimlerinin arasındaki iletişim eksikliği problemi çözülmelidir.

- Açık ve anlaşılır tanımlanmış bilgi sistemleri hedefleri konulmalıdır. Bu hedefler, işletme stratejisi ve devamında bilgi sistemleri stratejisinden gelmelidir. Bu hedefler birimdeki ilgili her çalışana iletilmeli ve herkes kendinden bekleneni tam olarak anlamalıdır.

- Personel verimliliği, sunulan servislerin kalitesi ve harcanan maliyetler ölçülmeli, öncesinde de bunun için metrikler geliştirilmelidir.

- Tüm bilgi sistemleri biriminin odağı iş tarafının hedeflerini gerçekleştirmek olmalıdır. Bilgi sistemlerinde gerçekleştirilen her iş, sunulan her servis, geliştirilen her uygulama sonuçta bu amaca hizmet etmelidir.

- Tüm işler, en karmaşık projeden en küçük işe kadar, planlanmalı ve gerekli kaynaklar plana göre hazırlanmalıdır.

- Yetki ve sorumluluk unsurlarının ayrılmaz ikili olduğu unutulmamalıdır.

- Bilgi sistemlerinin politika ve yönergelerine tüm işletme uymalıdır. Bunun bilgi sistemlerinin performansı için değil, tüm işletmenin performansı için olduğu bilinmelidir. Bunu sağlamanın yolu da işletmede kontrol ortamını olgunlaştırmak ve içselleştirmektir.

- Her zaman kontrol etmeye, ölçmeye ve güncelleştirmeye zaman ayrılmalıdır.

1.1.2.6. Bilgi Sistemleri Organizasyonunun Değerlendirilmesi

Bilgi sistemleri organizasyonunu değerlendirirken işe, ilgili tüm dokümantasyonun incelenmesiyle başlanmalıdır. Genel olarak incelenmesi gerekli görülen dokümanlar: Bilgi sistemleri stratejisi, buna göre geliştirilen planlar, politikalar, prosedür ve talimatlar, organizasyon şeması, görev tanımları ve geçmiş iç veya dış denetim raporlarıdır. Bu dokümanlardan ve işletme içinde yapılacak görüşmelerden bilgi sistemleri biriminin gerçekleştirdiği fonksiyonlar belirlenmelidir.

Bilgi sistemleri biriminin organizasyon şemasına bakılarak işletme içinde ve kendi içinde yapılanması incelenmelidir. Organizasyon şeması hazırlanmış ve onaylanmış olmalıdır. Bilgi sistemlerinin işletmede nereye bağlı olduğu önemlidir. Belli bir fonksiyonel birimin altındaysa bu durum diğer birimlerle ilişkide bir çatışmaya işaret edebilir.

Bilgi sistemlerinin gerçekleştirdiği her bir fonksiyonun (personel sayısından bağımsız olarak) organizasyon şemasında yer alması gerekir. Ayrıca dış kaynak kullanımı yoluyla edinilen faaliyetlere ilişkin yönetim fonksiyonunun da organizasyon şemasında yer alması önemlidir. Organizasyon

şemasında tüm birimlerin/fonksiyonların yer almasının önemli olmasının nedenlerinden biri, bunun birimin işlerinin işletmede "*görünürlüğü/bilinirliği*" ile ilgili olmasıdır.

Bilgi sistemlerinin tüm politika, prosedür ve talimatlarının yazılı ve onaylı olması; her sürecin sahibinin, amacının, girdi ve çıktılarının belirli olması; tüm görev tanımlarının yazılı ve onaylı olması ve en önemlisi de süreçlerin ve görev tanımlarının saha ile örtüşmesi özellikle değerlendirilmelidir.

Bilgi sistemleri organizasyonunun değerlendirilmesinde en önemli noktalardan biri bilgi sistemleri içinde görevler ayrılığı ilkesinin ne derece uygulandığının incelenmesidir. Bunun için güncel bir doküman olması (hangi görevin hangi görevle beraber yürütülemeyeceğini gösteren SoD matrisi veya benzeri bir doküman) tercih edilir. Dokümanın sahadaki karşılığı mutlaka değerlendirilmelidir.

Bilgi sistemleri biriminin herhangi bir şekilde denetime tabi olup olmadığı belirlenmelidir. Eğer iç ve/veya dış denetim geçirdiyse denetim raporları incelenmeli, varsa sorunlu alanlara karşı ne yapılacağı ve buna ilişkin bir planın varlığı sorgulanmalıdır. Eğer birim herhangi bir denetim sürecine tabi değilse, bilgi sistemleri kontrollerinin nasıl değerlendirildiği/ölçüldüğü incelenmelidir. Kontrollerin etkinliğinden ve yeterliliğinden her ne kadar üst yönetim sorumlu olsa da gerekli ölçme/değerlendirme işlemlerinin periyodik olarak ilk önce birim bazında yapılması uygun olacaktır.

1.1.2.7. Bilgi Sistemleri Yönetim Birimleri

1.1.2.7.1. Kaynak Yönetimi

İş hayatında bilindiği üzere, işler hep gecikmiştir, yeterli personel yoktur, bütçe kısıtlıdır, yeterli eğitim sağlanamaz veya yeterli araç yoktur. Bu liste, biraz da işin niteliğine ve çalışılan işletmeye göre uzayıp gider; ama kesin olan şey işletmelerde kaynakların hep kısıtlı olduğudur. Türü ne olursa olsun tüm kaynakların birincil ve ortak özelliği sınırlı olmasıdır.

İşte bu kısıtlı kaynaklarla işleri gerçekleştirebilmek amacıyla kaynak yönetimi pratikleri geliştirilmiştir. Amaç gereksinimleri karşılamak için kısıtlı kaynaklarla en yüksek faydayı sağlamak veya en az maliyetle hedeflere ulaşmaktır. Özünde, en çok örgütsel değeri elde etmek için kıt kaynakları tahsis etme, en iyi kaynak kombinasyonunu oluşturma sürecidir. İyi bir kaynak yönetimi, doğru iş için doğru zamanda, doğru kaynakların mevcut olmasını ve verimli bir şekilde kullanılmasını sağlar.

Bilgi sistemleri yönetişimi kapsamında kaynak yönetimi, bilgi sistemleri stratejisiyle ortaya konan hedeflerin ve devamında belirlenen aksiyonların/işlerin gerçekleştirilmesi sırasında bilgi sistemleri kaynaklarının etkin ve verimli şekilde nasıl yönetileceğidir.

Bilgi sistemleri birimlerinde kaynak yönetimi, kimin hangi işe atanacağından ve tedarik edilmesi gereken yeni donanımdan daha ötesini kapsamaktadır. Her ne kadar bilgi sistemleri birimleri iş tarafı ile stratejik ortak oldu denilse de, halen bilgi sistemleri kaynaklarının (özellikle işgücü ve zaman boyutunda) büyük kısmı gündelik işlere harcanmaktadır. Stratejik ortak olabilmek için yenilikçi çalışmalara ağırlık vermek gerekir; çünkü stratejik faaliyetler günümüze odaklı değildir (Innotas, 2012).

Kaynak yönetiminde kaynaklar, maddi kaynaklar ve maddi olmayan kaynaklar olarak ikiyi ayrılır. Bilgi sistemlerinde kaynak olarak sınıflandırılan unsurlar ise insan kaynağı, mevcut uygulamalar, mevcut teknoloji bileşenleri (yazılım, donanım), tesisler, veri, finansal kaynaklar ve zaman olarak sayılabilir.

1.1.2.7.1.1. Kaynak Yönetimi Uygulamaları

a. Kaynak Planlama Süreci

Kaynak planlaması sürecine örnek olabilecek bir akışa aşağıda yer verilmektedir.

i. Kaynak Planlaması

Bilgi sistemleri stratejisindeki hedeflere bağlı olarak belirlenen aksiyonların gereksinimleri belirlenir (genellikle yıllık olarak). Bir yıl içerisinde büyük ihtimalle gerçekleştirilecek birden çok aksiyon olabilir, bu arada süregelen işler ve bunların da kaynak ihtiyacı olacaktır. Eldeki kaynaklar iş

önceliklerine göre yeni geliştirmeler ve süregelen işler arasında paylaştırılmaya çalışılır. Burada dikkat edilecek konulardan biri hiçbir kaynağı (iş gücü dahil) fazladan rezerve etmemektir.

En önemli kaynak olarak insan kaynağı düşünülmelidir. Ancak insan kaynağının sadece sayısı değil, yetkinlik ve yeterliliği de önemlidir. Eldeki iş için yetkin çalışan yoksa, ya edinilmeli ya da mevcut çalışan yeterli hale getirilmelidir.

Planlamada en büyük hatalardan biri, çalışanların zamanlarının %100'ünü söz konusu işe/projeye ayıracağını varsaymaktır. Bu düşüncenin gerçek dünyada karşılığı yoktur. Gerek günlük işler (toplantı, e-postaların cevaplanması vs) gerekse araya giren çok acil işler nedeniyle bir çalışan zamanını bölmek zorundadır. İkinci bir hata ise, söz konusu iş/projeyle ilgili gereksinimlerin asla değişmeyeceğidir. Bilgi sistemleri söz konusu olduğunda bu durumun da gerçek dünyada karşılığı yoktur.

ii. Kaynak Tahsisi

Belirlenen önceliklere göre kaynaklar alternatifler veya kulanımlar arasında tahsis edilmeli veya gerekiyorsa temin edilmelidir. İşlerin aşamalara bölünmesi ve bu aşamaların zamanlaması kaynakların hazır olma/kullanılabilme durumuna göre ayarlanmalıdır. Böylece başlayıp hemen kaynak bekleme sürecine giren bir iş olmaz.

iii. Kontrol/İzleme

İşler başladıktan sonra gerçekleşmeler gözlenmelidir. Her proje aşamasına harcanan süre ve diğer kaynakların kullanımı önceden belirlendiği gibi mi? Aşamaların tahmini sürelerini değiştirmek, kaynakların kullanım sürelerini azaltıp artırmak gerekiyor mu? Yeni kaynak teminine ihtiyaç var mı?

İş gerçekleşmeleri kayda alınmalı ve bir sonraki planlama sürecinde hesaba katılmalıdır. Genellikle haftalık iş adımları belirlemek izlemeyi ve yönetmeyi kolaylaştırır (Holicky, 2021)(Avron, 2017).

b. Kaynak Yönetiminde Karşılaşılan Problemler

Bilgi sistemlerine ilişkin kaynak yönetiminde karşılaşılan en önemli problemlere aşağıda yer verilmektedir:

- Süreç: Onaylanmış bir kaynak yönetimi sürecinin olmaması.

- Önceliklendirme: Bilgi sistemleri birimlerinde genelde en son *"acil"* olarak gelen iş üzerinde çalışılır. Halbuki önceliklendirme geliş sırasına veya kullanıcıların aciliyet kavramına göre değil; iş hedeflerine katkı ölçeğinde yapılmalıdır.

- Tahsis: Gerçekçi kaynak dağıtımı yapılmaması (özellikle işgücü ve zaman konusunda).

- Değişiklik: Devamlı projenin/işin değiştirilmesi, işe başlama ve işler arası değişim için harcanan zamanı artırır.

- Kaynak yönetiminin düzgün yapılamaması: Fazla veya eksik kaynak teminine, kaynakların kullanımında çakışmalara ve işlerin birbirini beklemesine veya eldeki kaynakların kullanımının düşük olmasına yol açabilir.

c. Kaynak Yönetiminde En İyi Uygulama Örnekleri

Kaynak yönetimine ilişkin en iyi uygulama örneklerine aşağıda yer verilmektedir (Wanamaker, 2018)(Townsend, t.y.):

- Aktif işlerin çok sık kesilmesini/değiştirilmesini engellemek,

- Kaynakların kullanımını araçlar yardımıyla izlemek,

- İşlerin izlenmesi için anlamlı kategoriler oluşturmak; proje, eğitim, yardım masası, analiz toplantısı, araştırma gibi,

- İzlenen her iş için kimin/hangi seviyenin/hangi rolün kaynak olarak kullanıldığı, ayrıca donanım bilgisi, kullanıcı bilgisi,

- Kaynak yönetimi, risk yönetimini de içinde barındırır, bununla ilgili izleme de yapılmalı,

- İş zaman planını yaparken iş gücü için %100 müsaitlik düşünmemek gerekir, kimse bu kadar müsait olamaz, gündelik işlere de zaman ayırmak gerekir,

- Öncelik ve aciliyetine göre, projeler arasında kaynak aktarma olabilir,

- Öncelik ve aciliyet konusu rasyonel olarak değerlendirilmelidir. Çalışan bir sistemin arıza çıkarması *"acil"* kabul edilebilir ancak henüz geliştirilmeye başlanmamış veya yolun ortasında olan bir iş için acil deniyorsa çok daha önceden bir planlama hatası yapılmış demektir,

- İnsanların yoğun bir şekilde çalışması kaynakların verimli kullanıldığını göstermez, çıktı kalitesinin düşeceğini de gösterebilir,

- Bir çalışanın üzerinde çok fazla aktif iş olması onun çok çalışkan/verimli olduğunu göstermez, planlama hatası olduğunu da gösterebilir,

- Hangi kaynağın ne kadar kısıtlı olduğunun belirlenmesi. Her kaynak kısıtlı ama aynı derecede kısıtlı değildir.

d. İnsan Kaynakları

İnsan kaynağının yönetiminde özellikle planlama aşamasında yapılabilecek hatalara daha önce değinilmiştir. Bu hatalardan biri kaynak planlaması yapılırken çalışanların zamanlarının tümünü %100 verimlilikle mevcut işlere harcayacağının düşünülmesi, diğeri ise insan kaynağının sadece sayısal olarak değerlendirilmesi, gerekli ve yeterli yetkinlikte olup olmamasının hesaba katılmamasıdır. İşletme, gerekli iş gücü kapasitesini (yetkinlik/yeterlilik) ve sahip olduğu iş gücü kapasitesini (yetkinlik/yeterlilik) iyi belirlemelidir.

Diğer taraftan insan kaynağının yönetimi, işletmenin risk yönetimi içinde önemli bir yer teşkil eder. Genel bir kabul olarak, suistimal ve hedefli saldırıların dışarıdan olabileceği kadar içeriden de olabileceği bilinmektedir. İnsan kaynakları alanında güvenlik riskine karşı kullanılabilecek en önemli üç kontrole aşağıda yer verilmektedir:

- Geçmiş araştırması,

- Gizlilik anlaşması,

- Rekabet etmeme anlaşması.

İşe alım aşamasını geçtikten sonra da iş ortamına, işletmeye ve sektöre yönelik tüm bilgilendirmelerin uygun şekilde yapılması, gerekli materyallerin verilmesi (çeşitli politika, prosedürler, el kitapları gibi) ve eğitim gibi kontroller işletilmelidir.

Çalışma sırasında kullanılabilecek kontroller ise şunlardır:

- Zorunlu tatil,

- İş rotasyonu,

- Görevler ayrılığı,

- Eğitim.

İnsan kaynağı ile ilgili olarak doğru iş gücünü işe almaktan daha önemlisi, bu iş gücünü elinde tutabilmektir. Benzer şekilde, bu kaynağı yeterince motive edecek bir performans ve ödüllendirme sistemi kurarak çalışan bağımlılığı ve verimliliği artırarak iş kalitesi hedeflerine ulaşması sağlanmalıdır.

1.1.2.7.1.2. Kaynak Yönetiminin Değerlendirilmesi

Bilgi sistemleri biriminin kaynak yönetimi fonksiyonu değerlendirilirken, ilk önce sahip olunan kaynakların envanteri çıkarılıp incelenmelidir. Bu noktada izleme için bir araç kullanılıyorsa iş kolaylaşabilir ancak aracın kullanımı ve araçtan yararlanım da değerlendirilmelidir.

Kaynak tahsisi ile bilgi sistemleri ve işletme stratejisi beraber değerlendirilmelidir. Kaynak tahsisinin kurumsal önceliklere uyup uymadığı anlaşılmalıdır. Her bilgi sistemleri projesinin kazanımlarının ölçülebilir şekilde ifade edilip edilmediğine bakılmalıdır.

Kaynak yönetimi ile ilgili politika ve prosedürler güncelliği, uygunluğu ve işlerliği açısından değerlendirilmelidir. Kaynakların (insan kaynağı dahil) kullanımı, kullanılabilirlik durumu, iş ve projelerle ilişkisinin kayıt altına alınması ve takip edilmesinin değerlendirilmesi yapılmalıdır.

Kaynak yönetimiyle ilgili raporların işletmede kimlere gönderildiği, üst yönetim/yönetim kurulunun bunları inceleyip incelemediği ve cevap olarak alınan aksiyonların değerlendirilmesi de gerekmektedir.

1.1.2.7.2. Risk Yönetimi

Günümüzde bilgi sistemlerinin etkin ve verimli bir şekilde işleyip, amaçlarını gerçekleştirmesi için bu sistemlerin sahip olduğu bilgi varlıklarının ve yürüttüğü görevlerin korunması şarttır. Bunu gerçekleştirmek için ise risk yönetimi zorunlu hale gelmiştir.

1.1.2.7.2.1. Risk Yönetimi Kavramı

Risk; bir zarara uğrama tehlikesi, zarar görme olasılığıdır. Kurumsal anlamda risk, iş hedeflerine ulaşmaya engel olacak veya kurumsal kayba (değer kaybı, maddi kayıp, müşteri kaybı vb) sebep olacak olaylardır. İşletmenin hedefleri riskten etkilenir. Risk, işletme için bir maliyettir ve işletmeler bu maliyeti olabildiğince düşürmeye çalışır. Riski önlemek bir dereceye kadar mümkündür. Ancak bunun için kötü bir olayla karşılaşması muhtemel yapıları, ne gibi olayların ihtimal dahilinde olduğunu, böyle bir olayın gerçekleşme ihtimalini ve gerçekleştiğinde muhtemel etkisini bilmek ve buna göre önleyici birtakım tedbirler almak gerekir. Bu anlatılan işlemlerin tümü risk yönetimi fonksiyonunu oluşturur. Daha basit bir tanım yapmak gerekirse risk yönetimi; işletmenin faaliyetleri sırasında ortaya çıkabilecek riskleri fark etmek, tanımak, değerlendirmek, önlemek ve azaltmak için gerekli süreçlerin oluşturulması ve işletilmesidir.

Risk yönetimi, kategoriden bağımsız olan bir süreç olmasına rağmen, riskin tanınması, etkilerinin hesaplanabilmesi için risk kategorilerini belirlemek gereklidir. Riskler kolay yönetebilmek için belli kategorilere ayrılmalıdır. Bu kategorilere; finansal riskler, operasyonel riskler, yasal/mevzuattan kaynaklanan riskler, stratejik yönetimden kaynaklanan riskler, teknoloji riskleri, doğal afetlerden kaynaklı riskler örnek verilebilir.

Risk yönetimi, kurumsal bazda ele alınmalı, her birim kendi risk kategorileri ile risk yönetimine katılmalıdır. Risk yönetimi süreçleri/yöntemleri işletmede ortak olmalı, böylece farklı birimlerin yaptığı risk yönetiminin karşılaştırılabilir, birlikte yönetilebilir ve tekrar edilebilir olması sağlanmalıdır. Riskler farklı kategorilerde olsa da risk yönetim çerçevesinin/risk yönetim yönteminin işletmenin genelinde tek olması farklı kategorilerdeki risklerin yönetiminde tutarlık sağlar. Kurumsal risk yönetimi bu şekilde ortaya çıkmıştır.

Yıllar içinde gelişen yönetim yaklaşımları, bir işletmedeki risklerin yönetilmesinden üst yönetimi sorumlu tutmuştur. Bilgi sistemleri risk yönetimi de bilgi sistemleri yönetişiminin ayrılmaz bir parçasıdır ve işletmenin risk yönetiminin bir parçası olarak ele alınmalıdır.

Bilgi sistemleri riski nedir diye sorulursa, çok basit olarak, bilgi teknolojilerini/bilgi sistemlerini kullanmaktan kaynaklı riskler denilebilir. Bilgi sistemleri kullanımı başlı başına bir risk faktörüdür, tıpkı bilgi sistemleri kullanmamanın ayrı bir tür risk faktörü olduğu gibi.

İşletmelerin maruz kaldığı riskler çok çeşitli olabileceği için bir kişinin tüm risk yönetiminden sorumlu olması beklenemez. Burada uygun olan, uygulanacak risk yönetimi yaklaşımının belirlenmesi, daha sonra bu yöntemin her risk kategorisi için konuya hakim kişilerce/ekiplerce yürütülmesidir. Ancak işletmede risk yönetim tarzının, bu konudaki liderliğin, sorumluluğun ve risk iştahının/kabul edilebilir risk seviyesinin üst yönetim tarafından belirlenmesi esas olmalıdır.

Burada "*risk iştahı*" veya diğer bir ifadeyle "*kabul edilebilir risk seviyesi*" kavramını tanımlamak uygun olacaktır. Risk iştahı, bir işletmenin hedeflerine ulaşmak için çalışırken "*göze*

alabildiği", "*tolere edebildiği*" risk değeri/seviyesidir. Belirlenen bu risk seviyesini azaltmak için işletme bir aksiyon almaz, ancak bunun üzerinde kalan riskler için bir karar vermek, aksiyon almak durumundadır.

İşletmelerde belirlenen risk iştahı, işletmenin bütün faaliyetlerini doğrudan etkileyecek bir hususdur. Bu yüzden üst yönetim tarafından belirlenmelidir. İşletmenin yapısı, büyüklüğü, finansal durumu, içinde bulunduğu sektör, kurum kültürü, yasal çerçeve, faaliyetlerinin çeşitliliği ve elbette vizyonu risk iştahının belirlenmesinde birer faktördür. Genellikle sağlık, güvenlik gibi sektörlerde risk iştahı düşük, yenilikçi sektörlerde (özellikle teknoloji gibi) risk iştahı yüksektir. İşletmenin rakipleri de risk iştahını etkiler. Fazla rekabetin olduğu, hızlı değişen bir sektörde işletme rekabet edebilmek için risk iştahını yüksek tutmak isteyebilir. Büyük işletmelerin risk iştahı görece düşük olabilir buna karşın küçük işletmeler büyüyebilmek için risk iştahlarını yüksek tutabilir. İşletme içerisinde de farklı risk kategorilerine göre farklı yaklaşımlar benimsenebilir. Tüm bunların üst yönetimce değerlendirilmesi gerekir.

Risk iştahı, risk kapasitesi, risk limiti ve risk profiliyle birlikte risk iştahı çerçevesini oluşturur. Burada risk kapasitesi, işletmenin mevcut finansal, ekonomik ve hukuki ortamı dikkate alınarak alabileceği azami risk düzeyini ifade ederken; risk limiti risk iştahıyla paralel olan hedeflere ulaşılabilmesinde iş birimleri, personele vb. tahsis edilebilecek risk miktarını ifade eder. Üst yönetimin bu çerçeveyi işletme kültürüne yerleştirmesi ve uygulaması, işletme hedeflerinin başarılması açısından önem taşır.

Risk iştahı, sabit değildir. İşletmenin yer aldığı sektördeki değişiklikler, işletmenin stratejisindeki değişiklikler veya başka sebeplerle değişebilir. Ancak risk iştahı değiştikten sonra kontrollerde gerekli değişikliklerin de yapılması gerekir.

Riskten söz edilebilmesi için bazı ön koşulların varlığı gerekmektedir. Bunlar (Quinn, Ivy, Barrett, Feldman, Witte, Gardner, 2021):

- Değerli bir varlık/sistem/kaynak,
- Değerli varlığın yapısında mevcut bulunan bir zafiyet/zayıflık/açık,
- Bir tehdit unsuru,
- Zafiyetin tehdit tarafından kötüye kullanılması sonucunda oluşacak zararlı bir etki.

1.1.2.7.2.2. Risk Yönetimi Adımları

Risk yönetiminde farklı yaklaşımlar kullanılır. Burada anlatılan yaklaşımda önce yukarıdan aşağıya (top down) risklerden etkilenecek sistem/varlıklar belirlenir, daha sonra aşağıdan yukarıya (bottom up) söz konusu varlıkların maruz kalabileceği risklerin yönetimi varlıkların sorumluları tarafından gerçekleştirilir. Bu süreç aşağıdaki gibi özetlenebilir (aşamaların isimlendirmesi yaklaşımlara göre farklılaşabilir):

1. Risk Belirleme: Birinci adımda riskin teşhisi yapılır. Öncelikle işletme hangi risklerden korunmak istediğini belirlemelidir. İşletme, amaçlarına ulaşmasına engel olabilecek risklerden korunmak ister. Bunların belirlenmesi için de önce işletmenin amaçları incelenip, bu amaçları destekleyen sistemler/varlıklar belirlenir. Bu aşamada özellikle işletme stratejisi ve bilgi sistemleri stratejisi incelenmelidir. Böylece hem sistemin işleyişi hakkında bilgi edinilir hem de işletmenin varlıkları belirlenmiş olur. Varlıkların belirlenmesi konusunda dikkat edilmesi gereken bir husus da, sadece varlıkların bir listesinin oluşturulmasının yeterli olmadığıdır. Önemli olan varlığın işletme için değerinin belirlenmesidir ki; bu da ancak varlığın işletmede hangi iş sürecinde ve ne amaçla kullanıldığının anlaşılmasıyla mümkün olur.

2. Risk Analizi: Bu aşamada, risk kategorilerini kullanmak ve bu şekilde farklı ekipleri işin içine katmak gerekir. Bilgi sistemleri riskleri için bilgi sistemleri varlıklarının zafiyetleri ve bunlara yönelik tehditler belirlenir. Burada risk kategorisi *"teknoloji"*dir. Bu çalışmada bilgi sistemleri personeli görev almalıdır. Söz konusu personel, bir önceki aşamada belirlenen varlıkları (yazılım, donanım, altyapı vb) tek tek incelemeli ve her birinin zafiyetlerini, bu zafiyetleri kullanabilecek tehditleri,

tehditlerin gerçekleşme olasılığını ve gerçekleştiğinde ortaya çıkabilecek muhtemel etkiyi belirlemelidir.

3. Risk Değerlendirme: Bilgi sistemleri varlıklarına ilişkin bir riskin ortaya çıkması için yukarıda bahsedildiği gibi varlığın yapısında bir zafiyet bulunması ve bu zafiyeti istismar edebilecek/kötüye kullanabilecek bir tehdidin mevcut olması gerekir. Zafiyet yoksa risk oluşmaz veya tehdit olmazsa yine risk oluşmaz. Burada çeşitli yöntemlerle önceki adımlarda belirlenen değerler kullanılarak olasılığının ve soncunun birleşimini dikkate alarak her varlığa yönelik bir *"risk değeri"* belirlenir. Belirlenen risk değerine göre sıralama yapılır. Sıralamada risk iştahı veya kabul edilebilir risk seviyesinin üzerinde kalan risklerin uygun biçimde işlenmesi gerekir.

4. Risk İşleme: Riskin işlemesi, varlığın riskine karşı nasıl bir yol izleneceğinin belirlenmesidir. Burada, risk büyüklükleri değerlendirilerek, kabul edilebilir seviyeye indirilmesi üzerinde çalışılır. Risklerin azaltılması için sratejiler ve acil durum senoryaları geliştirilir. Benzer şekilde risklerin fırsata çevrilmesi üzerinde çalışılır. Genel kabul gören risk işleme seçeneklerine aşağıda verilmiştir.

- Riski azaltma (risk mitigation): Çeşitli kontroller yardımıyla riskin düşürülmesi. En çok tercih edilen seçenektir.

- Riski engelleme (risk avoidance): Riske sebep olan ürünün/sürecin kullanımına son verme. Kontrollerle kabul edilebilir seviyeye düşürülemeyecek risklerin tamamen engellenmesidir.

- Riski transfer etme/paylaşma (risk transfer/sharing): Riski üçüncü taraflara aktarma veya paylaşma. Dış kaynak kullanımı veya oluşacak tüm zararı sigorta ettirmek gibi yöntemler kullanılır. Böylece riskin yarattığı zararın tamamı veya bir kısmı üçüncü tarafça karşılanır. Ancak bu seçenek riskin gerçekleşmesi ihtimalini değiştirmez, sonuçların telafisine yöneliktir.

- Riski kabul etme (risk acceptance): Riske rağmen ürünün/sürecin kullanımına devam etme. En kötü seçenektir, çünkü risklerin bilinerek ilgili ürünün/sürecin kullanımına devam edilir.

5. Gözetim: Bu adımda, risk yönetimi uygulamasılarının performansı sistematik olarak değerlendirilerek izlenir. Yukarıdaki bütün adımlar gözden geçirilip, kayıt altına alınır. İşletmelerde risk yönetimi sürecinin varlığı ve işlerliği üst yönetimin sorumluluğundadır. Üst yönetim, risklerin gerektiği gibi yönetildiğinden ve sürecin tekrarlandığından emin olmalıdır.

Risk yönetiminde en sık karşılaşılan yönetim çerçevelerinden biri, ISO 31000 ailesi, diğeri ise COSO yönetim çerçevesidir.

Bilgi sistemleri özelinde değerlendirilirse, bilgi sistemleri riski aslında işletmedeki "*bilgi*"nin maruz kaldığı risktir. Ancak "*bilgi*" tek başına var olamaz. Bilgi ya üretilir/işlenir (yazılım-donanım), ya aktarılır (ağ ve diğer bileşenler), ya saklanır (depolama ortamları), ya elektronik ortamda ya da kağıt üzerindedir (dokümantasyon) ya da çalışanlardadır. İşte bilgi sistemleri riski tüm bu sayılan varlıkların maruz kaldığı risklerdir. Bilgi sistemleri risk yönetimi de bu varlıkların maruz kaldığı risklerin kabul edilebilir seviyelerde tutulması için kullanılan tüm politika, prosedür, süreç ve diğer mekanizmalardır. Risk değerlendirme/analizi için farklı yaklaşımlar bulunmaktadır. Hangi yöntem seçilirse seçilsin, önemli olan bilgi sistemleri risklerinin kurumsal risk yönetimi kapsamında ele alınması ve ölçülebilir, tekrar edilebilir bir yöntemin benimsenmesidir.

1.1.2.7.2.3. Risk Yönetimi En İyi Uygulama Örnekleri

Bilgi sistemleri risk yönetimi için en iyi uygulama örneklerine aşağıda yer verilmektedir.

- Bilgi sistemleri risk yönetimi, işletmede diğer işler bittikten sonra ele alınacak bir konu olmayıp, diğer iş süreçlerine entegre edilmelidir.

- Risk değerlendirmesi yılda en az bir kez düzenli olarak yapılmalı, bunun dışında bilgi güvenliği risklerini artırıcı (yeni tehditlerin belirlenmesi, yeni varlıklar edinilmesi) veya azaltıcı (yeni kontrollerin tasarlanması) gibi olaylardan sonra tekrarlanmalıdır.

- Sadece teknik kontroller yeterli olmaz, yönetimsel/idari kontroller de hazırlanmalıdır.

- Kontrollerin etkinliği düzenli ölçülmelidir.

- Bilgi güvenliği eğitimi sadece bir defaya mahsus olmamalı ve tüm personele, belirli periyotlarda yenilenmiş içerikle (güncel olayları içeren) eğitimler tekrar verilmelidir.

- Risk yönetiminin tek amacı "*uyum*" olmamalıdır.

- Bilgi güvenliği konusunda uyulacak bir düzenleme olmasa dahi bilgi güvenliği/risk yönetimi kurum kültürünün bir parçası olmalıdır.

- Risk her zaman kendi içinde bir bilinmezlik içerir. Bu nedenle, hiçbir zaman maruz kalınan risklerin tamamına vakıf olunamaz. Risk yönetiminin amacı risklerden tamamen arınmış bir ortam yaratmak olmamalıdır.

- Küçüğünden büyüğüne tüm işletmeler riske açıktır.

- İşletmenin faaliyetleri, iş öncelikleri ve hedefleri iyi anlaşılmalıdır. Bunların yardımıyla işletmedeki kritik iş, varlık ve süreç belirlenmelidir. Kritiklik ölçütü kesinlikle iş fonksiyonlarına bağlı olmalıdır.

- Hiçbir ürün, araç, teknoloji veya çerçeve/standart bir işletmeyi tüm risklerden koruyamaz.

- Bir riski düşürmeye çalışırken başka bir risk artabilir. Örneğin bir sürecin bilgi güvenliği riski belli bir kontrol sayesinde azaltılabilir ancak sürecin maruz kaldığı operasyonel risk artabilir. Bu yüzden risk yönetimi tek çatı altında koordineli olarak yapılırsa, maruz kalınan riskler daha iyi ve dengeli yönetilir (National Cyber Security Centre, 2018).

Risk yönetimi ile ilgili detaylı bilgiye ISO 31000 Risk Management (https://www.iso.org/iso-31000-risk-management.html) ve Committee of Sponsoring Organizations of the Treadway Commission-COSO (https://www.coso.org) kaynaklarından, bunlarla sınırlı olmamak üzere, ulaşılabilir.

1.1.2.7.2.4. Risk Yönetiminin Değerlendirilmesi

Risk yönetimini değerlendirirken, risk ve bilgi güvenliği kavramlarının farkındalığı beraber değerlendirilmelidir. Tüm risk kategorilerinin kurumsal düzeyde bütünleşik bir bakış açısıyla yönetilmesi gerekmektedir. Ancak değerlendirme aşamasında kapsam dolayısıyla özellikle bilgi sistemleri risklerinin anlaşılmasına/yönetilmesine odaklanmak gerekir.

Sermaye piyasası mevzuatı kapsamındaki işletmeler için bilgi sistemleri risklerinin yönetimine ilişkin gerekli süreçlerin ve mekanizmaların oluşturulması ve işlerliği mevzuatla hükme bağlanmıştır. Dolayısıyla bu süreç hakkındaki farkındalık eksikliği, sürecin hiç olmaması, çalışır halde olmaması veya etkin işletilmemesi doğrudan risk teşkil eder (hem uyum hem de güvenlik riski). Değerlendirme bu yönde yapılmalıdır.

Risk yönetiminde şu veya bu yaklaşımın benimsenmesi beklenmemektedir; ancak işletme kendi yapısına uygun bir risk yönetim çerçevesini/yaklaşımını seçmeli/oluşturmalı ve kurumsal düzeyde risk yönetimi buna uygun yapılmalıdır. Risk iştahının belirlenmesi süreci ayrıca değerlendirilmelidir.

Risk değerlendirmesine ilişkin olarak yöntem, zamanlama, görev alacak kişiler, sonuçların yorumlanması, yorumlayacak kişiler belirlenmiş ve yazılı olmalıdır. Tüm bu faaliyetlerin gerçekleşmeleri incelenmeli, özellikle kritik iş süreçlerinin, bunları destekleyen bilgi sistemleri varlıklarının ve bunların risk değerlerinin belirlenmesi, elde edilen sonuçlara göre alınan aksiyonlar ve yönetimce bunların takibinin yapılıp yapılmadığı değerlendirilmelidir.

1.1.2.7.3. Kalite Yönetimi

Kalitenin sözlük anlamı "*nitelik*"tir. ISO 9000 standartlarına göre kalite, bir şeyin sahip olması gereken/istenen özelliklere sahip olma derecesidir.

Bilgi sistemleri özelinde kalite, bilgi sistemlerine ait ürünlerin/hizmetlerin sahip olması gereken niteliklere ne derece sahip olduğunun ölçüsü olarak tanımlanabilir. Bu nitelikler/gereksinimler çeşitli aşamalarda çeşitli paydaşlarca belirlenmiş olabilir. Bunlar:

- Müşteri odaklı nitelikler: Ürünün/hizmetin müşterinin ihtiyaçlarını/beklentilerini karşılaması. Bu niteliklerin sağlanması müşteri memnuniyetini ve sadakatini artırır.

- Tasarım odaklı kriterler: Üründe/hizmette hata veya eksiklik/yetersizlik çıkmaması. Ürünün/hizmetin beklendiği gibi çalışmasının sağlanması. Bu niteliklerin sağlanamaması müşteri memnuniyetsizliğine, ayrıca ürün/hizmetin kullanılamamasına veya daha kötüsü kullanım sırasında hatalara sebep olur.

- Sözleşme/yasal düzenleme kaynaklı nitelikler: Söz konusu ürün/hizmet bir sözleşme çerçevesinde hazırlanıyorsa burada belirtilen veya yasal mevzuattan kaynaklanan niteliklerdir. Bu niteliklerin sağlanamaması ise doğrudan sözleşmeye veya yasal düzenlemelere aykırılık sonucunu doğurur.

Kalite yönetimi, yukarıda tanımlanan anlamda kalitenin sağlanması konusunda makul güvence vermek için kullanılan politika, prosedür, süreç ve mekanizmaların tümüdür. Kalite yönetimi sadece son üründe/hizmette olması istenen niteliklerin olup olmadığına bakmak ve "*kaliteli/kalitesiz*" gibi bir sonuca ulaşmak değildir. Kalite yönetimi, ürünün/hizmetin istenen niteliklerde tasarlanıp üretilmesi amacıyla en baştan bazı ilkelerin/yolların belirlenmesi, bu sürecin çeşitli aşamalarda kontrol edilmesidir. Ürünün/hizmetin gereken nitelikleri taşıyıp taşımadığı konusu, kalite yönetimi sürecinin sadece bir parçasıdır. Kalite yönetimi sadece ortaya çıkan ürün/hizmetle ilgilenmez, ürünün/hizmetin tüm geliştirme süreciyle de ilgilenir. Böylece istenen sonuçların tekrar edilebilir olması sağlanır. Kalite yönetimi iki aşamaya ayrılabilir:

- Kalite güvencesi: Ürün/hizmetin yaşam döngüsü boyunca tüm aşamalarını belirlenen standart ve gereksinimleri tam olarak karşılayacak şekilde oluşturulmasına yönelik planlı faaliyetler bütünüdür. Kalite planlaması ve hata önleme yaklaşımlarını içerir. Böylece tüm süreçler bütün olarak ele alınarak kalitenin sürekliliği ve iyileştirilmesi sağlanır. Sonuçta tüm aşamalar ürün/hizmetin istenen nitelikleri taşımasını güvenceye alacak biçimde düzenlenir ve iyileştirilir.

- Kalite kontrol: Ürün/hizmetin belirlenen standart ve gereksinimlere uygunluğunu denetlemek için gerçekleştirilen doğrulama faaliyetleri ile bu kapsamda kullanılan yöntem ve araçların tamamıdır. Diğer bir deyişle, istenen nitelikleri taşıyıp taşımadığının kontrol edilmesidir. Belirlenen standart ve gereksinimlere uygunluk test edilerek, yetersizlik ve uyumsuzlukların önlenmesi amaçlanır.

Kalite yönetim sistemini kuran işletme, kalite politikasını belirlemiş, hedeflerini açıklamış, kalite konusunda yapılacakları tespit etmiş ve dökümantasyonunu yapmış olmalıdır. Kalite yönetim sistemi oluşturmanın faydaları arasında aşağıdaki hususlar sayılabilir:

- Kurumsallaşmaya katkı sağlayarak daha iyi yönetim sağlar,

- Tüm çalışanların kalite sürecine katılmasını, ortak olmasını olanak sağlar,

- Çalışanların motivasyonunu, kalitesini ve verimliliğini artırır,

- Süreçlerin belirlenmesi, sorunların hızlı çözülmesini ve hızlı bilgi akışını sağlar,

- Yetki ve sorumlulukların dağıtımını kolaylaştırır,

- Kalitede sürekliliği sağlar,

- Gereksinimlerin daha doğru anlaşılmasını sağlayarak memnuniyeti artırır,

- Kalitesizlik ve işlem maliyetlerini azaltır,

- Çalışanlar arasında kaliteye ilişkin iletişimi artırır,

- İşletmenin rekabet gücünü artırır,

- Kalitenin sürekli iyileştirilmesine bir alt yapı sağlar,

- Ürün/hizmetlere ilişkin gereksinimlerin takibini sağlar,

- Etkin bir yönetim yoluyla sağlıklı kararlar alınmasını sağlar,

- Ürün/hizmetin kabul görme düzeyini artırır, işletmenin imajını güçlendirir.

Kalite yönetimi, bir sistem yaklaşımıdır. Bir proje olarak görülemez. Kalite için bilgi sistemleri biriminde ayrı bir ekip görevlendirilmesi tercih edilir; ancak hep belirtildiği üzere çok küçük işletmelerden bu beklenmemelidir. Küçük işletmelerde diğer görevlerinin yanında bu görevi de üstlenen çalışanlar olabilir. Ancak bilgi sistemleri kalite ekibinin hem ürün/hizmetin geliştirme aşamalarında bilgi sistemleri biriminde, hem de niteliklerin belirlenmesi aşamasında iş birimlerinde görevlendirilen kişilerle beraber çalışması gerekmektedir.

1.1.2.7.3.1. Kalite Yönetiminin Değerlendirilmesi

İşletmede bilgi sistemleri kalite yönetiminin değerlendirilmesi sırasında, yine işe önce konu hakkında farkındalığın olup olmadığının değerlendirilmesiyle başlanır. Daha sonra bu konuda geliştirilen politika, prosedür, süreç ve mekanizmalar incelenip bunların sahada uygulanma derecesi değerlendirilir. Bu noktada kalite yönetimiyle ilgili dokümanlar gözden geçirilmeli ve bilgi sistemleri tarafından üretilen ürün/hizmetlerin her birine ilişkin gerek bilgi sistemleri, gerek iş tarafı gerekse de yasal düzenlemeler/sözleşmelerden kaynaklanan gereksinimlerin belirlenip belirlenmediği ve bunların kontrolü, kontrol sonuçlarına göre alınan aksiyonlar incelenmelidir.

Diğer taraftan, kalite güvencesi sağlamak için kullanılan politika ve prosedürlerin incelenmesi, bunların sahadaki iş süreçlerine entegre edilip edilmediği değerlendirilmelidir. Yukarıda da belirtildiği gibi, kalite güvencesi, gerekli kontrollerin işin başlangıcından itibaren hayata geçirilmesiyle sağlanabilir, diğer durumlar (sadece son ürün/hizmete bakarak kalite sağlama çabası) kalite yönetimine ilişkin birer risk göstergesidir.

1.1.2.7.4. Performans Yönetimi

İşletmede bilgi sistemleri stratejisinin oluşturulması, bu stratejinin hayata geçirileceğinin garantisi değildir. Stratejik hedeflere ulaşılıp ulaşılmadığı, bu yolda ne kadar ilerlendiğinin ölçülmesi gerekir. Hep denildiği ve bu Çalışma Notu'nda da sıkça tekrar edildiği gibi, ölçülmeyen iyileştirilemez.

Performans yönetimi basit bir anlatımla hedeflerin, zamanında ve kaynakların verimli (sınırlar içinde) kullanımıyla gerçekleşmesi konusunda yönetime değerlendirme sağlayan süreçlerdir. Etkin bir performans yönetimi, performansı tanımlar, ölçme ve değerlendirme araçları kullanır ve performansa ilişkin geri bildirim sağlar. Performans yönetimi, yönetişimin temel süreçlerinden biridir. Stratejik hedeflere ulaşıp ulaşılmadığının ölçülmesi ve çıkan sonuçlara göre gerekli düzenlemelerin yapılmasını içerir. Diğer bir ifadeyle, performans yönetiminde bir ölçme, bir de ölçüm sonuçlarına göre iyileştirmelerin yapılma aşaması vardır.

Burada bilgi sistemleri veya işletme ayrımı yapılmamakla birlikte; performans yönetiminin amacı hem bilgi sistemleri düzeyinde, hem de kurumsal düzeyde aynıdır. Stratejik hedeflere belirlenen kısıtlar dahilinde ulaşılıp ulaşılmadığının ölçülmesi ve sürecin yönetilmesi önemlidir.

Performans ölçümünü yapmak için bir yöntem belirlemek gerekir. Ölçüm yöntemine göre kullanılacak kriterler/değerler değişebilir. Ancak ölçüm yönteminin, ölçüm zamanı geldiğinde değil, henüz strateji geliştirme aşamasında belirlenmesi gerekir. Bir diğer önemli nokta da, tutarlılık sağlaması ve maliyeti azalmak için, bilgi sistemleri performansının ölçümünde kullanılacak yöntemin, işletmenin diğer birimlerinde kullanılan performans ölçüm yöntemleriyle aynı olmasıdır.

1.1.2.7.4.1. Ölçüm Yöntemleri

Performans ölçümü yapmanın farklı yöntemleri vardır. İşletme kendi yapısına, büyüklüğüne, faaliyetlerine ve bulunduğu sektöre göre bir ölçüm yöntemi seçmeli/geliştirmeli ve tüm birimlerde bunun kullanılmasını sağlamalıdır.

Burada örnek olarak strateji ölçümünde en çok kullanılan yöntem olan Kurumsal Karne (Balanced Scorecard-BSC) yöntemi anlatılacaktır.

BSC, işletmelerde strateji performansını (başarımını) ölçmek için kullanılan bir yönetim aracıdır (Balanced Scorecard Institute, t.y.). Bu araç, kısa ve uzun dönemli amaçları; finansal veya finansal olmayan, işletme içi veya işletme dışı performans ve sonuç göstergeleri arasındaki ilişkiyi; neden sonuç hiyerarşisi içerisinde işletme stratejisine yansıtmayı amaçlar. Balanced (dengeli) ifadesiyle anlatılmak

istenen, sadece finansal değil, dört ayrı perspektifte ölçüm yapması, böylece yönetime daha dengeli bir bakış açısı sunmasıdır.

Ölçüm perspektifleri:

- Finansal → Kullanılan kaynaklar/edinilen sonuçlar bazında finansal ölçümler.

- Müşteri (iş tarafı) → Müşteriye sunulan ürün ve hizmetler bazında ölçümler.

- İç süreçler → İşletmenin iç süreçlerinin performansına ilişkin ölçümler.

- Kurumsal öğrenme, gelişim, kapasite → İşletmedeki insan kaynağı kapasitesi, eğitim faaliyetleri, yenilikçilik, teknolojik altyapı ve kapasite gibi, amaçların başarılmasında önemli olan faktörler bazında ölçümler.

Stratejik hedefler; misyon, vizyon ve stratejilerin "*gerçek*" işlere dönüştürülmüş halidir. Stratejik plan ancak stratejik hedeflerin "*yapılmasıyla*" gerçekleşmiş olur. İşte bu bahsedilen stratejik hedefler mutlaka yukarıda belirtilen dört perspektiften birinin alanına girer. Pratik olarak, özellikle küçük işletmelerde her bir stratejik hedef için bir iki metrik geliştirilmesi yeterli olur. Bu metriklere anahtar başarı göstergesi (Key Performance Indicator-KPI) denmektedir (KPI, t.y.).

KPI, belirli bir hedefin gerçekleşmesini ölçmeye yarayan göstergelerdir. Yukarıda belirtildiği üzere, her hedef için bir ya da iki KPI yeterli olur; ancak bu noktada işletmenin büyüklüğü de çok önemlidir. KPI seçilirken göz önünde bulundurulması gereken bazı noktalara aşağıda yer verilmektedir (Marr, 2021):

- KPI'lar işletmeye/birime/stratejiye özgü olmalıdır.

- Her bir KPI mutlaka belli bir stratejik hedefe ait olmalıdır.

- KPI'lar herkes tarafından anlaşılmalıdır. Her çalışan, yaptıklarının neye hizmet ettiğini ve işletmeye ne katacağını ve bunun ölçüleceğini bilmelidir. Bu, işi sahiplenmeyi de getirir.

- Veri ihtiyacı, ölçüm zamanı/periyodu, kimin ölçeceği, kimin yorumlayacağı ve kime rapor edileceği önceden belirlenmelidir.

- Ölçümün baz alacağı verinin güncelliği ve bütünlüğü kesinlikle sağlanmalıdır.

- Ölçüm sonuçlarının açık, anlaşılır ve akılda kalıcı şekilde raporlanması önemlidir.

- KPI'lar gözden geçirilmelidir. Stratejiyi gözden geçirmek kadar, KPI'ları gözden geçirmek de önemlidir. Amaca hizmet etmeyen, hazırlanması saatler süren, anlamlandırılması zor bir KPI kullanılmamalıdır.

Başlangıçta işletme stratejilerinin ölçülmesi için geliştirilen BSC, daha sonra bilgi stratejilerine uyarlanmış ve IT-BSC olarak adlandırılmıştır. Kavram olarak aynıdır; ancak ölçüm perspektifleri biraz farklıdır. Bu perspektifler:

- İş birimleri: İş birimlerince bilgi sistemlerinin işe katkısı, etkinliği.

- Kullanıcılar: Kullanıcı memnuniyeti. İş birimleri kullanıcıları kadar, eğer dışa açık ürün/hizmet geliştiriyorsa dış kullanıcıların da memnuniyeti.

- Bilgi sistemleri iş süreçlerinin performansı.

- Bilgi sistemlerinin insan kaynağı, yetkinleşme, gelişim ölçütleri ve altyapı kapasitesi.

BSC en geniş kullanım alanı bulan stratejik performans ölçüm aracı olmasına rağmen, kolay bir yöntem değildir ve her işletmede görülmesi mümkün olmayabilir. Benzer fakat daha basit yöntemler kullanılabilir. Ölçüm perspektifleri belirlenmeden doğrudan hedeflere ait KPI'lar geliştirilebilir ve bunlar kullanılabilir. Burada en önemli kriterler; ölçülebilir, ölçmesi kolay, tekrarlanabilir, hedefle ilişkisi kolayca görülebilen ve sonuçları kolayca yorumlanabilen metrikler geliştirilmesidir. Performans ölçümü asla bir yığın veri, rapor ve istatistikten oluşmamalıdır. Sürdürülemeyecek karmaşıklıkta yöntemler seçilmemelidir.

1.1.2.7.4.2. Performans Yönetimin Değerlendirilmesi

Denetim sırasında denetçinin görevi bizzat bilgi sistemleri stratejisinin başarısını ölçmek olmamakla birlikte, bununla ilgili mekanizmaların kurulu ve işler halde olup olmadığının değerlendirilmesi gerekmektedir. Bilgi sistemlerine ilişkin performans yönetimi sürecinin olmaması veya etkin şekilde işlememesi doğrudan risk göstergesidir. Bu durumda, bilgi sistemleri yatırımlarının işe yarayıp yaramadığı anlaşılamaz, bilgi sistemleri-iş uyumu da sağlanamaz.

Ölçüm metriklerinin kim tarafından nasıl hazırlandığı, üzerinde tüm taraflarca anlaşmaya varılıp varılmadığı değerlendirilmelidir. Metriklerin yukarıda belirlenen kriterlere uyup uymadığı değerlendirilmelidir. Bunun gibi, ölçüm zamanlarının belirlenip belirlenmediği (en az yılda bir, en fazla ayda bir olması önerilir), ölçümle ilgili roller ve sorumluluklar, ölçüm sonuçlarının yorumlanması ve değerlendirilmesiyle ilgili sorumluluklar yazılı olmalıdır. Denetçi, hem performans yönetimi sürecini, hem ölçüm için seçilen yöntemi, hem geçmiş ölçümleri hem de ölçüm sonuçlarına göre alınan aksiyonları ve bunların sahaya yansımasını değerlendirmelidir.

1.1.2.7.5. Dış Kaynak Yönetimi

Bilgi sistemlerinde dış kaynak kullanımı 1960'lı yıllardan günümüze kadar uzanan bir geçmişe sahiptir. Pek çok işletme için bilgi sistemlerinin yüksek tutarda yatırım ve yetkin insan kaynağı gerektirmesi, dış kaynak kullanımını zorunlu kılmıştır. Nitekim günümüzde dış kaynak kullanımı (outsourcing) stratejik yönetimin önemli konularından biri olmuştur. İşletmenin asıl faaliyetlerine odaklanarak, bilgi sistemleri de dahil olmak üzere bazı fonksiyon veya faaliyetlerinin dış kaynak kullanımı yoluyla temin etme uygulamalarının yaygınlaştığı görülmektedir.

1.1.2.7.5.1. Dış Kaynak Kavramı

Dış kaynak kullanımı, en basit anlatımla, bir işletmenin ürün veya hizmetlerinin bir kısmını kendi bünyesinde gerçekleştirmek yerine, başka bir işletmeyle anlaşarak ona yaptırmasıdır. Bir iş modeli olup, "*dış kaynak kullanımı*", "*dışarıdan temin*", "*dış kaynaktan alım*" şeklinde kullanılabilir. Bir başka tanıma göre, dış kaynak kullanımı, işletmenin normalde kendi geliştirdiği ürünü/hizmeti dışarıdan üçüncü bir tarafa yaptırmasıdır (Twin, 2021). Günümüzde maliyet avantajları nedeniyle işletme fonksiyonları için de dış kaynak kullanımına başvurulmaktadır. Aslında dış kaynak kullanımı, işletmenin asıl işine odaklanıp, uzmanlık alanı dışındaki faaliyetler için uzman taraflardan hizmet alması, üretim yaptırması anlamına gelmektedir. Burada tabi temel güdü maliyet avantajı sağlamasıdır.

Dış kaynak kullanımı, asıl olarak bilgi sistemlerine özel bir kavram değildir. İleride belirtileceği üzere, çeşitli sebeplerle bu iş modeli birçok farklı sektörde uygulanmakta ve güncelliğini korumaktadır. Ancak bu Çalışma Notu'nda sadece bilgi sistemleri bazında dış kaynak kullanımı ele alınacaktır. Ama önce bazı temel bilgilere değinilecektir.

Bir işletmenin iş fonksiyonlarının bir ya da birçoğunu dışarıdan temin etmesine, iş süreçlerinin dışarıdan temini anlamına gelen "*bussiness process outsourcing*" denir. Bilgi sistemlerine ilişkin birtakım fonksiyonların dış kaynak kullanımı yoluyla elde edilmesi de bu tanıma girer.

Dış kaynak kullanılmasının temelde teknolojik, ekonomik ve stratejik faydaları bulunmaktadır. Bu faydalar maliyet etkinliği, etkin performans ve genel memmuniyet başlıkları altında da toplanabilir. Daha spesifik olarak dış kaynak kullanımının tercih nedenleri arasında aşağıdaki hususlar sayılabilir:

- Teknolojik gelişmeleri takip edebilme. İleri teknolojiye erişebilme.

- Maliyetlerin azaltılması. İşletmede bilgi sistemleri yatırımlarının azaltılması ve buna ek olarak hizmet sağlayıcıların ölçek ekonomisi.

- Verimlilik artışı. Sadece esas faaliyet konusuna odaklanmak. Peter Drucker'ın ifadesiyle: *"En iyi yaptığını yap, gerisini dışarıya yaptır" ("Do what you do best, outsource rest").*

- Farklı hizmet sağlayıcılar arasında seçim yapabilme.

- Kapasiteyi ihtiyaca-iş modeline göre edinme.

- Bilgi sistemleri risklerinin paylaşımı.

1.1.2.7.5.2. Dış Kaynak Kullanım İlkeleri

Uluslararası Menkul Kıymetler Komisyonları Örgütü (IOSCO), sermaye piyasalarında görev alan ve ilgili ülkenin düzenleyici otoritesince yetkilendirilen işletmelerin alandan bağımsız olarak dış kaynak kullanımına ilişkin bir rapor yayınlamıştır. Bu raporda, işletmelere dış kaynak kullanımında rehberlik eden bazı ilkeler benimsenmiştir (IOSCO, 2021). Söz konusu ilkeler aşağıdaki gibi özetlenebilir:

1. İşletmeler dış kaynak sağlayıcılarını (hizmet/servis sağlayıcıları) dikkatle seçmeli ve süreci yönetmelidirler. Servis sağlayıcı seçimi aşağıda risk bölümünde incelenmiştir. İşletmenin potansiyel servis sağlayıcısını seçmek için yazılı süreçlere sahip olması ve sözleşme imzalandıktan sonra da sözleşme yönetimi sürecini işletmesi gerekir.

2. Yazılı anlaşma imzalanmalıdır. Bu konu, sözleşme konusu ürün/hizmetten bağımsız olarak işletmede özellikle hukuk biriminin yönlendirmesine ihtiyaç duymaktadır. Sermaye piyasası mevzuatında da dış kaynak yoluyla hizmet alınması esnasında düzenlenecek sözleşmelere dair birtakım gereksinimler yer almaktadır.

3. Hem servis sağlayıcı, hem de işletmenin kendi bünyesinde sözleşme konusu ürün/hizmetlere yönelik bilgi güvenliğini ve iş sürekliliğini sağlayacak kontroller hayata geçirilmiş olmalıdır.

4. İşletme, servis sağlayıcının işletmenin bilgilerini koruduğu ve üçüncü taraflarla paylaşmadığı konusunda gerekli kontrolleri kurmalıdır.

İşletmedeki müşteri bilgilerinin servis sağlayıcıya transferi ve/veya servis sağlayıcı tarafından bunlara erişilmesinin söz konusu olduğu durumda müşterilerin haberdar edilmesi değerlendirilmelidir.

5. İşletme, dış kaynak kullanımından dolayı maruz kaldığı riskler için uygun bir yöntemle risk yönetimi yapmalıdır.

6. İşletme, servis sağlayıcının düzenleyici otoritelerden veya işletmenin kendisinden kaynaklanacak bilgi taleplerine ve sistemlere erişim taleplerine uygun yanıt verilmesini garantileyecek kontrolleri düzenlemelidir. Sermaye piyasası mevzuatında da konuya ilişkin düzenlemeler mevcuttur.

7. İşletme, servis sağlayıcı ile yapılan anlaşmalarda, anlaşmanın herhangi bir şekilde sonlanmasına ilişkin hükümleri düzenlemelidir. Bu hükümler, sözleşme konusu ürün/hizmetlerin ait olduğu iş süreçlerinin normal çalışma düzeninin etkilenmemesini sağlamak amaçlıdır ve yine sermaye piyasası mevzuatında da konuya ilişkin düzenlemeler mevcuttur.

1.1.2.7.5.3. Dış Kaynak Kullanımı Riskleri ve Üstesinden Gelinmesi

Dış kaynak kullanımı önemli maliyet avantajları nedeniyle kullanılmasına karşın, bazen işletmeye sözleşme bedelinden daha fazlasına mal olabilmekte ve bazı özgül riskleri de beraberinde getirmektedir. İşletme, sözleşme konusu hizmeti/ürünü kendisinin yapması durumunda karşı karşıya kalacağı bazı risklerden kurtulmuş olabilir; ancak bu sefer de yeni risklere maruz kalır. Bu risklere aşağıda yer verilmektedir (Soucy, t.y.):

a. Kontrol Kaybı

İşletme, sözleşme konusu ürünü/hizmeti kendi bünyesinde geliştirse, sürecin her aşamasında %100 kontrol sahibi olacaktır. Ancak dışardan teminde sürece bu derece hakimiyet mümkün değildir.

Bunun üstesinden gelmek için sözleşme hükümlerinde bazı kontrollerin düzenlenmesi gerekmektedir. Bu kontrollere örnekler aşağıda verilmiştir:

- Servis sağlayıcı bünyesindeki iletişim noktaları ve bunlarla iletişim yönteminin belirlenmesi,
- Raporlama türlerinin belirlenmesi (periyodik raporlar, içerikleri, zamanlaması, olağan dışı durumların raporlanması),
- Ürünün/hizmetin ölçülebilir olmasını sağlamak için metriklerin geliştirilmesi,

- Dış kaynak kullanımı her ne kadar sözleşme konusuna yatırım yapılmaması için tercih edildiyse de yine de minimum bir kişinin sözleşmenin teknik hususları konusunda işletme bünyesinde istihdam edilmesi (sözleşme yönetimi yapacak gruba dahil de olabilir).

b. Servis Sağlayıcının Seçimi

Doğru servis sağlayıcının seçimi, dış kaynak kullanımının başarılı olmasında kritik bir karardır. Bu nedenle, servis sağlayıcının seçimi, başlı başına bir takım kriterlerin geliştirilmesini gerektirmektedir. Bunun için aşağıdaki hususlar bir başlangıç olabilir:

- Servis sağlayıcının kaç senedir sektörde olduğu (konu hakkındaki tecrübesini gösterir),
- Mali yapısı,
- Personel havuzu (sahip olduğu personel profili, sayısı, yetkinlikleri, organizasyon şeması),
- Personel hareketliliği (servis sağlayıcının yetkin ve tecrübeli personeli bünyesinde ne kadar tutabildiğini gösterir),
- Teknik kapasiteleri (sundukları ürün/hizmetler ve bu konuda sahip olunan yetkinlik),
- Gizlilik ve güvenlik yaklaşımları, sahip olunan sertifika ve standartlar, geçirmiş oldukları denetimler,
- Servis sağlayıcının işletmeyle organik bağı olup olmadığı (organik bağı olması farklı, olmaması farklı risk faktörlerine işaret eder),
- Referansları.

c. Gizlilik ve Güvenlik

Dış kaynak yönetimi, işin doğası gereği, işletmenin bazı kritik ve stratejik öneme sahip varlıklarını/iş süreçlerini/ticari sırlarını servis sağlayıcıya açmasını gerektirebilir. Bu da beraberinde gizlilik ve güvenlik riskini getirir. Gizlilik ve güvenlik riski, işletmelerin bilgi sistemlerinde dış kaynak kullanımını tercih etmemesinde en önemli nedenlerden biri olarak görülür. Bunun üstesinden gelmenin en iyi yollarından biri sözleşmeyi hukuki olarak bu konuda güçlü kılmaktır.

Servis sağlayıcının bünyesinde yaşadığı bilgi güvenliği olaylarının ve cevaben alınan aksiyonların (özellikle işletmeyi ilgilendirdiği ölçüde) mutlaka işletmeye bildirilmesi sözleşmeye bağlanmalıdır.

Bilgi sistemleri hizmetlerinin (tümünün veya bir alt kümesinin) dış kaynak yöntemiyle tedarik edilmesi, başlı başına bu madde üzerinde düşünmeyi gerektirir. Bu konunun değerlendirilmesi, bir önceki madde (servis sağlayıcı seçimi) ile başlar ve sözleşme hükümlerinin düzenlenmesiyle devam eder.

Sermaye piyasası mevzuatının gerektirdiği gibi, işletme dış kaynaktan tedarik sürecinde güvenlik ve gizlilikten ödün vermemelidir. İşletme, kendi güvenlik yaklaşımlarından, kendi kabul ettiği minimum seviyeden daha azına razı olmamalıdır. Diğer bir ifadeyle, servis sağlayıcı da en az işletmenin kendisi kadar gizlilik ve güvenliğe önem vermelidir. Doğal olarak, bunun kanıtı da ölçülebilir olmalıdır.

d. Sınırlar ve Sorumluluklar

Dış kaynak kullanımında, özellikle süresi uzun sözleşmelerde çok sık rastlanan ve işletme ile servis sağlayıcı arasında uzun tartışmalara yol açan konulardan biri de sözleşmede iki tarafın sınırlarının, işin kapsamının, yapılacakların ve yapılmayacakların sınırlarının çok net çizilememesidir. Bu durum aslında iki tarafın da aleyhine olup, sözleşme konusu işin kalitesini etkiler bir noktaya gelebilir. Bunu engellemenin en iyi yollarından biri, sözleşmede söz konusu hizmetin/ürünün en ince detayına kadar ve mutlaka ölçülebilir şekilde tanımlanması, ayrıca olağan dışı durumların, yeni taleplerin nasıl ele alınacağının ve sürecin nasıl ilerleyeceğinin sıkı hükümlere bağlanmasıdır.

e. Alan/İş Bilgisinin Noksanlığı

İşletme, bir hizmeti/ürünü dışarıdan temin etmeye karar verdiyse, bununla ilgili alan bilgisini de uygun yöntemle servis sağlayıcısına sağlamak durumundadır. Aksi takdirde elde edilecek ürün/hizmette eksikler olacaktır. Benzer şekilde, işletme bünyesindeki bilgi sistemleri birimi çalışanlarının mevcut bilgi/becerilerini kullanılmaması nedeniyle gerilemesi ve yeni bilgi/beceriler elde edilememesi durumları da ortaya çıkabilir. Tüm bunlar bu birim çalışanlarının motivasyonunu düşürerek, işletmeye katkılarının azaltılmasına neden olabilir.

f. Öngörülemeyen Maliyetler

Dış kaynak kullanımı işletmeye maliyet/hız avantajı sağlıyor olabilir; ancak dış kaynak kullanımının kendi özgül riskleri olduğu gibi, özgül maliyetleri de vardır. Bunlar aşağıdaki şekilde sıralanabilir:

- İşletmenin bir hizmeti/ürünü kendi geliştirmesi yerine hazır olarak dışarıdan tedarik etmeye karar vermesi, başlı başına bir değerlendirme sürecidir. Böyle bir karar titiz bir değerlendirme sonucunda verilmelidir, bu da bir maliyet unsurudur.
- İşletme, servis sağlayıcıyı seçmeden önce adayları çeşitli kriterlere göre değerlendirmelidir (mali güç, tecrübe, teknik kapasite ve yetkinlik). Bu konu sermaye piyasası mevzuatında düzenlenmiştir.
- Seçilen servis sağlayıcıya sözleşme konusu ürüne/hizmete ait bilgi transferi yapılmalıdır.
- Dış kaynak kullanımı kararının verilmesi işletmede istihdam edilen personelde değişiklik gerektirebilir, bu durumun da işletmeye belli bir maliyeti olabilir.
- Sözleşme yönetimi için personel ayırma, asla unutulmaması gereken bir noktadır. Dış kaynak kullanımı otonom bir süreç olmadığından, diğer tüm süreçler gibi birilerinin sahiplenmesini gerektirir.

g. İşletmenin Tecrübesizliği

Dış kaynak kullanımında, tüm riskler servis sağlayıcıya veya sözleşmenin tasarımına bağlı değildir. İşletmenin dış kaynak yönetimi tecrübesinin başarıda bir rolü bulunmaktadır. Özellikle ilk defa dış kaynak kullanımı yapacak işletmeler için bu önemli bir risk faktörüdür. Bu konuda tecrübesiz işletmeler, öncelikle dış kaynak yönetimi hakkında biraz bilgi edinmeli ve aşağıdaki noktaları akılda tutmalıdır:

- Dış kaynak kullanımı iş modelinin kendilerini masraftan tamamen kurtarmayacağı, aksine bu modele özgü bazı maliyetlerin ortaya çıkacağı,
- Özellikle ana iş fonksiyonlarından olmayan (işletmenin tecrübesi ve bilgisinin olmadığı, bilgi sistemleri gibi) bir ürün/hizmet dış kaynak kullanımıyla sağlanacaksa, bu süreci teknik olarak yönetecek en az bir personeli istihdam etmesi gerektiği,
- En nihayetinde dış kaynak yönetiminin bir defaya mahsus bir iş değil, bir yönetim süreci olduğu, dolayısıyla zaman ve iş gücü gerektiren ve belli bir maliyeti olan bir iş olduğu.

h. Ürün/Hizmetin Kalitesi

İşletme, servis sağlayıcıdan edindiği ürünü/hizmeti ölçmeli ve buna göre aksiyon almalıdır. Bunun için ilk olarak söz konusu ürün/hizmet sözleşmede en ince detayına kadar, ölçülebilir metriklerle tarif edilmelidir (hizmet seviyesi). Daha sonra da ölçüm zamanları, yöntemleri ve ölçüm sonuçlarına göre sürecin nasıl işleyeceği belirlenmelidir. Ölçüm zamanı ürünün/hizmetin teslim zamanı ve bir kereye mahsus bir eylem olmamalıdır. Sözleşme süresince belirli aralıkla ölçümleri gerçekleştirmek, hataların çok geç olmadan tespitini sağlayabilir.

i. Servis Sağlayıcının Yerleşimi

İşletme, dış kaynak kullanımı sırasında servis sağlayıcı seçimini farklı modellere göre yapabilir. Bunların her birinin de kendine göre riskleri olabilir. Bu modellere aşağıda yer verilmektedir.

- **Denizaşırı dış kaynak (offshore outsourcing):** Bu terim, esasen dış kaynak kullanımına dayanan iş modelinin ortaya çıkış şeklidir. Burada işletme, servis sağlayıcı olarak başka

bir ülkede yerleşik bir işletmeyi seçer. Özellikle iş gücü maliyetlerinin düşük olduğu ülkelerde bu model işletmeye ciddi maliyet avantajı sağlar. Ancak bu model aynı zamanda politik olarak da önemli bir modeldir. Çünkü özellikle finansal krizlerin yaşandığı yıllarda/ülkelerde, işletmelerin farklı ülkelerden dış kaynak tedariğine gitmesi eleştirilir. Bu durum ülkede iş kaybına yol açar. Burada aslında iki ayrı seçenek söz konusudur:

- **Yakın dış kaynak (nearshore outsourcing):** İşletmenin kendisiyle aynı coğrafi bölgeden fakat farklı bir ülkeden servis sağlayıcısını seçmesidir. Bu modelde iş gücü maliyetinden kaynaklanan kazanç azalabilir; ancak iletişim bariyeri de çok fazla yükselmez. Saat dilimi sorunu oluşmayacağından çevrim içi etkileşimleri kolaylaştırır. Kültürler yakın olasağından iletişim de kolay olur.
- **Uzak dış kaynak (distant outsourcing):** Bu modelde ise, işletme servis sağlayıcı olarak kendisinden çok uzak bir coğrafi lokasyonda yerleşik bir servis sağlayıcıyı seçer. Burada büyük ihtimalle seçilen lokasyona da bağlı olarak iş gücü maliyetinden sağlanan avantaj büyüktür. Ancak gerek kültürel farklar, gerek zaman farklarından dolayı iletişim bariyeri de büyüktür. İletişim bariyerini azaltmak için dikkatli bir planlama yapmak gerekir.

- **Yerel dış kaynak (onshore/domestic outsourcing)**: İşletmenin dış kaynak hizmet sağlayıcısı olarak kendisiyle aynı ülkede yerleşik bir işletmeyi seçmesidir. Burada iş gücü maliyetinden sağlanacak avantaj çok fazla olmayabilir. Ancak, işletmeyi bu tercihe yönelten başka kriterler vardır. Bu kriterlerden biri de, işletmenin tabii olduğu yasal düzenlemelerde dış kaynak iş modeline ilişkin bazı özel gereksinimler olmasıdır.

j. Servis Sağlayıcının Değişimi

Dış kaynak kullanımı sürecine başlamadan önce, hangi servis sağlayıcı seçilirse seçilsin, değiştirilmesi gereken durumların ortaya çıkabileceği unutulmamalıdır. Böyle bir durum ortaya çıktığında panik ve kaos ortamı yaşamamak için, bunu baştan kabullenip bir plan da bu durum için hazırlamak gerekir. Servis sağlayıcı niye değiştirilir?

- Her sözleşmenin bir süresi vardır, olmalıdır. Sözleşme sonunda ise yenileme/uzatma hükümleri bulunur. Günümüz ekonomik şartlarında bir sözleşmenin yıllarca sabit maliyetle yenilenmesi gerçekçi değil. Yenilenme süresi geldiğinde yeni bedel işletmeye fazla gelebilir.

- İşletme servis sağlayıcıdan memnun olmayabilir. Bilindiği üzere, her sözleşmede ceza maddeleri olur. Sözleşme konusu ürün/hizmet istenildiği gibi olmadığında bu maddeler işletilir. Ancak bu durumun çok fazla tekrar etmesi, devamlı ceza kesme yoluna gidilmesi çok da arzu edilen bir durum değildir. Cezai maddelerin işletilmesine sebep olan durumların altında yatan nedenleri iyi analiz edip düzeltmek gerekir, düzelmiyorsa da alternatifleri değerlendirmenin zamanı gelmiş demektir.

- İşletme, hangi sebepten olursa olsun, dışarıdan tedarik ettiği ürünü/hizmeti artık kendi bünyesinde gerçekleştirmek isteyebilir.

- Her sözleşmede en az iki taraf olduğundan, servis sağlayıcı da herhangi bir nedenle sözleşmeyi sonlandırmak isteyebilir. En sorunlusu da, sözleşme normal süresinden önce beklenmedik şekilde sonlanabilir. Özellikle bu durum işletmenin iş fonksiyonlarının sürekliliğini ciddi olarak tehdit eder. İşte bu durumların dış kaynak kullanımına başlamadan önce düşünülüp sözleşmeye buna uygun kontroller eklenmesi ve işletme içinde bir hazırlık yapılması gerekir. Bir nevi işletmenin dış kaynak tedariğine ilişkin "*B*" planının hazırlanması gerekir. Buna "*çıkış stratejisi (exit strategy)*" denir.

Strateji bölümünde anlatıldığı üzere, strateji bir amaca ulaşmak için planlama yapmaktır. Buradaki amaç ise, işletmenin sözleşme imzaladığı hizmet sağlayıcı ile sorunsuz bir şekilde (tüm haklarını alarak ve en önemlisi "*sözleşmeye konu olan ürün/hizmetlerin ait olduğu iş süreçlerini*

kesintiye uğratmadan") ilişkisini kesmektir. Bu strateji hazırlanırken aşağıdakileri göz önüne almak gerekir:

- İşletmede çıkış stratejisi hazırlanırken yazılı dokümanlar oluşturulmalı (izlenecek yol sadece akılda tutulmamalı),
- Çıkış sürecinde işletmede kimlerin görevli olacağı belirlenmeli,
- Servis sağlayıcıdan teslim alınacak her türlü fiziki veya elektronik ortamdaki materyal/bilgi/varlık, bunların transfer yöntemi yazılı olarak belirlenmeli ve sözleşmeye de eklenmeli,
- Alt yükleniciler varsa bununla ilgili düzenlemeler olmalı,
- Sözleşme işletme tarafından vaktinden önce sonlandırılıyorsa bununla ilgili maliyetler dikkate alınmalı,
- Çıkış sürecine ilişkin ortalama bir zaman hedefi belirlenmeli,
- Çıkış sürecinde yapılacak toplantılar belirlenmeli,
- Personele (veya yeni servis sağlayıcıya) yapılacak bilgi aktarımının içeriği belirlenmeli,
- Başarılı bir çıkış için kriterler belirlenmeli ve çıkış sonrası ölçülmeli.

k. Yoğunlaşma

Bu durum özellikle servis sağlayıcıların belli konularda uzmanlaştıkları ve sayıca az oldukları durumlarda ortaya çıkar. Servis sağlayıcılar bir çeşit "*piyasayı kontrol eder*" duruma ulaştıklarında, sözleşmelere işletme tarafından konulması istenen hükümleri kabul etmezler (işletmenin uymakla yükümlü olduğu mevzuat tarafından zorunlu olanları bile). Benzer şekilde, sunulan hizmetler için daha yüksek ücret talep ederler. Ayrıca, pazardaki gücüne güvenerek sunulan hizmetlerin iyileştirilmesi ve geliştirilmesi, teknoloji alanında büyük yatırımlar yapılması hususunda daha az istekli olurlar. Yoğunlaşma beraberinde servis sağlayıcının maruz kaldığı rekabeti azaltacağından, sunacağı hizmetin kalitesini de düşürür.

Bunun dışında, örneğin birçok sermaye piyasası kurumunun aynı konuda aynı servis sağlayıcıdan hizmet alması da sistemik riski artırıcı bir faktör olarak görülmektedir. Servis sağlayıcının yaşayacağı teknik sorunlar, hizmet sunumundaki gecikmeler ve yetersizlikler, işletmenin faaliyetlerini önemli ölçüde etkileyebilir.

l. Gözetim

İşletme tarafından dışarıdan temin edinilen ürün/hizmetlerin ait oldukları iş fonksiyonlarının düzenleyici otorite tarafından denetlenmesi konusu da ayrı bir risk faktörüdür. Özellikle düzenleyici otorite tarafından istenen tüm bilgi/belgenin zamanında alınabilmesi ile düzenleyici otorite yetkililerinin servis sağlayıcı nezdinde gerekli bilgi ve belgeye erişim hakkı sözleşmede mutlaka yer almalıdır. Bu gereksinim ülkemiz sermaye piyasası mevzuatında da bir zorunluluk olarak düzenlenmiştir. Bunun yanı sıra, işletmenin hizmetlere yönelik sözleşmede belirtilen koşulların sağlanıp sağlanmadığına yönelik olarak kendisinin de servis sağlayıcı nezdinde denetim yapma hakkı (right to audit) düşünülmeli ve gerekli görülüyorsa bu konu sözleşmeye eklenmelidir.

m. Bağımlılık

İşletmenin çok fazla ürünü/hizmeti tek bir servis sağlayıcıdan temin etmesi bir risk faktörüdür. Bu durumda işletme tek bir servis sağlayıcıya aşırı bağımlı hale gelmiş olabilir. Bu servis sağlayacının yaşayacağı teknik sorunlar veya hizmet sonumundaki yetersizlikler işletmenin aldığı hizmetlerde aksamalara yol açacak; bu durum da faaliyetlerini olumsuz etkileyecektir. Bu riski berteraf etmek için farklı ürün/hizmetlerin farklı servis sağlayıcıları aracılığıyla edinilmesi alternatif olarak düşünülebilir.

1.1.2.7.5.4. Sözleşme Yönetimi

Dış kaynak yoluyla sağlanacak hizmetler bir sözleşme kapsamında gerçekleştirilir. Ancak dış kaynak kullanımı, buna ilişkin sözleşmenin imzalanmasıyla bitmez, kendi içinde yönetilmesi gereken

bir süreçtir. Sözleşme yönetimi (contract management) terimi bunu ifade eder. Sözleşme yönetiminde amaç basit olarak, imzalanan sözleşmeden beklenen faydanın sağlanmasıdır. Sözleşme yönetimi, işletmede bir sözleşmenin imzalanmasından da önce başlayan (karar alma, servis sağlayıcı seçimi), sözleşmenin oluşturulması, imzalanması, icrasıyla devam eden ve sözleşmenin bitimiyle veya yenilenmesiyle tekrar icra aşamasına dönen bir süreçtir. Sözleşme imzalandıktan sonra, işletmenin ihtiyaçları ve sözleşmenin icrası kapsamında sürekli bir değişim içindedir ve bu değişimin doğru takibi önemlidir. Bu nedenle, işletmede bir sözleşme aktif olduğu, yaşadığı sürece, bunun yönetimi de yapılmalıdır. Sözleşme yönetimi, sistematik ve verimli olma, sözleşmenin değişiminin takibini sağlama, operasyonel ve finansal performansı artırma, riskleri azaltma ve istenmeyen durumlar için tedbirler alma faydaları sağlar. Sözleşmelerin yönetimini standarda bağlayarak, kaynak tasarrufu sağlar.

Sözleşme yönetimi veya "*sözleşme yaşam döngüsü yönetimi*" (contract life cycle management-CLM), sözleşmelerin imzalanmasından önceki başlatma, müzekare, düzenleme ve onay süreçleri ile imzalandıktan sonraki yürütme, izleme, denetim, raporlama ve yenileme süreçlerinin yönetimini kapsar. Esasen sadece dış kaynak kullanımıyla ilgili değildir; daha geniş bir kullanım alanı vardır. Bu süreç, dış kaynak kullanımı sözleşmeleri, satın alma sözleşmeleri, fikri mülkiyet hakları, gizlilik anlaşmaları, lisanslama sözleşmeleri gibi bir takım yükümlülükler içeren tüm sözleşmeleri kapsamaktadır.

Sözleşme yönetimi, işletmenin finans, hukuk, satın alma birimleri ile sözleşme konusu ürün/hizmet hakkında alan bilgisi bulunan birimi (konumuz özelinde bilgi sistemleri) içine alan bir ekip işidir. Ayrıca akılda tutulmalıdır ki, sözleşme yönetimi bir miktar esneklik gerektirir ve esasen bir çatışma yönetimidir.

Sözleşme yönetimi temel olarak aşağıdaki süreçlerden oluşur (buraya kadar dış kaynak kullanımı kararının verildiği ve servis sağlayıcının/tedarikçinin seçildiği varsayımıyla):

- Sözleşmenin yazılması (ki bu süreç çokça pazarlık ve değişiklik gerektirir),
- Sözleşmenin onaylanması,
- Sözleşmenin işletime alınması (ürün/hizmetin geliştirilmeye/sunulmaya başlaması, belirlenen plana göre durum raporları ile benzeri geri bildirimlerin ve toplantıların yapılması, kısaca sözleşme yükümlülüklerinin yerine getirilmesi),
- İzleme (gerek taraflarca sözleşmeye uyumun değerlendirilmesi, gerekse de sözleşme konusu ürün/hizmetin planlandığı gibi hayata geçmesi),
- Çatışmaların çözümü,
- Sözleşmeye ek yapılmasını gerektiren durumların yönetimi,
- Yenileme/sonlandırma (sözleşmenin hayata geçtiği andan itibaren toplanan verilerin değerlendirilmesi ve yenileme/sonlandırma kararının verilmesi).

1.1.2.7.5.5. Dış Kaynak Kullanımının Değerlendirilmesi

Dış kaynak kullanımı değerlendirilirken, yine işe işletmede bu konudaki farkındalığın değerlendirilmesiyle başlanır. Burada, her işletmede dış kaynak kullanımı var mı? Tüm işlerini kendisi yapan işletmeler yok mu? soruları akla gelebilir. Bilgi sistemleri özelinde bakılırsa, bugün neredeyse tüm işlerini kendisi yapan bir işletme yoktur denebilir. Konunun başlangıcında, dış kaynak kullanımı tanımlanırken "*işletmenin normalde kendi bünyesinde geliştirdiği ürün/hizmet*" ifadesine de yer verilmişti. Bu tanıma göre bazı işler (örneğin internet bağlantısı hizmeti) dış kaynak kullanımı değil, sadece bir "*satın alma*" olarak görülebilir. Ancak burada da yine bir servis sağlayıcı seçimi, sözleşme, verilen hizmet, sözleşme yönetimi, hizmet seviyesi gibi konular mevcut olduğu ve bu iş bir süreye yayıldığı için bu şekilde bir satın alma işlemi de dış kaynak kullanımı olarak kabul edilebilir. Sonuçta her bilgi sistemleri birimi bir şekilde dış kaynak kullanımı işine girecektir.

Dış kaynak kullanımı sürecini değerlendirirken, tıpkı tüm diğer süreçlerin değerlendirmesinde olduğu gibi önce sürecin farkındalığından başlanmalıdır. İlgili tüm politika, prosedür ve kontrollerin önce varlığı, sonra da uygunluğu ve işlerliği değerlendirilmelidir. Konunun başından itibaren tüm anlatılanlar, bir şekilde bu kontrollerde ele alınmış olmalı, ilgili taraflarca biliniyor olmalı (işletme

içinde sürecin yönetilmesiyle görevlendirilmiş ve bilgi sistemleri ile diğer taraflardan oluşan bir yapının var olması ön şarttır) ve işletiliyor olmalıdır. İşletmede bilgi sistemlerine ait herhangi bir aktif sözleşmenin varlığı süresince (sözleşmenin yaşam döngüsü süresince) bunun yönetimiyle ilgili ve en az bir bilgi sistemleri çalışanını da içeren bir ekip işbaşında olmalıdır.

Örnek Sorular:

Soru 1: İşletmede bilgi sistemleri stratejisi geliştirmek için atılacak ilk adım hangisidir?

A) İşletmenin bilgi sistemleri biriminin organizasyon yapısını oluşturmak

B) İşletmenin fonksiyonları için gerekli olacak iş uygulamalarını belirlemek

C) Dış kaynak kullanımı yoluyla edinilecek bilgi sistemleri fonksiyonlarını belirlemek

D) İşletmenin kurumsal stratejisini incelemek

E) İş birimleriyle görüşerek ihtiyaçlarını belirlemek

Cevap: D

Soru 2: Aşağıdakilerden hangisi dış kaynak kullanımında işletmenin kontrol kaybı riskine karşı geliştirilebilecek kontrollerden değildir?

A) Sözleşme konusu iş hakkında gelişim raporları düzenlenmesi

B) Servis sağlayıcının güvenlik politikalarının incelenmesi

C) Sözleşme konusu iş hakkında ölçüm metriklerinin belirlenmesi

D) İşletme bünyesinde sözleşmenin teknik hususlarından sorumlu bir kişinin istihdam edilmesi

E) Servis sağlayıcı ile iletişim yönteminin belirlenmesi

Cevap: B

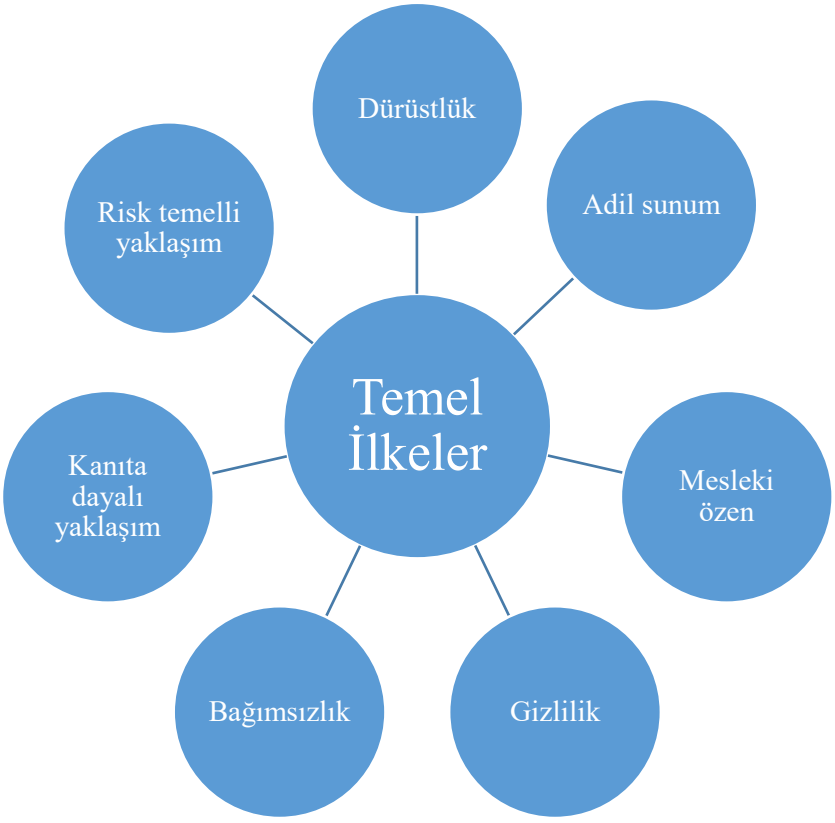
1.2. BİLGİ SİSTEMLERİ DENETİMİ

Bu bölümde, bilgi sistemleri denetimine ilişkin temel kavramlar tanımlanarak bilgi sistemleri denetim faaliyeti aşamalarıyla anlatılmaktadır.

1.2.1. Bilgi Sistemleri Denetim Kavramları

Denetim; ISACA terimler sözlüğünde "*Bir standarda veya bir dizi kılavuza uyulup uyulmadığını, kayıtların doğru olup olmadığını veya etkin ve etkili hedeflerin karşılanıp karşılamadığını kontrol etmek için yapılan resmi kontrol ve doğrulama*" olarak tanımlanmaktadır (ISACA, 2018). ISACA tarafından kabul gören tanımda bilgi sistemleri denetimi "*bir bilgisayar (veya bilgi) sisteminin varlıkları güvence altına alıp almadığı, veri bütünlüğünü sağlayıp sağlamadığı, kurumsal amaçlara etkin biçimde ulaşıp ulaşmadığı ve kaynakları verimli bir şekilde kullanıp kullanmadığını belirlemek amacıyla yapılan kanıt toplama ve değerlendirme sürecidir.*" Bilgi Teknolojisi Altyapı Kütüphanesi (ITIL) sözlüğünde de aynı şekilde tarif edilen denetim, Uluslararası Standartlar Teşkilatı ISO-19011 standart dokümanında "*Denetim kanıtlarının elde edilmesi ve denetim kriterlerinin ne ölçüde karşılandığının tarafsız olarak değerlendirilmesi için yapılan sistematik, bağımsız ve belgelenmiş süreç*" şeklinde ifade edilmektedir (TSE, 2018).

Denetimin bu genel tanımlamaları, bilgi sistemi denetimine ve konusundan bağımsız olarak bütün denetim alanlarına uygundur. Denetim kavramındaki unsurlara bakıldığında, temel olarak denetim kapsamında denetim konusunun karşılaştırıldığı bir referans standardın, kriterlerin veya ilkelerin olması gerektiği vurgulanmaktadır. Bununla birlikte, ISO-19011 standardında belirtilen etkili ve güvenilir bir denetim faaliyetini belirleyen 7 temel ilke aşağıdaki şekildedir (TSE, 2018):



Şekil 1: Denetim Faaliyeti Temel İlkeleri

Dürüstlük: Denetim çalışmalarının hiçbir etki altında kalmadan, adil, tarafsız, dürüst ve sorumluluk içinde yerine getirilmesi.

Adil Sunum: Denetim sonuçlarının doğru bir şekilde sunulması.

Mesleki Özen: Denetim çalışmalarında ayrıntılara verilen önem, dikkat, gayret ve titizlik.

Gizlilik: Denetim çalışmaları sırasında bilgi güvenliğine dikkat edilmesi, hassas ve gizli bilgilerin uygun şekilde ele alınması.

Bağımsızlık: Denetim çalışmalarında faaliyet alanından bağımsız olunması, her durumda önyargı ve çıkar çatışması olmadan hareket edilmesi.

Kanıta Dayalı Yaklaşım: Güvenilir ve tekrar edilebilir denetim sonuçlarına ulaşabilme yönteminin uygulanması.

Risk Temelli Yaklaşım: Risk ve fırsatları göz önüne alarak denetim çalışmalarının yürütülmesi.

1.2.1.1. Denetim Türleri

Denetim, genel olarak yapılış amaç, denetçinin statüsü ve yapılış zamanına göre değişik türlere ayrılmaktadır. Denetim, denetleyen ve denetlenen kişi ve kuruluşlar arasındaki ilişkiye (denetçinin statüsüne) göre "*İç Denetim*" ve "*Dış Denetim*" olarak iki kategori altında değerlendirebilir. Bu sınıflandırmada temel fark; iç denetim, işletmelerin kendi çalışanlarıyla kendi içinde gerçekleştirdiği denetim faaliyetiyken; dış denetim dışarıdan bir başka kişi ya da kuruluş tarafından yerine getirilmektedir. ISO-19011 standardında dış denetim de "*2. Taraf Denetim*" ve "*3. Taraf Denetim*" şeklinde ikiye ayrılmakta; 2. taraf denetimi, tedarikçi denetimleri gibi işletmenin kendi amaçları doğrultusunda bir başka kuruluşa yaptığı ve yaptırdığı denetim, 3. taraf denetim ise belgelendirme ve yasal denetimler gibi bağımsız kuruluşlar tarafından yapılan denetim olarak tanımlanmaktadır (TSE, 2018). İç veya dış denetim olarak gerçekleştirilen ve denetim alanı, amaç ve hedeflerine göre farklılık gösteren bazı denetim türlerine aşağıda yer verilmektedir.

a. Bilgi Sistemleri Denetimi (Information System Audit)

Bilgi sistemleri denetimi, bilgi sistemleri altyapısı içindeki çeşitli kontrollerin incelenmesiyle ilgilidir. Bu denetim faaliyeti; bilgi sistemleri, uygulamaları ve operasyonlarında tasarlanan ve uygulanan kontrollerin tasarım ve işlevlerine ilişkin kanıtların toplanmasını ve değerlendirilmesini içerir. Denetim kanıtları değerlendirildikten sonra, bilgi sistemlerinin varlıkları koruyup korumadığı, veri bütünlüğünü sürdürüp sürdürmediği ve kuruluşun amaç ve hedeflerine ulaşmak için, etkin ve verimli bir şekilde çalışıp çalışmadığı hakkında bir görüş oluşturulur. Bilgi sistemleri denetimi, finansal tabloların denetimiyle birlikte gerçekleştirildiği gibi çoğu zaman bağımsız olarak gerçekleştirilir (Hingarh ve Ahmed, 2013). Bilgi sistemleri denetiminin tanımı SPK'nın III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği'nde (BSBD Tebliği) de ele alınmıştır. Buna göre bilgi sistemleri bağımsız denetimi; bilgi sistemleri yönetimi ve işletimi kapsamında yer alan faaliyet, yazılım ve donanım gibi bilgi sistemi unsurları ile bu sistem dâhilinde tesis edilen kontrollerin bilgi sistemleri yönetim ilkeleri doğrultusunda değerlendirilmesi sonucunda görüş oluşturulması ve rapora bağlanması aşamalarından oluşan süreçtir. Bilgi sistemleri bağımsız denetiminin temel amacı denetlenenin bilgi sistemlerinin ve bu sisteme ilişkin iç kontrollerinin bilgi sistemleri yönetim ilkeleri doğrultusunda uyumluluk, etkinlik ve yeterliliği hakkında görüş oluşturulmasıdır.

Bilgi sistemleri denetimi, iç veya dış denetim olarak gerçekleştirilebilir. Bilgi sistemleri denetimi, iç denetimin parçası olarak bağımsız uzman bir grup tarafından yürütülebildiği gibi finansal ve uygunluk denetimleri ile bütünleşik bir şekilde yürütülebilir. Bunun yanında, dışarıdan bir kişi ya da kuruluş tarafından bilgi sistemleri denetim hizmeti de sağlanabilir.

b. Finansal Denetim (Financial Audit)

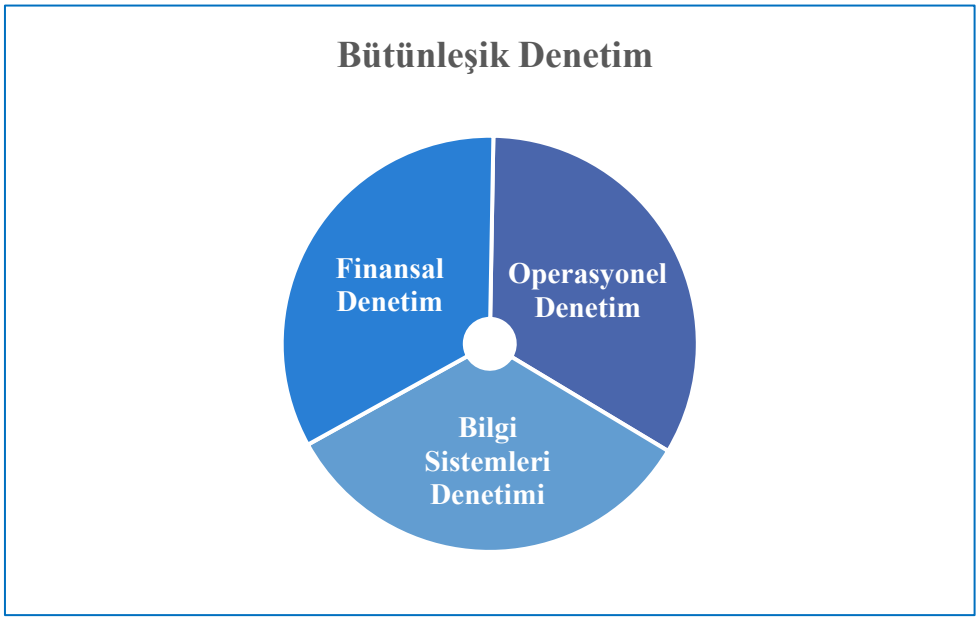
Finansal denetim, mali kayıtlar ve bilgilerin doğruluğunu saptamak için tasarlanmış bir denetim türüdür (ISACA, 2018). Bu denetim faaliyetinde bir işletmenin finansal tablolarının incelenmesi yapılarak genel kabul görmüş muhasebe ilkelerine ve yasal düzenlemelere uygunluk ve finansal tabloların gerçek finansal durumu yansıtıp yansıtmadığı konusunda bir görüş oluşturulur (İSMMMO, t.y.). Denetim kavramının en sık kullanımı finansal tabloların denetlenmesi faaliyeti içindir ve bu faaliyet alanı, teknolojinin her alanda yoğun olarak kullanılmasıyla bilgi sistemleri denetimiyle de yakından ilgilidir.

c. Operasyonel Denetim (Operational Audit)

Operasyonel denetim, yönetsel kontrol altındaki bir işletmenin operasyonlarının etkinlik ve verimliliği ile stratejilerine uyumunun; organizsayon yapısı ve kültürünün iş hedeflerine uyumunun değerlendirildiği denetim türüdür. Operasyonel denetimde işletme politika, süreçleri ve prosedürleri temel odak noktasıdır. "*İş hedeflerinin gerçekleştirileceğine dair ve istenmeyen olayların önleneceği, tespit edilebileceği ve düzeltileceğine dair makul güvence sağlamak üzere tasarlanmış olan politikalar, prosedürler, uygulamalar ve organizasyonel yapılar"* iç kontrol olarak tanımlanmaktadır (ISACA, 2018). Belirli bir alanda bu iç kontrollerin mevcut olup olmadığı ve düzgün bir şekilde işleyip işlemediği değerlendirilerek iyileştirme yollarının belirlenmeye çalışıldığı denetim çalışmasıdır (Gantz, 2013).

d. Bütünleşik Denetim (Integrated Audit)

Bütünleşik denetim, genel olarak Şekil 2'de görüldüğü üzere; finansal (mali) denetim, operasyonel denetim ve bilgi sistemleri denetimi süreçleri bir takım çalışmasıyla birlikte kapsanarak risk odaklı bir yaklaşımla ilgili iç kontroller değerlendirilerek gerçekleştirilir. Bu tarz bütünleşik bir denetim süreci sonunda tek bir konsolide rapor ortaya çıkar (ISACA, 2019: 63). ISO-19011 rehberinde farklı yönetim sistemlerinin tek bir yönetim sistemi olarak entegre şekilde denetimi bütünleşik denetim olarak açıklanmaktadır (TSE, 2018). Bu denetim yaklaşımı ile büyük resim oluşturularak denetim paydaşları arasında denetimle ilgili farkındalık artmakta, etkin ve verimli bir iç kontrol ortamı oluşturulmakta, zaman ve maliyet açısından kazanımlar sağlanmaktadır (ISACA, 2019: 64).



Şekil 2: Bütünleşik Denetim

e. Uyum Denetimi (Compliance Audit)

Uyumluluk, ISACA sözlüğünde "*Sözleşmesel yükümlülükler ve iç politikalardan kaynaklanan gönüllü gereksinimlerin yanı sıra yasalar ve düzenlemelerle belirlenen zorunlu gereklilikleri yerine getirme ve bunlara bağlılığı gösterme yeteneği*" olarak ifade edilmektedir (ISACA, 2018). Bu bağlamda, uyum denetimi önceden belirlenmiş belirli yasalara, düzenlemelere ve uygulamalara uyumlu olunup olunmadığının incelenmesidir ve kavramsal olarak finansal denetim, operasyonel denetim gibi diğer denetim türleriyle örtüşmektedir. Kurumsal olarak belirlenmiş politika, prosedür, yönerge ve kılavuzlara uyum denetimleri, genellikle iç denetim kapsamında ele alınmaktadır. Yasalar ve düzenlemelerle belirlenen zorunlu gerekliliklere uygun davranılıp davranılmadığının belirlenmesi ise genellikle dış denetim ile sağlanmaktadır (Gantz, 2013).

f. İdari Denetim (Administrative Audit)

İdari denetim, bir kuruluş içindeki belirli bir bölümün operasyonel verimliliğinin incelenmesidir (Gregory, 2019).

g. Adli Denetim (Forensic Audit)

Bu denetim türü, dolandırıcılar veya suçlular tarafından bir işletmenin veya kişinin finansal kayıtlarında gerçekleştirilen eylemlere yönelik, bu eylemleri ve gerçekleştirenleri tespit etmeyi, parasal boyununu ortaya koymayı ve adli makamlar ve kolluk kuvvetleri tarafından kullanılabilecek yasal olarak kabul edilebilir kanıtların elde etmeyi amaçlamaktadır. Bu bağlamda, kanıtların korunması ve gözetimini de içerecek şekilde katı bir denetim sürecinin uygulanmasını gerektirir (Gregory, 2019).

h. Dolandırıcılık Denetimi (Fraud Audit)

Dolandırıcılık denetimi, bir kuruluşta kasıtlı olarak aldatmaya yönelik gerçekleştirilen veya şüphelenilen usulsüzlükleri ve yasa dışı eylemleri tespit edebilmek için belirli araçlar ve veri analizi teknikleri kullanılarak yürütülen detaylı incelemedir (ISACA, 2019: 48).

i. Üçüncü Taraf Hizmet Denetimi (Third-party Service Audit)

Bilgi sistemlerinde hizmet olarak yazılım (SaaS) modellerinin, bulut bilişimin ve harici ortamlarda barındırılan sistem ve altyapı bileşenlerinin ortaya çıkması ve bilgi sistemleri hizmetlerinin dış kullanımının artmasıyla birlikte dışarıdan kuruluşlara sağlanan bu hizmetlerin denetiminin de kuruluşlar tarafından bilgi sistemleri denetimi kapsamında ele alınması gerekmektedir (Gantz, 2013). Bu kapsamda, bir işletmenin iş süreçlerine ait, üçüncü taraf hizmet sağlayıcılar tarafından dışarıdan sağlanan hizmetlerin denetimi üçüncü taraf hizmet denetimi kapsamında ele alınır. Bu denetim çalışması sonunda çıkacak sonuç raporları, üçüncü taraf hizmeti alan kuruluşun bilgi sistemleri denetimi sürecinde değerlendirilmektedir (ISACA, 2019: 48).

Şekil 3:Üçüncü Tarat Hizmet Denetimi Raporu Kullanımı

j. Adli Bilişim Denetimi (Computer Forensic Audit)

Adli bilişim, "*Yargı incelemesinde olgusal bilgi oluşturmak için bilimsel yöntemin dijital medyaya uygulanması*" olarak tanımlanır (ISACA, 2018). Adli bilişim sürecinde, adli bilişim donanım ve yazılımlarıyla bir mahkemede kabul edilebilir bir şekilde bilimsel yöntemler ile veri toplamak ve analiz etmek birincil amaçtır. Bu süreçte kullanılan adli bilişim araçlarının; silinen dosyaların veya kolayca erişilemeyen dosyaların bulunması, şifre kırma, şifre çözme ve etkili bir şekilde arama ve filtreleme yetenekleri bulunmaktadır. Kişisel bilgisayarlar, mobil cihazlar, ağ ve taşınabilir depolama ortamları gibi veri depolayan herhangi bir bilgi sistemi ortamı adli bilişim kapsamında incelenebilmektedir (Hayes, 2020). Bir adli bilişim denetimiyle, adli bilişim inceleme çalışmalarında yardımcı olunarak; "*yasal olarak kabul edilebilir bir şekilde dijital kanıtları tanımlama, koruma, analiz etme ve sunma süreci*"ne (ISACA, 2018) uyumlu davranılıp davranılmadığının denetimi gerçekleştirilir (ISACA, 2019: 48). Sonuçta bu denetim türü, dijital kanıt/delil üzerine yoğunlaşır. Dijital kanıt, bilgi sistemlerinin veya elektronik cihazların veri depolama medyaları üzerinde bulunan ya da bu medyalar üzerinden geçen suç ile ilgili kanıt niteliği taşıyabilecek ve suçun aydınlatılmasını sağlayacak verilerdir.

Bilgi sistemlerindeki kanıt olarak kullanılması muhtemel bulguların tespit edilmesi ve kanıt olarak ortaya konulması, verilerin bulundukları veya saklandıkları manyetik dijital ortamlardan anlaşılır bir şekilde çıkartılarak metinler haline dönüştürülmesi ile mümkündür.

k. Fonksiyonel Denetim (Functional Audit)

Fonksiyonel denetim, işletme içindeki finans, insan kaynakları, pazarlama gibi bölümlerin işlevlerinin incelenmesine ve değerlendirilmesine odaklanır. Amacı, ilgili departmanların etkin ve verimli bir şekilde mevzuata ve işletmenin amaç ve hedefleriyle uyumlu çalışıp çalışmadığı belirlemektir. Fonksiyonel denetim süreci; politikaların, prosedürlerin, kontrollerin ve performans verilerinin gözden geçirilmesinin yanı sıra işlevi yerine getirmek için kullanılan kaynakların, süreçlerin ve sistemlerin değerlendirilmesini içerir. Pek çok işletmede bilgi sistemlerinin ayrı bir departman olarak örgütlenmesi, bu denetim türünün ilgili departmanın işlevselliğinin denetimini kapsayabileceği gibi daha alt faaliyetlerin işlevselliğinin denetimini kapsayabilir. Bu denetim ile bilgi sistemlerinde, bir yazılımın işlevselliği ve performansı açısından bağımsız değerlendirilmesi yapılarak yazılım gereksinimlerinin karşılanıp karşılanmadığının doğrulanması amaçlanır. Bu manada, yazılım uygulama sürecinden sonra ve yazılım tesliminden önce gerçekleştirilir (ISACA, 2019: 48).

Yukarıda detay açıklamalarına yer verilen denetim türlerine ilişkin özet bilgiler, aşağıdaki tabloda yer verilmektedir.

Bilgi sistemleri denetimi

- Bilgi sistemlerinin varlıkları koruyup korumadığı, veri bütünlüğünü sürdürüp sürdürmediği ve kuruluşun amaç ve hedeflerine ulaşmak için, etkin ve verimli bir şekilde çalışıp çalışmadığını belirlemek

Finansal denetim

- Mali kayıtların ve bilgilerin doğruluğunu saptamak

Operasyonel denetim

- Belirli bir alanda iç kontrollerin olup olmadığının, düzgün bir şekilde işleyip işlemediğinin değerlendirilmesi ve iyileştirme yollarının belirlenmesi

Bütünleşik denetim

- Finansal denetim ile birlikte operasyonel ve bilgi sistemleri denetiminin entegre bir şekilde gerçekleştirilmesi

Uyum denetimi

- Önceden belirlenmiş belirli yasalara, düzenlemelere ve uygulamalara uyumlu olunup olunmadığının incelenmesi

İdari denetim

- Bir kuruluşun belirli bir bölümünün operasyonel verimliliğinin incelenmesi

Adli denetim

- Dolandırıcılar ve suçlular tarafından gerçekleştirilen eylemlere yönelik yasal olarak kabul edilebilir kanıtların elde edilmesi

Dolandırıcılık denetimi

- Bir kuruluşta kasıtlı olarak aldatmaya yönelik gerçekleştirilen veya şüphelenilen usulsüzlüklerin ve yasa dışı eylemlerin tespit edilmesi

Üçüncü taraf hizmet denetimi

- Hizmet sağlayıcılar tarafından dışarıdan sağlanan hizmetlerin denetimi

Adli bilişim denetimi

- Yargı incelemesinde olgusal bilgi oluşturmak için bilimsel yöntemin dijital medyaya uygulanması

Fonksiyonel denetim

- Bir yazılımın işlevselliğinin ve performansının gereksinimleri karşılaması açısından değerlendirilmesi

1.2.1.2. Kontroller

İşletme hedeflerine katkı sağlayacak şekilde bilgi sistemlerinden beklenen işlevselliği sağlamak amacıyla kontroller kullanır. Bu nedenle, bilgi sistemi denetiminde ele alınan unsurlar arasında kontroller önemli bir yer tutar. Kontrol kavramı önlem ve tedbir ile eş anlamlı olarak da kullanılır ve bu yönde bir işletmenin risklerini yönetmek için idari, teknik, yönetim veya yasal nitelikte olabilecek politikalar, prosedürler, kılavuzlar, uygulamalar veya organizasyon yapılarından oluşur (ISACA, 2018). Bir işletme tarafından uygulanan etkili bir kontrol; olması muhtemel bir olayı önleyen, tespit eden veya sınırlayan ve bir risk olayından kurtulmayı sağlayan bir kontroldür (ISACA, 2019: 41).

Daha önce belirtildiği üzere iç kontroller; bir işletme tarafından iş hedeflerinin gerçekleştirileceğine dair ve istenmeyen olayların önleneceği, tespit edilebileceği ve düzeltileceğine dair makul güvence sağlamak üzere geliştirilir. İş hedefi, "*iş amaçlarının daha da geliştirilerek taktik*

hedeflere, arzulanan sonuçlara ve çıktılara dönüşmesi" olarak tanımlanır. İç kontrol tanımından da anlaşılacağı üzere; iç kontrol oluşturulurken belirlenen iş hedeflerine ulaşmak ana motivasyon kaynağıdır ve belirlenen bu hedeflere yönelik çalışmak bir işletmedeki her bir çalışanın görevi olmakla birlikte birincil sorumluluk üst yönetimdedir. Yönetim tarafından kurumsal hedeflerin gerçekleştirilmesine yönelik planlama, organizasyon ve yönlendirme çalışmaları gerçekleştirilir ve bu yönde gerekli kontroller oluşturulur ve sürekli izlenir (ISACA, 2019: 41; Cascarino, 2012).

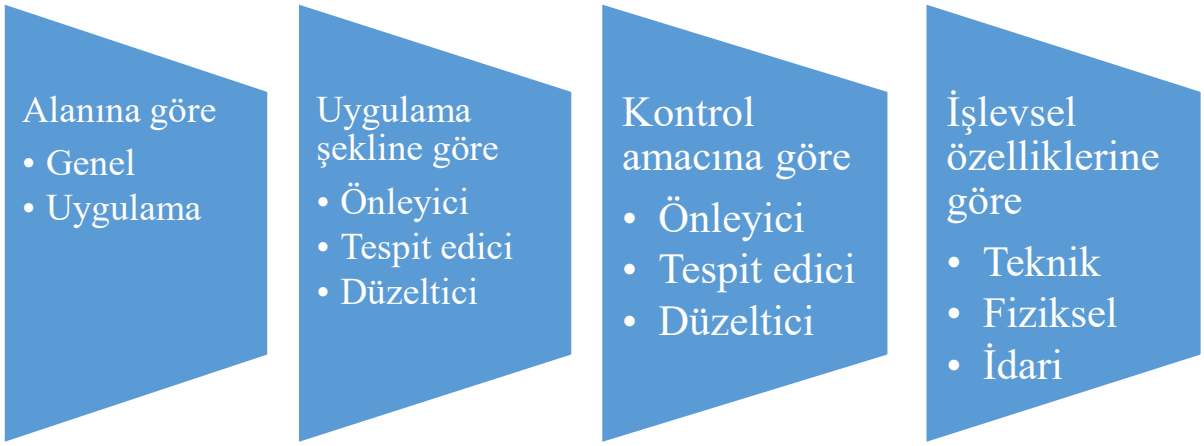
Kontroller bir işletmede esas olarak;

a) İstenen olayların gerçekleşmesini sağlamak,

b) İstenmeyen olayların önlenmesine yardımcı olmak,

şeklinde iki farklı hususu ele alır (Gregory, 2019).

Kontrollerin genel kabul görmüş belirli bir sınıflandırması yoktur. Gantz (2013) bu durumu; "*Kontroller mevcut çerçeveler, metodolojiler ve kılavuzlarda birçok farklı şekilde sınıflandırılmaktadır ve kuruluşlar, harici bir çerçeve veya metodolojide belirtilen bir yaklaşımı seçebilir veya uyarlayabilir, kendi sınıflandırmasını geliştirebilir veya kuruluşun karşılaması gereken yasal, düzenleyici veya politika gereksinimlerinde belirlenen standartları takip edebilir.*" şeklinde ifade etmektedir. Kontroller için farklı kriterler baz alınarak oluşturulan bazı ortak sınıflandırma yaklaşımları aşağıdaki tablo kapsamında açıklanmaktadır.



Şekil 4: Kontrol Sınıflandırması

1.2.1.2.1. Kontrol Alanına Göre Kontrol Türleri

Kontroller, kontrol alanına bağlı olarak genel kontroller ve uygulama kontrolleri olarak iki kategoride ele alınır.

a. Genel Kontroller

Genel kontroller, işletmenin tüm bilgi sistemleri altyapısı ve destek hizmetleri dâhil olmak üzere faaliyetlerinin sürekliliğinin sağlanmasına yönelik politika, prosedür ve uygulamalara yönelik kontrollerdir. Bu kontroller, uygulama yazılımları ve bunlara ilişkin kontroller için güvenli ortam sağlar. Genel kontroller; yönetim kontrolleri, fiziksel ve çevresel kontroller, ağ yönetimi ve güvenliği kontrolleri, mantıksal erişim kontrolleri, işletim kontrolleri, değişim yönetimi kontrolleri, acil durum ve iş sürekliliği planlaması kontrollerini içerir (Sayıştay, 2013: 11).

- Yönetim Kontrolleri: İşletme yönetimi tarafından güvenli ve yeterli bir bilgi sistemleri ortamının sağlanması için uygun politika, prosedür ve uygulamalar oluşturarak işletmenin bilgi sistemlerinin işletme amaçlarına uygun çalışması ve işlevlerini doğru bir şekilde yerine getirmesini sağlayacak tedbirleri alınarak oluşturulan kontrollerdir. Bu kontroller, denetçiye alt düzeydeki ayrıntılı kontrollerin varlığı ve etkinliği konusunda bir güvence sağlar. Yönetim kontrolleri, stratejik planlama, güvenlik politikaları, organizasyon, varlık yönetimi, personel ve eğitim politikaları ile yasal düzenlemelere uygunluk alanlarından oluşur. Örneğin; bilgi sistemlerine ilişkin yazılı bir strateji ve bu stratejinin uygulanmasına ilişkin planın olması, düzenli risk değerlendirilmesi yapılması, yönetimce

onaylanmış ve tüm personele dağıtılmış yazılı bilgi güvenliği politikası oluşturulması, güvenlik politikasının belirli aralıklarla güncellenmesi, bilgi sistemlerinin etkin bir şekilde yönetilmesini sağlayacak organizasyon yapısı oluşturulması, bilgi sistemleri varlık envanteri çıkarılması, personelin düzenli bir şekilde bilgi güvenliğine ilişkin eğitim ve güncelleme programlarına katılımının sağlanması, bilgi sistemlerine ilişkin düzenleme gereklerinin yerine getirilmesi ve bunun için denetlenmesi vb. yönetsel kontrolleridir (Sayıştay, 2013: 11-27).

- Fiziksel ve Çevresel Kontroller: Fiziksel ve çevresel kontrollerin amacı, bilgi sistemleri donanım ve yazılımının kasten ya da kasıtsız olarak oluşan hasarlara, izinsiz erişim sonucu bozulma veya çalınma ile her türlü çevresel tehlikelere karşı korumaktır. Bilgi sistemleri, bu sistemlere erişme yetkisi olmayan kişilerin yol açabilecekleri hasarlara ve müdahalelere karşı fiziksel engeller konulmak suretiyle korunurken; yangın, su, elektrik, voltaj dalgalanmaları veya güç yetersizlikleri gibi çevresel tehlikelere karşı ise, bunlara ilişkin uygun önlemler alınarak korunmalıdır. Örneğin; işletmenin izinsiz fiziksel erişime ve çevresel tehlikelere ilişkin yazılı güvenlik politika ve prosedürlere sahip olması, bilgi sistemlerinin bulunduğu ortamlara izinsiz fiziksel erişimin engellenmesi, fiziksel erişimin yetki dahilinde sağlanması, yangın belirleme ve söndürme sistemlerinin kurulması, su basmalarına karşı otomatik su veya nem detektörleri kullanılması, elektrik kesintilerine karşı kesintisiz güç kaynakları kullanılması, bilgi sistemleri elemanlarının toz, nem ve sıcaklıktan korumak için uygun havalandırma ve soğutma sistemleri kullanılması, donanım ve yazılımların bulunduğu ortamların düzenli bakım onarımının yapılması vb. fiziksel ve çevresel kontrolleridir (Sayıştay, 2013: 28, 29).

- Ağ Yönetimi ve Güvenliği Kontrolleri: Bu kontrollerin amacı, gerek iç gerekse dış ağ sistemini oluşturan tüm varlıkların korunması, ağ hizmetlerinin güvenli bir şekilde yürütülmesi ve ağ aracılığıyla gerçekleşebilecek izinsiz erişim ve bunlar dolayısıyla oluşabilecek tehlikelerin önlenmesidir. Güvenlik önlemlerinin tesis edilmesinde, bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği katmanlı güvenlik mimarisi esas alınır. Örneğin; güvenlik politikasının bir parçası olarak ağ ve internet kullanım politikası oluşturulması, ağ ve internet kullanımına ilişkin prosedürler ve işletim talimatları oluşturulması, ağ kablolama diyagramları gibi ağın fiziksel yerleşimine ilişkin belgeler oluşturulmalı, ağ işletim sorumluluğunun tecrübeli personel tarafından yapılması, ağ olaylarının otomatik olarak ağ işletim sistemi tarafından kaydedilmesi, ağda kurulu sistemlerin ve ağ aktif cihazları üzerindeki yazılımların güvenlik sorunu olup olmadığının düzenli takip edilmesi, ağ üzerinde işleyen sunucu yazılımlarının incelenmesi ve gerekli olmayanların durdurulması, ağ üzerinde anti-virüs sistemleri kurulması ve düzenli olarak güncellenmesi, bazı durumlarda ağ üzerinde veri aktarımlarında kriptolama yapılması, iletişim kurma veya veri iletmeye ilişkin riskleri azaltmak için özel hat kurulması vb. ağ yönetimi ve güvenliği kontrolleridir (Sayıştay, 2013: 36-38).

- Mantıksal Erişim Kontrolleri: Bu kontrollerin amacı, işletim sistemine, ağa, veri tabanına ve uygulama programlarına izinsiz erişimin önlenmesi ve bilginin değiştirilmesi, açığa çıkarılması ve kaybına karşı sistemin korunmasıdır. Mantıksal erişim kontrolleri, hem sistem hem de uygulama düzeyinde ortaya çıkabilir. Bilgi sistemlerindeki erişim kontrolleri işletim sistemine, ağa, sistem kaynaklarına, veri tabanına ve uygulama programlarına erişimi sınırlandırırken; uygulama düzeyindeki kontroller, tek tek uygulamalar bünyesindeki kullanıcı faaliyetlerini kısıtlar. Örneğin; mantıksal erişim politikası oluşturulması, şifre politikası oluşturulması, erişim yöntemi prosedürleri oluşturulması, sistem ve uygulama programlarına erişimlerin kayıt altına alınması ve izlenmesi, yetkisiz erişimlerin raporlanması vb. mantıksal erişim kontrolleridir (Sayıştay, 2013: 64).

- İşletim Kontrolleri: Bu kontrollerin amacı, bilgi sistemlerinin kendisinden beklenen faaliyetlerin sürekliliğini ve güvenliğini sağlayacak şekilde işletilmesidir. Bu kontroller, işletim sistemi ve bilgisayar işlemleri kontrolleri ve veri tabanı güvenlik kontrolleri olarak incelenir. İşletim sistemi ve bilgisayar işlemleri kontrolleri, uygulama yazılımları üzerinde çalışan işletim sisteminin kurulum ve işletilmesi ile bakım işlemlerinin sorunsuz yürütülmesi ve tüm işlemlerin güvenli şekilde gerçekleştirilmesine sağlamaya yönelik her türlü kontrolü kapsar. Veri tabanı güvenlik kontroleri ise, birbiriyle ilişkili verilerin güvenli bir şekilde kaydedilip dopolanması, belgelendirilmesi ve gerektiği zaman güvenli ve çok amaçlı kullanılmasını sağlayacak her türlü kontroleri kapsar. Örneğin; işletim sisteminin seçimi ve kurulumuna ilişkin prosedürler tanımlama, işletim sisteminin güvenli yönetilmesine ilişkin tüm süreçler ve bunlara yönelik görev ve sorumluluklar ile onay işlemlerini yazılı

prosedürlere bağlama, sisteme ilişkin güncel yamaların takip edilerek gerektiğinden kullanılmasını sağlayacak prosedürler bulundurma, işletim sisteminin güçlendirilmesine yönelik kontrol listeleri hazırlama, sistemin düzenli bakım ve kontrolünün yapılmasını sağlama, belirli aralıklarla geri yükleme noktası oluşturma, sisteme ilişkin kapasite tahminleri ve planlar yapma, bilgi işlem biriminde devamlı personel bulundurma, bilgi ortamı araçlarının işlemlerini etkin bir şekilde yönetme, bilgi sistemleri biriminin diğer birimlere sunacağı hizmetleri yazılı olarak tanımlama, olay yönetimine ilişkin prosedürler tanımlama vb. işletim kontrolleridir (Sayıştay, 2013: 74-75).

- Sistem Geliştirme ve Değişim Yönetimi Kontrolleri: Bu kontrollerin amacı, sistem geliştirme üzerindeki tüm proje yönetimi ve kontrollerinin tatmin edici olmasını, kalıcı ve yeterli iç kontrol ve denetim izine sahip olmasını, sistem geliştirme kalitesinin artırılmasını ve sistemin kullanıcıların ihtiyaçlarını karşıladığı kadar kurumun stratejik amaçlarını da desteklemesini sağlamaktır. Örneğin; sistem geliştirme projeleri için standart politika ve prosedürler oluşturma, yeterli tecrübe ve birikime haiz proje yönetimine sahip olma, yeterli finansal ve insan kaynağına sahip olma, proje takibi için iş programları ve çizelgeler hazırlama, ayrıntılı proje planı hazırlama, risk değerlendirmesi yapma, proje teklif belgesi hazırlama, projeye ilişkin fizibilite raporu hazırlama, sistemi belgelendirme, sistem kurulum sürecinin yürütülmesine ilişkin politika ve prosedürleri bir tasarım belgesine dayandırma, bütünlük ve doğruluk testlerinin yeterli bir şekilde gerçekleştirme, kullanıcı kabul testleri yapma, uygulamaya geçişe ilişkin prosedürler belirleme, veri aktarım işlemleri için prosedürler oluşturma, paralel çalıştırma ve sonuçlarının değerlendirilmesine ilişkin ortam oluşturma, uygulama sonrasında sistem, iş amaçlarına uygunluk, kullanıcı beklentileri ve diğer teknik koşulların karşılanmasına yönelik izlemeye alma vb. sistem geliştirme ve değişim yönetimi kontrolleridir (Sayıştay, 2013: 87-94).

- Acil Durum ve İş Sürekliliği Planlaması Kontrolleri: Bu kontrollerin amacı, acil durum nedeniyle bilgi sistemlerinin geçici veya sürekli olarak aksaması durumunda işletmenin işlevlerini sürdürebilmesi ve tutulan bilginin işlenmesi, erişilmesi ve korunmasına ilişkin kapasitesinin kaybedilmemesini sağlamaktır. Acil durum, deprem, yangın, fırtına, sel, bombalama, sabotaj, donanım veya yazılım hatası, elektrik ve telekomünikasyon kesintisi gibi önceden tahmin edilebilen veya edilemeyen iç veya dış faktörler sonucu meydana gelen ve işletmenin faaliyetlerini sürdürmesi durumunu aksatan her şey olabilir. Örneğin; acil durum ve iş sürekliliği için yönetim süreci oluşturma, risk değerlendirmesi yapma, her bir risk için gerekli tedbirleri alma, acil durum ve iş sürekliliği planı hazırlama, bu planı sürekli olarak gözden geçirme, güncelleme ve test etme, sistem yazılımları, finansal uygulamalar ve bunları destekleyen dosyaları düzenli olarak (günlük, haftalık, veya aylık şeklinde) yedekleme vb. acil durum ve iş sürekliliği planlaması kontrolleridir (Sayıştay, 2013: 99-100). İşletme, bir felaketle karşı karşıya kaldığında herhangi bir acil durum ve iş sürekliliği planını devreye sokamadığı takdirde, yasal sorumluluklarını veya üçüncü kişilere karşı olan sorumluluklarını yerine getirememe, ana faaliyetlerine makul bir süre içerisinde geri dönememe, felaketin sebep olduğu kayıplarda artış gibi risklere maruz kalabilir. İşletme, bu riskleri en aza indirebilmek için iç veya dış faktörler sebebiyle meydana gelme ihtimali olan acil ve beklenmedik durumlara karşı hazırlıklı olmalı ve acil durum ve iş sürekliliği planına sahip olmalıdır. Ayrıca, işletmenin ana faaliyetlerini kesintiye uğratacak çevresel faktörleri belirlemek için risk değerlendirmesi yapmalı, bu riskleri en aza indirmek için uygun maliyetle gerekli tedbirler alınmalıdır (Yıldırım, 2017: 32).

b. Uygulama Kontroller

Uygulama kontrolleri, bilgilerin sistemlere ya da programlara eksiksiz olarak, zamanında ve sadece bir kere girilmesi, bilgi sistemleri ortamında tüm işlem ve süreçlerin istenilen sıra ve düzen içinde gerçekleşmesi, raporların tam ve güvenilir olarak üretilmesi, yetkili kişilere ulaştırılması ve uygun şekilde arşivlenmesini sağlayan kontrollerdir. Uygulama kontrolleri değerlenirilmeden önce işletmenin uygulama programları tanınmalıdır. Bunun için veri akışları temin edilmeli ve işletme tarafından oluşturulmuş manuel ve otomatik kontroller belirlenmelidir. Ayrıca, uygulamanın yasal düzenlemeler ve muhasebe sistemi ile ilişkileri iyi anlaşılmalıdır. Uygulama kontrolleri değerlendirilirken, uygulamaların güvenilirliğine ilişkin makul bir güvence elde edebilmek amacıyla uygulamalarda olması gereken kontroller test edilerek kanıt toplanır. Bu aşamada bilgisayar destekli denetim tekniklerinden (BDDT) de yararlanılır. Uygulama kontrolleri; girdi kontrolleri, veri transfer kontrolleri, işlem kontrolleri ve çıktı kontrollerini içerir (Sayıştay, 2013: 107).

- Girdi Kontrolleri: Bu kontrollerin hedefi, verilerin inceleme konusu bilgi sistemlerine tam, doğru ve yetkili bir kişi tarafından girilip girilmediğinin sağlamasını yapmaktır. Bu kapsamda, yetkisiz kişilerce veri girişini engellemek, hatalı veya eksik veri girişlerini önlemek veya mükerrer kayıtların önüne geçmek amacıyla, denetim sırasında incelenen bilgi sistemlerinde çalışan uygulama programlarına ilişkin teknik dokümanlar veya kullanım rehberleri hazırlanmalı, hatalı veri girişlerini engelleyecek otomatik kontrol mekanizmaları uygulamanın arka planında yürütülmeli, hatalı veya yetkisiz veri girişleri raporlanmalı ve görevler ayrılığı ilkesine uyum sağlanmalıdır. Örneğin, uygulama programlarına ilişkin teknik dökümanlar ve kullanım rehberleri hazırlama, kaynak belgelerin kullanılmasına ilişkin prosedürler tanımlama, tüm veri hazırlama, veri giriş işlemleri ve dosyalardaki değişikliklerin yetki dahilinde yapılması, hatalı veri girişlerini önleyecek otomatik kontrol mekanizmaları kurmak, hatalı ve kural dışı veri girişlerini raporlama vb. girdi kontrolleridir (Sayıştay, 2013: 108).

- Veri Transfer Kontrolleri: Bu kontrollerin amacı, bilgi sistemlerinde bir uçtan başka bir uca verilerin tam, doğru, zamanında ve güvenli bir şekilde transferini sağlamaktır. Transfer edilen verinin transfer esnasında bozulması, kaybolması, çalınması veya değiştirilmesi mümkün olabilir. Bunun yanı sıra verinin iletilememesi, iletildiğinin bilinememesi, birkaç kez gönderilmesi veya veri transferinin reddedilmesi gibi sorunlar da meydana gelebilir. Bu gibi risklerin önüne geçebilmek amacıyla sistemler arasında yapılan veri transferlerinin tam ve doğru olarak yapılmasını sağlayan manuel veya otomatik kontroller oluşturulabilir. Bu süreçteki en önemli husus ise, veri transferinden sorumlu personele rehberlik edecek politika ve prosedür setlerinin tanımlanmış olmasıdır (Sayıştay, 2013: 108).

- İşlem Kontrolleri: Bu kontrollerin amacı, uygulama içerisinde kullanılan verinin tam, doğru ve işletmenin iş süreçlerine uygun olarak işleme tabi tutulmasını ve denetlenebilir olmasını sağlamaktır. İşletmenin iş süreçlerinin uygulama kontrolleri üzerinden yanlış bir şekilde işletilmesi, sistematik hataların oluşması, yanlış verilerin işleme tabi tutulması, yanlış dosyaların işleme tabi tululması, hataların tespit edilip düzeltilmemesi, denetim izinin kaybolması, işlemlerin doğrulanamaması veya mantıksız işlemlerin meydana gelmesi gibi riskler oluşabilir. Bu riskler kapsamında, kullanıcı ve işletim personeli tarafından anlaşılır iş ve zaman çizelgesi hazırlanmalı, bilgisayar işlemlerinin doğru zamanda ve doğru bir silsile ile işletildiğinin teyidini sağlayan yeterli bir kontrol mekanizması kurulmalı, süreçte başarısızlık veya problemle karşılaşıldığında, personeli işlemleri onaylandıkları en son noktadan yeniden başlatabilmeli ve bütün işlemler ve bilgisayar kaynaklı hatalar hata ve beklenmedik durum raporlarında yer almalı ve bunlar yönetim tarafından gözden geçirilmelidir (Sayıştay, 2013: 116).

- Çıktı Kontrolleri: Bu kontrollerin amacı, çıktıların tam, doğru ve zamanında üretilmesi, doğru yer/kişilere dağıtılması, gizliliklerinin korunması, tespit edilen hataların detaylı incelenmesi ve gereğinin yapılmasını sağlamaktır. Bu kontrollerin yetersizliği nedeniyle, çıktıların tam ve doğru olmaması, uygun şekilde sınıflandırılıp dağıtılamaması, yetkisiz kişilerin eline geçmesi, hataların tespit edilip düzeltilememesi, elde edilen çıktıların muhafaza edilememesi gibi riskler meydana gelebilir. Bu risklerin azaltılması amacıyla işletmenin çıktıların elde edilmesi ve muhafaza edilmesine ilişkin yazılı prosedürlerinin olması, çıktıların dağıtımına ilişkin prosedürler oluşturulup uygulanması, çıktı raporlarının doğruluğunun gözden geçirilip hataların düzeltilmesi, çıktılara ilişkin hata veya beklenmedik durum raporu üretilmesi ve gözden geçirilmesi, çıktılarda meydana gelen hatalara ilişkin gözden geçirme ve doğrulama işlemlerinin yetkili personelce yapılması, çıktılar arşiv prosedürlerine göre saklanması gerekmektedir (Sayıştay, 2013: 119).

1.2.1.2.2. Uygulanmasına Bağlı Kontrol Türleri

Kontroller nasıl uygulandığına bağlı olarak otomatik ve manuel olarak iki kategoride ele alınmaktadır.

c. Otomatik Kontroller

Otomatik kontroller; benzer işlemlerin sürekli olarak yapıldığı durumlarda daha uygundur ve çalışma prensipleri daha önceden belirlenerek gerekli işlevlerin kendiliğinden gerçekleştiği sürece insanın daha az müdahalede bulunduğu veya hiç bulunmadığı, uygulama ve teknoloji tabanlı kontrollerdir. Kontrolün otomatik olarak tasarlanmasıyla insan hatası olasılığı azalmakta ve daha güvenilir ve doğru kontroller oluşmakta; ancak teknoloji riski ve karmaşıklık da artmaktadır. Örneğin;

uygulamalar üzerinde verinin uygulamaya girilmesi, uygulama üzerinde işlenmesi ve kullanıcılara sunulması sürecinde; işlemi yapan kullanıcıların doğrulanması, kullanıcıların yetkili olduğu işlemleri yapması, veri girişlerinin belirli bir formata uygun alınması, belirli şablonlarda raporlamaların oluşturulması, hata durumunda uyarı oluşturulması vb. otomatik uygulama kontrolleridir (Gregory, 2019).

d. Manuel Kontroller

Manuel kontroller, insan tarafından gerçekleştirilen işlevleri gerektirir. İnsan eylemlerine dayalı olması sebebiyle hata ve tutarsızlık oluşması riski artmaktadır. Ancak felaket ve acil durumlar vb. insan tarafından müdahale edilmesi ve karar verilmesi gereken süreçlerde, otomatik kontrollerin uygulama maliyetinin yüksek olması nedeniyle veya otomatik kontrolleri izlemek için manuel kontroller kullanılmaktadır. Bir kontrol amacına yönelik otomatik ve manuel kontrolleri birlikte kullanmakta mümkündür. Örneğin, bir uygulama veya sistem tarafından tutulan işlem, performans, hata vb. logların periyodik olarak gözden geçirilmesi (Gregory, 2019).

1.2.1.2.3. Amacına Göre Kontrol Türleri

Kontroller amacına göre önleyici, tespit edici ve düzeltici olarak üç sınıfa ayrılmaktadır.

a. Önleyici Kontroller

Önleyici kontroller, "*Kurumun; bir proses veya nihai ürün üzerinde önemli bir olumsuz etkinin olabileceğini belirlediği istenmeyen olayları, hataları ve diğer oluşumları önlemek için kullanılan bir iç kontrol*" olarak tanımlanmaktadır (ISACA, 2018). Bu kapsamda, uygulanan kontrollerde temel amaç kuruluş için tehlike ve risk oluşturabilecek, gerçekleşmesi muhtemel sorunların ortaya çıkmadan önce öngörülmesi ve gerekli aksiyonların alınarak oluşabilecek hata, ihmal ve kötü niyetli hareketlerin meydana gelmesinin önüne geçmektir (ISACA, 2019: 42). Örneğin (Doshi, 2020):

- Yetkin personelin istihdam edilmesi,
- Görevler ayrılığı prensibi ve rotasyonun uygulanması,
- Rutin işlemlerin adım adım anlatıldığı talimat dokümanlarının (SOP-Standart Operation Procedure) oluşturulması,
- Kartlı giriş sistemleri kullanılması,
- Güvenlik görevlilerine sahip olunması,
- Güvenlik duvarı üzerinden internete erişim sağlanması,
- Bir sisteme girişi yapılacak bir veri içeriğinin, beklenen mantıksal yapıda, biçimde, aralıkta veya özelliklerde olduğunun kontrollerinin yapılması,
- Kullanıcı bilgisayarlarında anti-virüs programlarının kullanılması,
- Kullanıcıların bir yazılımı kullanımında erişim kontrolü yöntemlerinin uygulanması,
- Periyodik olarak kullanıcı verilerinin yedeğinin alınması,
- Çitler, kilitler, biyometri, aydınlatma ve alarm sistemlerinin kullanılması,
- Saldırı önleme sistemleri kullanılması,
- Etik kodlar oluşturulması.

b. Tespit Edici Kontroller

Tespit edici kontroller; "*hataların, ihmallerin ve yetkisiz kullanımların veya kayıtların meydana geldiği zamanları tespit etmek ve raporlamak için vardır*" (ISACA, 2018). Hata, ihmal veya kötü niyetli kullanımları önlemek kadar, bu olaylar önlenemediğinde meydana gelip gelmediğinin ve nasıl meydana geldiğinin belirlenmesi de bu tür olayların etkisinin azaltılması için büyük önem arz etmektedir (Gregory, 2019; Doshi, 2020). Mesela; bir sisteme düzenli olarak yetkisiz giriş denemeleri olabilir ve kayıt altına alınan bu olaylar gözden geçirilip raporlanabilir. Olayın daha hızlı farkına varılabilmesi ve

duruma göre aksiyon alınabilmesi için tespit edici bu kontroller üzerinden oluşturulacak alarm mekanizmaları da kurulabilir. Bazı tespit edici kontrollere aşağıda yer verilmektedir (ISACA, 2019: 42):

- İç denetim gerçekleştirilerek operasyonel süreçlerin gözden geçirilmesi,
- Bilgi sistemleri tarafından tutulan iz kayıtlarının izlenmesi,
- Yazılım kalite güvence (QA) faaliyetleriyle yazılım geliştirme süreçlerinin izlenmesi,
- Bir dosyadaki belirli alanların sayısal toplamı alınarak özet toplamının (hash total) oluşturulması ve karşılaştırmak üzere saklanması,
- Uygulama kaynak kodu incelemesi,
- Ağ trafiği üzerinde saldırı tespit sistemlerinin (IDS) kullanılması,
- Bir sunucun periyodik olarak performans raporlarının alınması,
- Yapılan hesaplamaların tekrar edilerek kontrolü,
- CCTV (Closed-Circuit Television) güvenlik kamera görüntülerinin kaydedilmesi,
- Balküpü (honeypot) tuzak sistemlerinin kullanılması.

c. Düzeltici Kontroller

Düzeltici kontroller; "*Hatalar, eksiklikler ve yetkisiz kullanımlar ve izinsiz girişler tespit edildikten sonra bunları düzeltmek için tasarlanmıştır*" (ISACA, 2018). Bilgi sistemlerinde istenmeyen bir olayın meydana geldiği tespit edici kontrollerle belirlendikten sonra belirlenen sorunların düzeltilerek bilgi sistemlerinin sağlıklı bir şekilde çalışır haline getirilmesi için gereken planlamalardan ve kontrollerden oluşur. Bu kontrollerde amaç; sorunun kaynağına yönelik uygun çözümler geliştirilerek doğru ve zamanında bir müdahaleyle tehdidin ortadan kaldırılması, etkisinin azaltılması ve hataların düzeltilmesidir. Düzeltici kontrol örneklerine aşağıda yer verilmektedir (ISACA, 2019: 42):

- İş sürekliliği planı,
- Yedekten dönme prosedürü,
- Felaket kurtarma planı,
- İşlem tersine çevirme veya geri alma,
- Bir bilgisayara bulaştığı tespit edilen bir virüsün karantina altına alınması,
- Yangın söndürücüler,
- Sistemin ağ bağlantısının koparılması, izole edilmesi,
- Sisteme yama geçilerek güncellenmesi,
- Siber olay müdahale planı,
- Arıza onarım sözleşmesi.

1.2.1.2.4. İşlevsel Özelliklerine Göre Kontrol Türleri

İşlevsel özelliklerine göre kontroller, teknik, fiziksel ve idari olarak üç türde sınıflandırılır.

a. Teknik Kontroller

Bu kontrol türü, genellikle fiziksel olmayan, soyut kontrollerden oluşur ve mantıksal kontrol olarak da ifade edilir. Bu sınıflandırmadaki kontroller teknoloji bağımlıdır, bilgi sistemlerinin kullanıldığı kontrollerdir (Gregory, 2019). Bilgi sistemleri donanım ve yazılım unsurlarının kullanıldığı teknik kontrollerden bazıları aşağıdaki gibidir (Swanagan, t.y.):

- Güvenlik duvarı,
- Saldırı tespit ve önleme (IDS/IPS),
- Şifreleme,

- Güvenlik bilgileri ve olay yönetimi yazılımı (SIEM),
- Erişim kontrol listesi (ACL),
- Antivirüs yazılımı,
- Veri sızıntısı önleme (DLP),
- Balküpü (honeypot) tuzak sistemi,
- Ağ erişim kontrolü sistemi (NAC),
- Çok faktörlü kimlik doğrulama (MFA),
- Güvenlik açıklığı yaması.

b. Fiziksel Kontroller

Fiziksel kontroller, teknik kontrollerin tersine fiziksel dünyada mevcut olan somut kontrollerdir. Fiziksel ve çevresel risklere karşı önlem alarak söz konusu risklerin azaltılmasına yönelik fiziksel kontroller tasarlanır. Örnek olarak (Başaranoğlu, 2020):

- Güvenlik görevlisi,
- Gaz, hareket, sıcaklık vb. sensörü,
- Biometrik sistem,
- Yangın söndürücü,
- Kilitli kapı,
- Kesintisiz güç kaynağı (UPS),
- Işıklandırma,
- Kamera,
- Çit, duvar,
- Kablolama.

c. İdari Kontroller

İdari kontroller, kurumsal politika ve prosedürlerden oluşan yönetsel kontrollerdir. Bu tür kontrollerin ayırt edici özelliği; insan faktörünü göz önünde bulundurarak "*operasyonel etkinlik, verimlilik ile mevzuata ve yönetim politikalarına uyum ile ilgili kurallar, prosedürler ve uygulamalar*"dan oluşmasıdır (ISACA, 2018). Örnek olarak (Başaranoğlu, 2020):

- Güvenlik politikası,
- Görevler ayrılığı,
- İşte rotasyon,
- Veri sınıflandırması,
- Çalışanların işe alınması, işten çıkarılması,
- Farkındalık eğitimi,
- İç denetim,
- Zorunlu izin kullandırılması,
- Felaket kurtarma planı,
- Bilgi sistemi kullanım kuralları.

Kontrollerin farklı açılardan ne şekilde tasarlanacağını ve uygulanacağını anlamak, bir işletme tarafından tasarlanan ve uygulanan kontrollerin değerlendirilerek kontrol alanlarındaki eksikliklerin

tespit edilebilmesi ve görüş oluşturulması için faydalı olacaktır. Bahsi geçen kontrol tipleri dışında birkaç kontrol kavramına aşağıdaki gibi bir örnek üzerinden değinilmektedir.

Veri merkezine girişte, kartlı giriş sistemi kullanılarak yalnızca veri merkezine yetkili personelin girmesini sağlamak bir *önleyici tedbirdir*. Veri merkezine girişin yasak olduğunu giriş kapısında uyarı yazısıyla bildirmek ise *caydırıcı kontrol* olarak uygulanır. Caydırıcı kontrolün önleyici kontrolden farkı, istenmeyen faaliyetleri yapılmasını engellemez; ancak gerçekleştirilmemesi yönünde uyarıcı ve ikna edici mahiyettedir.

Bir kontrol özelliği itibariyle birden çok kontrol tipine uygun olabilir ve farklı sınıflandırmalarda yer alabilir. Yukardaki senaryoda, kapı girişini bir güvenlik kamerasıyla kaydetmek *tespit edici* bir kontrol olarak uygulanabilir ve kartlı giriş sistemindeki bir problemde kapının açık kalması veya kapıyı zorlayarak girişlerin belirlenebilmesi gibi riskleri azaltmaya yönelik olarak *telafi edici kontrol* olarak tanımlanabilir (Gregory, 2019).

Kartlı giriş sistemine ek olarak veri merkezine girişi kısıtlamak için anahtarla açılabilen kapı kilidi kullanılması ise *örtüşen kontroldür*. Veri merkezine girişin kısıtlanması için iki kontrol de tek başına yeterli kontrollerdir ve birlikte uygulanarak aynı amaca yönelik birbirini tamamlamaktadır (ISACA, 2019: 43).

Bir işletme tarafından uygulanan kontroller;

- Etkinlik,
- Verimlilik,
- Uygunluk,
- Güvenilirlik,
- Gizlilik,
- Bütünlük,
- Erişilebilirlik

kavramlarıyla yakından ilgilidir (Firebrand Training Ltd., 2017). İşletmeler, iş hedeflerini gerçekleştirmek ve belirli riskleri yönetmek için bu ana kavramlar çerçevesinde oluşturulan kontrol hedeflerine ulaşmak için kontrol faaliyetlerini yerine getirir. Kontrol hedefi, "b*elirli bir süreçte kontrol prosedürlerinin uygulanmasıyla elde edilecek istenen sonucun veya amacın ifadesi*" olarak tanımlanmaktadır (ISACA, 2018). Bu kapsamda, kontroller tasarlanırken kontrol hedeflerinin de belirli olması gerekir. Çünkü uygulanan kontrollerin izlenmesi sürecinde etkinliği, belirlenen kontrol hedeflerine ne kadar ulaşılıp ulaşılamadığı ile ölçülür. Bu bağlamda, her bir kontrol faaliyeti bir kontrol hedefi ile ilgili olmalı, her bir kontrol hedefi için de gerekli bütün kontrol faaliyetleri tanımlı olmalıdır (Clarke, 2018). Bir kontrol hedefi genel olarak aşağıdaki hususları ele alır (Cascarino, 2012):

- Operasyonel süreçlerin etkinliği ve verimliliği,
- Yasal mevzuata ve düzenlemelere uygunluk,
- Varlıkların korunması,
- Bilginin güvenilirliği ve bütünlüğü.

Kontrol hedeflerinin gerçekleştirilmesine katkıda bulunan faaliyetler, kontrol önlemi olarak tanımlanmaktadır (ISACA, 2019: 42). Kontrol önlemleri, tehdit oluşma riskini önlemek, ortadan kaldırmak veya azaltmak için uygulanan faaliyetlerdir (Doshi, 2020). Kontrol hedefleriyle birlikte kontrol önlemleri, çalışanların iş tanımlarında bir rol tanımı olabilecek şekilde kurumsal amaçların daha küçük amaçlara ve faaliyetlere ayrıştırılmasına hizmet eder.

Bilgi sistemleriyle ilgili kontrol hedefi ve kontrol örneklerine aşağıdaki tabloda yer verilmektedir (Hingarh ve Ahmed, 2013; ISACA, 2019: 42; DDO, 2020; TSE, 2013; Polat, 2021a).

KONTROL HEDEFLERİ	KONTROLLER
Kullanıcı bilgisayarlarının internet üzerinden yetkisiz erişimlere karşı korunması	İşletim sistemi ve uygulamaların en kararlı, güncel ve güvenilir güncellemelerinin ve yamalamalarının yapılması Zararlı yazılımların çalışmasını önleyici uygulamaların kullanılması İşletim sistemi varsayılan ayarları kullanılmayarak güvenlik sıkılaştırmalarının yapılması İnternet ağ trafiği üzerinde güvenlik duvarı, antivirüs, saldırı tespit ve önleme sistemleri kullanılması Düzenli veri yedeği alınması Kullanıcı farkındalığı eğitimlerinin verilmesi
Bilgi sistemleri ile ilgili yasal mevzuat ve düzenlemelerden kaynaklanan gerekliliklere uyumun sağlanması	Yasal mevzuat ve düzenlemelerden gelen gerekliliklerin belirlenmesi Gerekliliklerin nasıl karşılandığı ile birlikte dokümante edilmesi ve güncel bir şekilde tutulması Gerekliliklere uyumun düzenli gözden geçirilmesi
Bilgi sistemleri üzerindeki verilerin gizliliğinin sağlanması	Veri envanterinin oluşturulması Veri sınıflandırılması yapılması Veri saklama ve imha prosedürünün oluşturulması Kritik verilerin şifrelenerek saklanması ve iletilmesi Bilgi sistemlerine erişim denetimi politikasının oluşturulması
Geliştirilen uygulamalarda veri bütünlüğünün sağlanması	İşlem ve iletim kayıtlarının tutulması Veri mutabakatı Hata düzeltme Sıra, limit, aralık vb. veri doğrulamalarının yapılması Kritik verilerin güvenli alanda depolanması Hazır raporlama şablonların kullanımı
Bilgi Sistemlerinin erişilebilirliğinin sağlanması	İş sürekliliği planları Felaket kurtarma planları Yedekleme prosedürleri Kapasite ve yedeklilik planlaması Personel eğitimi
Uygulama geliştirme güvenliğinin sağlanması	Uygulama güvenlik ve performans gereksinimlerinin belirlenmesi Güvenli sistem geliştirme ortamlarının kullanılması Değişiklik yönetiminin yapılması Dışarıdan sağlanan geliştirme hizmetlerinin izlenmesi Gerçek ortama geçişte güvenlik testlerinin yapılması
Operasyonel süreçlerin etkinliğinin ve verimliliğinin sağlanması	Operasyonel süreçleri destekleyen politika ve prosedürlerinin oluşturulması Değişikliklerin yönetilmesi Kaynakların kullanımının izlenmesi Kullanıcı, yönetici işlemleri, hatalar, bilgi güvenliği ihlalleri kayıt ve gözden geçirilmesi
Etkin siber güvenlik olay yönetimiyle bilgi sistemleri güvenliğinin sağlanması	Siber olay müdahale planının hazırlanması Siber olaylara müdahale ekibinin oluşturulması Siber olayları iletişim bilgilerinin tutulması Tehdit bildirimlerinin yönetilmesi Periyodik siber tatbikat yapılması

1.2.1.3. Denetimde Önemlilik ve Risk

Önemlilik ve risk kavramları, denetim sürecinin etkin bir şekilde yürütülmesi için anlaşılması gereken temel kavramlardandır. Bir işletme, iş hedeflerine ulaşabilmesi yönünde risklerini yöneterek olması muhtemel olayları önlemek, tespit etmek ve sınırlamak için idari, teknik, yönetim veya yasal nitelikte olabilecek politikalar, prosedürler, kılavuzlar, uygulamalar veya organizasyonel yapılardan oluşan kontrolleri uygular. Bilgi sistemleri denetimi, bilgi sistemleri kontrolleriyle yakından ilişkilidir ve işletmelerin sahip olduğu kontrol hedeflerinin tam tersi yönde yer alan bilgi sistemlerindeki riskler gibi bilgi sistemi denetim amaçlarına ulaşılabilmesi için denetim sürecinde de bilinmesi gereken risk unsurları bulunur. Bu bağlamda, etkin bir denetim süreci yürütülerek denetim görüşüne makul güvence sağlanması, denetim riski ve önemlilik kavramlarının birlikte değerlendirilerek denetim planlaması ve yürütülmesinde göz önünde bulundurulmasına bağlıdır.

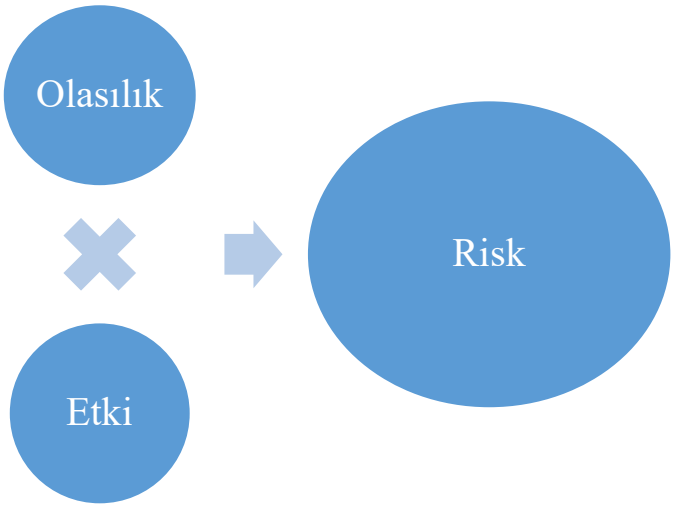
Bu kavramlara değinmeden önce riskin genel olarak tanımını yapmakta fayda bulunmaktadır. Riskin farklı kaynaklardaki tanımları şu şekildedir:

- "*Kurum ya da işletmenin amaç ve hedeflerine ulaşmasına ve görevlerin ifasına engel olabilecek veya belirlenmeyen zararlara (sonuçlara) yol açabilecek durum ya da olaylar*" (Aksoy, 2018),

- "*Bir olay olasılığının ve sonuçlarının kombinasyonu*" (ISACA , 2018),

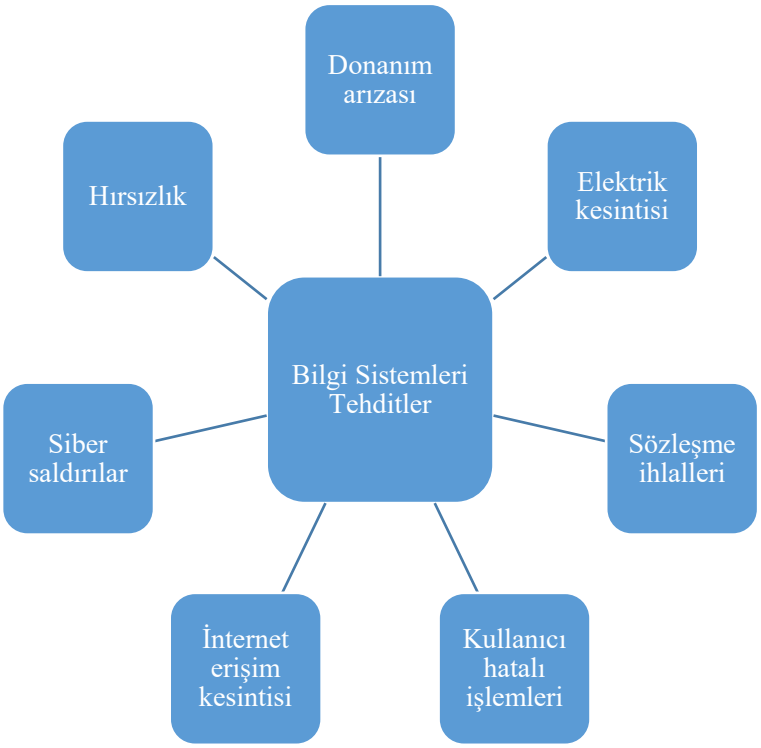
- "*İşletmeyi etkileyebilecek olası olaylar*" (Doshi, 2020).

Tanımlardan anlaşılacağı üzere, risk kapsamında olasılık ve etki olmak üzere iki temel unsurun ilişkisi ele alınmaktadır. Bir olayın gerçekleşme olasılığı ile etkisi eşit derecede önemlidir ve ancak birlikte değerlendirilerek oluşabilecek risk konusunda bir sonuca ulaşılabilir. Bu çerçevede, riski aşağıdaki formülle modellenebilir (Doshi, 2020):



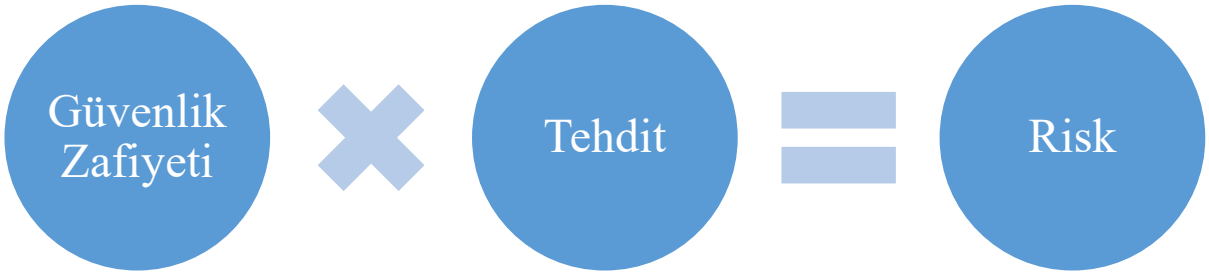
Şekil 5: Risk Formül-1

Risk kavramı, yukarıdaki formül ile somutlaştırılmaya çalışılmıştır. Buna ilave olarak; genel iş hedefleri, kontrol hedefleri veya bütünlük, gizlilik, erişilebilirlik gibi temel hedefler ile birlikte bu hedefleri etkileyen olayları birlikte dikkate almak, riskleri belirlemenin ve anlayabilmenin en kolay yoludur. Bilgi sistemleri özelinde risk oluşturabilecek olayların bazılarına aşağıdaki şekilde yer verilmektedir (IA COP, 2014):



Şekil 6: Bilgi Sistemleri Risk Oluşturabilecek Olaylar

Bilgi sistemlerinde risk oluşturabilecek olay örneklerinde de görüleceği üzere, işletmeler bilgi sistemleri özelinde birçok riske maruz kalmaktadır. Bu risk oluşturabilecek olaylar, daha önce de belirtildiği üzere operasyonel süreçlerin etkinliği ve verimliliği, yasal mevzuata ve düzenlemelere uygunluğu, bilginin güvenilirliği ve bütünlüğü, varlıkların korunması gibi konularda işletmelerin kontrol hedeflerini etkileyen olaylardır. Bilgi sistemleri denetiminde, kontrol hedeflerine ulaşılması yönünde kontrollerin uygulanmaması veya yetersiz uygulanması nedeniyle ortaya çıkabilecek risklerle ilgilenilir (Hingarh ve Ahmed, 2013). Bu noktada, bilgi sistemlerine ait söz konusu riskler, bir başka yöntem olarak bilgi sistemi güvenlik zafiyeti ve tehdit kavramları üzerinden oluşturulan aşağıda yer alan formül üzerinden incelenebilir (Doshi, 2020).



Şekil 7: Risk Formül-2

Riskin tanımlandığı bu ikinci formülde terimler arasında matematiksel bir çarpma işlemi olduğu düşünülmemeli, riski anlamanın bir başka yolu olarak bilgi sistemi güvenlik zafiyetleri ve tehditlerin birleşiminden oluşan bir model olarak görülmelidir. Bu formülde risk, bilgi sistemi varlığındaki güvenlik zafiyetlerinden faydalanan bir tehdidin varlığa doğrudan zarar verme potansiyeli şeklinde ifade edilmektedir. Söz konusu bileşenlerin tanımları aşağıdaki gibidir.

Güvenlik Zafiyeti: Sistemi tehdit olaylarından kaynaklanan tehditlere maruz bırakabilecek bir sürece ait tasarım, uygulama, işletim veya iç kontrolündeki bir zayıflıktır (ISACA, 2018).

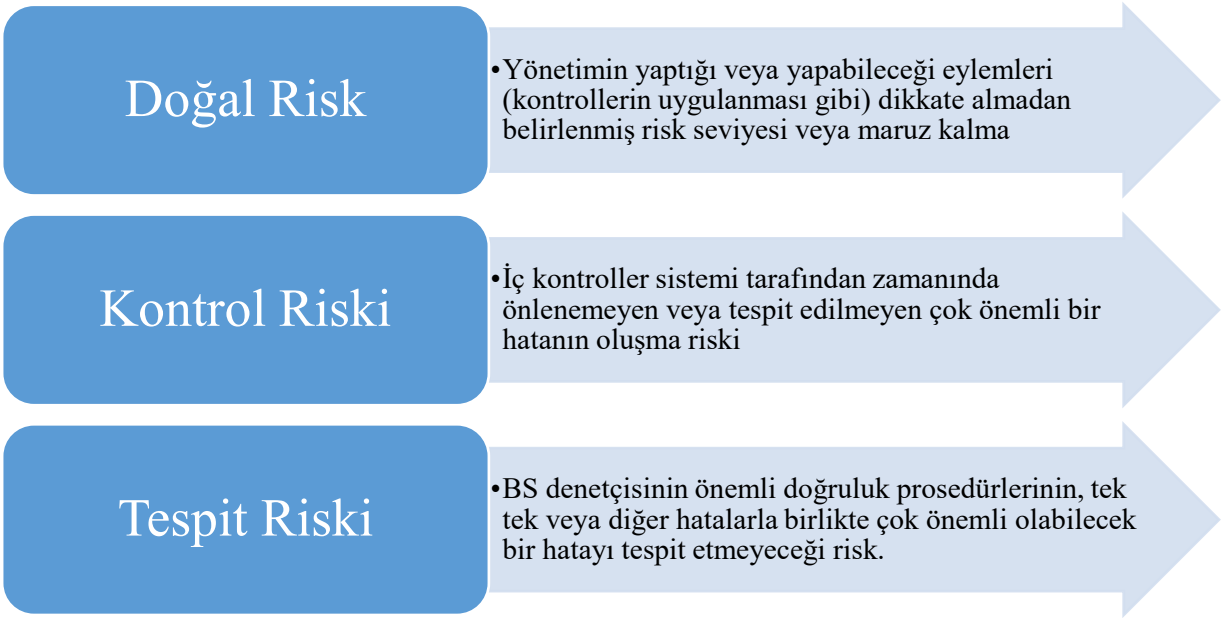
Tehdit: Tehdit, bir varlığa karşı, zararla sonuçlanabilecek şekilde hareket edebilecek herhangi bir şeydir (nesne, madde, insan vb.). İstenmeyen bir olayın potansiyel nedenidir (ISACA, 2018).

Güvenlik zafiyeti, bilgi sisteminde yer alan güvenlik açıklığıdır ve işletme tarafından kontrol edilebilir. Tehdit ise bu açıklıktan yararlanan işletmenin kontrolünde olmayan bir unsurdur. Zayıf şifreleme teknikleri, güncelleme eksikliği, yetkilendirme ve yapılandırma eksikliği, anti-virüs programının olmaması gibi iç unsurlar genellikle güvenlik zafiyetlerini oluştururken; tehditler genellikle hırsızlık, donanım arızası, internet üzerinden saldırılar, doğal afetler vb. dış unsurlardan oluşur (Doshi, 2020).

Kısacası, risk oluşabilmesi için bir olayın gerçekleşme olasılığı, olayın etkisi, güvenlik zafiyetleri ve bu zafiyetleri kullanacak tehditlerin bulunması gerekir. Bahsedilen her iki formülde de göz önünde bulundurulması gereken ortak bir husus da riske karşı korunmak istenen bilgi sistemi varlığının işletme tarafından atfedilen değeridir. Bu kapsamda, bir varlık üzerindeki risk düzeyinin belirlenmesinde varlığın değeri de önemli bir çarpandır.

İşletmeler riskleri ortadan tamamen kaldıramayacağı için yönetim sorumluluğunda iş hedeflerine yönelik söz konusu riskleri yönetirler. Denetim faaliyetleri de risklerin ne kadar iyi yönetildiğini izlemeye yönelik yönetime yardımcı olur (Cascarino, 2012). Kurumsal risk yönetimiyle aynı şekilde, denetim faaliyetleri yerine getirilirken de bir takım belirsizliklerin olduğu kabul edilip uygun bir biçimde riskler yönetilmelidir. Bu kapsamda, etkin bir denetim süreci gerçekleştirmek için, işletmenin maruz kaldığı riskler kadar denetim riski de iyi anlaşılmalıdır.

Denetim riskinin, sözlük tanımı "*denetim bulgularına dayanarak yanlış bir sonuca varma riski*" şeklindedir (ISACA, 2018). Bir diğer ifadeyle, denetim sürecinde "*toplanan bilgilerin denetim sırasında tespit edilemeyen önemli bir hata içermesi riski*" olarak tanımlanabilir (ISACA, 2019: 44). Denetim riski aşağıda verilen üç risk bileşeninden etkilenir (ISACA, 2018):



Şekil 8: Denetim Riskini Etkileyen Risk Bileşenleri

Doğal risk, bir kontrol uygulamadan önce bilgi sistemi varlıklarının, bilgi güvenliğini tehlikeye atma eğilimidir (Hingarh ve Ahmed, 2013). Herhangi bir önlem alınmamış en kötü senaryoyu ifade eder (Cascarino, 2012). İnternet erişimi olan bir bilgisayara virüs bulaşması ihtimali buna örnek verilebilir. Doğal riskler, denetimden bağımsız olduğundan denetim kapsamında bu riskin sadece etkileri değerlendirilmeye çalışılır (Aksoy, 2018). Bunun için işletme faaliyetleri iyi anlaşılmalı, hangi faktörlerin bir riskin var olduğunu gösterdiği dikkate alınmalıdır (Cascarino, 2012). Bu riski etkileyebilecek faktörler (*Chapter 7 Assessing the Risk of Material Misstatement*, t.y.):

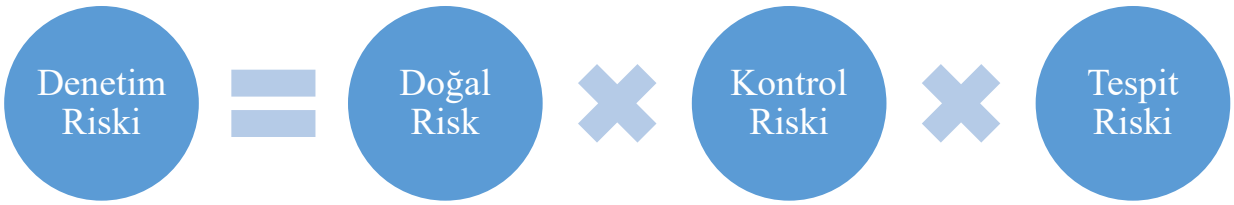
- İşletmenin yapısı,
- Yönetimin dürüstlüğü,
- Önceki denetim çalışmalarının sonuçları,

- Denetimin ilk kez yapılacak olması,
- İlgili taraflar,
- Olağanüstü işlemler,
- İşletmede süregelen sorunlar,
- Personeldeki sürekli değişim,
- Teknolojik gelişmeler.

Doğal risk azaltılmak için işletmeler tarafından kontroller uygulanır. Bu yönde yeterli kontrollerin tasarlanıp tasarlanmadığı, tasarlanan kontrollerin verimli bir şekilde çalışıp çalışmadığı ile ilgili riskler ise kontrol riskleridir. Bir bilgisayarda anti-virüs programı kullanılması virüslerin bulaşmasını önleyici bir kontroldür fakat bu programın en güncel virüs tanımlamalarını içermemesi kontrolün verimsiz çalışmasıdır (Hingarh ve Ahmed, 2013). Doğal riskleri azaltmak için kontrollerin uygulandığı gibi kontrollerin önleyememesi veya tespit edememesi risklerini azaltmak için kontrollerin denetimi gerçekleştirilir. Bu süreçte kontrollerin doğru bir şekilde değerlendirilebilmesi için kontrollerin etkinliğinin nasıl ölçüleceğinin anlaşılmasıyla birlikte hedeflerin gerçekleştirilmesi ve riskin azaltılmasına yönelik en yüksek derecede güvence sağlayan kontrollerin belirlenebilmesi gerekir (Cascarino, 2012). Etkin kontrollerin uygulanması neticesinde kontrol riski azalacaktır.

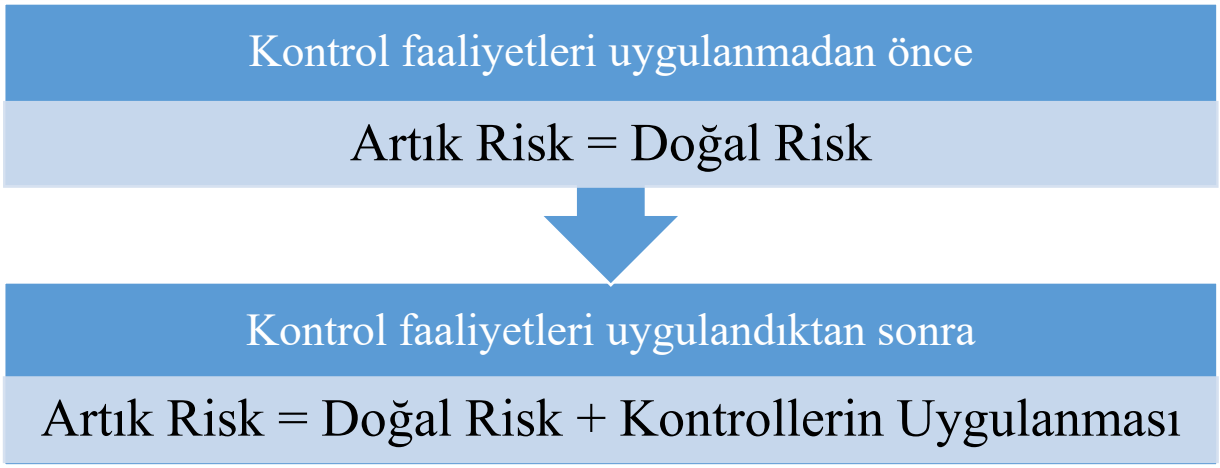
Doğal risk ve kontrol risk, önemli yanlışlık riskinin bileşenleridir. Önemli yanlışlık riski, denetim öncesinde denetlenecek unsurlarda önemli bir yanlışlığın bulunması riskidir. Doğal riskin ve kontrol riskinin, bilgi sistemlerinin önemli bir yanlışlık içerme risklerine karşılık geldiği gibi, bilgi sistemleri denetimi sırasında bu hataların fark edilmeme olasılığı bulunmaktadır. İşte özellikle önemli bir yanlışlığı bilgi sistemleri denetimlerinin tespit edememe veya önleyememe ihtimalini de tespit riski ifade eder (Hingarh ve Ahmed, 2013; Doshi, 2020). Tespit riskinde, diğer risklerden farklı olarak denetçinin iradesi söz konusudur. Başka bir ifadeyle, tespit riski denetim tekniklerinin nitelik, zamanlaması ve kapsamıyla etkin bir şekilde uygulanıp uygulanmadığına bağlı olarak şekillenir (Aksoy, 2018).

Denetim riskini doğal risk, kontrol riski ve tespit riski arasındaki ilişkiye göre aşağıdaki formülle modelleyebiliriz (Doshi, 2020).



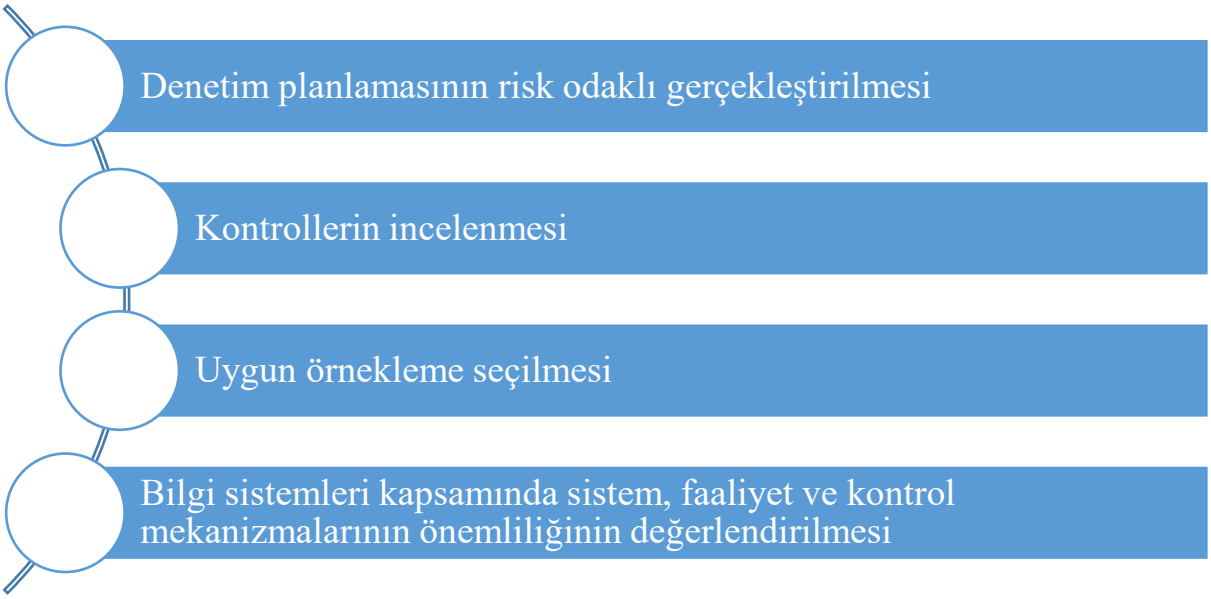
Şekil 9: Denetim Risk Modeli

Denetim riski, "*bilgilerin veya finansal raporların önemli hatalar içermesi ve denetçinin meydana gelen bir hatayı tespit edememesi olasılığı*"dır (ISACA, 2019: 44). Diğer bir değişle, bilgilerin veya finansal raporların önemli yanlışlık içermesine rağmen denetçinin duruma uygun olmayan bir denetim görüşü verme riskidir. Önemli yanlışlık riski (doğal risk ve kontrol riski) ile tespit edememe riskinin bileşenidir. Formüldeki ilk iki bileşenin risk değerlendirilmesinin uygun bir şekilde yapılması, denetim kapsamının önemli riskleri ele alabilmesini sağlar. Bu da hedeflerin net olarak anlaşılması ve bu hedefleri etkileyen olası olayların belirlenmesinden geçer. Denetim planlamasında temel odak noktası, yüksek "*artık risk*" seviyelerini belirleyebilmektir. Hedeflere yönelik kontrollerin tasarlanıp uygulanmasından sonra kalan risk "*artık risk*" olarak ifade edilir. Herhangi bir kontrol uygulanmadığı durumda faaliyetlerin oluşturduğu doğal risk, artık risk olarak ilgi merkezi olacaktır (IA COP, 2014). Bu kapsamda, artık risk ve doğal risk aşağıdaki şekilde şematize edilebilir.



Şekil 10: Artık Risk

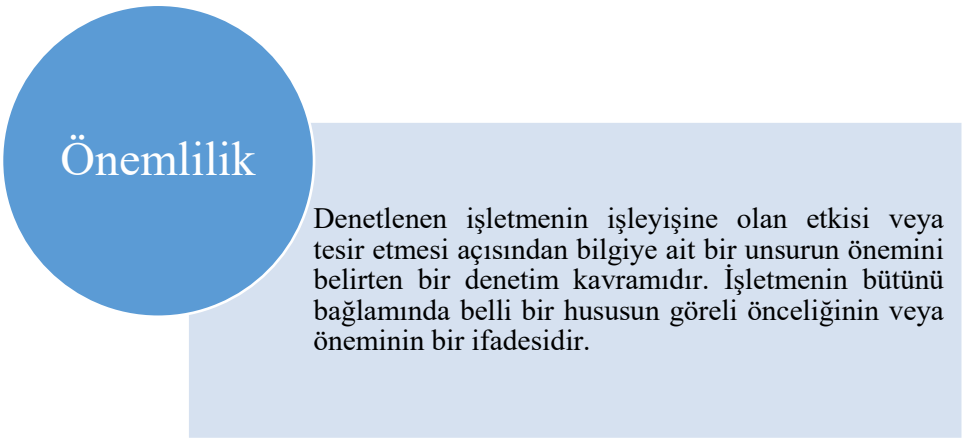
Denetim riskini azaltmak için tespit riski azaltılarak denetlenen tarafından azaltmaya çalışılması gereken artık riskler belirlenmelidir. Bu yönde aşağıdaki şekilde yer alan hususlar uygulanır (Doshi, 2020).



Şekil 11: Denetim Riskinin Azaltılması

Denetim riski; BSBD Tebliği'nde ele alınmış ve denetçinin yapısal, kontrol ve tespit risklerine bağlı olarak doğru görüş verememesi olasılığı olarak tanımlanmıştır. Yapısal risk, kontrolün olmaması nedeniyle, en azından kayda değer olan bir kontrol eksikliğinin var olması riski; kontrol riski ise kontrolün layıkıyla çalışmaması sebebiyle, en azından kayda değer olan bir kontrol eksikliğini önleyememesi, ortaya çıkaramaması veya zamanında düzeltememesi riski; tespit riski ise denetçinin, denetlenenin bilgi sistemlerinde yer alan en azından kayda değer olan bir kontrol eksikliğini ortaya çıkaramaması riski olarak ifade edilmiştir. Önemli veya kayda değer kontrol eksikliği riski ise denetlenenin bilgi sistemlerinde en azından kayda değer olan bir kontrol eksikliğinin bulunması riskini ifade eder. Önemli ya da kayda değer kontrol eksikliği riski, yapısal risk ve kontrol riskinden kaynaklanır. Denetçinin, denetim riskini makul düzeye indirebilmek için, önemli veya kayda değer kontrol eksikliği riskinin yüksek olduğu alanlarda tespit riskini düşürecek şekilde uygun denetim tekniklerini kullanması gerekir.

Denetim kapsamında göz önünde bulundurulması gereken bir diğer kavram ise önemliliktir. Önemlilik, ISACA terimler sözlüğünde (2018) aşağıdaki şekilde tanımlanmıştır.



Şekil 12: Önemlilik Kavramı

Önemlilik, denetim riskiyle yakından ilişkili olup, aralarında her zaman tersine bir ilişki vardır. Denetim riski yüksek olan alanların denetimi, daha ayrıntılı şekilde gerçekleştirilir ve daha fazla kanıta başvurulur. Önemlilik, denetim riski ile birlikte denetimin planlanması ile gerekli alanlarda yoğunlaşarak yürütülmesi aşamalarında dikkate alınır. Bununla birlikte, denetim bulgularının etkisi değerlendirilirken de göz önünde bulundurulur (Aksoy, 2018). Daha yüksek önemliliğe sahip denetim alanlarında denetim riskini azaltmak için tespit riski ve kontrol riskinin azaltılmasına yönelik çalışmalar genişletilerek daha kapsamlı bir inceleme yürütülür. Değişik denetim türlerinde önemlilik değişik şekillerde yer alır.

BSBD Tebliği'nde denetimin planlama ve yürütülmesindeki öneminden ötürü önemlilik hususu düzenlenmiştir. Önemliliğin, mesleki bilgi ve tecrübeye dayalı bir mütalaa konusu olduğu belirtilerek, bilgi sistemlerinde kontrol zayıflıkları sonucu ortaya çıkabilecek hataların, ihmallerin, prosedürlere aykırılıkların ve hukuka aykırı fiillerin, denetlenenin finansal verilerini raporlamalarına, güvenli ve kesintisiz hizmet sağlamalarına etkisinin değerlendirilmesi olarak tanımlanmıştır. Önemlilik, denetimin planlanması, gerekli alanlarda yoğunlaştırılması, bulguların değerlendirilmesi ve raporlanması için kullanılabilir. Başta finansal veriler olmak üzere denetlenen açısından hassasiyet arz eden verilerin bütünlüğü, tutarlılığı, güvenilirliği, gereken durumlarda gizliliği ve faaliyetlerin sürekliliği önemlilik kavramı kapsamında dikkate alınması gereken temel unsurlardır.

Finansal raporları etkileyen kontrollerin değerlendirilmesinde;

- süreç veya sistem tarafından yürütülen finansal işlemin değeri,
- işlem sıklığı,

Finansal işlemlere ilişkin olmayan kontrollerin değerlendirilmesinde ise;

- iş sürecinin kritikliği,
- sistem ve operasyonların maliyeti,
- hataların muhtemel sonuçlarının büyüklüğü,
- bir zaman aralığında gerçekleşen işlem/sorgu sayısı,
- tutulan dosyaların ve üretilen raporların niteliği, zamanlaması ve kapsamı,
- hizmet seviyesi anlaşmalarının gerekleri,
- ceza maddelerindeki para cezası tutarları

gibi öğeler kullanılır.

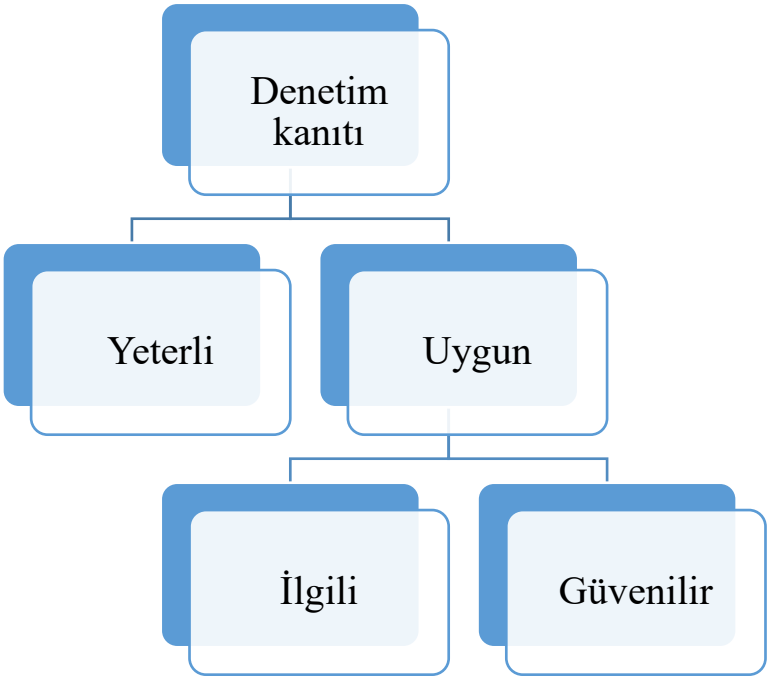
1.2.1.4. Kanıt Toplama ve Örnekleme

Denetim faaliyetleri sonucunda ulaşılacak geçerli bir görüşe temel oluşturmak üzere gerçekleştirilmesi gereken kanıtların toplanması ve örnekleme çalışmaları denetim sürecinde bahsedilmesi gereken diğer önemli ana hususlardır. Bu bölümde öncelikle denetim kanıtı kavramı,

kategorileri ve toplama yöntemleri ele alındıktan sonra denetim örneklemesi, türleri, riski ve terimleri ile uyumluluk testi (kontrol testi) ve önemli doğruluk testi (maddi doğrulama prosedürleri) konularına yer verilmektedir.

1.2.1.4.1. Kanıt Toplama

Kanıt, *"belirtilen bir sorunu kanıtlayan ve aksini kanıtlayan bilgiler*"dir. Denetim kanıtı ise tanım olarak "*denetim görüşünü desteklemek için kullanılan bilgiler*" şeklinde açıklanmaktadır (ISACA, 2018). Denetim faaliyetlerinin çoğunluğunu, denetim görüşünün oluşturulması için denetim kanıtlarının toplanması ve değerlendirmesi çalışmaları oluşturmaktadır. Denetim görüşüne makul güvence sağlanması, denetim riskinin kabul edilebilir bir seviyeye indirecek yeterli ve uygun olarak sınıflandırılabilecek denetim kanıtlarıyla mümkün olmaktadır. Denetim kanıtının yeterliliği kanıtın miktarının ölçütüyken; denetim kanıtının uygunluğu ise kanıtın kalitesinin ölçütüdür. Denetimin yeterliliği ve uygunluğu birbiriyle ilişkilidir; denetim kanıtının kalitesi arttıkça daha az miktarda denetim kanıtı yeterli olabilir (KGK, 2019). Denetim kanıtlarının sınıflandırmalarına ait tanımlar aşağıda yer almaktadır (Cascarino 2012; ISACA, 2018; KGK, 2019).



Şekil 13: Denetim Kanıtı Özellikleri

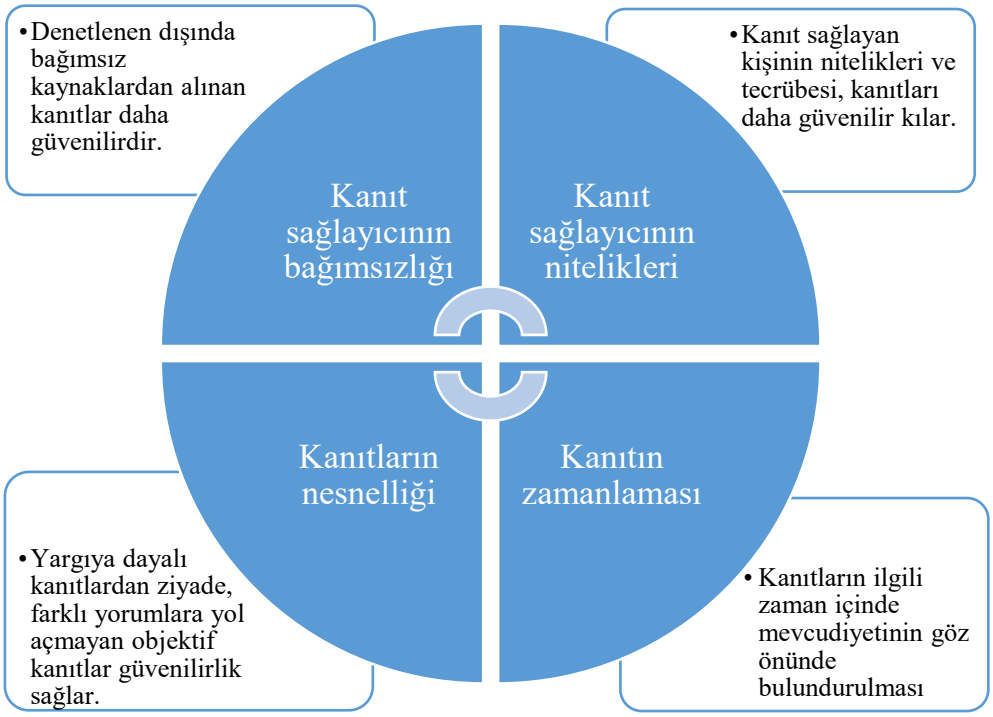
- **Yeterli (sufficient)**, ihtiyatlı bir kişinin de denetçiyle aynı sonuçlara varabileceği şekilde gerçekçi, yeterli miktarda ve inandırıcı olması,

- **Uygun (appropriate/competent)**, denetçi görüşünün dayanağını oluşturan sonuçların desteklenmesi bakımından ihtiyaca uygunluğu ve güvenilir olması,

- **İlgili (relevant)**, denetim bulgularını ve tavsiyelerini desteklemesi ve denetimin hedefleriyle tutarlı olması,

- **Güvenilir (reliable)**, denetçi görüşüne göre geçerli, olgusal, nesnel ve destekleyici nitelikte olması.

Denetim kanıtları, nitelik olarak kümülatiftir ve uygulanan denetim prosedürlerinden elde edilir. Denetim görüşüne dayanak oluşturacak yeterli ve uygun denetim kanıtlarının elde edilip edilmediği mesleki muhakeme konusudur. Önemlilik ve risk, bu muhakeme sürecine etkisi olan önemli faktörler arasındadır. Denetim kanıtının güvenilirliği, kanıtın kaynağı ile niteliğinden etkilenir ve kanıtın elde edildiği şartlara bağlıdır (KGK, 2019). Denetim kanıtının güvenilirliğine etki eden faktörler aşağıdaki gibidir (Doshi, 2020; Gregory 2012):

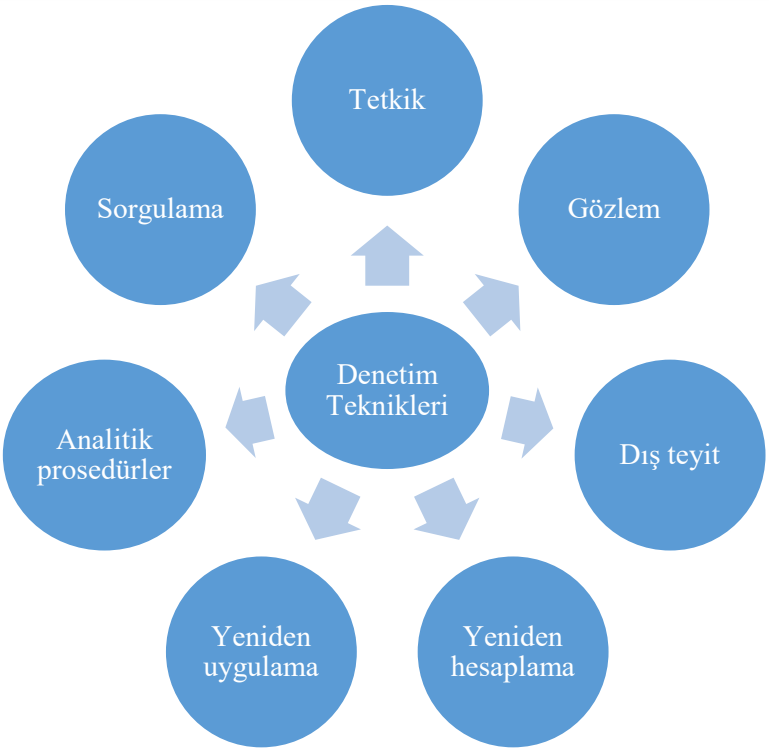


Şekil 14: Denetim Kanıtı Güvenilirliğine Etki Eden Faktörler

Denetim kanıtlarının en sık karşılan kategorileri şunlardır (ISACA, 2019: 54; Gregory, 2012):

- Gözlemler,
- Görüşme notları,
- Yazışmalar,
- Diğer denetçilerden bağımsız teyitler,
- Dahili süreç ve prosedür belgeleri,
- Test sonuçları,
- İş kayıtları,
- Sayımlar,
- Dış teyitler.

Kanıt elde etmek amacıyla kullanılan yöntemlere denetim teknikleri denilmektedir, Denetim sürecinde farklı denetim kanıtları toplama yöntemleri (denetim teknikleri) aşağıdaki gibidir (KGK, 2019):



Şekil 15: Denetim Kanıtı Toplama Yöntemleri

Tetkik: İşletme içinden veya dışından elde edilen, basılı veya elektronik ortamda ya da başka bir depolama ortamında bulunan kayıt veya belgelerin incelenmesi ya da varlıkların fiziki olarak incelenmesi,

Gözlem: Bir süreç veya prosedürün uygulanması esnasında hazır bulunularak izlenmesi,

Dış Teyit (Doğrulama): Üçüncü bir taraftan işletmeye ait bilgileri teyit amaçlı basılı, elektronik ortamda ya da başka bir depolama ortamında yazılı yanıtların alınması,

Yeniden Hesaplama: Belge veya kayıtların matematiksel doğruluğunun kontrolü,

Yeniden Uygulama: İşletmenin iç kontrolünün bir parçası olarak uygulanmış olan prosedür veya kontrollerin, bağımsız bir şekilde yürütülmesi,

Analitik Prosedürler: Denetlenen süreçlerin ve faaliyetlerin makul olup olmadığını belirlemek için karşılaştırmaların ve ilişkilerin kullanılması,

Sorgulama: İşletme içindeki veya dışındaki bilgili kişilerden sözlü veya yazılı bilgi alınması.

Bilgi sistemleri denetimi kapsamında ayrıca aşağıdaki tekniklerde kullanmaktadır (DDO, 2021:24):

Güvenlik Denetimi: Bilgi sistemleri kurallarının, sıkılaştırma ve yapılandırma çalışmalarının teknik olarak denetlenmesi,

Sızma Testi: Bilgi sistemleri kapsamında güvenlik açıklarının tespit edilmesini sağlayan, yetkin kişiler tarafından ve düzenlemelere uygun olarak gerçekleştirilen güvenlik testleri,

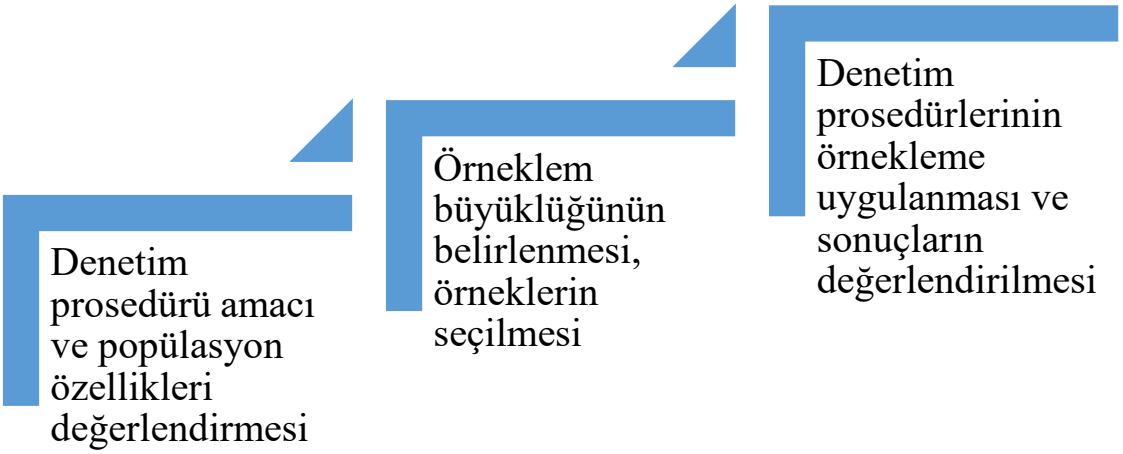
Kaynak Kod Analizi: Güvenli yazılım geliştirme konusunda yetkin kişiler tarafından kaynak kodların incelenmesi ve güvenlik açıklarının tespit edilmesini sağlayan denetim çalışması.

1.2.1.4.2. Denetimde Örnekleme

Denetim teknikleri uygulanırken zaman ve maliyet faydası nedeniyle denetim örnekleme yöntemine başvurulur. Denetim örneklemesi, denetim için popülasyon (anakitle) hakkında bir sonuca ulaşılmak istenilen veri setinin tamamının içerisinden bir alt küme (örneklem) oluşturularak örnekler seçme işlemidir ve "*Popülasyonun belirli bir özelliği hakkında denetim kanıtını elde etmek için bir*

popülasyonda bulunan öğelerin yüzde 100'ünden daha azına denetim prosedürlerinin uygulanması" şeklinde tanımlanır (ISACA, 2018). Örneklemenin, seçildiği popülasyon veri setinin tamamı hakkında sonuçlara varmak için makul bir dayanak oluşturması amaçlanır. Bu şekilde, örnekleme denetim kanıtı toplamada zaman ve maliyet açısından verimlilik ve etkinlik sağlar (Cascarino, 2012). Denetim örneklemesi ile ilgili iki temel yaklaşım bulunur:

- İstatiksel örnekleme,
- İstatistiksel olmayan örnekleme.



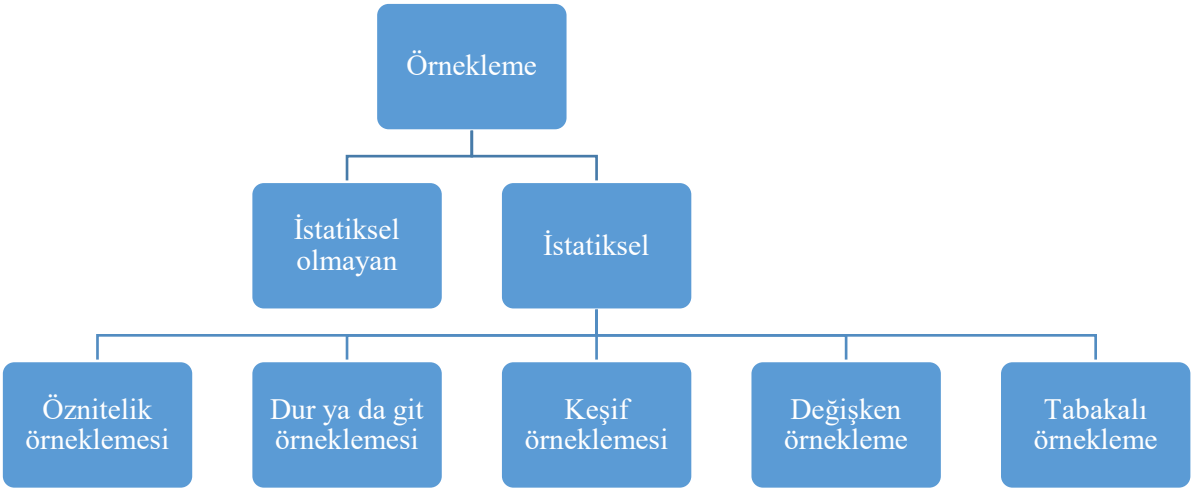
Şekil 16: Denetim Örnekleme Süreci

Denetim örneklemesinde, örnekleme yaklaşımından bağımsız olarak, yukarıda şekilde yer verildiği üzere örnekleme büyüklüğünün belirlenmesi, örneklerin seçilmesi ve örneklerin değerlendirilmesi aşamaları gerçekleştirilir. Hem istatiksel hem de istatiksel olmayan örnekleme yaklaşımında, mesleki muhakeme örneklerin planlamasında, testlerin yürütülmesinde ve toplanan kanıtların değerlendirilmesinde kullanılır. Fakat örnekleme riski noktasında aralarında temel bir fark bulunmaktadır. İstatiksel olmayan örneklemede, örnekleme riski sayısal olarak hesap edilemezken; istatiksel örneklemede örnekleme riski matematiksel olarak ölçülebilmektedir. Örnekleme sonuçlarının popülasyonun genelinde tahmin edilebilmesi istatiksel örneklemeyle mümkünken istatiksel olmayan örnekleme sonuçları popülasyonun tamamına yansıtılamayabilir. İstatiksel örnekleme ve istatiksel olmayan örneklemenin karşılaştırmasına aşağıdaki tabloda yer verilmektedir (van der Nest vd., 2015).

İstatiksel Örnekleme	**İstatiksel Olmayan Örnekleme**
"*Bir popülasyonun bir bölümünü, tüm popülasyonun özellikleri ile ilgili bilimsel ve matematiksel olarak çıkarımlarda bulunma amacıyla matematiksel hesaplamalar ve olasılıklar aracılığıyla seçme yöntemi.*" (ISACA, 2018)	"*Bir önermenin hızlı bir şekilde teyit edilmesi amacıyla, bir toplumun bir kısmının kendi yargısı ve deneyimi aracılığıyla seçilmesi yöntemi. Bu yöntem, tüm popülasyonda matematiksel sonuçların elde edilmesine ve kullanılmasına izin vermez.*" (ISACA, 2018)
Nesnel bir yöntem	Öznel bir yöntem
Her bir kalemin eşit olasılıkta rastgele seçimi	Risk, önemlilik vb. kriterlere göre kişisel seçim
Sonuçların nicel olarak popülasyonun geneli için tahmin edilmesi	Popülasyonun geneli hakkında bir çıkarımda bulunamayabilir
Örnekleme riskinin hesap edilebilmesi	Örnekleme riski sayısal olarak hesap edilemez
Daha maliyetli	Daha az maliyetli
Karmaşık	Basit

Her iki yaklaşımdan uygun olanın seçilmesinde risk, popülasyon özellikleri ve test hedefleri belirleyici etkenlerdir (Cascarino, 2012). Popülasyonun tamamı hakkında bir sonuca ulaşılmak isteniyorsa istatiksel örneklem yaklaşımı kullanılmalıdır (ISACA, 2019: 52). İstatistiksel örneklem

yaklaşımı kapsamında uygulanan örneklem yöntemleri ve bunlara ilişkin açıklamalar aşağıda yer almaktadır (Gregory, 2019; Doshi, 2020).



Şekil 17: Örnekleme Yöntemleri

a. Öznitelik Örnekleme

Öznitelik örneklemesi, *"belli bir özelliğin varlığı veya yokluğuna dayalı olarak bir popülasyonun bir bölümünü seçme yöntemi*" (ISACA, 2018) olarak, bir popülasyonun özelliklerini incelemek ve "*Kaç tane?*" sorusuna cevap vermek için kullanılır. Seçilen örneklerin ne kadarında belirlenen özelliğin olduğu belirlenerek, sorunun cevabı genelde yüzde olarak ifade edilir.

b. Değişken Örnekleme

Bu örnekleme; "*bir örneğe bağlı olarak bir popülasyonun ortalama veya toplam değerini tahmin etmek için kullanılan bir örnekleme tekniği; parasal tutar gibi niceliksel bir özelliği yansıtmak için kullanılan istatistiksel bir model*" (ISACA, 2018) olarak nitelik verisinden daha fazla veri içerir. Değişken örnekleme ile "*Ne kadar?*" sorusuna cevap verilir ve tahmin edilen değer parasal değer, ağırlık, boy vb. ölçü birimleriyle ifade edilir.

c. Dur ya da Git Örneklemesi

Dur ya da git örneklemesi, popülasyonda düşük bir risk ve hata olma oranının beklendiği durumlarda, yeterli sonuca ulaşır ulaşmaz örnekleme durdurularak fazla örnekleme yapılmamasını sağlar. İlk değerlendirme neticesinde bir kanaate ulaşılmadıysa, örnek sayısı arttırılarak istenilen sonuca ulaşılana kadar denetim testine devam edilir. Bu şekilde mümkün olan en erken zamanda testin bitmesine izin vermek için kullanılır.

d. Keşif Örneklemesi

Yukarıdaki üç örnekleme yöntemi, örnekleme popülasyonun özelliklerinin belirlenmesi için kullanılıyorken; keşif örneklemesi popülasyon içerisinde en az bir istisna, hata bulmaya çalışırken kullanılır. Denetim kapsamında dolandırıcılık veya usulsüzlükler belirlenmek istendiğinde keşif örneklemesi kullanılır. Örnekleme büyüklüğü hatayı bulabilecek seviyede olmalıdır. Bir hatanın bulunmasıyla bütün popülasyonun hileli/düzensiz olduğu kanaatine varılarak olabilecek diğer istisnaların tespiti için daha yoğun çalışılmasını gerektirir. Adli bilişim çalışmaları, keşif örneklemesinin iyi bir örneği olarak kabul edilir (Polat, 2021c).

e. Tabakalı Örnekleme

Tabakalı örneklemede bir popülasyonun niteliklerinden birinin değerine göre sınıflara (katman, tabaka) ayrılarak oluşturulan homojen alt gruplardan seçilen örnekler üzerinden sınıflar özelinde veya

popülasyonun tamamı için tek bir sonuç oluşturulması gerçekleştirilmektedir. Popülasyon özellikleri bakımından önemli farklılıklar ve geniş dağılım gösteriyorsa, katmanlı seçim uygulanmaktadır ve tabakalı örnekleme nitelik örneklemesinden daha çok nicelik örneklemesinde kullanılmaktadır (Anadolu Üniversitesi, 2018).

Bu yönteme örnek olarak "*...bir organizasyonda sistem kullanıcılarının organizasyon dışına ilettikleri verilerin durumunu belirlemeye yönelik bir çalışma yapıldığını varsayalım. Denetim kapsamı 6 aylık bir süre olarak belirlenmiş. DLP kayıtlarından alınan listeyi daha iyi anlamlandırabilmek için, örnekleri, mesai saatleri içi, mesai saatleri dışı ve hafta sonları ile izin günleri olarak sınıflandırdık. Ayrıca yine iletilen dosya büyüklüklerine göre de bir sınıflandırma yapıldığını düşünelim. Bu örneğimizde; hafta sonu veya izin günlerinde organizasyon dışı veri aktarımları, yüksek boyuttaki veri aktarımlarını riskli olarak gördüğümüz için bu kategoriye giren örneklerin tamamını incelemeye aldık.*" verilebilir (Polat, 2021c).

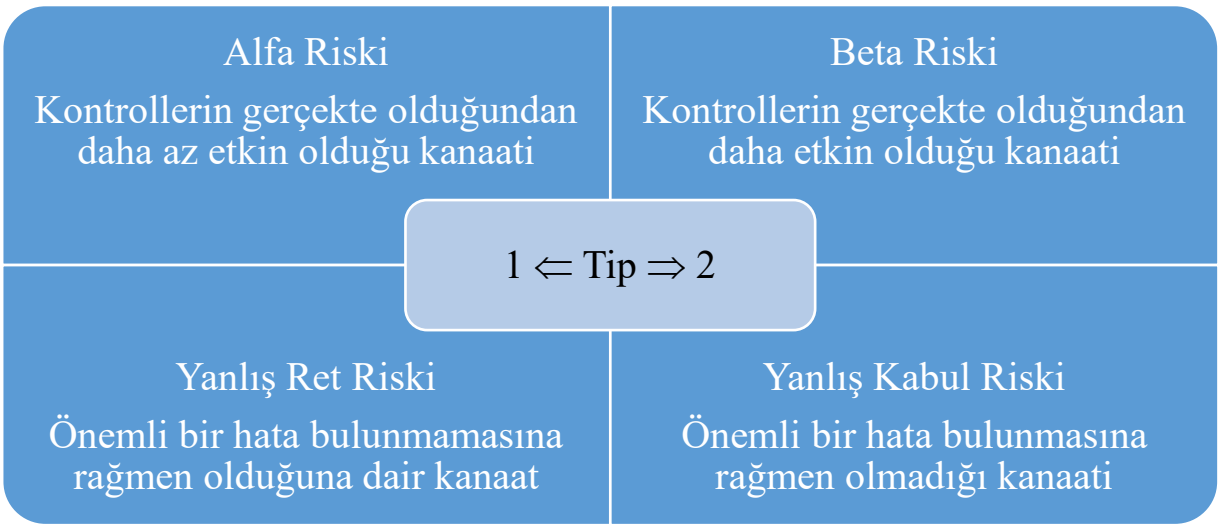
Denetim örneklemesi süreciyle ilgili örnekleme riski ve diğer istatistiksel terimler aşağıda açıklanmaktadır (Doshi, 2020; Geregory 2019).

a. Örnekleme Riski (Sampling Risk)

Denetim çalışmasında örnekleme yapıldığı takdirde, popülasyonun tamamı incelenmediği için yanlış bir sonuca ulaşma olasılığı, başka bir ifadeyle örnekleme riski ortaya çıkar. Örnekleme riski "*denetçinin örneklemi temel alan sonuçlarıyla evrenin tamamına aynı yolla uyguladığı testlerden elde edeceği sonuçlar arasında fark olması olasılığıdır. Başka bir anlatımla denetçinin oluşturduğu örneklemi inceleyerek elde ettiği sonuçların gerçek durumdan farklı olması olasılığı, örnekleme riskidir ve aradaki fark, "örnekleme hatası" olarak nitelendirilir.*" şeklinde ifade edilir. Örnekleme iki tür hatalı sonuca sebep olabilir. Söz konusu örnekleme riski tipleri uyumluluk testleri açısından alfa riski ve beta riski; önemli doğruluk testleri açısından ise yanlış ret riski ve yanlış kabul riski olarak aşağıda açıklanmaktadır (Anadolu Üniversitesi , 2018; KGK, 2019).

Tip-1: Uyumluluk testleri açısından, kontroller yeterince güvenilir olduğu halde denetçinin örneklemden elde ettiği sonuçlara bakarak kontrollerin yeterli güveni sağlamadığı kanısına varması; önemli doğruluk testleri açısından da önemli bir eksiklik olmadığı halde örneklem sonuçlarının önemli bir eksikliğin olduğu sonucunu desteklemesi riskidir.

Tip-2: Uyumluluk testleri açısından, kontroller yeterince güvenilir olmadığı halde denetçinin örneklemden elde ettiği sonuçlara bakarak kontrollerin yeterli güveni sağladığı sonucuna ulaşması; önemli doğruluk testleri açısından da önemli bir eksiklik olmadığı sonucuna ulaşıldığı halde önemli bir eksikliğin bulunması riskidir.



Şekil 18: Örnekleme Riski Tipleri

b. Güven Katsayısı (Confidence Coefficient)

Güvenilirlik faktörü, güven düzeyi olarak da bilinmekte olup, bir örneğin kalitesiyle ilgili doğruluk ve güvenin bir ölçüsü olarak yüzde olarak ifade edilir. Örnekleme sonuçlarının güvenilirliği anlamında, genellikle yüzde 95'lik bir güven katsayısının yüksek olduğu kabul edilir. Güven katsayısı, işletmenin iç kontrol yapısı incelendikten sonra yapılacak örneklemenin sonuçlarının güvenilirliği olarak açıklar ve örneklem büyüklüğü ve iç kontrol yapısıyla ters ilişkisi vardır (Anadolu Üniversitesi, 2018: 162). Bu kapsamda, kontrollerin etkinliği arttıkça, güvenilirlik faktörü ve örneklem büyüklüğü düşürülür. Diğer taraftan, güven katsayısı örneklem büyüklüğüyle doğru orantılıdır ve ne kadar yüksekse örneklem büyüklüğü de o kadar yüksek olacaktır.

c. Risk Seviyesi (Level of risk)

Risk seviyesi, güven katsayısı ile birlikte toplandığında yüzde 100'e ulaşılır. Bu durumda, güven katsayısı yüzde 95 ise risk seviyesi yüzde 5 olacaktır.

d. Kesinlik (Precision)

Kesinlik, örneklemin popülasyonu ne kadar yakından temsil ettiğini gösterir. Daha düşük miktarda örnek ile birlikte kesinlik azalırken, daha yüksek örnek miktarında kesinlik artar.

e. Beklenen Hata Oranı (Expected Error Rate)

Beklenen hata oranı bütün popülasyonda bulunabilecek hataların yüzde olarak tahminini ifade eder. Beklenen hata oranı yüksek olduğu takdirde, daha fazla inceleme yapılması gerekecek ve örneklem büyüklüğü de yüksek olacaktır.

f. Örneklem Ortalaması (Sample Mean)

Örneklem ortalaması, örneklerin tümünün toplanması ve örnek sayısına bölünmesi sonucu bulunan değerdir.

g. Örneklem Standart Sapması (Sample Standard Deviation)

Örneklem standart sapması, örneklem değerlerinin yayılımının bir ölçütüdür. Örneklem ortalamasından değerlerin değişkenliğini ifade eder.

h. Popülasyon Standart Sapması (Population Standard Deviation)

Popülasyon standart sapması, bütün popülasyon için değerlerin ortalamadan sapmasını gösterir. Popülasyon standart sapması arttıkça, daha yüksek oranda örneklem büyüklüğü oluşturulması gerekecektir.

i. Kabul Edilebilir Hata Oranı (Tolerable Error Rate)

Kabul edilebilir hata oranı, önemli bir yanlışlık beyan edilmeden denetim sonucunda var olabilecek en fazla hata miktarının yüzde olarak ifadesidir.

Denetim görüşüne dayanak oluşturan makul sonuçlara ulaşmak için denetim kanıtları denetim prosedürleri uygulanarak elde edilir. Denetim prosedürlerinin niteliği, risk olarak değerlendirilen hususlara denetim sürecinde karşılık verilmesinde en önemli unsurdur. Denetim prosedürlerinin niteliği; tetkik, gözlem, sorgulama, teyit etme, yeniden hesaplama, yeniden uygulama, analitik prosedür gibi türleriyle birlikte denetim prosedürlerinin amaçlarını ifade eder. Kanıt toplamayla ilgili denetim prosedürleri amaçlarına göre uyumluluk testi (kontrol testi) ve önemli doğruluk testi (maddi doğrulama prosedürü) olarak iki sınıfta yer almakta olup, BDS 500 Bağımsız Denetim Kanıtları Standardında (BDS 500) aşağıdaki gibi tanımlanmaktadır (KGK, 2019):

- **Kontrol testleri**, kontrollerin yönetim beyanı düzeyindeki önemli yanlışlıkların önlenmesi veya tespit edilerek düzeltilmesi konusundaki işleyiş etkinliğini değerlendirmek amacıyla tasarlanır. Kontrol testlerinin ihtiyaca uygun denetim kanıtı elde etmek amacıyla tasarlanması, bir kontrolün performansını gösteren tanımlayıcı şartlar (özellik veya nitelikler) ile yeterli performanstan uzaklaşıldığına işaret eden sapma şartlarının belirlenmesini içerir. Bu şartların mevcudiyeti veya yokluğu daha sonra denetçi tarafından test edilebilir.

- **Maddi doğrulama prosedürleri**, yönetim beyanı düzeyindeki önemli yanlışlıkların tespit edilmesi için tasarlanır ve detay testleri ile analitik maddi doğrulama prosedürlerinden oluşur. Maddi doğrulama prosedürlerinin tasarlanması, ilgili yönetim beyanında yanlışlık oluşturan ve testin amacıyla ilgili olan şartların belirlenmesini kapsar.

ISACA terimler sözlüğünde bu terimler aşağıdaki şekilde ifade edilmektedir:

- **Uyumluluk testi (Kontrol testi)**, denetim süresince hem kontrollerin etkinliği hem de bunların operasyonları hakkında denetim kanıtı elde etmek için tasarlanan kontrol testleridir.
- **Önemli doğruluk testi (Maddi doğrulama prosedürü)**, denetim dönemi boyunca faaliyetlerin veya işlemlerin eksiksizliği, doğruluğu veya varlığı hakkında denetim kanıtı elde etmek için uygulanan testlerdir.

Uyumluluk testlerinde kontrollerin uygun olarak tasarlanıp tasarlanmadığı, tasarlandığı gibi çalışıp çalışmadığı ve çalışanlar tarafından uygulanıp uygulanmadığı yönünde süreçler değerlendirilir. Önemli doğruluk testlerinde ise incelenilen süreçlerde yer alan herhangi bir bilginin ve işlemin tam ve doğru şekilde beklenilen sonuçlar oluşturup oluşturmadığı değerlendirilir. Güçlü bir kontrol ortamı, konrollerin tasarım ve etkinliğine duyulan güveni artıracağından daha az önemli doğruluk testi yapılmasını sağlayacaktır. Aşağıdaki tabloda bu testlere ilişkin örneklere yer verilmektedir (Doshi, 2020; Polat 2021b).

Uyumluluk Testi	Önemli Doğruluk Testi
Sistem erişim haklarının gözden geçirilmesi	Fiziksel envanterin sayılması ve doğrulanması
Güvenlik duvarı konfigürasyonunun incelenmesi	Borç verenlerle iletişime geçilerek kredi bakiyelerinin doğru olduğunun onaylanması
Şifre politikasının gözden geçirilmesi	Nakit bakiyelerinin sayılması ve onaylanması
Yama yönetimi prosedürlerinin incelenmesi	Envanter değerleme hesaplarının doğrulanması
Uzaktan erişim politikasının gözden geçirilmesi	Sistem odasına giriş kayıtlarının incelenerek sadece yetki verilmiş kişilerin giriş yaptığının teyit edilmesi

Genel olarak uyumluluk testi ardından önemli doğruluk testleri yapılır. Uyumluluk testleri, önemli doğruluk testlerine temel oluşturur. Uyumluluk testleri kontrollerin varlığını incelerken, önemli doğruluk tetleri, teste tabi unsurların (işlemlerin, verilerin, çıktıların, raporların) tamlığı ve doğruluğunu ortaya koymak için yapılır. Şöyle ki, kontrollerin varlığının değerlendirmesi sonucunda eğer kontroller etkindir kanaatine ulaşılıyorsa, işlemlerin bütünlüğünün incelenmesi için detaylı testlere gerek duyulmayabilir veya daha az gerek görülebilir. Bununla birlikte; denetim örneklemesi sürecinde hangi örnekleme yönteminin uygulanacağı test amaçlarıyla ilişkilidir. Bu yönde; uygunluk testinde öznitelik örneklemesi (attribute sampling) tercih edilirken, önemli doğruluk testinde değişken örnekleme (variable sampling) tercih edilir. Uyumluluk testi ve önemli doğruluk testi karşılaştırması aşağıdaki tabloda yer almaktadır (Doshi, 2020).

Uyumluluk Testi	Önemli Doğruluk Testi
Kontrollerin varlığının değerlendirmesi	İşlemlerin veya herhangi bir bilginin bütünlük ve doğruluk değerlendirmesi
Örneğin, envantere kayıt prosedürlerinin varlığı ve uygunluğunun incelenmesi	Örneğin, varlık envanterinin fiziksel olarak sayılarak doğrulanması
Önce gerçekleştirilir	Uyumluluk testi sonucuna bağlıdır, gerek görülen durumlarda sonra gerçekleştirilir
Öznitelik örneklemesi kullanılır (Örneğin, kullanıcı erişim haklarının örneklem üzerinden gözden geçirilmesi)	Değişken örnekleme kullanılır (Örneğin, dokümantasyonun doğrulanması için karmaşık bir hesaplama işleminin örneklem üzerinde gerçekleştirilmesi)

1.2.2. Bilgi Sistemleri Denetim Faaliyeti

BSBD Tebliği'nde bilgi sistemleri denetimi, bilgi sistemleri yönetimi ve işletimi kapsamında yer alan faaliyet, yazılım ve donanım gibi bilgi sistemi unsurları ile bu sistem dâhilinde tesis edilen kontrollerin bilgi sistemleri yönetim ilkeleri doğrultusunda değerlendirilmesi sonucunda görüş oluşturulması ve rapora bağlanması aşamalarından oluşan süreç olarak tanımlanmıştır. Bu tanım kapsamında, denetimin temel amacı bilgi sistemlerinin ve bu sisteme ilişkin iç kontrollerinin bilgi sistemleri yönetim ilkeleri doğrultusunda uyumluluk, etkinlik ve yeterliliği hakkında bir görüşe ulaşmaktır.

Denetim faaliyetleri, temel olarak denetim işinin kabul edilmesiyle başlar ve denetim raporunun sunulmasıyla sona erer. Bilgi sistemleri denetimi faaliyetleri diğer denetim türleri ile benzer şekilde planlama, kanıt toplama, değerlendirme ve raporlama aşamalarından oluşur. Denetim kaynaklarının sınırlı olması ve denetim fonksiyonunun işletmeye değer katıcı şeilde yönetilebilmesi bakımından denetim kaynaklarının riskli alanlara yönlendirilmesini zorunlu kılar. Söz konusu denetim faaliyetlerinin gerçekleştirilmesinde denetimin kilit noktalarından birisi olan ve denetim sürecinin en etkili şekilde neticelenmesi için denetim çalışmalarının merkezinde değerlendirilmesi gereken risk unsurunun önemine bağlı olarak risk tabanlı (bazlı) denetim yaklaşımı benimsenir. Risk tabanlı denetim yaklaşımında; risk yönetim sürecinin temel aşamaları denetim faaliyetleriyle bütünleşik olarak uygulanır (Çelik, 2021: 223). Bilgi sistemleri denetimi yürütülürken risk tabanlı denetim yaklaşımına uygun olarak aşağıdaki genel çerçeve izlenir:

- Öncelikle incelenen bilgi sisteminden kaynaklanabilecek riskler belirlenir,

- Riskleri minimize edecek kontrol mekanizmaları belirlenir,

- Kontrol mekanizmalarının işletmenin yapısı göz önünde bulundurularak oluşturulup oluşturulmadığı, oluşturulmuş ise etkin çalışıp çalışmadığı incelenir,

- İnceleme sonrası, iç kontrollerdeki zayıflıklar değerlendirilir ve

- Elde edilen bulgular belli bir prosedüre göre raporlanır.

Denetim alanı ne olursa olsun bu denetim faaliyetinin bütüncül bir yaklaşımla ve etkin bir şekilde gerçekleştirilmesi için denetim alanını etkileyen bilgi sistemleri unsurlarının ve bilgi sistemleri denetimi için entegrasyon noktalarının anlaşılması büyük önem taşır.

Bu kapsamda bilgi sistemleri denetimi üç aşamadan oluşur. Bilgi sistemleri denetimi faaliyetleri aşamaları; denetim planlama, denetim gerçekleştirme ve raporlama şeklinde 3 başlık altında ele alınabilir.

Şekil 19: Denetim Süreci

1.2.2.1. Denetimin Planlaması

Denetimin planlanması, denetim hedeflerini gerçekleştirmek amacıyla izlenmesi gereken adımların belirlenerek bir yol haritasının oluşturulma sürecidir. Denetimin bir bütün olarak ele alınması ve verimli bir şekilde yürütülmesi için zorunludur. Bu kapsamda bilgi sistemleri denetim faaliyeti için incelenecek sistem, faaliyet ve kontrollere yönelik olarak, risk odaklı bir bakış açısıyla ve önemlilik kriteri esas alınarak yazılı bir plan oluşturulur. Denetim görüşüne makul güvence sağlayacak şekilde denetimin planlanması, gerçekleştirilmesi ve denetim görüşünün bir raporla sunulması çalışmalarının her bir aşamasının etkin bir proje yönetimi bakış açısıyla yürütülmesi, etkin bir denetim süreci gerçekleştirilmesini sağlar. Denetim sürecinin bu yönde başarıya ulaşmasında ilk aşama denetim planlamasıdır. BDS 300 Finansal Tabloların Bağımsız Denetiminin Planlanması Standardına (BDS 300) göre denetçinin amacı denetimin etkin şekilde yürütülmesini sağlayacak şekilde planlamak olmalıdır.

Denetim planlaması, denetime yönelik genel denetim stratejisinin oluşturulması ve denetim planının oluşturulmasını içerir (KGK, 2017a). ISACA terimler sözlüğünde, denetim planı aşağıdaki gibi tanımlanmaktadır:

"*1. Bir görüş oluşturmak üzere yeterli uygun denetim kanıtı elde etmek için görevli ekip üyeleri tarafından uygulanacak denetim prosedürlerinin niteliğini, zamanlamasını ve kapsamını içeren bir plan (Denetlenecek alanları, planlanan işin türünü, işin üst düzey amaçlarını ve kapsamını ve bütçe gibi konuları, kaynak tahsisini, zamanlama tarihlerini, rapor türünü ve hedef kitlesi ve işin diğer genel yönleri gibi konuları içerir.),*

2. Belli bir zaman periyodunda yapılacak denetim çalışmalarının üst düzey bir tanımlaması."

Planlama aşamasında, denetim çalışmaları başlamadan denetim sürecinin ana hatlarını açık bir şekilde içeren bir yol haritası çıkarılır. Denetim kapsamının belirlenmesi ve uygulanacak denetim planının hazırlanması risk değerlendirme çalışmalarının bir sonucu olduğu için bu aşama denetim sürecinin en etkili kısmını oluşturur (Çelik, 2021: 223). BDS 300'e göre yeterli bir planlamanın, denetim sürecine katkıları aşağıdaki gibi açıklar (KGK, 2017a):

- Denetimin önemli alanlarına dikkatini yoğunlaştırması konusunda denetçiye yardımcı olmak.
- Muhtemel problemlerin zamanında belirlenmesi ve çözüme kavuşturulması konusunda denetçiye yardımcı olmak.
- Denetimin etkin ve verimli biçimde yürütülmesi için denetimin düzgün biçimde düzenlenmesi ve idare edilmesi konusunda denetçiye yardımcı olmak.
- Öngörülen risklere karşılık verecek kabiliyet ve yetkinlik sahibi denetim ekibi üyelerinin seçilmesi ve bu kişiler arasında uygun bir iş dağılımı yapılması konularında denetçiye yardımcı olmak.
- Denetim ekibi üyelerinin yönlendirilmesini, gözetimini ve yaptıkları çalışmanın gözden geçirilmesini kolaylaştırmak.
- Uygun hâllerde, topluluğa bağlı birimlerin denetçileri ile uzmanlar tarafından yapılan çalışmanın koordinasyonunda yardımcı olmak.

Denetim planlaması süreci temel olarak aşağıdaki adımlardan oluşur (Çelik, 2021: 224):

- Denetim amaç ve kapsamın belirlenmesi,
- Denetim ekibi oluşturulması,
- Risk değerlendirilmesinin gerçekleştirilmesi,
- Başlangıç düzeyinde bir denetim programının tanımlanması.

Denetim planının hazırlanması için öncelikle denetim stratejisi oluşturulması gerekir. Denetim stratejisi, denetim çalışmasına ilişkin daha genel bir çerçeve sunarken, denetim planı daha ayrıntılı hususları içerir. Bir bütün olarak denetim stratejisi, denetim sözleşmesinin özelliklerini, raporlama hedeflerini, anlamlı unsurları, anlamlı değişiklik ve gelişmeleri, denetimde kullanılacak kaynakların niteliğini, zamanlamasını ve kapsamını içerir (Çelik, 2021: 224).

Denetim stratejisinin oluşturulması ve denetim planının hazırlanması çalışmaları, denetim işinin alınması ve denetim sözleşmesinin yapılması ile başlar. Bu kapsamda denetim amaç ve kapsamının öncelikli olarak tanımlanması gerekir. Denetime ait amaçlar çoğunlukla iş riskini azaltmak için iç kontrollerin varlığını doğrulamaya odaklanmır (ISACA, 2018). Bilgi sistemleri denetimlerinde, bilgi sistemleri hedeflerine ulaşılması, veri akışının anlaşılması, kontrol etkinliğinin belirlenmesi ve denetim kanıtlarının belirlenmesine odaklanılmalıdır. Bilgi sistemleri denetimi, bir yönetim kontrolü olarak ele alınmalı ve teknoloji, esas tema olarak değil, kolaylaştırıcı olarak gözden geçirilmelidir (Hingarh ve Ahmed, 2013).

Denetim amaçlarına ulaşmak için risk odaklı denetim yaklaşımıyla yüksek riskli alanlara odaklanılarak denetim gerçekleştirilir. Denetim evreni, denetim planlama işlemi sırasında denetim

alanlarını belirlemek üzere derlenen ve muhafaza edilen denetim alanlarının envanteri, denetim kapsamındaki denetlenebilir bütün süreç ve sistemleri içerir. Denetim evreninin belirlenmesi, sonrası denetim kapsamının ve planının oluşturulması için risk değerlendirilmesi gerçekleştirilecektir. Denetim planının eksiksiz olarak hazırlanması için denetçinin riski yüksek alanlara odaklanmasını sağlayan etkili bir risk değerlendirilmesi gerekir. Denetçinin risk değerlendirmesi yaparak en riskli alanları belirlemesi ve bu kapsamda bir denetim planı hazırlaması denetçinin kaynakları verimli kullanmasını sağlar (Çelik, 2021: 224).

Risk değerlendirmesi aşağıdaki çalışmaları içerir (Çelik, 2021: 233):

Risk Tanımlama: Teknolojik gelişmeler, rekabet ortamı, ekonomik gelişmeler gibi dış faktörler ile personel kalitesi, işletme faaliyetlerinin yapısı, bilgi sistem süreçlerinin özellikleri gibi iç faktörlerden etkilenen risklerin belirlenmesi.

Risk Analizi: Önemli risklerin tahmin edilmesi, oluşma ihtimalleri ve etkilerinin değerlendirilmesi.

Bilgi sistemleri denetimi kapsamında risk değerlendirme, risk faktörleri ve risk değerlendirme yaklaşımı dikkate alınarak, işletmenin karşı karşıya olduğu bilgi sistemleri risklerinin,

- Stratejik etki,
- Hizmetler/faaliyetler,
- Düzenlemelere uyum,
- Bilgi sistemleri kaynakları,
- Organizasyon yapısı,
- Finansal, sosyal ve itibar etkileri,

gibi unsurlar çerçevesinde değerlendirilmesinden oluşur. Denetim planlaması yapılırken gerçekleştirilen risk değerlendirmesi;

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

konularında yardımcı olur (İDKK, 2014:30-31).

Daha önceki bölümlerde bahsedildiği üzere risk ve önemlilik denetim planlaması aşamasında önemli unsurlardır. Denetim riskinin kabul edilebilir seviyelerde olması veya makul bir düzeye indirilebilmesi, doğal risk ile kontrol riskinin yüksek olduğu alanlara odaklanarak tespit riskinin düşürülmesine bağlıdır. Söz konusu risk unsurları göz önünde bulundurularak, risk odaklı bir bakış açısıyla, önemlilik kriteri esas alınarak ve denetim görüşüne makul güvence sağlamak için yeterli denetim kanıtı elde edecek şekilde denetim kapsamı yazılı bir plan dahilinde belirlenmelidir.

Denetim amaç ve kapsamı belirlendikten sonra, gerekli denetim çalışmasını gerçekleştirebilecek tecrübe ve uzmanlığa sahip bir denetim ekibi oluşturulur. Denetlenecek alanların seçilmesi, kaynak gereksinimlerinin, sınırlamalarının belirlenmesi ve her denetim alanı için kaynak dağılımının yapılması gibi denetim planlamasının diğer hususları üzerinde çalışılır. Aslında, risk değerlendirme denetim işinin kabul edilmesi, denetim sözleşmesinin yapılması, denetim evreninin belirlenmesi, denetim kapsamı ve denetim planının oluşturulması çalışmalarının her bir aşamasını etkiler ve bütünleşik bir şekilde gerçekleştirilir. Planlama çalışmasının son adımı, denetimin tamamlanması için yapılması gereken adım adım denetim teknik ve yöntemlerini içeren bir denetim programı hazırlamaktır. Denetim programı kapsamında, denetim riskini en aza indirecek ve denetim amaçlarını gerçekleştirecek denetim testlerinin ve yöntemlerinin doğası, kapsamı ve zamanlaması yer alır (Çelik, 2021: 225).

Denetim programı, denetim metodolojisi olarak da adlandırılır ve incelenecek bilgi sistemi kontrolleriyle ilişkili olarak aşağıdaki şekilde gruplandırılabilir (SPK, 2018b):

- Organizasyon ve yönetim,

- Varlık yönetimi,
- Görevler ayrılığı prensibi,
- Fiziksel ve çevresel güvenlik,
- Ağ güvenliği,
- Kimlik doğrulama,
- Yetkilendirme,
- İşlemlerin, kayıtların ve verilerin bütünlüğü,
- Veri gizliliği,
- Bilgi sistemlerine ilişkin dış kaynak yoluyla alınan hizmetlerin yönetimi,
- Üçüncü taraflarla bilgi değişimi,
- Kayıt mekanizmasının oluşturulması,
- Zaman senkronizasyonu,
- Bilgi güvenliği ihlali,
- Bilgi sistemleri edinimi, geliştirilmesi ve bakımı,
- Bilgi sistemleri sürekliliği,
- Değişiklik yönetimi.

1.2.2.2. Denetimin Gerçekleştirilmesi

Planlama aşamasında oluşturulan denetim programı kapsamında denetimin bu safhasında denetim kanıtı toplama ve değerlendirme faaliyetleri yürütülür. Denetim görüşüne dayanak oluşturacak makul sonuçlara ulaşabilmek amacıyla yeterli ve uygun denetim kanıtı elde edilmesini sağlayacak denetim prosedürleri uygulanır. Bu sürece ilişkin denetim kavramı, kanıt toplama yöntemleri, denetim örnekleme, kontrol testi ve önemli doğruluk testleri kavramları daha önceki bölümlerde açıklanmıştır. BDS 330 Bağımsız Denetçinin Risk Olarak Değerlendirilmiş Hususlara Karşı Yapacağı İşler Standardında (BDS 330) da belirtildiği üzere; denetçinin amacı, "*önemli yanlışlık*" riski olarak değerlendirdiği risklere karşı yapılacak uygun işleri tasarlamak ve uygulamak suretiyle yeterli ve uygun denetim kanıtı elde etmektir. Denetim planlaması aşamasında risk değerlendirmesi çerçevesinde yürütülen risklerin tanımlanması ve analiz çalışmalarına karşılık, denetim gerçekleştirme aşaması yüksek riskli alanlara odaklanılarak yapılan denetim kanıtları toplama çalışmalarıyla riske karşılık verme aşamasını oluşturur.

Kanıt, herhangi bir iddiayı doğrulayan veya onu çürüten bilgidir. Denetim kanıtı, denetçinin görüşüne dayanak oluşturan sonuçlara ulaşırken kullandığı bilgilerdir. Denetim kanıtı, savunulan iddianın doğruluğu hakkında makul bir güvence oluşturmak için toplanır. Diğer bir deyişle, denetim çalışmasının doğası ve maliyetlerinin yüksek olmasından dolayı tam bir güvence amaçlanmaz ve denetim sonucunun yanlış olması ile sonuçlanacak bir takım riskler kabul edilir. Bir bilginin denetim kanıtı olarak kabul edilebilmesi için yeterli ve uygun özellikte olması gerekir. Bu kapsamda, denetim gerçekleştirme aşamasında çalışanların faaliyetlerini gözlemlemek, belgeleri gözden geçirmek, çalışanlarla görüşme yapmak, işlemleri yeniden çalıştırmak, analitik inceleme yapmak vb. farklı test ve yöntemler kullanılarak denetim kanıtı toplamaya çaba sarf edilir. Denetimde takip edilecek denetim prosedürlerinin amaç ve yapısını tecrübeyle kazanılacak olan mesleki yargı belirler. Hangi denetim prosedürünün hangi denetim çalışmasına uygun olduğuna karar vermek ve güvenilir denetim kanıtları elde etmek mesleki bilgi ve yetenek gerektirir (Çelik, 2021: 241).

Denetim prosedürleri kapsamında aşağıdaki hususlar göz önünde bulundurulmalıdır (Gregory, 2019):

- Görüşülecek kişiler ve sorulacak sorular,

- Talep edilecek belgeler,
- Kullanılacak denetim araçları,
- Örnekleme yöntemleri,
- Kanıtların nasıl değerlendirileceği, nasıl saklanacağı,
- Bulguların nasıl raporlanacağı.

Bilgi sistemleri denetimi sırasında en sık kullanılan denetim kanıtı toplama yöntemleri (Gregory, 2019; Hingarh ve Ahmed, 2013):

- Personel görev tanımları ve organizasyon şeması gözden geçirilmesi,
- Bilgi sistemleri politika, yönerge ve prosedürlerinin edinilmesi ve incelenmesi,
- Risk yönetim süreciyle ilgili dokümanların talep edilmesi ve gözden geçirilmesi,
- Geliştirilen yazılımlara ait dokümantasyonların incelenmesi,
- Dış kaynak yoluyla alınan hizmet sözleşmelerinin temin edilerek işlerin işleyişi hususunda bilgi edinilmesi,
- Bilgi güvenliği ihlal olay kayıtlarının gözden geçirilmesi,
- Bilgi sistemleri performans ve kullanımına ait periyodik raporların gözden geçirilmesi,
- İş sürekliliği planının elde edilerek incelenmesi,
- Ağ topolojisinin gözden geçirilmesi,
- Bilgi sistemlerin tasarımı, kullanımı, işleyişi ile ilgili personel ile görüşmelerin gerçekleştirilmesi,
- Bilgi sistemleri süreçlerinin yürütülmesi esnasında gözlemlenmesi,
- Bilgi sistemlerinin fiziksel olarak incelenmesi,
- Sistem günlükleri ve denetim izlerinin sistemdeki hatalara yönelik incelenmesi.

Bilgi sistemleri kontrolleri genellikle bilgi sistemleri içerisinde yer alır. Bilgi sistemleri denetimi;

- Bilgi sistemleri işletme seviyesi kontrolleri ve bilgi sistemleri yönetişim kontrolleri,
- Bilgi sistemleri yönetim süreçleri,
- Uygulama kontrolleri,
- Bilgi güvenliği teknik kontrolleri

olmak üzere dört ana unsur üzerinde gerçekleştirilir. Anahtar kontroller belirlenerek, söz konusu kontrollerin süreç içinde tasarlandığı şekilde çalışıp çalışmadığı veya etkin bir şekilde işletilip işletilmediği incelenir. Anahtar kontrollerin etkin bir şekilde işlemesi, sürece ait riskleri önemli ölçüde düşürecektir. Bir kontrolün, tasarım etkinliği ve yeterliliği açısından ilgili olduğu riskleri karşılayıp karşılamadığının değerlendirilmesi kapsamında aşağıdaki sorulardan da faydalanılabilir (İDKK, 2014:53):

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

Kontrollerin varlığına ve etkinliğine dair gerekli kanıtların toplanabilmesi için bilgi sistemleri ile etkileşime girilmesi gerekir (Hingarh ve Ahmed, 2013). Kanıtların değerlendirilmesi sürecinde doğrudan kaynaktan toplanan kanıtlar daha güvenilir kabul edilir. Bu bağlamda Bilgisayar Destekli Denetim Teknikleri (BDDT'ler), bilgi sistemleri ortamları için en etkili denetim araçlarıdır. BDDT'ler büyük ve karmaşık verileri toplamak ve analiz etmek için otomatik bir denetim tekniği olarak denetim sürecinde veri analizi ile eş anlamlı olarak kullanılır ve aşağıdaki araç ve teknikleri içerir (ISACA, 2018):

- Genelleştirilmiş denetim yazılımı (GAS),
- Test veri üreteçleri,
- Bilgisayarlı denetim programları,
- Özel denetim araçları.

Genel olarak BDDT'ler finansal denetimler için tasarlanmıştır (Hingarh ve Ahmed, 2013). Bilgi sistemleri denetimlerinde veritabanı sistemlerinden verilerin alınıp analiz edilmesine, işlemlerin beklenen sonuçları verip vermediğinin test edilmesine, bilgi sistemlerinde yapılandırma ayarlarını ortaya çıkarılabilmesine ve sistemlerin güvenlik açısından test edilmesine yönelik araç seçenekleri bulunur (Gregory, 2019). Bu araçların denetim sürecinde kullanım amaçlarına örnekler (Doshi, 2020):

- Verilerin detaylı analizinin yapılması,
- İşlemlerin doğrulanması,
- Kontrollere uygunluğun tespit edilmesi,
- Güvenlik açıklıklarının tespit edilmesi,
- Uygulama kaynak kodu güvenlik analizi ve güvenlik testlerin yapılması,
- Ağ ve işletim sistemi kontrollerinin değerlendirilmesi.

BDDT'lerin kullanımıyla tutarlı bir yöntem uygulanmış olur ve denetçilerin insan gücü kaynaklarının korunması, denetim maliyetlerinin azaltılması, denetim görevlerini yerine getirmek için harcanan zamanın azaltılması, denetim kalitesinin arttırılması, işletmelerin işletme verimliliğinin ve genel performansının iyileştirilmesi gibi avantajlar sağlar. BDDT'lerin kullanımının sürekli hale getirildiği sürekli denetim yaklaşımı ile bilgi sistemleri denetimlerinde sistem güvenilirliğinin sürekli olarak izlenebilmesi ve bilgisayar aracılığıyla seçici denetim kanıtlarının toplanabilmesi sağlar (ISACA, 2018). Sürekli denetim yaklaşımında, bir bilgi sistemleri denetçisinin gerçek zamanlı veya gerçek zamanlıya yakın bir ortamda testler ve değerlendirmeler yapması mümkün olur ve işletmelerin kendileri tarafından gerçekleştirilen bilgi sistemleri performansının sürekli izlenmesi süreciyle arasında ayrım bulunur. Bir diğer ifadeyle, sürekli denetim, sürekli izlemeden bağımsızdır ve iki süreç birlikte gerçekleştirilerek süreklilik güvencesi tesis edilebilecektir (ISACA, 2019: 58).

Sürekli denetim yaklaşımında yaygın olarak kullanılan yöntemler aşağıdaki gibidir (Doshi, 2020):

a. Entegre (Bütünleşik) Test Tesisi (ITF)

Entegre test tesisi, denetçi tarafından sağlanan ve bilgi sistemine dahil edilen program, kod veya ek verilerden oluşan bir bilgi sistemi içinde yerleşik test ortamıdır. Bu kontrol yönteminde sahte/hayali kayıtlar oluşturulur, bilgi sistemi aktif kullanımdayken gerçek verilerle birlikte test verileri aynı anda işlenir ve daha sonra beklenen sonuçlarla karşılaştırması yapılır. Bu kapsamda, bu yöntemin avantajı normal üretim ortamında gerçekleştirildiği için ayrı test süreçleri gerektirmemesidir. Ancak, üretim verilerinin test verilerinden izolasyonuna dikkat edilmelidir ve doğrulama testleri tamamlandıktan sonra oluşan test verileri silinmelidir.

b. Sistem Kontrol Denetimi İnceleme Dosyası ve Yerleşik Denetim Modülleri (SCARF/EAM)

Bu yöntem çerçevesinde bilgi sistemi üzerindeki işlemleri sürekli izlemek ve denetim açısından önemli olabilecek işlemler hakkında veriler toplamak için bilgi sistemine yerleşik denetim modülleri

kullanılır Bir başka deyişle, bilgi sistemlerinde yeterli denetim izleri tutulmayabilir, kısa süreli veya kesintili kayıtlar var olabilir ve denetçi tarafından daha sonra incelenmek üzere seçilen verilerin toplanması ve saklanması için bir tesis inşa edilmesi gerekebilir. Bu kapsamda, bilgi sistemine yerleşik denetim modülleriyle, denetlenecek işlemlerin seçilmesi, ek günlük kaydı tutulması ve ek kontrol işlevleri gerçekleştirilebilir. Örneğin, belirli bir limitin üzerindeki işlemler, istisnai durumlara ilişkin işlemler veya kurumsal politikalardan belirli sapmalar daha sonra denetçi tarafından gözden geçirilmek üzere kaydedilebilir. Bu yöntem, bilgi sistemlerindeki normal işlemler kesintiye uğratılamadığı durumlarda faydalı olur.

c. Anlık Görüntü (Snapshots)

Anlık görüntü yöntemiyle işlemlerin işlenme şekli incelenir. Seçilen işlemler, anlık görüntü sürecini tetikleyen özel bir kodla işaretlenir ve bilgi sistemlerindeki denetim modülleri marifetiyle söz konusu işlemler yürütülme süreci öncesi ve sonrası kayıt altına alınır. Daha sonra işlemler, bu alınan anlık resimler üzerinden gözden geçirilerek işleme adımlarının uygun şekilde yürütüldüğü doğrulanır. Anlık görüntü yöntemi, işlemlere ilişkin bir denetim izi gerektiğinde kullanışlı olur.

d. Denetim Kancası (Audit Hook)

Denetim kancaları, şüpheli işlemleri işaretleyen denetim rutinleridir. İstisnaları ve şüpheli işlemleri yakalamak için bilgi sistemlerine yerleştirilmiş denetim kancaları, hata veya hile durumlarına karşı belirli kriterlere göre seçilen işlemlerin gözden geçirilmesi gerektiği durumlarda kullanılır. Bu yöntem vasıtasıyla dolandırıcılık veya hata kaynaklı usulsüzlüklerin erken tespiti mümkün olur.

e. Sürekli ve Aralıklı Simülasyon (CIS)

Sürekli ve aralıklı simülasyon yönteminde, bir veritabanı yönetim sistemine (DBMS) yerleştirilen denetim modülü kullanılır. SCARF ile benzer şekilde denetim modülü vasıtasıyla DBMS'e gelen bütün işlemler belirli kriterlere göre incelenir. Denetim açısından önemli olarak belirlenen işlemler, uygulama sistemine paralel bir simülasyon programı üzerinden bağımsız olarak işlenerek gerekli doğrulama işlemleri gerçekleştirilir. Başka bir deyişle, önceden tanımlanmış parametrelere uyan işlemler için uygulama sistemi tarafından üretilen sonuçlarla, simülatör tarafından ulaşılan sonuçlar karşılaştırılarak tutarsız durumlar bu yöntemle kayıt altına alınır.

Yukarıda detay açıklamalarına yer verilen sürekli denetim yaklaşımında kullanılan yöntemlere ilişkin özet bilgilere aşağıdaki tabloda yer verilmektedir.

Entegre Test Tesisi	Bilgi Sistemine yerleşik gerçek verilerle birlikte test verilerinin aynı anda işlendiği test ortamı
Sistem kontrol denetimi inceleme dosyası ve yerleşik denetim modülleri	Denetim açısından önemli olabilecek işlemler hakkında veriler toplamak için bilgi sistemine yerleşik denetim modülleri
Anlık görüntü	İşlemlerin işlenme şekli incelenmekte denetim izi gerekli olduğu durumlarda kullanılır.
Denetim Kancası	İstisnaları ve şüpheli işlemleri yakalamak için bilgi sistemlerine yerleştirilmiş denetim rutinleri
Sürekli ve Aralıklı Simülasyon	Veritabanı yönetim sistemine (DBMS) yerleştirilen denetim modülüyle DBMS'e gelen bütün işlemler belirli kriterlere göre incelenir.

1.2.2.3. Denetimin Raporlanması

Bilgi sistemleri denetimi sürecinin bu aşamasında, gerçekleştirilen denetim çalışmaları ve değerlendirmeleri sonucu ulaşılan görüşü içeren bir raporun hazırlanması ve yönetime ve ilgili taraflara bildirilmesi gerçekleştirilir. Denetim raporu denetim çalışmasının nihai ürünü olarak; denetim hedefleri, denetimin kapsamı, değerlendirilen kontroller, bu kontrollerin etkinliğine ve bütünlüğüne ilişkin görüşler ve iyileştirme önerilerini açıklar (Gregory, 2019).

Denetim raporu tam, güvenilir, objektif, yeterli kanıta dayalı, açık, öz ve anlaşılır olmalıdır. Raporun tam olması; denetimden beklenen amaçların tamamının raporda yer alması, raporda yer verilmeyen hususlara ilişkin olarak objektif kriterlere dayalı açıklamaların yapılmasıdır. Raporun güvenilir olması; raporda yer alan bulguların yeterli ve ispat edilebilir kanıtlara dayalı olmasını ve raporun tam olmasını gerektirir. Raporun objektif olması; denetim sonucu elde edilen bulguların tarafsız bir şekilde rapora yansıtılmasıdır. Raporda denetimin tarafsızlığını zedeleyebilecek savunucu ve/veya suçlayıcı ifadelerden kaçınılmalıdır. Raporun yeterli kanıta dayalı olması; denetim sonunda elde edilen bulgu ve sonuçların yeterli sayıda ve ikna edici nitelikte olmasıdır. Raporun açık, öz ve anlaşılır olması; yazılacak ifadelerin sade ve kısa olmasını, gereksiz detay ve tekrarlardan, teknik terim ve kısaltmalardan kaçınılmasını gerektirir. Teknik terimlerin veya kısaltmaların kullanılması gerekli olduğu durumlarda bu terimler ayrıca açıklanır ve kullanılan kısaltmalara ilişkin bilgilere raporda ayrı bir bölümde yer verilir (Sayıştay, 2013:123).

Denetlenen süreçler, uygulamalar ve diğer unsurlara ilişkin kontrollerin tasarımı ya da işletimine dair tespit edilen zayıflık veya eksiklikler bulgu olarak raporlanır. Bir hususun bulgu olarak nitelendirilebilmesi için konu ile ilgili alınan bilgi, belge ve kanıtların denetçi tarafından değerlendirilmesi. analiz edilmesi ve ardından olumsuz bir kanaate varılması gerekmektedir. Bulguların hazırlanması sırasında aynı kontrol hedefine ait hususlar ya da birbirleriyle benzerlik ve bütünlük arz eden konular mümkün olduğunca birleştirilmeye çalışılır. Raporlanan bulgular, içeriğini, nedenini, bulgunun yaratabileceği riskleri net olarak anlatacak şekilde basit bir dile sahip olmalı, ek bir bilgiye ya da belgeye ihtiyaç duyulmadan bulgu hakkında fikir sahibi olunacak şekilde gerekli tüm detayları içermeli ve tarafsız (objektif) bir şekilde ifade edilmelidir. Bulguların sunumu sırasında tespit edilen hususların önem derecesine göre hazırlanmış olması, denetlenen birim tarafından yürütülecek düzeltici ve önleyici faaliyetlerin hangi alanlarda önceliklendirilmesi gerektiği konusunda yardımcı olacaktır. Bulguların önem düzeyi genellikle kritik, yüksek, orta ve düşük olarak belirlenir. Bulguların hazırlanması sırasında bulgulara ait aşağıdaki hususlar kayıt altına alınmalıdır:

- Bulguya ilişkin mevcut durum,
- Bulgunun sebebi/kök nedeni,
- Bulguya ilişkin risk ve etkiler,
- Kriter (Sayıştay, 2013:58).

Denetim amacına ulaşılabilmesi için etkili bir denetim çalışmasının gerçekleştirilmesi ve çalışma bulgularının etkili bir şekilde değerlendirilebilmesi gerekir. Denetim kanıtları toplanması sonrası ulaşılan sonucu kesinleştirmeden önce yapılmış olan çalışmalar bir bütün olarak yeniden incelenmelidir. Bu kapsamda, denetim çalışmalarının yeniden gözden geçirilmesindeki temel amaç, hedeflenen denetim amaçlarının gerçekleştirildiğinden emin olmak ve denetim programının tamamıyla uygulandığını garanti altına almaktır. Bu adımda denetim çalışmasının eksiksiz bir şekilde gerçekleştirilip gerçekleştirilmediğinin anlaşılması için denetim kanıtlarının yeterliliği, bulguların etkisi ve önemlilik açısından değerlendirilmesi göz önünde bulundurulmalıdır (Anadolu Üniversitesi, 2018: 204). Ulaşılan ve kesinleşen nihai sonuç bir rapor halinde yönetime teslim edilir. Denetim raporu sunulan görüşlerle birlikte yönetimin yanında denetimden sorumlu komiteye, yönetim kuruluna ve diğer ilgili taraflara iletilir.

Denetimin etkinliği ve verimliliği açısından, denetimin bütün sürecinde denetimden sorumlu komite ve yönetim ile etkin ve açık bir iletişimin sağlanması gerekir. Denetçi iç kontrol zayıflıkları ve eksiklikleri, hile ve usulsüzlükleri, denetimin kapsamı ve zamanlaması ile ilgili bilgileri ve önemli denetim bulguları dahil tüm bilgileri üst yönetimden sorumlularla paylaşmalıdır. Daha etkin ve verimli bir sürecin sürdürülmesi amacıyla denetçi, her türlü kontrol zayıflığına ve/veya hile usulsüzlüklere işaret eden durumlara ilişkin bilgi aktarımı gerçekleştirerek iletişimi sağlamalıdır. Denetçi bu iletişimi

denetimden sorumlu komite ile kurabileceği gibi yönetim kurulu ile de kurabilir (Anadolu Üniversitesi, 2018:205). Benzer şekilde, denetimin raporlanması sürecinde de, gerçekleştirilen denetim faaliyetleriyle ilgili yönetimle iletişim kurulmalıdır. Bu noktada denetim sonuçlarının iletilmesi, yanlış anlaşılmaların veya yorumlamaların önüne geçilmesi için denetim raporu yayımlanmadan önce yönetimle bir kapanış toplantısı düzenlenmelidir. Bu toplantının amaçları aşağıda yer verilmektedir (Doshi, 2020):

- Bulguların raporda uygun ve doğru bir şekilde yer alması,
- İyileştirme önerilerinin yönetimle müzakere edilmesi,
- Kabul edilen önerilere ilişkin uygulama tarihlerinin belirlenmesi.

Denetçi yönetim iddiaları doğrultusunda uygun ve yeterli sayıda denetim kanıtını bir araya getirip değerlendirerek bir görüşe ulaşır (Çelik, 2021: 241). Yeterli ve uygun denetim kanıtlarıyla desteklemek suretiyle kayda değer kontrol eksikliklerini ve önemli kontrol eksikliklerini sınıflandırarak raporlar. Tespitler ifade edilirken, denetim amaçlarının gerektirdiği kadarıyla, bu tespitlerin kriter ve durumlarına ilişkin bilgilere yer verilir. Denetçi, geçmiş dönemlerde tespit edilmiş ve bir önceki dönem raporunda halen giderilmediği ifade edilmiş olan tüm kontrol zayıflığı ve eksikliklerini raporunda değerlendirir. Bu kontrol zayıflığı ve eksikliklerinin son durumlarına, devam edip etmediklerine ve denetlenenin taahhüt ettiği aksiyon planına uyumuna ilişkin açıklamalarına raporunda yer verir. Denetçi, denetim amaçları, denetim tespitleri ve varsa denetlenenin görüşlerini yorumlayarak kendi çıkarımları ve görüşleri doğrultusunda değerlendirmelere raporunda yer verir.

Denetim raporunda sunulabilecek dört çeşit görüş vardır (SPK, 2018a):

Olumlu Görüş: Herhangi bir önemli kontrol eksikliğinin bulunmaması ve denetim kapsamında herhangi bir engelleme ve kısıtlama ile karşılaşılmaması durumunda sunulan görüş olumlu olacaktır.

Şartlı Görüş: Aşağıdaki durumlarda şartlı görüş bildirilir;

- Önemli kontrol eksikliği bulunmakla birlikte bilgi sistemlerinin bütününün veya büyük bir kısmının etkilenmediğinin düşünülmesi,
- Görüş bildirmekten kaçınmayı gerektirecek önemde olmamakla birlikte denetim faaliyetlerini sınırlayan hususların varlığı veya yeni tesis edilmiş bir sistem hakkında bilgi edinilememesi veya görüş oluşturulabilmesi için yeterli ve uygun denetim kanıtı toplanamaması.

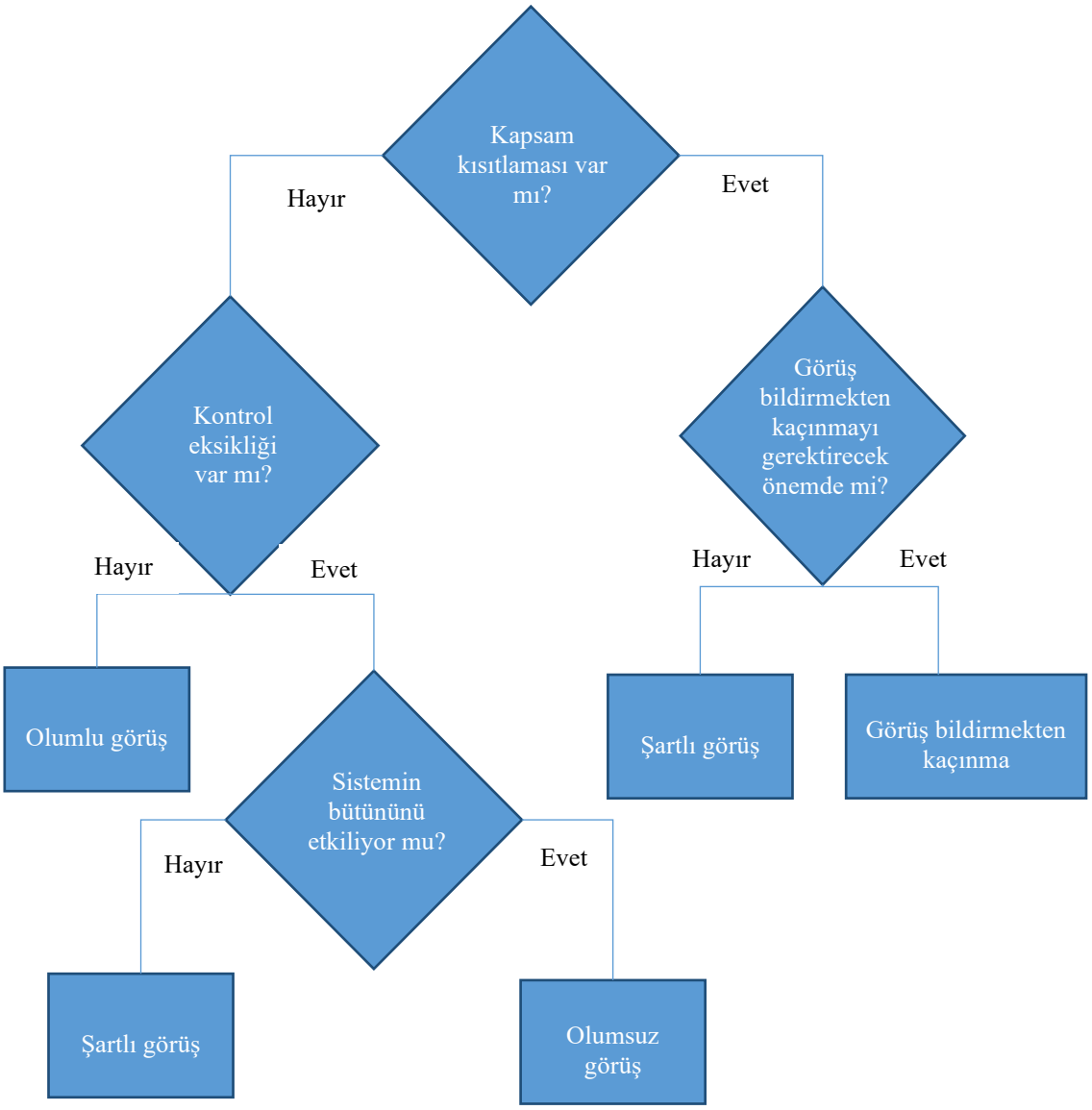
Olumsuz Görüş: Denetim kapsamında tespit edilen önemli kontrol eksiklikleri tek başına veya beraber değerlendirildiğinde;

- Bilgi sistemlerinin bütününü veya büyük bir kısmını etkilediğine ilişkin kanaat edinilmesi veya,
- Yönetim beyanı ile denetlenenin bünyesinde gerçekleştirilen denetim sonrasında önemli bir kontrol eksikliğinin bütün önemli taraflarıyla eksik veya yanlış aktarılmasından kaynaklanan bir farklılık bulunması

durumlarında olumsuz görüş bildirilir.

Görüş Bildirmekten Kaçınma: Kanıt yetersizliğinden ve denetim çalışmalarında karşılaşılan belirsizlik ve sınırlamalardan dolayı görüş bildirmekten kaçınma yoluna gidilir. Görüş bildirmekten kaçınmada olumlu veya olumsuz görüşe vurgu yapılmaz, sadece denetçinin görüş bildirecek dayanaklara sahip olmadığı belirtilir (Çelik, 2021:228). Bu durumda, denetim raporunda görüş bildirmekten kaçınmaya yol açan nedenlere yer verilir.

Denetim görüşü türleri aşağıdaki şekilde şematize edilmektedir:



Şekil 20: Denetim Görüşü Türleri

Denetim süreci, ilgili standartlara uygun bir şekilde yeterli ve uygun denetim kanıtı toplanıp tamamlandığında bilgi sistemleri üzerindeki kontrollerin bütününün etkin, yeterli ve uyumlu olduğuna ikna olunursa olumlu görüş bildirilir. Denetim görüşü oluştururken göz önünde bulundurulan iki ana hususun kontrol eksikliği (standartlarla belirlenen ilkelerden sapmalar) veya kapsam kısıtlaması (yeterli ve uygun denetim kanıtı elde edilip edilmediği) olduğu görülmektedir. Bu bağlamda, olumlu bir görüş dışında verilecek görüş türlerinde de bu konuların denetçi muhakemesiyle nitelikleri ve yaygınlıkları incelenir (Anadolu Üniversitesi, 2018: 215). Bilgi sistemlerinin bütününü veya büyük bir kısmını etkilediğine kanaat getirilen kontrol eksikliklerinin tespiti durumunda olumsuz görüş söz konusuyken; kanıt yetersizliği durumlarında yeniden kanıt toplama yoluna gidilir; şartlı görüş bildirilme ya da kanıt yetersizliğinden dolayı görüş bildirmekten kaçınma yoluna gidilir (Çelik, 2021:227).

Bu aşamadan sonra yapılması gereken, ulaşılan nihai görüşün gerekçeleriyle birlikte bir rapor halinde belirlenen çerçeveye göre sunulmasıdır. Her düzenleme ve standart çerçevesinde farklı şekillerde hangi bilgilerin yer alacağı ve hangi biçimde raporun hazırlanacağı belirtilmekle birlikte; denetim raporu genel olarak aşağıdaki unsurları içerecek şekilde hazırlanır (Doshi, 2020):

- Denetimin kapsamı, denetimin sınırları, denetim amacı, denetim dönemi vb. denetim çalışmasına ilişkin bilgiler,
- Bulgular, öneriler,

- Kontrollerin etkinliği, yeterliliği ve uyumluluğu hakkında görüş.

Denetim raporu hatasız, tarafsız, açık, özlü, tam, yapıcı ve zamanında hazırlanarak aşağıdaki amaçların karşılanması sağlanır (Cascarino, 2012; Doshi, 2020):

- Denetim sonuçlarının bütün ilgililere usulüne uygun olarak sunulması,
- Denetim sözleşmesinin resmi olarak sona erdirilmesi,
- Düzeltici faaliyetlerin gerektiği alanların belirlenmesi ve denetlenene güvence sağlanması,
- Denetleneni araştıran herhangi bir taraf için referans olması,
- Denetim bulgularının takibi ve sonuçların izlenmesi için temel oluşturması,
- Denetimin güvenilirliğinin arttırılması.

Denetimin sonrasında, bulgulara ilişkin tavsiyelerin uygulanması hususunda denetlenenin üzerinde takip gerçekleştirilir. Denetim kapsamında söz konusu iyileştirmeleri uygulamak için kullanılan yöntemlere karar vermek, çözümlerine ilişkin aksiyon planlarını yürütmek denetlenenin yönetiminin sorumluluğundadır ve bu süreçte ilerlemeyi izlemek için bir takip süreci oluşturulmalıdır. Denetçi, genellikle denetlenenin yanıtlarını ve düzeltici eylemleri gözden geçirilmeli, bu yanıtların ve düzeltici eylemlerin yeterliliğini değerlendirerek, takip bulgularını rapor etmelidir (Cascarino, 2012). Takip faaliyetleri gerçekleştirilirken, düzeltici faaliyetlerin uygulanıp uygulanmadığı hususunda yönetim tarafından belirlenmiş olan aksiyon planı ve zaman çizelgesi esas alınır (Doshi, 2020).

Eğer düzenli bir izleme faaliyeti söz konusu değil ise denetçi önceki dönemlerde yapılan bilgi sistemleri denetimlerine ilişkin raporları inceleyerek bu raporlarda yer alan bütün bulguları kendi denetimi sırasında değerlendirir. Bu bulguların son durumlarına,konuya ilişkin kurum açıklamalarına ve açıklığın devam edip etmediklerine ilişkin değerlendirmelerine raporunda yer verir (Sayıştay, 2013:126).

Örnek Sorular

Soru 1: Aşağıdakilerden hangisi denetim raporunda yer verilen görüş türlerinden biri değildir?

A) Olumlu Görüş
B) Görüş Bildirmekten Kaçınma
C) Şartlı Görüş
D) Önermeli Görüş
E) Olumsuz Görüş
Cevap: D

Soru 2: Aşağıdakilerden hangisi denetim planlaması süreci adımlarından biri değildir?

A) Denetim amaç ve kapsamın belirlenmesi
B) Denetim ekibi oluşturulması
C) Başlangıç düzeyinde bir denetim programının tanımlanması
D) Risk değerlendirilmesinin gerçekleştirilmesi
E) Uyumluluk testi yapılması
Cevap: E

1.3. BİLGİ SİSTEMLERİ YÖNETİMİ VE DENETİMİNE İLİŞKİN MEVZUAT

Bu bölümde, bilgi sistemleri yönetimi ve denetimine ilişkin sermeye piyasası mevzuatı başta olmak üzere diğer ilgili mevzuatlar ele alınmaktadır.

1.3.1. Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ Seri:X, No:22

Kamunun aydınlatılması ilkesi kapsamında sermaye piyasalarında karar vericilerin temel finansal bilgi kaynakları arasında yer alan finansal raporların[3] gerçeğe uygun sunumu büyük önem taşımaktadır. Bu kapsamda, bağımsız denetim dışarıdan üçüncü bir taraf olarak finansal raporların güvenilirliğinin artırılması fonksiyonunu üstlenmiş ve sermaye piyasaları açısından önemli bir sermaye piyasası faaliyeti olmuştur. Bu nedenle, Kurul 1987 yılından beri ülkemiz sermaye piyasalarında bağımsız denetim faaliyetlerini düzenlemektedir. Son olarak, sermaye piyasasında bağımsız denetim faaliyetine, bu faaliyette bulunmak üzere Kurul'ca yetkilendirilecek bağımsız denetim kuruluşlarına ve bağımsız denetçilere ilişkin standart, ilke, usul ve esasları belirleyen Seri:X, No:22 sayılı Sermaye Piyasasında Bağımsız Denetim Standartları Tebliği (Seri: X, No: 22 Tebliği veya Tebliğ) 02.06.2006 tarih ve 26196 sayılı Mükerrer Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

Bu Tebliğ, yayımlandığı tarihteki Uluslararası Denetim Standartları (UDS) ile uyumlu olarak oluşturulmuş ve 34 kısmı UDS'nin ilgili standart çevirilerini kapsamıştır. Daha sonra, 6362 sayılı Sermaye Piyasası Kanunu'nun (SPKn veya Kanun) 14'üncü maddesi uyarınca bağımsız denetimin Türkiye Denetim Standartları'na (BDS) göre yapılacağının hüküm altına alınması ile 6102 sayılı Türk Ticaret Kanunu (TTK) ve 660 sayılı Kamu Gözetimi Muhasebe ve Denetim Standartları Kurumunun Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin (660 sayılı KHK) yürürlüğe girmesini müteakip, 2014 yılından itibaren Kamu Gözetimi Muhasebe ve Denetim Standartları Kurumu (KGK) tarafından UDS'ler ile uyumlu BDS'lerin yayınlanması ile birlikte, Seri:X, No:22 Tebliği'nin Başlangıç Hükümleri Kısmı, İkinci Kısım, Üçüncü Kısmın bağımsız denetim sözleşmesinin feshi hükümleri ve Son Hükümler Kısmı hariç diğer kısımlarının uygulaması kalmamıştır. Başlangıç Hükümleri Kısmı'nda, amaç, kapsam, dayanak, tanımlar ve denetime tabi işletmelere ilişkin esaslar; İkinci Kısım'da sermaye piyasasında faaliyette bulunma şartları, Üçüncü Kısım'da bağımsız denetim sözleşmesinin feshi hükümleri ve Son Hükümler Kısmın'da ise istisna hükümler düzenlenmiştir.

Sermaye piyasasında bilgi sistemleri bağımsız denetimine ilişkin mevzuat, Seri:X, No:22 Tebliği ile düzenlenen hususlara benzerlik taşımakta olup, bazı hususlarda anılan Tebliğ'e atıflar bulunmaktadır. Bu nedenle, anılan Tebliğ sermaye piyasasında bilgi sistemleri bağımsız denetim mevzuatı ile ilişkilidir. Bu bölümde, Seri:X, No:22 Tebliği kapsamında anılan kısımlarda düzenlenen bağımsız denetime ilişkin esaslara yer verilecektir.

1.3.1.1. Denetime Tabi İşletmeler

Tebliğ'de bağımsız denetim, sınırlı bağımsız denetim (inceleme) ve özel bağımsız denetim olmak üzere 3 tür denetim düzenlenmiştir. Denetim türlerine bağlı olarak da denetime tabiiyet belirlenmiştir.

Bağımsız Denetim: Bağımsız denetim, işletmelerin kamuya açıklanacak veya Kurul'ca istenecek yıllık finansal tablo ve diğer finansal bilgilerinin, finansal raporlama standartlarına uygunluğu ve doğruluğu hususunda, makul güvence sağlayacak yeterli ve uygun bağımsız denetim kanıtlarının elde edilmesi amacıyla bağımsız denetim standartlarında öngörülen gerekli tüm bağımsız denetim tekniklerinin uygulanarak, defter, kayıt ve belgeler üzerinden denetlenmesi ve değerlendirilerek rapora bağlanmasıdır.

Sınırlı Bağımsız Denetim (İnceleme): Sınırlı bağımsız denetim, ara dönem finansal tabloların Kurul'ca yayımlanan finansal raporlama standartlarına uygun olarak hazırlanıp hazırlanmadıklarının öncelikle bilgi toplama (soruşturma) ve analitik inceleme teknikleri kullanılarak incelenmesi ve

[3] *Bağımsız denetim tarihsel süreç içerisinde finansal tabloların denetimi kapsayacak şekilde oluşup, gelişmesine karşın; zamanla finansal raporların bir unsuru olan yönetim kurulu faaliyet raporunun denetimini de kapsamıştır. Ülkemizde TTK'nın yürürlüğe girmesi ile birlikte yönetim kurulu faaliyet raporlarının da denetimi de bağımsız denetimin kapsamına girmiştir. Söz konusu denetim, yönetim kurulu faaliyet raporlarında finansal tablo bilgilerinin kullanılması durumunda, bu bilgilerin finansal tablolarla tutarlılığını denetlemekle sınırlıdır.*

değerlendirilerek rapora bağlanmasıdır. Tanımdan da görüleceği üzere bağımsız denetim, denetim sırasında gerekli tüm denetim tekniklerinin uygulanmasını gerektirirken; sınırlı bağımsız denetim sadece bilgi toplama ve analitik inceleme tekniklerinin uygulanmasını zorunlu kılar. Bağımsız denetimde, denetçi görüş bildirirken; sınırlı bağımsız denetimde bağımsız denetçi bir görüş bildirmez, sonuç bildirir.

Özel Bağımsız Denetim: Özel bağımsız denetim, sermaye piyasası araçlarının halka arzı için Kurul'a başvuru sırasında veya birleşme, bölünme, devir ve tasfiye durumunda bulunan işletmelerce, bu amaçlarla herhangi bir tarih itibariyle düzenlenmiş finansal tabloların bağımsız denetimidir. Özel bağımsız denetim, nitelik, uygulanan denetim teknikleri, sunduğu güvence düzeyi ve görüş bildirmesi bakımından bağımsız denetimle aynıdır.

Tebliğ'de düzenlenen bağımsız denetim temelde işletmeleri (ihraççı ve sermaye piyasası kurumları) kapsar. İşletme ise, ihraç ettiği sermaye piyasası araçları bir borsada ve/veya teşkilatlanmış diğer piyasalarda işlem görenler dahil, ortaklıklar ve sermaye piyasası kurumları ile Kurul'un finansal raporlama standartlarına ilişkin düzenlemeleri kapsamında konsolidasyona dahil edilen işletmeler ile bağlı ortaklık, müşterek yönetime tabi teşebbüs ve iştirak niteliğindeki diğer işletmelerdir.

a. Bağımsız Denetime Tabi İşletmeler

Bağımsız denetime tabi olacak işletmeler belirlenirken, TTK'nın 397'nci maddesinin dördüncü fıkrası kapsamında Cumhurbaşkanı Kararı ile belirlenen anonim şirketler ile uyum gözetilmiştir[4]. Yıllık finansal raporları bağımsız denetime tabi olanlar:

1) TTK'nın 397'nci maddesinin dördüncü fıkrası uyarınca Cumhurbaşkanlığı Kararı[5] ile belirlenen işletmeler,

2) Yatırım fonları,

3) Konut ve varlık finansmanı fonları.

TTK'nın 397'nci maddesinin dördüncü fıkrası uyarınca alınan Kararda; SPKn kapsamında Kurul'un düzenleme ve denetimine tabi şirketlerden;

a) Yatırım kuruluşları (Aracı kurumlar ve bankalar),

b) Kolektif yatırım kuruluşları,

c) Portföy yönetim şirketleri,

d) İpotek finansmanı kuruluşları,

e) Varlık kiralama şirketleri,

f) Merkezi takas kuruluşları,

g) Merkezi saklama kuruluşları,

h) Veri depolama kuruluşları,

i) Derecelendirme kuruluşları,

j) Değerleme kuruluşları,

k) Sermaye piyasası araçları bir borsada veya teşkilatlanmış diğer piyasalarda işlem gören veya işlem görmeleri amacıyla SPK'ca onaylanmış geçerlilik süresi bulunan izahname veya ihraç belgesi bulunan anonim şirketler,

l) Bir borsada veya teşkilatlanmış diğer piyasalarda işlem görmemekle birlikte halka arz edilmeksizin pay hariç sermaye piyasası aracı ihraç eden (ihraç ettikleri sermaye piyasası araçlarının itfa

[4] TTK'nın 397'nci maddesi ile anonim şirketlerin yıllık finansal raporlarının bağımsız denetimi düzenlenmiş olup, sermaye piyasası mevzuatında tüzel kişiliği olmayan yatırım fonları gibi sermaye piyasası kurumlarının da bağımsız denetimi ile ara dönem finansal raporların da sınırlı bağımsız denetiminin düzenlenmesi gerekmiştir.

[5] Mevcut yürürlükteki liste Bakanlar Kurulu Kararı ile belirlenmiş olup, 2018'den sonraki güncellemeler için Cumhurbaşkanı Kararı geçerli olacaktır.

edildiği hesap döneminin sonuna kadar) veya bu amaçla Kurul'ca onaylanmış geçerlilik süresi bulunan ihraç belgesi olan anonim şirketler,

m) Sermaye piyasası araçları bir borsada veya teşkilatlanmış diğer piyasalarda işlem görmeyen ancak halka açık sayılan şirketlerden (ortak sayısı nedeniyle halka açık sayılan) aşağıdaki üç kriterden ikisini art arda iki hesap döneminde sağlayanlar:

1) Aktif toplamı 30 milyon Türk Lirası ve üzeri,

2) Yıllık net satış hasılatı 40 milyon Türk Lirası ve üzeri,

3) Çalışan sayısı 50 kişi ve üzeri.

b. Sınırlı Bağımsız Denetime (İncelemeye) Tabi İşletmeler

Tebliğ hükümleri uyarınca;

1) Yatırım kuruluşları (Aracı kurumlar ve bankalar),

2) Yatırım fonları hariç kolektif yatırım kuruluşları,

3) İpotek finansmanı kuruluşları,

4) Sermaye piyasası araçları bir borsada ve/veya teşkilatlanmış diğer pazar yerlerinde işlem gören anonim ortaklıkların,

6 aylık ara dönem finansal raporları sınırlı bağımsız denetime (incelemeye) tabidir.

Borsa İstanbul A.Ş. (BİAŞ veya Borsa) düzenlemeleri kapsamında payları Piyasa Öncesi İşlem Platformu'nda (PÖİP) işlem gören işletmelerin 6 aylık ara dönem finansal tabloları sınırlı bağımsız denetim (inceleme) kapsamında değildir. Ancak, Kurul'un 15.10.2020 tarih ve 2020/63 sayılı Bülteni'nde yayınlanan i-SPK. II-17.6 (15.10.2020 tarihli ve 64/1284 s.k.) sayılı İlke Kararı uyarınca fiili dolaşım oranının %5'in altına düşmesi nedeniyle payları PÖİP'e alınan ortaklıkların 6 aylık ara dönem finansal tabloları incelemeye (sınırlı bağımsız denetime) tabidir.

Diğer taraftan, sermaye piyasası mevzuatı hükümleri uyarınca halka açık sayılan kooperatif şirketleri bağımsız denetim bakımından borsa şirketlerinin tabi olduğu hükümlere tabidir. Bu nedenle, kooperatif şirketlerinin yıllık finansal raporlarının bağımsız denetim; 6 aylık finansal raporları ise sınırlı bağımsız denetim yükümlülüğü bulunmaktadır.

c. Özel Bağımsız Denetime Tabi İşletmeler

Özel bağımsız denetim, sermaye piyasası araçlarının halka arzı için Kurul'a başvuru sırasında veya birleşme, bölünme, devir ve tasfiye durumunda bulunan işletmelerce, bu amaçlarla herhangi bir tarih itibariyle düzenlenmiş finansal tabloların bağımsız denetimini ifade eder.

Sermaye piyasası araçları bir borsada ve/veya teşkilatlanmış diğer pazar yerlerinde işlem gören anonim ortaklıkların, sermaye piyasası araçlarının halka arzında veya mevcut paylarının hissedarları tarafından halka arzında, Kurul'un sermaye piyasası araçlarının kayda alınmasına ilişkin düzenlemelerinde öngörülen ara dönem finansal tabloları sınırlı bağımsız denetime tabidir.

Özel bağımsız denetim gerektiren haller, Kurul'un sermaye piyasası araçlarının kayda alınmasına ilişkin düzenlemeleri ile diğer ilgili düzenlemeleri çerçevesinde belirlenir. Özel bağımsız denetimde, bağımsız denetime tabi tutulacak finansal tabloların bağımsız denetim çalışmasının başladığı ay sonu veya daha sonraki bir tarih itibariyle hazırlanmış olması zorunludur. Özel bağımsız denetim çalışmasının, bağımsız denetim sözleşmesinin imzalandığı tarihte başladığı kabul edilir.

Özel bağımsız denetimi yapılan finansal tablo döneminden önceki yıllara ilişkin finansal tabloların bağımsız denetiminde, süre faktörü nedeniyle uygulanamayan bağımsız denetim tekniklerinin var olması halinde, "*bağımsız denetimde önemlilik kavramı*" hükümleri göz önünde bulundurularak yapılacak değerlendirme sonucunda bağımsız denetim görüşü oluşturulur ve raporlanır.

1.3.1.2. Bağımsız Denetimin Amacı ve Genel İlkeleri

1.3.1.2.1. Bağımsız Denetimin Amacı ve Kapsamı

Finansal tabloların bağımsız denetiminin amacı; finansal tabloların finansal raporlama standartları doğrultusunda bir işletmenin finansal durumunu ve faaliyet sonuçlarını tüm önemli yönleriyle gerçeğe uygun ve doğru bir biçimde gösterip göstermediği konusunda bağımsız denetçinin görüş bildirmesini sağlamaktır.

Bağımsız denetimi amacına uygun olarak gerçekleştirmek için uygulanan bağımsız denetim yöntem ve teknikleri bağımsız denetimin kapsamını oluşturur. Bağımsız denetimin gerçekleştirilebilmesi için uygulanacak bağımsız denetim yöntem ve tekniklerinin belirlenmesinde, bu Tebliğde yer alan hükümler, BDS'ler, Kurul'un konuya ilişkin düzenlemeleri ve yerine göre bağımsız denetim sözleşmesi ile raporlama gereklilikleri göz önünde bulundurulur. Bağımsız denetim sırasında uygulanacak denetim yöntem ve teknikleri esas olarak ilgili BDS'lerde düzenlenmektedir.

1.3.1.2.2. Bağımsız Denetime İlişkin Genel İlkeler

a. Mesleki Şüphecilik

Mesleki şüphecilik, denetçinin sorgulayıcı bir yaklaşımla hareket ederek, hata veya hile kaynaklı yanlışlığa işaret eden durumlara karşı dikkatli olmayı ve denetim kanıtlarını titiz bir biçimde değerlendirmeyi içeren tutumdur[6].

Bağımsız denetçi, bağımsız denetimi planlarken ve gerçekleştirirken, finansal tabloların işletmenin gerçek finansal durumunu ve faaliyet sonuçlarını göstermesine engel teşkil edebilecek ölçüde önemli yanlışlıkları içerebileceği varsayımını göz önünde bulundurarak, mesleki şüphecilik anlayışıyla hareket etmek zorundadır. Mesleki şüphecilik; bağımsız denetçinin, sorgulayıcı bir yaklaşımla, kanıtların geçerliliğini incelemesi ve kanıtların, işletme yönetiminin açıklamaları ve diğer bilgi ve belgeler ile çelişki içinde olup olmadığını değerlendirmesidir. Bağımsız denetçinin mesleki şüphecilik anlayışıyla hareket etmesi; bağımsız denetim sürecinde şüpheli olayların gerekli özen gösterilmeden değerlendirilmesi, bağımsız denetim kanıtlarından sonuca ulaşırken gereğinden fazla genelleme yapılması, bağımsız denetimin mahiyet, zamanlama ve kapsamının belirlenerek bağımsız denetim yöntem ve tekniklerinin seçimi ve sonuçlarının değerlendirilmesinde yanlış varsayımların kullanılması gibi bağımsız denetim risklerini azaltır. Bağımsız denetçi, bağımsız denetimi planlarken ve gerçekleştirirken işletme yönetiminin ne dürüst olmadığı ne de kuşku götürmez bir şekilde dürüst olduğu varsayımıyla hareket eder. Bu çerçevede; bağımsız denetçinin raporuna temel oluşturacak kanıtların toplanmasında, işletme yönetiminin açıklamaları yeterli ve uygun bağımsız denetim kanıtı olarak kabul edilemez.

Denetimde başlangıç noktası olan işin kabulünden başlamak üzere, özellikle elde edilen denetim kanıtlarının değerlendirilmesi olmak üzere, denetimin her aşamasında denetçinin mesleki şüpheciliği sürdürmesi gerekmektedir. Mesleki şüpheciliğin sağlanması ve sürdürülmesi bağımsız denetim amacının gerçekleştirilmesi; makul güvence sunulmasına dayanak yeterli ve uygun denetim kanıtlarının toplanmasını sağlar. Bu nedenle, denetçinin denetim sırasında yeterli düzeyde şüpheci bir tavır içerisinde olması, ön yargısız ve sorgulayıcı bir yaklaşımla hareket etmesi gerekmektedir.

b. Mesleki Muhakeme

Denetimin yürütülmesi sırasında mevcut olan şartlara uygun olarak atılacak adımlara yönelik bilgiye dayalı kararlar alınırken; mevzuat, BDS'ler, finansal raporlama standartları ve etik standartlar çerçevesinde, sahip olunan eğitim, bilgi ve deneyimin kullanılmasıdır. Bu kavram mesleki yargı olarak da kullanılır.

Bağımsız denetçi, denetimin planlanması ve yürütülmesi sırasında, denetimin doğru bir şekilde yapılması için mesleki muhakemesini kullanması gerekmektedir. Bunun temel nedeni, denetim boyunca gerekli ve yeterli bilgiler kapsamında kararlar alınması gerekmektedir. Mesleki muhakeme özellikle;

---

[6] BDS 200 Bağımsız Denetçinin Genel Amaçları ve Bağımsız Denetimin Bağımsız Denetim Standartlarına Uygun Olarak Yürütülmesi Standardı 13. paragraf.

- Önemlilik düzeyi ve denetim riskinin belirlenmesinde,
- Denetim yöntem ve tekniklerinin kapsam, içerik ve zamanlamasının belirlenmesinde,
- Yeterli ve uygun denetim kanıtı toplanıp toplanmadığının belirlenmesinde,
- Daha fazla denetim kanıtına ihtiyaç olup olmadığının belirlenmesinde,
- Müşteri yönetiminin muhakemelerinin değerlendirilmesinde,
- Elde edilen denetim kanıtlarına dayanılarak görüş veya sonuçlara ulaşılmasında

kullanır.

Mesleki muhakemenin ayırt edici niteliği, bu yargının makul yargılara varmak için gerekli bilgi ve deneyime sahip denetçi tarafından yapılmış olmasıdır. Mesleki muhakeme bilinen durum ve gerçekler kapsamında kullanılır. Denetim sürecinde ihtilaflı veya zor konularda denetim ekibinin kendi içinde ve diğer uygun kişiler ile görüşmeler yapması, bilgiye dayalı makul yargılara ulaşılmasına yardımcı olur. Mesleki muhakeme, varılan yargının;

- Denetim ve muhasebe ilkelerinin yetkin bir şekilde uygulanmış olduğunu yansıtıp yansıtmadığı ve
- Rapor tarihine kadar denetçi tarafından bilinen durum ve gerçekler ışığında uygun olup olmadığı ve tutarlı olup olmadığı

esas alınarak yürütülebilir.

Mesleki muhakemenin denetim sürecinde sağlanıp, sürdürülmesi ve belgelendirilmesi gerekir. Bu kapsamda, çalışma kağıtlarının denetim sırasında ortaya çıkan önemli hususlarda sonuçlara varılırken kullanılan önemli yargıları, anılan denetimle bağlantısı bulunmayan tecrübeli bir denetçinin anlayabilmesine olanak sağlayacak şekilde hazırlanması gerekir.

c. Makul Güvence

Makul güvence, bağımsız denetim kapsamında yüksek ancak mutlak olmayan güvence düzeyidir. Bağımsız denetim, finansal tabloların önemli bir yanlışlık içermediği konusunda makul bir güvenceyi sağlayacak şekilde tasarlanır. Makul güvence, bir bütün olarak finansal tabloların nitelik ve nicelik bakımından önemli bir yanlışlık içermediğine dair bir sonuca varmada yeterli ve uygun bağımsız denetim kanıtının toplanmasını gerektirir. Denetçi, işletme yönetiminin doğru ve dürüst olduklarına ilişkin edindiği kanaat nedeniyle makul güvence sağlamak için gerekli olan denetim kanıtlarından daha azıyla yetinemez. Makul güvence bağımsız denetimin tüm aşamalarında göz önünde bulundurulur. Makul güvencenin elde edilemediği ve denetçi raporundaki sınırlı olumlu görüşün (şartlı görüşün), hedef kullanıcılara yapılacak bildirim açısından, yetersiz kaldığı tüm durumlarda, BDS'ler denetçinin görüş bildirmekten kaçınmasını veya mevzuata göre çekilmenin mümkün olması hâlinde denetimden çekilmesini gerektirir.

Bağımsız denetimde, bağımsız denetçinin finansal tablolara ilişkin önemli yanlışlıkları ortaya çıkarmasını önleyen, yapılan işin niteliğinden kaynaklanan ve aşağıda örneklerine yer verilen kısıtlamaların bulunması durumunda, bağımsız denetçilerin finansal tablolara ilişkin mutlak bir güvence elde etmesi mümkün olmayabilir. Bu kısıtlamalar şunlardır:

a) Örnekleme yönteminin kullanılması,

b) İşletme yönetiminin kontrol sistemini devre dışı bırakacak şekilde hareket etme ve/veya muvazaalı işlem yapma olasılığı gibi, muhasebe ve iç kontrol sistemlerinin yapısından kaynaklanan doğal kısıtlamalar,

c) Bağımsız denetim kanıtlarının pek çoğunun sonuca yönelik olmaktan ziyade ikna edici özellikte olması,

d) Gerek bağımsız denetim yöntem ve tekniklerinin yapısı, zamanlaması ve kapsamının tespiti gibi kanıt toplama sürecinde ve gerekse toplanan kanıtlardan hareketle, muhasebe tahminlerinin makul olup olmadığının değerlendirilmesi gibi bir görüşe ulaşılması aşamasında bağımsız denetçinin yaygın

olarak kendi kanaatini kullanması,

e) İlişkili taraflar arasında yapılan işlemler gibi, finansal tablolara ilişkin bir sonuca varmayı sağlayacak kanıtların ikna ediciliği ile ilgili diğer sınırlamalar.

Bu sınırlamaların söz konusu olması halinde; finansal tablolarda normal koşullarda beklenenin ötesinde önemli ölçüde yanlışlık riskini artıran olağandışı durumlar veya önemli bir yanlışlık olduğunu gösteren herhangi bir belirti bulunmasa dahi, ilave bağımsız denetim yöntem ve teknikleri kullanılarak yeterli ve uygun bağımsız denetim kanıtı elde edilir. Mesleki muhakeme, denetime ilişkin durum ve gerçeklerle veya yeterli ve uygun denetim kanıtıyla desteklenmeyen kararların gerekçesi olarak kullanılamaz.

d. Önemlilik

Bağımsız denetçi, finansal tablolardaki önemli yanlışlıklarla ilgilidir ve bir bütün olarak finansal tablolardaki önemli olmayan yanlışlıkların tespit edilmesinden sorumlu değildir. Genel olarak eksiklik ve yanlışlıkların, tek başına veya toplu olarak, finansal tablo kullanıcılarının bu tablolara dayanarak alacakları ekonomik kararları etkilemesi makul ölçüde bekleniyorsa, söz konusu eksiklik ve yanlışlıklar önemli olarak kabul edilir. Önemliliğe ilişkin yargıya içinde bulunulan şartlar çerçevesinde varılır ve bu yargılar, denetçinin finansal tablo kullanıcılarının finansal bilgiye olan ihtiyaçlarını algılayışından, yanlışlığın büyüklüğünden veya niteliğinden ya da bu ikisinin bileşiminden etkilenir. Geçerli raporlama çerçevesinde yer alan önemliliğe ilişkin husus, denetim için önemliliğin belirlenmesinde denetçiye referans olur. Önemliliğin belirlemesinde, finansal tablo kullanıcıların finansal bilgiye olan ihtiyaçları dikkate alınarak, mesleki muhakeme kullanılır. Bağımsız denetçi, genel denetçim stratejisinin hazırlarken bir bütün olarak finansal tablolar için bir önemlilik belirler. Bu önemlilik düzeyi, denetim sırasında farklı bir tutar belirlemesine sebep olacak bilgiden haberdar olunması veya bilginin oluşması durumunda değiştirilir.

Bağımsız denetçi, denetimi planlarken önemli olarak nitelendirilecek yanlışlıkları büyüklüğü hakkında yargıda bulunur. Bağımsız denetçi, tespit etmiş olduğu düzeltilmemiş yanlışlıkların hem münferit hem de toplu olarak, finansal tablolar üzerinde önemli bir etkiye sahip olup olmadığını dikkate alır. Denetçi görüşü finansal tabloları bir bütün olarak ele alır ve denetçi, finansal tabloların bütünü açısından önemlilik arz etmeyen yanlışlıkların tespit edilmesinden sorumlu değildir.

Önemlilik ve bağımsız denetim riski birbiriyle ilişkilidir. Bir bütün olarak finansal tabloları önemli ölçüde etkileyebilecek yanlışlıkların tespitine yönelik bağımsız denetim teknikleri tasarlanırken, finansal tabloların önemli bir yanlışlık içerme riski; hem finansal tabloların geneli düzeyinde hem de işlem sınıfları, hesap bakiyeleri, dipnotlar ve işletme yönetiminin bu konulara ilişkin açıklamaları düzeyinde değerlendirilir.

e. Bağımsız Denetim Riski

İşletmeler, amaçlarını gerçekleştirmek üzere çeşitli stratejiler uygular ve faaliyetlerine, faaliyetlerinin karmaşıklığına, faaliyet gösterdikleri sektörlere, büyüklüklerine ve tabi oldukları düzenlemelere bağlı olarak, çeşitli ticari risklerle karşı karşıya kalırlar. Bu tür risklerin ortaya çıkarılması ve bunlara karşı gerekli önlemlerin alınması esas itibariyle işletme yönetiminin sorumluluğundadır. Bununla birlikte; finansal tabloları etkileyen risklerin ortaya çıkarılarak, finansal tablolara doğru olarak yansıtılıp yansıtılmadığının kamuya açıklanmasından bağımsız denetçiler de sorumludur.

Bağımsız denetçi, finansal tabloların Kurul'un finansal raporlama standartlarına ilişkin düzenlemeleri çerçevesinde tam ve doğru bir şekilde düzenlenip düzenlenmediği hakkında makul bir güvence elde edebilmek için bağımsız denetim kanıtları toplar ve toplanan bu kanıtları değerlendirir. Makul güvence kavramı, bağımsız denetçi tarafından verilen görüşün uygun görüş olmama riskini de içerir. Finansal tabloların önemli bir şekilde hatalı veya yanlış sunulduğu hallerde, bağımsız denetçi tarafından uygun olmayan bir görüş verilme riski, bağımsız denetim riski olarak adlandırılır.

Bağımsız denetçi, bağımsız denetim riskini, bağımsız denetimin amacına uygun bir şekilde kabul edilebilir düşük bir seviyeye indirmek üzere bağımsız denetim faaliyetlerini planlar ve yürütür. Bağımsız denetçi, görüşüne esas teşkil edecek makul sonuçlara ulaşabilmek için, yeterli ve uygun

bağımsız denetim kanıtlarının toplanmasına yönelik bağımsız denetim tekniklerini tasarlamak ve uygulamak suretiyle bağımsız denetim riskini azaltabilir. Bağımsız denetim riski kabul edilebilir düşük bir seviyeye indirildiğinde, makul güvence elde edilmiş sayılır. Denetim riski sıfıra indirilemeyeceğinden, denetçinin denetim riskini sıfıra indirmesi beklenmez. Dolayısıyla, finansal tabloların hata veya hile kaynaklı önemli bir yanlışlık içermediğine dair mutlak bir güvence elde edilemez. Bunun sebebi, denetçinin vardığı sonuçların ve görüşüne dayanak teşkil eden denetim kanıtlarının çoğunun, denetimin yapısal kısıtlamaları sebebiyle, kesin olmaktan ziyade ikna edici olmasıdır. Bir denetimin yapısal kısıtlamaları;

- Finansal raporlamanın niteliğinden,

- Denetim prosedürlerinin niteliğinden ve

- Denetimin makul bir sürede ve makul bir maliyetle yürütülmesi gerekliliğinden

kaynaklanır.

Denetim riski, finansal tabloların önemli yanlışlıkları içerme riski, önemli yanlışlık riski ile bağımsız denetçinin bu yanlışlığı ortaya çıkaramama riskinin bir fonksiyonudur. Bağımsız denetçi, finansal tabloların önemli yanlışlıkları içerme riskini değerlendirmek üzere bağımsız denetim teknikleri uygular ve bu değerlendirmeye dayanarak ilave bağımsız denetim teknikleri uygulamak suretiyle tespit edememe riskini sınırlandırmanın yollarını araştırır.

İşletme yönetimince bağımsız denetçiye sunulan bilgi ve belgeler ile yapılan açıklamalar kapsamında finansal tabloların önemli bir yanlışlık içerme riski iki bileşenden oluşur. Bunlar bağımsız denetim riskinin unsurları olarak ifade edilir. Bu unsurlar:

a) "*Yapısal risk*", ilgili kontrol mekanizmasının bulunmadığı varsayımı altında, münferit ya da diğer yanlışlıklarla birlikte toplulaştırılmış olarak, işletme yönetiminin sunduğu bilgi ve belgelerin ve yaptığı açıklamaların önemli bir yanlışlık içerme olasılığıdır. Bu açıklamalardan bazılarının, ilgili işlem türleri, hesap bakiyeleri ve dipnot açıklamalarına ilişkin taşıdığı bir yanlışlık riski, diğerlerine göre daha yüksek olabilir.

Yapısal risk, işletmenin yapısal risk faktörlerinden etkilenir. Yapısal risk seviyesi, yönetim beyanının yanlışlığa olan açıklığı ne ölçüde yapısal risk faktörlerinden etkilendiğine bağlı olarak, yapısal risk aralığı olarak ifade edilen bir ölçeğe göre farklılık gösterir. Karmaşık hesaplamaların önemli yanlışlıkları içerme riski basit hesaplamalara göre daha fazladır. Önemli bir değerleme belirsizliği taşıyan hesap kalemlerine ilişkin muhasebe tahminlerinden türetilen tutarlar, göreceli olarak rutin ve gerçek veriler içeren hesap kalemleri tutarlarına göre daha büyük bir risk taşır. İşletmenin ticari riskini artıran dış koşullar, aynı zamanda yapısal riski de etkileyebilir. Bu kapsamda, teknolojik gelişmeler belirli bir ürünü modası geçmiş hale getirmiş olabilir ve bu durum stokların finansal tablolarda olduğundan daha fazla bir değerle gösterilmesine yol açabilir.

b) "*Kontrol riski*", münferit veya diğer yanlışlıklarla birlikte toplulaştırılmış olarak, işletme yönetimi tarafından sunulan bilgi ve belgelerde bulunabilecek önemli bir yanlışlığın, işletmenin iç kontrol sistemi tarafından zamanında engellenememe veya tespit edilip düzeltilememe olasılığıdır. Bu risk, işletmenin finansal tablolarının düzenlenmesi, iç kontrol sisteminin tasarımı ve işleyişinin etkinliğine bağlı olarak değişir. Bazı durumlarda kontrol riski, iç kontrol sisteminin niteliği gereği sahip olduğu doğal sınırlamalar nedeniyle, mevcudiyetini daima korur.

Kontrol riski, işletmenin finansal tabloların hazırlama amaçlarına ulaşılmasını tehdit eden belirlenmiş riskleri ele almak amacıyla yönetim tarafından kontrollerin tasarlanma, uygulanma ve sürdürülme etkinliğinin bir fonksiyonudur. Kontroller ne kadar iyi tasarlanmış ve uygulanmış olursa olsun, yapısal kısıtlamalar (kişilerin hatası, yönetimin muvazaalı işlemleri sonucu iç kontrolün ihlal edilmesi gibi) sebebiyle finansal tablolardaki "*önemli yanlışlık*" risklerini ortadan kaldırmaz, sadece azaltabilir.

Yapısal risk ve kontrol riski, işletmenin riskleridir ve finansal tabloların denetiminden bağımsız olarak ortaya çıkar. Bağımsız denetçinin, ilave bağımsız denetim tekniklerinin gerekip gerekmediğine karar verebilmesi için, kayıt ve belgeler ile işletme yönetimince yapılan açıklamaları finansal tabloların önemli bir yanlışlık içerme riski açısından değerlendirmesi gerekir. Bu değerlendirme, riskin tam olarak

ölçülmesinden ziyade bağımsız denetçinin mesleki kanaati niteliğindedir. Bağımsız denetçinin finansal tabloların önemli bir yanlışlık içerme riskine ilişkin değerlendirmesinin işletmenin kontrol mekanizmasının etkinliğine yönelik hususları da kapsaması durumunda; bağımsız denetçi, bu risk değerlendirmesini desteklemek üzere kontrol testleri yapar. Yapısal risk ile kontrol riskinin ayrı ayrı ele alınmasından ziyade, bunların birlikte finansal tabloların önemli bir yanlışlık içerme riski olarak değerlendirilmesi amaçlanmaktadır. Finansal tabloların önemli yanlışlık riski içerip içermediğine ilişkin değerlendirme, niteliksel olarak veya yüzde veriler halinde niceliksel olarak ifade edilebilir.

"*Tespit edememe riski*", bağımsız denetçinin, münferit ya da diğer yanlışlıklarla birlikte toplulaştırılmış olarak, finansal tablolardaki önemli bir yanlışlığı ortaya çıkaramama olasılığıdır. Tespit edememe riski, bağımsız denetçinin uygulamaları ile bağımsız denetim tekniklerinin etkinliğine bağlı olarak değişir. Bağımsız denetçinin işlem türleri, hesap bakiyeleri veya dipnot açıklamalarının tamamına ilişkin bir inceleme yapma olanağının bulunmaması ve diğer faktörler nedeniyle, tespit edememe riski hiçbir zaman sıfıra indirilemez. Söz konusu diğer faktörler arasında; bağımsız denetçi tarafından uygun olmayan bir bağımsız denetim tekniğinin seçilmiş olması, bağımsız denetim tekniklerinin yanlış uygulanması veya bağımsız denetim sonuçlarının yanlış yorumlanması sayılabilir. Ancak, yeterli ve uygun planlama yapılması, bağımsız denetim ekibinin doğru seçilmesi ve yönlendirilmesi, mesleki şüpheciliğin uygulanması, yapılan bağımsız denetim çalışmalarının kontrol ve gözetimi suretiyle diğer risk faktörlerinin ortaya çıkmaları engellenebilir veya etkileri ortadan kaldırılabilir.

1.3.1.2.3. Bağımsız Denetim Faaliyetinde Bulunma Şartları

Sermaye piyasasında bağımsız faaliyeti, Tebliğ'de belirtilen şartları taşıyan ve Kurul'ca yetkilendirilen bağımsız denetim kuruluşları tarafından gerçekleştirilir. Bağımsız denetim kuruluşlarının aşağıdaki şartları taşımaları gerekmektedir:

a) KGK tarafından yetkilendirilmiş olması,

b) Organizasyon, mekan, teknik donanım, belge ve kayıt düzeninin sermaye piyasasında bağımsız denetim işini yürütecek düzeyde bulunması,

c) Bağımsız denetim kuruluşunun kalite kontrol sisteminin işleyişinden ve gözetiminden sorumlu en az bir sorumlu ortak başdenetçi nezaretinde çalışacak yeter sayıda denetçi veya konusunda uzman personelden oluşan bir Kalite Kontrol Güvence Komitesi'ne sahip olması,

d) 660 sayılı KHK uyarınca yaptırması zorunlu mesleki sorumluluk sigortasının asgari tutarının 200.000 TL'den az olmamak üzere bir önceki faaliyet döneminde bağımsız denetim faaliyetinden elde edilen gelirin iki katından az olmayacak şekilde belirlenmesi.

Bağımsız denetim kuruluşlarının, yönetici ve denetçilerinin aşağıdaki koşulları sağlaması gerekmektedir:

a) KGK tarafından sermaye piyasasında bağımsız denetim yapmak üzere yetkilendirilmiş olması,

b) KGK tarafından yetkilendirildikleri tarihi takiben, her yıl en az bir olmak üzere, iki yılda iki adet SPKn kapsamında olmayan ortaklıkların bağımsız denetim çalışmasında fiilen yer almış veya sermaye piyasasında bağımsız denetim yapmaya yetkili kuruluşlarda denetçi yardımcısı olarak fiilen iki yıl çalışmış olması (Sermaye piyasasında bağımsız denetim lisansına sahip olanlar bu şartı sağlamış sayılır.),

c) Sorumlu ortak baş denetçi olabilmek için, en az iki yıl Kurul'un listesinde yer alan bağımsız denetim kuruluşlarında sermaye piyasası kurumları ve halka açık anonim ortaklıkların bağımsız denetiminde fiilen denetçi, kıdemli denetçi veya baş denetçi unvanı ile faaliyet göstermeleri,

d) Sermaye piyasası mevzuatı veya diğer mevzuat uyarınca bağımsız denetim yapma yetkisi iptal edilmiş olan kuruluşlarda yetki iptaline neden olan bağımsız denetim faaliyetlerinde sorumluluklarının tespit edilip bağımsız denetim faaliyetinde bulunmaktan sürekli olarak yasaklanmamış ve bağımsız denetim faaliyetinde bulunması süreli olarak yasaklananların ise yasaklarının süresi sonunda Kurul'ca kaldırılmış olması,

e) Faaliyet yetki belgelerinden biri veya birden fazlası iptal edilmiş yahut borsa üyeliği iptal edilmiş işletmelerde iptalde sorumluluğu bulunan kişilerden olmaması,

f) Sermaye piyasası mevzuatına muhalefetten dolayı haklarında verilmiş mahkumiyet kararının bulunmaması.

Bağımsız denetçi yardımcılarının yukarıda (d) (e) ve (f) bentlerinde sayılan koşullara sahip olmaları ve 3568 sayılı Kanunda belirlenen yüksek öğrenim şartını sağlamaları gereklidir.

1.3.1.2.4. Bağımsız Denetim Sözleşmeleri

İşletmeler, bağımsız denetim sözleşmesini BDS 210 Bağımsız Denetim Sözleşmesinin Şartları Üzerinde Anlaşmaya Varılması Standardı (BDS 210) kapsamında hazırlar ve imzalar. Anonim ortaklık niteliğindeki işletmeler, bağımsız denetim kuruluşlarının seçimini TTK hükümlerine ve KGK düzenlemelerine uygun olarak yapar. Genel kurulda seçilen bağımsız denetim kuruluşu ile yapılan bağımsız denetim sözleşmesi müşterinin yönetim kurulu ve bağımsız denetim kuruluşu tarafından birlikte imzalanarak yürürlüğe girer. Yatırım fonlarının bağımsız denetim kuruluşlarının seçimi, kurucu yönetim kurulu; konut ve varlık finansmanı fonlarının bağımsız denetim kuruluşlarının seçimi ise fon kurulu tarafından yapılır. Bir bağımsız denetim kuruluşunun, müşteriye vereceği denetim hizmetinin azami süresi ve kısıtlamaları hususlarında, TTK ve KGK düzenlemelerinde yer alan hükümler geçerlidir.

Bağımsız denetim kuruluşu seçiminin, hesap dönemi bitimini takip eden 3 ay içerisinde yapılması gereklidir. Bağımsız denetim kuruluşunun herhangi bir nedenle seçilememesi halinde, konu en geç durumun ortaya çıktığı tarihi izleyen ilk iş gününde Kurul'a bildirilmelidir.

Bağımsız denetim kuruluşu ile müşterisi (işletme) anlaşarak bağımsız denetim sözleşmesini sona erdiremezler. Ancak müşteriler, Kurul tarafından onaylanacak haklı gerekçelerin varlığı halinde; bağımsız denetim kuruluşları ise, müşteri tarafından çalışma alanının önemli ölçüde sınırlandırılması nedeniyle finansal tablolara ilişkin bilgi ve belgeleri elde edememesi durumunda ya da BDS'lerde sözleşmenin sona erdirilmesine ilişkin belirtilen haklı gerekçelerin varlığı hallerinde, yazılı gerekçe göstermek koşuluyla bağımsız denetim sözleşmesini Kurul'dan görüş alarak sona erdirebilirler. Sona erme durumunda, bağımsız denetim kuruluşunun çalışma notlarını ve gerekli tüm bilgileri, yerine geçecek olan bağımsız denetim kuruluşuna devredilmek üzere Kurul'a teslim etmesi zorunludur.

1.3.1.2.5. Bağımsız Denetçilerin Nitelikleri

Sermaye piyasasında bağımsız denetim faaliyeti gerçekleştirecek bağımsız denetçilerin Tebliğ'de belirtilen nitelikleri taşımaları gerekmektedir.

a. Bağımsız Denetçi Unvanları

Bağımsız denetçilerin alabilecekleri unvanlar kıdem sırasına göre; sorumlu ortak baş denetçi, baş denetçi, kıdemli denetçi, denetçi ve denetçi yardımcısıdır.

Sorumlu ortak baş denetçi, bağımsız denetim kuruluşunda pay sahibi olup baş denetçi unvanını haiz ve bağımsız denetim çalışmasını kuruluş adına kendi kişisel sorumluluğu ile yürüten ve kuruluş adına bağımsız denetim raporlarını imzalamaya yetkili gerçek kişidir.

Baş denetçi unvanının kazanılması için en az fiilen 10 yıl, kıdemli denetçi unvanının kazanılması için en az fiilen 6 yıl ve denetçi unvanının kazanılması için en az fiilen 3 yıl mesleki deneyim şarttır. Denetçi yardımcılığında geçen süre bu hesaplamada dikkate alınır. Mesleki deneyim süresinin tespitinde, bir bağımsız denetim kuruluşunda tam zamanlı olarak geçen fiili çalışma süresi esas alınmakla birlikte, finansal raporların hazırlanması ve/veya denetlenmesi ile yetkili olarak özel sektör ve/veya kamu kurumlarında geçen fiili hizmet süreleri de mesleki deneyim süresinin hesaplanmasında dikkate alınır.

Bilgi, deneyim ve yetenekleri bir üst kıdemin gerektirdiği nitelikte olmayanlar sürelerini doldursalar dahi bağımsız denetim kuruluşunun yetkili organlarınca bir üst unvana terfi ettirilemezler.

b. Mesleki Yeterlik

Bağımsız denetim kuruluşları, bağımsız denetçilerinde mesleki yeterliği aramak ve sağlamak zorundadırlar. Mesleki yeterlik, lisans düzeyinde ve sonrasında eğitim ve öğrenim ile mesleki deneyimin bağımsız denetim yapabilecek düzeyde olmasını ifade eder.

Yapılacak bağımsız denetim sonuçlarından yararlanacak olan tüm ilgili taraflar, bu alanda yapılan bağımsız denetim çalışmalarının yürütülüp sonuçlandırılması sorumluluğunu üstlenecek bağımsız denetçilerin mesleki bakımdan yeterli olmalarını beklemek ve aramak hakkına sahiptirler. Bağımsız denetim kuruluşları ve bağımsız denetçiler, kaliteli bir bağımsız denetim hizmeti sunmak ve müşterinin kendilerinden bu yükümlülüğü yerine getirmelerini beklediğinin bilincinde olmak zorundadırlar.

c. Mesleki Yeterliğin Sağlanması ve Geliştirilmesi

Bağımsız denetim kuruluşları denetçi yardımcılarının işe alınmalarında, mesleki eğitime yeterli bir temel oluşturacak lisans düzeyinde eğitim gördüklerini araştırmak, istihdam ettikleri denetçi yardımcılarına gerekli mesleki eğitim ve deneyimi kazandıracak tedbirleri almak, bağımsız denetçi sıfatı verilecek denetçi yardımcılarında bir önceki maddede öngörülen mesleki yeterliğin varlığını, mülakat sonuçları, kurs değerlendirme tutanakları, tezkiyeler, bağımsız denetim kuruluşunca veya ilgili meslek kuruluşlarınca yapılan sınav sonuçları gibi belgelerle tespit etmek zorundadırlar.

Bağımsız denetim kuruluşları, istihdam ettikleri bağımsız denetçilerin mesleki gelişmelerini sürekli olarak sağlayacak tedbirleri almakla da yükümlüdürler. Bağımsız denetçiler kendilerinin ve yanlarında çalışan denetçi ve denetçi yardımcılarının mesleki yeterliklerinin sağlanması, korunması ve geliştirilmesinden sorumludurlar. Mesleki yeterliğe ulaşamayan veya bu özelliklerini kaybeden bağımsız denetçilerin işine son verilir, durum en geç 6 iş günü içinde Kurul'a bildirilir. Bağımsız denetçi ve bağımsız denetçi yardımcılarının yetişmesinde kendi gayret ve çalışmaları esastır. Bu amaçla, her düzeydeki bağımsız denetçi ve bağımsız denetçi yardımcısı, mesleki yeterliğin bir gereği olarak, bağımsız denetim mesleği ile ilgili mevzuatı, ulusal ve uluslararası gelişmeleri ve yayınları, düzenlenen kurs, seminer ve konferansları izlemek zorundadır.

d. Hizmet İçi Eğitim ve Refakat Çalışması

Bağımsız denetim kuruluşları, mesleki deneyime sahip olmaksızın ilk kez işe aldıkları denetçi yardımcılarını staja tabi tutarlar. En az fiilen 2 yıl süren bu staj döneminde denetçi yardımcıları, 4 ay süre ile muhasebe ve bağımsız denetim teori, standart ve teknikleri, finansal analiz, iç kontrol, bilgi işlem, para ve sermaye piyasası, şirketler hukuku, kurumsal yönetim, ticaret hukuku, vergi mevzuatı ve bankacılık konularında eğitime tabi tutulurlar. Bu eğitimin sonuçları, bağımsız denetim kuruluşlarınca veya ilgili meslek kuruluşlarınca yapılacak sınavla değerlendirilir. Bu kurslar, toplam iki yüz saatten az olamaz. Bağımsız denetim kuruluşları, denetçi yardımcılarının eğitimleri için müşterek eğitim programları ve sınavlar düzenleyebilirler. Staj döneminde, denetçi yardımcılarının birden çok işte ve birden çok denetçi refakatinde çalıştırılması için her türlü tedbir alınır. Hizmet içi eğitim ve refakat çalışmalarının, sorumlu ortak baş denetçinin gözetim ve sorumluluğu altında planlı olarak yürütülmesi zorunludur.

e. Tam Zamanlılık

Tam zamanlılık, bağımsız denetçilerin mesleki yeterliğinin sağlanması ve geliştirilmesi suretiyle bağımsız denetimin kalitesinin artırılması ve kurumsallığın sağlanması açısından mevcut çalışma ortamında sürekli bir şekilde faaliyet gösterilmesini ifade eder. Bu kapsamda, bağımsız denetim kadrosunda yer alan bağımsız denetçilerin bağımsız denetim kuruluşunda tam zamanlı olarak görev yapmaları zorunludur. Tam zamanlılık, bağımsız denetçilerin yarı zamanlı eğitmen ya da öğretim görevlisi olarak hizmet vermelerine engel teşkil etmez. Tam zamanlılık bağımsız denetimi üstlenilen işletmelerin münhasıran bağımsız denetimi sürecinde bulunulması ile sınırlı değildir.

1.3.1.2.6. Bağımsız Denetim Kuruluşları ve Bağımsız Denetçilerin Uyacakları Etik İlkeler

Bağımsız denetim kuruluşları ile bağımsız denetçilerin uyacakları etik ilkeler esas olarak KGK tarafından yayınlanan Bağımsız Denetçiler İçin Etik Kurallar'da (Etik Kurallar) düzenlenmiştir. Beş

temel etik ilke bulunmaktadır. Bunlar dürüstlük, tarafsızlık, mesleki yeterlilik ve özen, sır saklama (gizlilik) ve mesleğe uygun davranıştır. Etik Kurallar, bu Çalışma Notu'nda ayrı bir bölüm olarak ele alınacak olup, burada Tebliğ'de düzenlenen denetçilerin uyması gereken etik kurallar ile diğer kurallara yer verilmektedir.

a. Mesleki şüphecilik

Elde edilen bağımsız denetim kanıtlarının geçerliliğinin sorgulayıcı bir anlayışla değerlendirilmesi mesleki şüpheciliği ifade eder. Bağımsız denetçi, finansal tablo ve diğer finansal bilgilerin önemli bir yanlışlık içerebileceğini dikkate alarak, bağımsız denetimi, mesleki şüphecilik anlayışıyla planlayarak yürütür.

b. Bağımsızlık

Bağımsızlık, mesleki faaliyetin dürüst ve tarafsız yürütülmesini sağlayacak bir davranış ve anlayışlar bütünüdür[7]. Bağımsız denetim kuruluşları ve bağımsız denetçiler, bağımsız denetim çalışmalarında bağımsız olmak zorundadırlar. Bağımsız denetçilerin dürüst ve tarafsız olmaları yanında, bağımsızlıklarını ortadan kaldırabilecek özel durumlarının da bulunmaması gerekir.

Bağımsız denetçiler;

a) Çalışmaları sırasında mesleki şüphecilik anlayışıyla hareket etmek,

b) Ortaya çıkabilecek çıkar çatışmalarından uzak kalmak,

c) Karşılaştığı etik çatışmaların çözümünü sağlayabilmek için en yakın amirinden başlayarak çatışmaya konu olan hususu üstlerine taşımak, konu kuruluş içinde çözümlenemezse ilgili yasal düzenleyici kurumlara ve Kurul'a başvurmak,

d) Dürüstlük ve tarafsızlıklarını etkileyebilecek hiçbir müdahaleye imkan vermemek,

e) Bağımsız denetim sonucunda ulaştıkları görüşlerini, başkalarının doğrudan veya dolaylı çıkarlarını düşünmeksizin raporlarında açıklamak

zorundadırlar.

Bağımsız denetçinin, bağımsızlığını tehdit eden unsurlar ile bunlara karşı oluşturulan önlem mekanizmalarını çalışma kağıtlarında belgelemesi ve söz konusu hususları denetimden sorumlu komiteler ile tartışmaları zorunludur. Ayrıca, bağımsız denetçi bağımsız denetimlerde bağımsız olduğunu doğrulayan yazılı bir beyanı müşterinin denetimden sorumlu komitesine sunar. Bağımsız denetim kuruluşları da bağımsızlığı tehdit eden hususlar konusunda alınabilecek önlemleri önemlilikleri bakımından belirleyerek, bağımsızlıkla ilgili politikalarını yazılı hale getirirler.

c. Bağımsızlığı Ortadan Kaldıran Durumlar

Bağımsız denetim kuruluşu veya bağımsız denetçilerde, bağımsızlığın zedelendiğine dair tereddüt oluşması halinde bağımsızlığın ortadan kalktığı kabul edilir. Bağımsızlığın ortadan kalkmış sayılacağı durumlar, bunlarla sınırlı olmamak üzere:

a) Bağımsız denetim kuruluşunun ortak, yönetici, bağımsız denetçileri, denetçi yardımcıları ve bunların üçüncü dereceye kadar (üçüncü derece dahil) kan ve sıhri hısımları ile eşleri veya bağımsız denetim kuruluşları tarafından;

1) Müşteriden veya müşteri ile ilgili olanlardan, doğrudan doğruya veya dolaylı olarak bir menfaat elde edildiğinin ortaya çıkması veya bunlara bir menfaat sağlanacağı vaadinin, ilgili bağımsız denetçi tarafından bağımsız denetim kuruluşunun yönetimine yazılı olarak bildirilmemiş olması,

2) Müşteriyle veya müşterinin ortaklarıyla veya müşterinin yönetim, denetim veya sermaye bakımından dolaylı veya dolaysız olarak bağlı bulunduğu veya nüfuzu altında bulundurduğu gerçek

[7] *Etik Kurallar'da, bağımsızlık, esasta bağımsızlık ve görünüşte bağımsızlıktan oluşur. Esasta bağımsızlık, denetçinin dürüstlük, tarafsızlık ve mesleki şüphecilik içinde hareket etmesini teminen, mesleki muhakemesini olumsuz etkileyebilecek tesirlerden ari olarak görüş/sonuç açıklamasıdır. Şekilde bağımsızlık ise denetim kuruluşu veya denetçinin makul ve bilgi sahibi üçüncü kişilerde, dürüstlük, tarafsızlık ve mesleki şüphecilikten ödün verdiği intibaını oluşturabilecek durum ve davranışlardan sakınmasıdır.*

veya tüzel kişilerle ortaklık ilişkisine girilmiş olduğunun belirlenmiş olması,

3) Müşteri ile bağlı ortaklıkları, müşterek yönetime tabi teşebbüsleri ve iştiraklerinde kurucu, yönetim kurulu başkan veya üyesi, şirket müdürü veya yardımcısı olarak veya işletmede önemli karar, yetki ve sorumluluğu taşıyan başka sıfatlarla görev alınması,

4) Müşteri veya bağlı ortaklıkları, müşterek yönetime tabi teşebbüsleri ve iştirakleri ile olağan ekonomik ilişkiler dışında borç-alacak ilişkisine girilmiş olması,

b) Geçmiş dönemlere ilişkin bağımsız denetim ücretinin, geçerli bir nedene dayanmaksızın, müşteri tarafından ödenmemesi ve

c) Bağımsız denetim ücretinin, bağımsız denetim sonuçları ile ilgili şartlara bağlanmış olması veya piyasa rayicinden bariz farklılıklar göstermesi, bağımsız denetimin kalitesine dair belirsizlikler yaratması, bağımsız denetim kuruluşu tarafından müşteri işletmeye sunulan diğer hizmetler dikkate alınarak belirlenmesi.

Bağımsız denetçiler, fiilen bağımsız denetimini yaptıkları işletmelerde, işletmenin finansal tabloları hakkında düzenlenen en son bağımsız denetim raporu tarihinden itibaren 2 yıl (cooling off period) geçmedikçe, söz konusu işletmede yönetim kurulu başkan ve üyeliği, genel müdür, müdür ve yardımcılığı ile önemli karar, yetki ve sorumluluğu taşıyan pozisyonlarda görev alamazlar.

Bağımsız denetim kuruluşları ile bunların bağımsız denetçileri ve diğer personeli, bu Tebliğe göre bağımsız denetim hizmeti verdikleri işletmelere, bağımsız denetim hizmeti verdikleri dönemde, bedelli veya bedelsiz olarak;

a) Muhasebe defterlerinin tutulması ve buna ilişkin diğer hizmetlerin verilmesi,

b) Finansal bilgi sistemi kurulması ve geliştirilmesi ile işletmecilik, muhasebe, finans konularındaki uygulamalarla ilgili danışmanlık hizmeti verilmesi, belge düzenlenmesi ve rapor hazırlanması,

c) Değerleme ve aktüerya hizmetleri verilmesi veya ekspertiz ve uygunluk raporu hazırlanması,

d) İç denetim fonksiyonunun yerine getirilmesi ya da iç denetim fonksiyonuna destek hizmeti verilmesi,

e) Yönetim veya insan kaynakları fonksiyonlarının yerine getirilmesi,

f) Aracılık veya yatırım danışmanlığı hizmetlerinin verilmesi,

g) Hukuki danışmanlık veya diğer uzmanlık hizmetlerinin verilmesi,

h) Tahkim ve bilirkişilik yapılması ve

i) Kurul tarafından yapılmasına izin verilmeyen alanlarda hizmet sunulması

faaliyetlerinde bulunamazlar. Söz konusu faaliyetleri, bağımsız denetim hizmeti verdikleri işletmelere, aynı dönemde bedelli veya bedelsiz olarak; merkezi yurtdışında bulunan aynı bağımsız denetim kuruluşu ile hukuki bağlantısı olan Türkiye'de yerleşik diğer kuruluşlar aracılığı ile de yerine getiremezler. Ancak, 3568 sayılı Kanun çerçevesinde; finansal tabloların ve beyannamelerin vergi mevzuatı hükümlerine uygunluğunu incelemek ve uygunluğu tasdik etmek, konu hakkında yazılı görüş vermek ve rapor düzenlemek faaliyetleri dördüncü fıkrada belirtilen yapılamayacak faaliyetler kapsamında değerlendirilmez.

Bağımsız denetim kuruluşunun yönetim veya sermaye bakımından doğrudan ya da dolaylı olarak hakim bulunduğu veya ilişkili olduğu bir danışmanlık şirketi, bağımsız denetim kuruluşunun hizmet verdiği müşterisine, aynı dönem için danışmanlık hizmeti veremez. Bu kapsama, bağımsız denetim kuruluşunun gerçek kişi ortakları ve yöneticileri tarafından verilen danışmanlık hizmetleri de dahildir.

d. Mesleki Özen ve Titizlik

Mesleki özen ve titizlik, basiretli bir bağımsız denetçinin aynı koşullar altında ayrıntılara vereceği önemi, göstereceği dikkat ve gayreti ifade eder. Bağımsız denetçiler, bağımsız denetimin

planlanması, yürütülüp sonuçlandırılması ve bağımsız denetim raporunun hazırlanması safhalarında gerekli mesleki özen ve titizliği göstermek zorundadırlar. Gerekli özen ve titizliğin asgari kıstası, bağımsız denetim standartlarına eksiksiz uyulmasıdır. Buna göre, bir bağımsız denetçi bağımsız denetim faaliyetini gerektiği şekilde planlamak, program yapmak, yeterli miktarda, uygun nitelikte ve güvenilir bağımsız denetim kanıtı toplayarak inceleme yapmak, temiz ve düzenli çalışma kağıtları hazırlamak, finansal tabloların gerçekliği ve doğruluğu hakkında dürüst ve doğru bir yargıya ulaşmak ve görüşünü, özen ve titizlikle düzenleyeceği bağımsız denetim raporunda açıklamak zorundadır.

e. Ticaret ve Mesleğe Aykırı Faaliyet Yasağı

Bağımsız denetim kuruluşları ve bağımsız denetçiler:

a) Mesleki faaliyetler dışında ticari, sınai ve zirai hiçbir işle uğraşamazlar (ticaret şirketlerinin yönetim kurulu başkan ve üyeliği, genel müdür, genel müdür yardımcılığı ile önemli karar, yetki ve sorumluluğu taşıyan başka pozisyonlar dahil),

b) Başka bir bağımsız denetim kuruluşunda ortak olamazlar, yönetici ve bağımsız denetçi olarak çalışamazlar (başka bir bağımsız denetim kuruluşu ile birleşilmesi veya merkezi yurtdışında bulunan bir kuruluşun aynı çalışma yöntemleri ile ülkemizdeki bir kuruluşa katılması halleri hariç) ve

c) Meslek ve meslek onuru ile bağdaşmayan faaliyetlerde ve davranışlarda bulunamazlar.

f. Reklam Yasağı

Bağımsız denetim kuruluşları, iş elde etmek için dolaylı ve dolaysız reklam yapamazlar, reklam sayılabilecek faaliyetlerde bulunamazlar ve iş öneremezler. Ancak, bağımsız denetim kuruluşları, tanıtıcı bilgiler içeren broşürler hazırlayıp dağıtabilirler, kendileri veya müşterileri için eleman aramaya yönelik ilanlar verebilirler, mesleki konularda bilimsel nitelikte yayın yapabilirler. İlan ve broşürlerde;

a) İşin sonucu ile ilgili vaat ve taahhütlerde bulunulmaması,

b) İşini gerektirdiği ciddiyette ve ölçüde kalınması,

c) Abartılmış, hissî, gerçeğe uymayan ve kamuoyunu aldatıcı ve yanıltıcı, deneyim noksanlıklarını istismar edici söz, görüntü ve bilgi unsurlarına yer verilmemesi veya bu izlenimin yaratılmaması,

ç) Yapılabilecek iş ve hizmetler konusunda somut temeli olmayan bekleyişler yaratılmaması ve

d) Bağımsız denetim kuruluşunun diğer bağımsız denetim kuruluşlarıyla karşılaştırılmaması

gerekmektedir.

Reklam yasağı, bağımsız denetim kuruluşlarının bağımsız denetçileri için de geçerlidir.

g. Sır Saklama Yükümlülüğü

Bağımsız denetim kuruluşlarının yöneticileri, bağımsız denetçileri ve bütün çalışanları ile bağımsız denetim kuruluşlarına dışardan hizmet verenler, işleri dolayısıyla sahip oldukları sırları açıklayamazlar, bu sırları kendilerinin veya üçüncü kişilerin menfaatlerine kullanamazlar. Aşağıda yer alan hususlar sır sayılmaz:

a) Bağımsız denetim standart, ilke ve kuralları ile meslek ahlakı gereği yapılması zorunlu açıklamalar,

b) Kamuyu aydınlatma amacıyla mevzuat gereği yapılan ilave duyurular,

c) Adlî veya mevzuatla yetkili ve görevli kılınmış olmak kaydıyla idari ve her türlü inceleme ve soruşturma halleri ile suç oluşturan durumlara ilişkin olarak, sır sayılan bilgilerin yetkililere verilmesi.

h. Karşılıklı İlişkiler ve Haksız Rekabet

Bağımsız denetim kuruluşları ile bağımsız denetçiler, bağımsız denetim faaliyetinin niteliğini herhangi bir suretle olumsuz yönde etkileyebilecek veya meslektaşlarına zarar verebilecek tarzda ve ölçüde rekabete giremezler. Özellikle bağımsız denetim ücreti, personel ve iş alma gibi konulardaki mesleki kurallar, teamül ve bağımsız denetim standart, ilke ve kurallarına aykırı davranışlarda

bulunamazlar. Diğer düzenlemelerde yer alan haksız rekabet halleri saklıdır.

Bir bağımsız denetim kuruluşu, özel bağımsız denetim veya Kurul tarafından gerekli görülen haller hariç olmak üzere, başka bir bağımsız denetim kuruluşu ile bağımsız denetim hizmeti ilişkisi devam eden bir işletmenin aynı döneme ilişkin bağımsız denetim hizmet talebini kabul edemez.

1.3.1.2.7. Diğer Görev, Yetki ve Sorumlulukları

a. Ekip Çalışmasında Görev, Yetki ve Sorumluluk

Her bir bağımsız denetim için en az 3 asil ve 3 yedek olmak üzere 6 kişiden oluşan bir bağımsız denetim ekibi oluşturulmalı ve her bir bağımsız denetim en az 3 kişi olmak üzere işin gerektirdiği sayı ve nitelikte bağımsız denetçilerden oluşan ekip tarafından gerçekleştirilmelidir. Sorumlu ortak baş denetçi başkanlığında, baş denetçi, kıdemli denetçi ve denetçiden oluşan ekiplerdeki görev, yetki ve sorumluluk dağılımı aşağıdaki kıstaslara göre yapılır:

a) Sorumlu ortak baş denetçi, baş denetçi, kıdemli denetçiler ve denetçilerin görev, yetki ve sorumluluklarına ilave olarak, finansal tabloların mevzuat ve finansal raporlama standartlarına uygunluğu konusunda karar vermekle yükümlüdür.

b) Baş denetçi ve kıdemli denetçi, bağımsız denetim faaliyetlerinin planlanması, yürütülmesi, çalışma kağıtlarının incelenmesi, gereken revizyonların yapılması ve müşteri yetkilileri ile görüşülmesi gibi konularda denetçilerin sorumluluklarını paylaşır, önemli durumlarda son kararı vermesi için sorumlu ortak baş denetçiye başvurur.

c) Denetçi, bağımsız denetim programının hazırlanması gibi işin ayrıntılı çalışmalarından sorumludur.

Denetçi, denetçi yardımcılarını işe tahsis etmek, onların çalışmalarına nezaret etmek ve hazırladıkları çalışma kağıtlarını incelemek, işin daha karmaşık ve zor bölümlerini bizzat yürütmek, çalışma programında gereken değişiklikleri yapmak ve çalışmaları süresince müşteriyle olan görüşmeleri yönetmek gibi konularda yetkili ve yükümlüdür.

b. Gözetim ve Koordinasyon

Sorumlu ortak baş denetçi, bağımsız denetim programının uygulanmasından ve bağımsız denetim çalışmalarının yeterli ve etkin bir şekilde gözetim ve koordinasyonundan sorumludur. Bu sorumluluk, bağımsız denetçilerin faaliyet hakkında bilgilendirilmesi ve yönlendirilmesini, bu kişilerin görev ve sorumluluklarının açıkça belirlenmesini, yürütülen faaliyetin süreç içinde sık sık gözden geçirilmesini, çalışmalarla ilgili olarak ortaya çıkan problemlerin çözümlenmesini ve faaliyetin çalışma kağıtlarından izlenebilmesi için gerekli kayıt düzeninin sağlanmasını kapsar.

Bağımsız denetim kuruluşları yaptıkları işin kalitesinin korunması ve artırılması amacıyla yürütülmekte olan bağımsız denetim işinin gözetiminde bulunarak, ulaşılan sonuçlar ve bağımsız denetim sırasında alınan önemli kararların objektif bir şekilde değerlendirilmesini yaparlar. Bağımsız denetimle eş zamanlı olarak bağımsız denetimin kontrolü ile görevlendirilen bağımsız denetçiler de, denetimden sorumlu ekibin bağımsızlık konusunda yaptığı değerlendirmeleri önemlilik kavramı çerçevesinde inceleyerek risklerin belirlenmesine, tereddütlü konularda yeterli danışmanlık hizmeti alınıp alınmadığına, kurumsal yönetim ilkelerinin uygulanmasından sorumlu yöneticilerle yapılan görüşmelerin niteliğine ilişkin hususlarda konuyla ilgili çalışma kağıtları ve raporları inceleyerek bağımsız denetim çalışmasının gözetimini yaparlar. Bağımsız denetim kuruluşları ayrıca belirli dönemler itibariyle tamamlanan bağımsız denetim çalışmalarının kalite kontrolünü de, öncelikle kalite kontrol politikalarını oluşturmak ve süreçleri belirlemek suretiyle yapmak zorundadırlar.

c. Bağımsız Denetçilerin Yetkileri

Bağımsız denetçiler;

a) İşletmelerin genel kurul toplantılarına katılmak ve bu toplantılarda istendiği taktirde, bağımsız denetim faaliyetini ve sonuçlarını ilgilendiren konularda açıklamalarda bulunmak,

b) Bağımsız denetim sözleşmesinin sona erdirilmesi durumunda, izleyen ilk genel kurul

toplantısına katılmak, gerekli gördüğü taktirde konuyla ilgili açıklamalar yapmak ve

c) Bağımsız denetimi ilgilendiren tüm bilgileri müşterilerden veya karşı inceleme gereksinimi duydukları hallerde diğer ilgililerden istemek

ile yetkili kılınmış sayılırlar.

1.3.1.2.8. Denetim Raporları

a. Bağımsız Denetim ve İnceleme Raporunun Kesinleşmesi

Bağımsız denetim ve inceleme raporları, bağımsız denetim raporlarına ilişkin BDS'ler kapsamında hazırlanır. Bağımsız denetim raporu ve inceleme raporu, sorumlu ortak baş denetçi tarafından imzalandığında kesinleşir. Bağımsız denetim raporunun ve inceleme raporunun bir örneği, bağımsız denetim kuruluşunu temsil ve ilzama yetkili kişinin imzasını taşıyan bir yazı ekinde en geç izleyen ilk iş günü mesai saati bitimine kadar müşterinin yönetim kurulu başkanlığına teslim edilir.

Bağımsız denetim ve inceleme raporları, denetlenen işletme tarafından sermaye piyasası mevzuatında belirlenen esaslar kapsamında Kamuyu Aydınlatma Platformu (KAP) veya Kurul'a bildirilir.

Bağımsız denetim kuruluşları, hakkında rapor düzenledikleri finansal tabloların aynen ilan edilip edilmediğini izlemek zorundadırlar.

1.3.1.2.9. Diğer Hususlar

a. Denetimden sorumlu komiteler

Payları Borsada işlem gören işletmeler, Kurumsal Yönetim İlkeleri çerçevesinde, en az iki üyeden oluşan denetimden sorumlu komite kurmak zorundadırlar. Denetim komitesi kurma zorunluluğu bulunmayan işletmelerde, denetim komitesince yapılan işler, yönetim kurulunca yerine getirilir.

Denetimden sorumlu komite; işletmenin muhasebe sistemi, finansal bilgilerin kamuya açıklanması, bağımsız denetimi ve iç kontrol sisteminin işleyişinin ve etkinliğinin gözetimini yapar. Bağımsız denetim kuruluşunun seçimi, bağımsız denetim sözleşmelerinin hazırlanarak bağımsız denetim sürecinin başlatılması ve bağımsız denetim kuruluşunun her aşamadaki çalışmaları denetimden sorumlu komitenin gözetiminde gerçekleştirilir.

İşletmenin hizmet alacağı bağımsız denetim kuruluşu ile bu kuruluşlardan alınacak hizmetler denetimden sorumlu komite tarafından belirlenir ve genel kurulun onayına sunulmak üzere yönetim kuruluna bildirilir.

Bağımsız denetim kuruluşu; işletmenin muhasebe politikası ve uygulamalarıyla ilgili önemli hususları, daha önce ortaklık yönetimine ilettiği Kurul'un muhasebe standartları ile muhasebe ilkeleri çerçevesinde alternatif uygulama ve kamuya açıklama seçeneklerini, bunların muhtemel sonuçlarını ve uygulama önerisini, ortaklık yönetimiyle arasında gerçekleştirdiği önemli yazışmaları, derhal denetimden sorumlu komiteye yazılı olarak bildirir.

İşletmenin muhasebe ve iç kontrol sistemi ile bağımsız denetimiyle ilgili olarak ulaşan şikayetlerin incelenmesi, sonuca bağlanması, çalışanların, muhasebe ve bağımsız denetim konularındaki bildirimlerin gizlilik ilkesi çerçevesinde değerlendirilmesi konularında uygulanacak yöntem ve kriterler denetimden sorumlu komite tarafından belirlenir. Denetimden sorumlu komite, kamuya açıklanacak yıllık ve ara dönem finansal tabloların, işletmenin izlediği muhasebe ilkelerine, gerçeğe uygunluğuna ve doğruluğuna ilişkin olarak işletmenin sorumlu yöneticileri ve bağımsız denetçilerinin görüşlerini alarak, kendi değerlendirmeleriyle birlikte yönetim kuruluna yazılı olarak bildirir.

Denetimden sorumlu komite; en az üç ayda bir olmak üzere yılda en az dört kere toplanır ve toplantı sonuçları tutanağa bağlanarak yönetim kuruluna sunulur. Denetimden sorumlu komite kendi görev ve sorumluluk alanıyla ilgili olarak ulaştığı tespit ve önerileri derhal yönetim kuruluna yazılı olarak bildirir. Denetimden sorumlu komitenin görev ve sorumluluğu, yönetim kurulunun TTK'dan doğan sorumluluğunu ortadan kaldırmaz.

b. Finansal tablo ve yıllık rapor hazırlanma ve bildiriminde sorumluluk

Finansal tablo ve raporların finansal raporlama standartlarına uygun olarak hazırlanmasından, sunulmasından ve gerçeğe uygunluğu ile doğruluğundan, TTK ve sermaye piyasası mevzuatı çerçevesinde işletme ile kusurlarına ve durumun gereklerine göre işletmenin yönetim kurulu üyeleri sorumludur[8]. İşletmenin yönetim kurulu, belirtilen kapsamda hazırlanacak finansal tablolar ve yıllık raporların kabulüne dair ayrı bir karar almak zorundadır.

Finansal tabloların bağımsız denetime tabi tutulmuş olması işletme yönetim kurulunun sorumluluğunu ortadan kaldırmaz. Ayrıca işletmelerin finansal tablo ve yıllık raporlarının ilanı ve bildirimi sırasında söz konusu yıllık ve ara dönem finansal tabloları ile yıllık raporların; işletme genel müdürü, finansal tablo ve yıllık raporların hazırlanmasından sorumlu bölüm başkanı veya bu sorumluluğu üstlenmiş görevli ile yönetim kurulunca bir iş bölümü yapılmış ise, finansal tablo ve yıllık raporların hazırlanmasından sorumlu yönetim kurulu üyesi tarafından imzalanmış sorumluluk beyanına kamuya yapılacak açıklamalarda yer verilmesi zorunludur.

İşletme yönetim kurulu; finansal tablo ve yıllık raporları imzalamakla yükümlü olan görevlilerin, ortaklıkla ve konsolide finansal tablolar kapsamına giren bağlı ortaklıklar, iştirakler ve müşterek yönetime tabi teşebbüsler ile ilgili önemli bilgilere ulaşmalarını sağlayacak tedbirleri almakla yükümlüdür. İmza yükümlüsü görevliler, gerek işletmenin iç kontrol sistemiyle, gerekse kendilerinin bilgiye ulaşma sistemiyle ilgili eleştiri ve önerilerini işletme yönetim kuruluna, denetimden sorumlu komiteye, işletmenin bağımsız denetimini yapmakta olan bağımsız denetim kuruluşuna bildirmekle ve raporu incelemeleri sırasında kullandıkları iç kontrol sistemi hakkında bilgi vermekle yükümlüdürler.

c. Bağımsız Denetim Kuruluşlarının Bildirim Yükümlülükleri

Bağımsız denetim kuruluşları;

a) Esas sözleşmeleri,

b) Şubeleri dahil merkez adresleri,

c) Ortakları, yöneticileri ve bağımsız denetçileri,

d) Bağımsız denetim sözleşmelerinde belirtilen bağımsız denetim ekibi ve

e) Merkezi yurtdışında bulunan bir başka bağımsız denetim kuruluşu ile olan hukuki bağlantıları hakkındaki

her türlü değişikliği en geç 6 iş günü içinde elektronik ortamda Kurul'a bildirmekle yükümlüdür.

Bağımsız denetim kuruluşlarının imzaladıkları bağımsız denetim sözleşmelerini en geç 6 iş günü içinde elektronik ortamda Kurul'a göndermeleri gereklidir. Ayrıca, oluşturulması gereken Kalite Kontrol Güvence Komitesi tarafından hazırlanan ilgili finansal raporlama dönemlerine ilişkin kalite kontrol raporlarının özetinin her yıl Ağustos ayı sonuna kadar bağımsız denetim kuruluşları tarafından Kurul'a gönderilmesi gereklidir.

Bağımsız denetim kuruluşları; yıllık finansal tablolarını, merkezi yurtdışında bulunan bir başka bağımsız denetim kuruluşu ile olan ilişkilerinden kaynaklanan gelir ve giderleri dahil olmak üzere bağımsız denetim ve diğer hizmetlerden doğan gelir ve giderlerin ayrıntılı dökümüyle birlikte bilanço tarihini izleyen en geç dönemin bitimini izleyen Mart ayı sonuna kadar[9] elektronik ortamda Kurul'a bildirmek zorundadırlar.

Bu bilgilerden Kurul'ca gerekli görülenler, Kurul'un resmi internet sitesinde yayımlanmak suretiyle kamuya açıklanır.

d. Bağımsız Denetimin Geçerliliği

Bağımsız denetim standartlarına aykırı olan ve aykırılığı giderilemeyen veya bağımsızlığı ortadan kaldıran durumların varlığı halinde, bağımsız denetim hiç yapılmamış sayılır. Geçersiz sayılan

[8] *Sermaye Piyasasında Finansal Raporlamaya İlişkin Esaslar Tebliği (II-14.1), md. 9/1.*
[9] *Sermaye Piyasasında Finansal Raporlamaya İlişkin Esaslar Tebliği (II-14.1), md. 10/2. Bu süre, eneflasyon uygulaması nedeniyle Kurul'un 28.12.2023 tarih ve 81/1820 sayılı Kararı ile 2023 yılı finansal tabloları için 10 hafta uzatılmıştır.*

bağımsız denetime ilişkin bağımsız denetim raporunun daha önce finansal tablolarla birlikte ilan edilmiş olması halinde, bağımsız denetimin geçersiz sayıldığı hususu ilgili finansal tablolarla birlikte aynı usul ve esaslar dahilinde yeniden ilan edilir. Ayrıca, kamunun doğru aydınlatılması için Kurul tarafından gerekli diğer tedbirler alınır.

Bağımsız denetimin geçersiz sayılmasında bağımsız denetçinin açık bir kusurunun tespiti halinde, yapılabilecek duyuru masrafları dahil meydana gelecek diğer zararlardan ilgili sorumlu ortak baş denetçi ve bağımsız denetim kuruluşu müteselsilen sorumludur.

e. Hukuki ve Cezai Sorumluluk

Bağımsız denetimin, bağımsız denetim standartlarına uygun yapılmaması nedeniyle müşteri ve üçüncü şahıslara karşı doğacak zararlardan, genel hükümler saklı kalmak kaydıyla, bağımsız denetim kuruluşu ile birlikte bağımsız denetim raporunu imzalayanlar müteselsilen sorumludur. Bağımsız denetim standartlarına aykırı olarak bağımsız denetim raporu düzenleyenler ve düzenlenmesini sağlayanlar hakkındaki cezai sorumluluk, SPKn'nda belirtilen özel hükümlere tabidir.

f. Bağımsız Denetim Faaliyetinde Bulunma Yetkisinin İptali

SPKn'nun 96'ncı maddesi çerçevesinde, aşağıda yer alan aykırılıkların varlığı halinde bağımsız denetim kuruluşunun sermaye piyasasında bağımsız denetim faaliyetinde bulunma yetkisi Kurul'ca iptal edilebilir.

a) Kuruluş şartlarının kaybedilmesi,

b) Bağımsız denetim standartlarına aykırı olarak; görev kabulüne ve değişimine ilişkin bağımsız denetim standart, ilke ve kurallarına uyulmaması, bağımsız denetimlerde Kurul'a bildirilen bağımsız denetim sözleşmesinde yer alanlar dışında fiilen başka bağımsız denetçi görevlendirilmesi, bağımsız denetim planı ve çalışma kağıtları ile bunları destekleyici diğer bilgi ve belgelerin bağımsız denetim çalışmasını kanıtlayacak düzeyde bulunmaması, uygun bağımsız denetim tekniklerinin kullanılmaması nedeniyle gerekli bağımsız denetim kanıtlarının elde edilememesi ve raporlamaya ilişkin temel ilkelere uyulmaması,

c) Finansal tabloların güvenirliğini önemli ölçüde etkileyecek hususların tespiti halinde, bağımsız denetim kuruluşunun bağımsız denetim standartlarına tam olarak uyulduğunu kanıtlayamaması,

d) Yapılan bağımsız denetim çalışmalarında, sorumlu ortak baş denetçi dahil bağımsız denetim ekibinin dürüstlük, tarafsızlık, mesleki yeterlilik ve özen, bağımsızlık, güvenilirlik ve mesleki davranış gibi etik ilkelere uymaması,

e) Bildirim yükümlülüklerinin zamanında, tam ve doğru olarak yerine getirilmemesi ya da Kurul'ca veya Kurul tarafından görevlendirilenlerce istenen bilgi ve belgelerin zamanında, tam ve doğru olarak verilmemesi,

f) Hatalı, eksik, yanıltıcı ve gerçeğe aykırı bağımsız denetim ve inceleme raporu düzenlenmesi,

g) Sermaye piyasasında kesintisiz olarak 5 yıl süreyle fiilen bağımsız denetim faaliyetinde bulunulmamış olması.

Yukarıda yer verilen (d) bendinde belirtilen hususlarda bir sorumluluk tespit edilmesi halinde, sorumluluğun içeriğine göre, Kurul sadece ilgili sorumlu ortak baş denetçi ve/veya bağımsız denetçi/denetçilerin sermaye piyasasında bağımsız denetim yapmasını 2 yıldan az olmamak kaydı ile süreli veya süresiz olarak yasaklayabilir.

1.3.2. Bilgi Sistemleri Yönetimi Tebliği VII-128.9

Sermaye piyasasında bilgi sistemleri yönetimine ilişkin esaslar VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği (BSY Tebliği) ile düzenlenmiştir.

BSY Tebliği, SPKn'nun 128/1-(h) maddesine dayanılarak 05.01.2018 tarih 30292 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. BSY Tebliği ile sermaye piyasasında bilgi sistemleri yönetim ilkelerine ilişkin usul ve esaslar belirlenmiştir.

BSY Tebliği'nin dört bölümden oluşan hükümlerine devam eden bölümde yer verilmekte olup, Tebliğ'in tamamı ve güncellenecek hallerine Kurul'un internet sitesinin mevzuat bölümünden erişim sağlanabilir.

1.3.2.1. Bilgi Sistemleri Yönetimi İle İlgili Genel Esaslar

İşletmelerin bilgi sistemlerinin yönetimi için usul ve esaslar belirleme ihtiyacı, bilgi sistemlerinden kaynaklanan risklerin artmaya başlaması, bu durumun işletmelerin iş hedeflerini gerçekleştirmesini zorlayıcı hatta engelleyici hale gelmesi ve doğal olarak işletmelerin müşterilerinin/yatırımcılarının haklarının zedelenmesine yol açmasıyla ortaya çıkmıştır. Bu duruma bir çözüm olabilmek için gerek ulusal gerekse de uluslararası düzeyde bilgi sistemlerinin yönetimine dair çeşitli detayda ve içerikte birtakım rehber, yönetim çerçevesi ve standart yayınlanmıştır.

Belirli bir düzenleme/standart/rehber göz önüne alınmaksızın yönetilen bilgi sistemlerinde aşağıdaki sorunlar gözlenmektedir:

- İş yapış şekillerinde belli bir düzen/yöntem olmaması, işi yapan kişilere bağımlılık gelişmesi, kişiler değiştikçe yöntemlerin değişmesi ve kurumsal hafıza oluşmaması,
- Bilgi teknolojilerinin iş hedefleri üzerindeki dönüştürücü ve geliştirici potansiyelinden tam olarak faydalanamama,
- Dışarıdan kaynak kullanımı yoluyla edinilen ürün ve hizmetlerde servis sağlayıcılara bağımlılık gelişmesi,
- Çalışan profilinde yetkinlik ve yeterlilik sağlanamaması, çalışanların sık değişmesi,
- Olağan üstü durumlara hazırlıklı olamama, iş operasyonlarının kesintiye uğraması,
- Bilgi güvenliği ihlalleri ve siber saldırılara karşı hazırlıksız olunması,
- Bilgi sistemleri kullanımından kaynaklanan risklerin artması,
- Bilgi sistemleri uygulamalarıyla iş hedefleri arasında uyum sağlanamaması.

Belirtilen sorunları sermaye piyasaları özelinde çözebilmek, böylece sermaye piyasasında faaliyet gösteren işletmelerin yatırımcılara istikrarlı, güvenli, etkin, doğru ve verimli hizmet vermelerini sağlamak ve bu şekilde yatırımcıların haklarını koruyabilmek için işletmelerin bilgi sistemlerinin yönetimine dair bir düzenleme yapılması yoluna gidilmiştir.

30.12.2012 tarih ve 28513 sayılı Resmi Gazete'de yayınlanan SPKn'nun "*Kurulun görev, yetki ve sorumlulukları*" başlıklı 128'inci maddesinin birinci fıkrasının (h) bendinde "*Sermaye piyasası kurumlarının, halka açık şirketlerin, borsaların ve öz düzenleyici kuruluşların bilgi sistemlerinin işletimine ve bu Kanun çerçevesindeki denetimine ilişkin usul ve esasları belirlemek*" hükmü bulunmaktadır. Anılan SPKn'dan önceki kanunlarda, Kurul'un görev ve yetkileri arasında bilgi sistemlerine ilişkin usul ve esas belirleme yetkisi bulunmamaktaydı. Yeni SPKn ile Kurul'a verilen bu görev çerçevesinde BSY Tebliği hazırlanmıştır. Bu düzenleme ile;

- Bilgi sistemleri yönetiminde en iyi uygulama pratiklerinin yerleşmesi,
- İş hedeflerine uygun bilgi sistemleri stratejilerinin geliştirilmesi, kapasite planlaması ve kaynak yönetiminin etkin bir şekilde yapılması,
- Bilgi sistemlerinden kaynaklanan risklerin yönetilmesi,
- Yılda en az bir defa gerçekleştirilecek sızma testleri ile siber saldırılara karşı daha hazırlıklı olunması,
- Bilgi sistemleri sürekliliğine ilişkin gerekli tedbirlerin alınması, birincil ve ikincil sistemlerin ve verilerin yurt içinde bulundurulmasının sağlanması,
- Müşteri bilgilerinin, finansal ve operasyonel bilgilerin gizliliğinin ve bütünlüğünün sağlanması

hedeflenmektedir.

Diğer taraftan, 02.07.2024 tarihli ve 32590 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 7518 sayılı "*Sermaye Piyasası Kanunu'nda Değişiklik Yapılmasına Dair Kanun*" ile ülkemizde faaliyet gösteren veya gösterecek olan kripto varlık hizmet sağlayıcıları, SPKn kapsamında Kurul'un düzenleme ve denetimi yetkisi altına alınmıştır. SPKn'un 35/B maddesinin birinci fıkrasında, kripto hizmet sağlayıcılarının kuruluşlarına ve faaliyete başlamalarına, ortaklarına, yöneticilerine, personeline, organizasyonuna, sermayelerine ve sermaye yeterliliğine, yükümlülüklerine, **bilgi sistemleri ve teknolojik altyapılarına**, pay devirlerine, yapabilecekleri faaliyetlere, faaliyetlerinin geçici veya sürekli olarak durdurulmasına ilişkin esaslar ile faaliyetleri sırasında uymaları gereken diğer ilke ve esasların Kurul tarafından belirleneceği; ikinci fıkrasında ise kripto varlık hizmet sağlayıcıların kuruluşlarına ve/veya faaliyete başlamalarına Kurulca izin verilebilmesi için bilgi sistemleri ve teknolojik altyapıları konularında Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'nun (TÜBİTAK) belirleyeceği kriterlere uygunluk aranacağı hüküm altına alınmıştır. Kripto hizmet sağlayıcılarının tabi olacağı bilgi sistemlerine ilişkin ikincil düzenleme çalışmaları devam etmektedir.

1.3.2.2. Bilgi Sistemleri Yönetiminde Temel Kavramlar

BSY Tebliğ'inde tanımlanan temel kavramlara aşağıda yer verilmektedir.

Birincil Sistemler: İşletmelerin SPKn ve SPKn'na ilişkin alt düzenlemelerden kaynaklanan görevlerini yerine getirmeleri için gerekli bilgilerin, elektronik ortamda güvenli ve istenildiği an erişime imkan sağlayacak şekilde kaydedilmesini ve kullanılmasını sağlayan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamıdır.

İkincil Sistemler: Birincil sistemler aracılığı ile yürütülen faaliyetlerde bir kesinti olması halinde, bu faaliyetlerin iş sürekliliği planında belirlenen kabul edilebilir kesinti süreleri içerisinde sürdürülür hale getirilmesini ve SPKn ve SPKn'na ilişkin alt düzenlemelerde işletmeler için tanımlanan sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilere kesintisiz ve istenildiği an erişilmesini sağlayan birincil sistem yedekleridir.

Bütünlük: Bilginin doğruluğu ve tamlığını koruma özelliğidir.

Denetim İzi: Finansal ya da operasyonel işlemler ile bilgi güvenliği ihlal olaylarının başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtlar ile bu kayıtlar üzerinde yapılan işlemleri gösteren kayıtlardır.

Erişilebilirlik: Bilginin yetkili kullanıcı, uygulama veya sistem tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğidir.

Gizlilik: Bilgi sistemlerine ve bilgiye sadece yetkili kullanıcı, uygulama veya sistem tarafından erişilebilmesidir.

Kontrol: Bilgi sistemleri süreçleriyle ilgili olarak gerçekleştirilen ve iş hedeflerinin gerçekleştirilmesi, istenmeyen olayların belirlenmesi, engellenmesi ve düzeltilmesine ilişkin yeterli derecede güvenceyi oluşturmayı hedefleyen politikalar, prosedürler, uygulamalar ve organizasyonel yapıların tamamıdır.

Politika: İşletmelerin hedef ve ilkelerini ortaya koyan ve üst yönetimi tarafından onaylanmış dokümanlardır.

Prosedür: Süreçlere ilişkin işlem ve eylemleri tanımlayan dokümandır.

Süreç: Bir işin yapılış ve üretiliş biçimini oluşturan sürekli işlem ve eylemlerdir.

1.3.2.3. BSY Tebliğ Kapsamına Giren İşletmeler

Sermaye piyasası mevzuatına tabi ortaklık, sermaye piyasası kurumları, borsalar ve öz düzenleyici kuruluşların (bundan sonra topluca işletme denilecektir) bilgi sistemlerinin yönetimine ilişkin bir düzenleme olan BSY Tebliği'nin kapsamına aşağıdakiler girmektedir:

a) Borsa İstanbul A.Ş.,

b) Borsalar ve piyasa işleticileri ile teşkilatlanmış diğer pazar yerleri,

c) Emeklilik yatırım fonları,

d) İstanbul Takas ve Saklama Bankası A.Ş.,

e) Merkezi Kayıt Kuruluşu A.Ş.,

f) Portföy saklayıcısı kuruluşlar,

g) Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.,

h) Sermaye piyasası kurumları,

i) Halka açık ortaklıklar,

j) Türkiye Sermaye Piyasaları Birliği,

k) Türkiye Değerleme Uzmanları Birliği.

Yukarıdaki işletmelerden, banka ve sigorta şirketleri ile finansal kiralama, faktoring ve finansman şirketlerinin bilgi sistemlerinin, kendi özel mevzuatlarında belirlenen ilkeler çerçevesinde yönetilmesi, bu Tebliğ'de öngörülen yükümlülüklerin yerine getirilmesi hükmündedir. Bu düzenleme ile, işletme kapsamına giren banka, sigorta şirketleri, finansal kiralama şirketleri, faktöring şirketleri ve finansman şirketlerinin kendi mevzuatlarında bilgi sistemleri yönetimine ilişkin düzenleme bulunması durumunda, bu düzenlemeye uymaları durumunda, bu Tebliğ'e de uymuş sayılacaktır. Böylece, sermaye piyasası mevzuatında finansal raporlama ve bilgi sistemleri bağımsız denetiminde olduğu gibi, anılan işletmelere kolaylık sağlanarak, mevcut olması durumunda kendi mevzuatlarına uymaları yeterli görülmüştür. Bu Çalışma Notu'nun 1.3.4. bölümünde yer verildiği üzere anılan işletmelerin düzenleyici otoriteleri olan Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) ve Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumu'nun (SEDDK) konuya ilişkin mevzuatları bulunmaktadır.

Bu Tebliğ hükümleri esas olmak üzere, tezgahüstü türev araç işlemi gerçekleştiren aracı kurumların bilgi işlem altyapılarına ilişkin olarak ilgili Kurul düzenlemelerinde belirlenen ilke ve esaslara uyulur.

1.3.2.4. Bilgi Sistemlerinin Yönetilmesi

a. Bilgi Sistemlerinin Oluşturulması ve Hayata Geçirilmesi

Bilgi sistemleri yönetiminin kurumsal yönetim uygulamalarının paralelinde ele alınması, bilgi sistemleri stratejilerinin iş hedefleri ile uyumlu olması, bilgi sistemlerinin güvenliğini, performansını, etkinliğini, doğruluğunu ve sürekliliğini hedefleyerek gerekli kaynakların tahsis edilmesi öngörülmüştür.

İşletme, bilgi sistemlerinin yönetimine ilişkin gerekli tüm kontrolleri düzenlemeli, güncellemeli ve ilgililere duyurulmasını sağlamalıdır.

b. Bilgi Güvenliği Politikası

Bilgi sistemlerinin kurulması, işletilmesi ve yönetilmesine ilişkin olarak bilginin gizliliğini, bütünlüğünü ve doğruluğunu sağlayacak bilgi güvenliği politikasının üst yönetim tarafından hazırlanması, yönetim kurulu tarafından onaylanması ve onaylanan politikanın tüm çalışanlara duyurulması gerekmektedir. Bu politika, bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin ve sorumlulukların tanımlanmasını, bilgi sistemlerine ilişkin risklerin yönetilmesine dair süreçlerin oluşturulmasını, kontrollerin tesis edilmesini ve gözetimini kapsamalıdır.

c. Üst Yönetimin Gözetim Sorumluluğu

Üst yönetime aşağıda özetlenen görevler verilmiştir:

- Bilgi güvenliği politikasının uygulanmasının gözetimi,
- Bilgi güvenliği politikası kapsamında bilgi sistemleri üzerinde etkin ve yeterli kontrollerin tesis edilmesi,

- Yeni bilgi sistemlerinin kullanıma alınmasına ilişkin kritik projelerin gözden geçirilmesi ve sahip olduğu risklerin değerlendirilerek onaylanması,
- Kritik projelerin işletme içi veya dışı kaynaklarla geliştirilmesine bakılmaksızın gerekli uzmanlığın, işletmede olmasının sağlanması ve bu yapıyı desteklemek için oluşturulacak yönetsel rol ve sorumlulukların belirlenmesi,
- Bilgi güvenliği önlemlerinin uygun düzeye getirilmesine yönelik olarak yeterli kaynağın tahsis edilmesi,
- Bilgi güvenliğinin sağlanmasına ilişkin aşağıdaki faaliyetlerin yerine getirilmesinin sağlanması:

a) Bilgi güvenliği politikası ve sorumluluklarının her yıl gözden geçirilmesi ve onaylanması,

b) Bilgi sistemlerine ilişkin risk yönetimi faaliyetlerinin gerçekleştirilmesi,

c) Bilgi güvenliği ihlallerinin izlenmesi ve her yıl değerlendirilmesi,

d) Tüm çalışanlara yönelik bilgi güvenliği farkındalığının artırılmasına yönelik olarak gerekli çalışmaların yapılması ve eğitimin verilmesi.

- Bilgi sistemleri organizasyonunun oluşturulması ve işlerliğine ilişkin gözetimin yapılması,
- Bilgi sistemleri güvenliğiyle ilgili süreçleri takip edip üst yönetime rapor verecek, gerekli teknik bilgi ve tecrübeye sahip "*bilgi sistemleri güvenliği sorumlusu*" belirlenmesi,
- Risk önceliklerine göre kritik iş süreçlerinin sürekliliğini sağlamaya yönelik iş sürekliliği planının hazırlanması.

d. Bilgi Sistemleri Risk Yönetimi

İşletmenin, bilgi sistemleri kullanımından kaynaklanan riskleri uygun bir şekilde ölçmesi, izlemesi, işlemesi ve raporlaması amacıyla risk yönetimi süreç ve prosedürlerini tesis edip, güncelliğini sağlaması gerekmektedir. Risk yönetim sürecinde aşağıdaki hususlar dikkate alınmak durumundadır:

- Bilgi teknolojilerindeki hızlı gelişmelere uyum sağlayamamanın muhtemel sonuçları, diğer yandan yeni teknolojilere uyum zorluğu, ayrıca yasal mevzuatın değişme ihtimali,
- Bilgi sistemleri kullanımının öngörülemeyen hata ve hileli işlemlere sebebiyet verebilmesi,
- Bilgi sistemlerinde dış kaynak yoluyla hizmet alımının servis sağlayıcılara bağımlılık geliştirme ihtimali,
- İş ve hizmetlerin önemli oranda bilgi sistemlerine bağlı hale gelmesi,
- Bilgi sistemleri üzerinden gerçekleştirilen işlemlerin, verilerin ve denetim izlerine ilişkin tutulan kayıtların güvenliğinin sağlanmasının zorlaşması.

Bilgi sistemlerine ilişkin risk analizinin yılda en az bir defa veya bilgi sistemlerinde meydana gelen önemli değişikliklerden sonra tekrar edilmesi, bilgi teknolojilerinde ortaya çıkan teknik zafiyetlere ilişkin zamanında bilgi edinilmesi ve gerekiyorsa uygun tedbirlerin alınması gerekmektedir.

İşletmenin, bilgi sistemlerini yılda en az bir defa sızma testine tabi tutması, bu hizmetin dış kaynak kullanımı yoluyla veya kendi bünyesinde sağlaması gereklidir. Ancak sızma testi işletmenin kendi personeli eliyle gerçekleştirilecekse, testi gerçekleştirecek çalışanların işletme bünyesinde bilgi güvenliği tedbirlerinin seçilmesi ve uygulanması sürecinde görev almamış olması gerekmektedir. Sızma testini gerçekleştirecek gerçek veya tüzel kişilerin sızma testi konusunda ulusal veya uluslararası geçerliliği bulunan belgeye sahip olması da bir gereksinim olarak düzenlenmiş olup test sırasında uyulacak usul ve esaslara BSY Tebliği'nin ekinde yer verilmiştir. Benzer şekilde bu Çalışma Notu'nun da 1 numaralı ekinde yer almaktadır.

Diğer taraftan, Kurul'un 21.03.2023 tarih ve 2023/18 sayılı Bülten'inde yayımlanan i-SPK 128.20 (21/03/2023 tarihli ve 17/352 s.k.) sayılı İlke Kararı ile 01.04.2024 tarihinden itibaren geçerli

olmak üzere, sızma testini gerçekleştirecek kişilerin bir önceki paragrafta belirtilen hususların yanı sıra, BSBDL'ye sahip olması gerektiğine karar verilmiştir. Bu kapsamda, 01.04.2024 tarihinden sonra gerçekleştirilecek sızma testlerinin BSBDL'ye sahip kişiler tarafndan gerçekleştirilecektir.

1.3.2.5. Bilgi Sistemleri Kontrollerine İlişkin Esaslar

BSY Tebliği'nin bu kısmında bilgi sistemleri kontrollerine ilişkin 19 alanda usul ve esaslar belirlenmiştir. Bu alanlara ilişkin usul ve esaslar bu bölümde ele alınmaktadır.

a. Bilgi Sistemleri Kontrollerinin Tesisi ve Yönetilmesi

İşletme üst yönetimi, bilgi güvenliği politikası kapsamında, bilgi sistemlerinden kaynaklanan güvenlik risklerinin yeterli düzeyde yönetildiğinden emin olmak için, bilgi sistemlerinin ve üzerinde işlenmek, iletilmek, depolanmak üzere bulunan verilerin gizlilik, bütünlük ve erişilebilirliklerini sağlayacak önlemlere ilişkin kontrollerin geliştirilmesini, işletilmesini, güncelliğini sağlamak ve gerekli yönetsel sorumlulukları tanımlamakla yükümlüdür.

Bilgi sistemleri kontrolleri kapsamında asgari olarak aşağıdaki hususlar dikkate alınmalıdır:

- Her kontrol süreci için süreç sahibinin, rollerin, faaliyetlerin ve sorumlulukların açık bir şekilde tanımlanması,
- Kontrol süreçlerinin periyodik biçimde tanımlanması,
- Her kontrol sürecinin hedef ve amaçlarının açıkça tanımlanmış olması ve performansının ölçülebilir olması.

Bu kapsamda, bilgi sistemleri kontrollerine ilişkin etkinlik, yeterlilik ve uygunluk ile öngörülen risk ya da risklerin etkisini azaltmaya yönelik faaliyetler devamlı bir şekilde takip edilmeli, değerlendirilmeli ve değerlendirme sonucunda tespit edilen önemli kontrol eksiklikleri üst yönetime raporlanarak gerekli önlemlerin alınması sağlanmalıdır.

b. Varlık Yönetimi

İşletme, sahip olduğu bilgi varlıklarını ve bu varlıkların sorumlularını belirlemeli, bu varlıkların envanterini oluşturmalı ve güncelliğini sağlamalıdır. Bilgi varlıkları sınıflandırılmalı, taşınabilir ortamlar içerdiği bilgilerin sınıfına göre kaybolma veya hırsızlık risklerine karşı korunmalı ve önem derecesi yüksek bilgileri veya bu bilgilere erişim sağlayan yazılımları barındıran taşınabilir ortamlar yetkilendirme olmaksızın işletme dışına çıkarılmamalıdır. İşletme dışına çıkartılan varlıkların üzerinde işletmeye ait bilgi veya lisanslı yazılım bulunmaması sağlanmalıdır. Temiz masa ve temiz ekran ilkeleri benimsenmelidir.

c. Görevler Ayrılığı Prensibi

İşletme, bilgi sistemlerinin kullanımında hata ve suistimal risklerini azaltmak için görevler ayrılığı ilkesini benimsemelidir. Sistem, veri tabanı ve uygulamaların geliştirilmesi, test edilmesi ve işletilmesine ilişkin görevler ayrılığı prensibine uygun kontroller uygulamaya konmalıdır. Görev ve sorumluluklar belirli aralıklarla gözden geçirilip güncellenmelidir. Bu kapsamda kritik işlerin tek bir personele veya servis sağlayıcıya bağımlı olmaması, görevlerin uygun şekilde birbirinden ayrılamadığı durumlarda ise telafi edici kontrollerin uygulamaya alınması gerekmektedir. Görevlerin tam ve uygun şekilde ayrılmasının mümkün olmadığı durumlarda oluşabilecek hata, eksiklik veya kötüye kullanımı önlemeye veya tespit etmeye yönelik telafi edici kontroller tesis edilmelidir.

d. Fiziksel ve Çevresel Güvenlik

Fiziksel erişime karşı güvenli alanların uygun kontrollerle korunması, güvenli alanlara giriş ve çıkışların kayıt altına alınması, gerekçelendirilmesi ve izlenmesi, ayrıca yangın, sel, deprem, patlama, yağma gibi doğal veya insan kaynaklı felaketlerden kaynaklanan hasara karşı fiziksel koruma sağlamak amacıyla uygun kontrollerin tesis edilmesi gerekmektedir.

e. Ağ Güvenliği

İşletme bünyesinde kurulu olan ağların tehditlere karşı uygun şekilde korunması, iletişim

altyapılarının dinlemeye ve fiziksel hasara karşı korunması, mobil cihazların ağ erişimine ilişkin risklere yönelik güvenlik önlemlerinin alınıp uygulanması, ağa yetkisiz erişimlerin engellenmesi, ağın gözetim altında tutulması ve yüksek riskli uygulamaların güvenliğini artırmak amacıyla gerekiyorsa bağlantı sürelerine sınırlama getirilmesi gerekmektedir. Ayrıca, iç veya dış kaynak yoluyla sağlanmasına bakılmaksızın ağ hizmetlerinin güvenlik kriterlerinin, hizmet seviyelerinin belirlenmesi ve gözetim altında tutulması, uzaktan erişime ilişkin gerekli yetkilendirmeler yapılması, ek kontroller düzenlenmesi, kurumsal ağ dışındaki ağlarla olan iletişimde dış ağlardan gelebilecek tehditler için sürekli gözetim altında tutulan güvenlik duvarı çözümleri kullanılması ve iç ağın farklı güvenlik gereksinimlere göre bölümlere ayrılması sağlanmalıdır.

f. Kimlik Doğrulama

Bilgi sistemleri üzerinden gerçekleşen işlemler için, risk değerlendirmesi sonucuna uygun kimlik doğrulama yöntemi belirlenmelidir. Yöntem belirlenirken, bilgi sistemleri üzerinden gerçekleştirilmesi planlanan işlemlerin niteliği, doğurabileceği finansal veya finansal olmayan etkilerinin büyüklüğü, işleme konu verinin hassasiyeti ve kimlik doğrulama yönteminin kullanım kolaylığı göz önünde bulundurulmalıdır.

Kimlik doğrulama yöntemi, müşterilerin ve çalışanların bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek tüm süreci kapsayacak şekilde uygulanmalıdır. Kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek gerekli önlemler alınmalıdır. Parola kullanımı gerektiren kimlik doğrulama yöntemlerinde, parolaların tahmin edilmesi ve kırılması zor bir karmaşıklıkta ve uzunlukta olması sağlanmalıdır.

Kullanılan kimlik doğrulama verilerinin tutulduğu ortamların ve bu amaçla kullanılan araçların güvenliğini sağlamaya yönelik gerekli önlemler alınmalıdır. Bu önlemler asgari olarak kimlik doğrulama verilerinin şifreli olarak saklanması, bu veriler üzerinde yapılacak her türlü değişikliği algılayacak sistemlerin kurulması, yeterli denetim izlerinin tutulması ve güvenliğinin sağlanması hususlarını içermelidir. Kimlik doğrulama verilerinin aktarımı sırasında gizliliğinin sağlanmasına yönelik önlemler alınmalıdır.

g. Yetkilendirme

İşletme, bilgi sistemlerine erişim için uygun bir yetkilendirme ve erişim kontrolü tesis etmelidir. Yetkilendirme düzeyi ve erişim haklarının atanmasında görev ve sorumluluklar göz önünde bulundurularak, gerekli olacak en düşük yetkinin atanması ve en kısıtlı erişim hakkının verilmesi yaklaşımı esas alınmalıdır. Atanacak yetkiler ve sorumluluklar görevler ayrılığı ilkesi ile tutarlı olmalıdır. Tüm yetkiler ve erişim hakları her yıl güncel durumla uyumlulukları açısından değerlendirmeye tabi tutulmalıdır.

Yetkilendirme verilerinin güvenliği sağlanarak, bu veriler üzerinde yapılacak her türlü değişikliği algılayacak sistemler kurulmalıdır. Yetkilendirme verilerinin tutulduğu ortamlara yetkisiz erişim teşebbüsleri kayıt altına alınarak, düzenli olarak gözden geçirilmelidir. Çalışanların istihdamının sonlanması durumunda, ilgili tüm yetkilendirmeler ivedilikle iptal edilmelidir.

h. İşlemlerin, Kayıtların ve Verilen Bütünlüğü

İşletme, bilgi sistemleri üzerinden gerçekleşen işlemlerin, kayıtların ve verilerin bütünlüğünün sağlanmasına yönelik gerekli önlemleri almalıdır. Bütünlüğü sağlamaya yönelik önlemler verinin iletimi, işlenmesi ve saklanması aşamalarının tamamını kapsayacak şekilde oluşturulmalıdır. Bilgi sistemlerine ilişkin dış kaynak hizmeti alınan işletmeler nezdinde gerçekleşen işlemler için de aynı yaklaşım gösterilmelidir. Kritik işlemler, kayıtlar ve verilerde meydana gelebilecek bozulmaları saptayacak teknikler kullanılmalıdır.

i. Veri Gizliliği

İşletme, bilgi sistemleri faaliyetleri kapsamında gerçekleşen işlemlerin ve bu işlemler kapsamında iletilen, işlenen ve saklanan verilerin gizliliğini sağlayacak önlemleri almalıdır. Gizliliği sağlamak için;

- Bilgi sistemleri yapısı ile iş ve işlem çeşitliliği göz önünde bulundurularak, verilerin önem derecesine uygun önlemlerin alınması,
- Verilere erişim haklarının kişilerin görev ve sorumlulukları çerçevesinde belirlenmesi, erişimlerin kayıt altına alınması, bu kayıtların yetkisiz erişim ve müdahalelere karşı korunması,
- Veri gizliliğini sağlamada şifreleme tekniklerinin kullanılması durumunda, güvenilirliği ve sağlamlığı ispatlanmış algoritmaların kullanılması; geçerliliğini yitirmiş, çalınmış veya kırılmış şifreleme anahtarlarının kullanılmasının engellenmesi, verinin ve operasyonun önem düzeyine göre anahtarların değiştirilme sıklıklarının belirlenmesi

gerekmektedir.

İşletme, bilgi sistemleri faaliyetleri kapsamında gerçekleşen işlemlere ilişkin iletilen, işlenen ve saklanan önem derecesi yüksek verilerin kasten veya yanlışlıkla işletme dışına sızmasını önlemeye yönelik olarak gerekli önlemleri almalıdır.

j. Bilgi Sistemlerine İlişkin Dış Kaynak Yoluyla Alınan Hizmetlerin Yönetimi

İşletme üst yönetimi tarafından bilgi sistemleri kapsamında dış kaynak yoluyla alınacak hizmetlerin doğuracağı risklerin yeterli düzeyde değerlendirilmesine, yönetilmesine ve dış kaynak yoluyla alınan hizmeti sağlayan kuruluşlarla ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayacak bir gözetim mekanizması oluşturulmalıdır. Tesis edilecek gözetim mekanizması asgari olarak aşağıda belirtilen hususları içermelidir:

- Dış kaynak yoluyla alınan bilgi sistemleri hizmeti kapsamındaki tüm sistem ve süreçlerin işletmenin kendi risk yönetimi, güvenlik, gizlilik ve müşteri gizliliğine ilişkin ilkelerine uygun olması,
- İşletme verilerinin hizmet sağlayıcı kuruluşa aktarılmasının gerekli olduğu durumlarda, söz konusu kuruluşun bilgi güvenliği konusundaki ilke ve uygulamalarının en az işletmenin uyguladığı düzeyde olması,
- Hizmete ilişkin hususların işletmenin iş sürekliliği göz önünde bulundurularak düzenlenmesi ve gerekli önlemlerin alınması,
- Hizmetlerde ölçme, değerlendirme, raporlama ve güvenlik fonksiyonlarında nihai sorumluluğun işletmede olması,
- Hizmetin, işletmenin yasal yükümlülüklerini yerine getirmelerini ve etkin biçimde denetlenmelerini engelleyici nitelikte olmaması,
- İşletmenin önem arz eden konulara ilişkin dış kaynak hizmeti aldıkları kuruluşlarla sözleşme imzalamadan önce ilgili kuruluş bünyesinde hizmeti istenilen kalitede gerçekleştirebilecek düzeyde teknik donanım ve altyapı, mali güç, tecrübe, bilgi birikimi ve insan kaynağı bulunup bulunmadığı hususlarını da dikkate alacak şekilde inceleme ve değerlendirme çalışması yapmaları ve bu çalışma sonucunda hazırlanacak teknik yeterlilik raporunun üst yönetime sunulması.

Diğer taraftan, dış kaynak kullanımına ilişkin koşul, kapsam ve her türlü diğer tanımlamanın, hizmet sağlayıcı kuruluşça imzalanmış olacak şekilde sözleşmeye bağlanması ve bu sözleşmenin asgari olarak aşağıdaki hususları içermesi gerekmektedir:

- Hizmet seviyelerine ilişkin tanımlamalar,
- Hizmetin sonlandırılmasına ilişkin koşullar,
- Hizmetin, beklenmedik şekillerde sonlandırılması veya kesintiye uğraması durumunda uygulanacak yaptırımlar,
- İşletmenin bilgi güvenliği politikası dâhilinde önem arz eden konulara ilişkin gereklilikler,

- Sözleşme kapsamında üretilecek ürün bulunması halinde, ürünün sahipliği ile fikri ve sınai mülkiyet haklarını da göz önünde bulundurarak düzenleyen hükümler,
- Sözleşmede hizmet sağlayıcı kuruluşlar için yükümlülük teşkil eden hükümlerin, alt yüklenici kuruluşlar ile yapılacak olan sözleşmelerde de bağlayıcı maddeler olarak yer almasını sağlayacak hükümler,
- Hizmet sağlayıcı kuruluşun, sermaye piyasası mevzuatı kapsamında Kurul tarafından talep edilecek bilgileri istenen zamanda ve nitelikte sağlamasına ilişkin yükümlülüğü ve Kurul'un sözleşme kapsamında sunulan hizmet ile ilgili olarak hizmet sağlayıcı bünyesindeki gerekli gördüğü her türlü bilgi, belge ve kayda erişim hakkı.

Hizmet sağlayıcı kuruluşlara verilen erişim hakları özel olarak değerlendirilmeli; fiziksel veya mantıksal olabilecek bu erişimler için risk değerlendirmesi yapılarak, gerekiyorsa ek kontroller oluşturulmalıdır. Risk değerlendirmesi yapılırken ihtiyaç duyulan erişim türü, erişilecek verinin önemi ile erişimin bilgi güvenliği üzerindeki etkileri dikkate alınmalıdır. Alınan hizmetin sonlanması durumunda ilgili tüm erişim hakları iptal edilmelidir.

İşletme üst yönetimi, dış kaynak yoluyla gerçekleştirilen hizmetler için hizmetin erişilebilirliğini, performansını, kalitesini, bu hizmet kapsamında gerçekleşen güvenlik ihlali olayları ile dış kaynak yoluyla hizmet sağlayan kuruluşun güvenlik kontrollerini, finansal koşullarını ve sözleşmeye uygunluğunu yakından takip etmek için yeterli bilgi ve tecrübeye sahip sorumluları belirlemelidir.

k. Müşteri Bilgilerinin Gizliliği

İşletme, bilgi sistemleri aracılığıyla edindiği veya sakladığı müşteri bilgilerinin gizliliğini sağlamaya yönelik kontrolleri oluşturmak ve bunların gerektirdiği önlemleri almakla yükümlüdür. İşletme, personelin kişisel verilerin korunması ve işlenmesine uygun davranışlarını temin etmelerine yönelik gerekli tedbirleri almalıdır. Müşteri bilgilerinin gizliliğine ilişkin BSY Tebliği'nde düzenlenmeyen hususlarda, 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümleri geçerlidir.

l. Müşterilerin Bilgilendirilmesi

İşletme tarafından elektronik ortamda sunulan hizmetlerden yararlanacak müşteriler, sunulan hizmetlere ilişkin şartlar, riskler ve istisnaî durumlarla ilgili olarak açık bir şekilde bilgilendirilmeli ve söz konusu hizmetlere ilişkin risklerin etkisini azaltmaya yönelik olarak benimsenen bilgi güvenliği ilkeleri ve bu risklerden korunmak için kullanılması gereken yöntemler müşterilerin dikkatine sunulmalıdır. Ayrıca, bilgi sistemlerinden ve bunlara dayalı olarak verilen hizmetlerden dolayı müşterilerin yaşayabileceği sorunların takip edilebileceği ve müşterilerin şikâyetlerini ulaştırmalarına imkân tanıyacak mekanizmalar oluşturulmalı; şikâyet ve uyarılar değerlendirilerek aksaklıkları giderici çalışmalar yapılmalıdır.

m. Üçüncü Taraflarla Bilgi Değişimi

İşletme, üçüncü taraflara bilgi sistemine erişim hakkı vermeden önce gerekli güvenlik gereksinimleri tanımlamalı ve uygulamalıdır. İşletme bilgi içeren ortamları, üçüncü taraflar ile yapılan bilgi aktarımları sırasında gerçekleşebilecek kötüye kullanım veya bozulmaya karşı korumaya yönelik tedbirler almalıdır. Ancak, bu tedbirler Kurul'un bilgi alımı faaliyetlerine engel teşkil edemez.

n. Kayıt Mekanizmalarının Oluşturulması

İşletme, bilgi sistemleri üzerindeki riskleri, sistem veya faaliyetlerin karmaşıklığını ve kapsamının genişliğini göz önünde bulundurarak bilgi sistemlerinin kullanımına ilişkin etkin bir denetim izi kayıt mekanizması oluşturmalıdır. Böylece, bilgi sistemleri dâhilinde gerçekleşen ve işletmenin faaliyetlerine ait kayıtlarda değişiklik ve silmeye sebep olan işlemlere ilişkin denetim izlerinin yeterli detayda ve açıklıkta kaydedilmesi sağlanır. Kayıt mekanizmasının yetkisiz sistemsel ve kullanıcı erişimlerine karşı korunmasına yönelik önlemler alınmalıdır.

Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli teknikler kullanılmalıdır. Denetim izlerinin bütünlüğü düzenli

olarak gözden geçirilerek, olağandışı durumlar üst yönetime raporlanmalıdır. Denetim izlerinde asgari olarak aşağıdaki bilgiler tutulmalıdır:

- Yapılan işlemlerin türü ve niteliği,
- İşlemlere ilişkin yetkisiz erişim teşebbüsleri,
- İşlemi gerçekleştiren uygulama,
- İşlemi gerçekleştiren kişinin kimliği,
- Yapılan işlemlerin zamanı.

Denetim izlerinin asgari beş yıl saklanması, denetim izlerinin güvenliğinin sağlanması ve yedeklerinin alınması suretiyle yaşanması muhtemel olumsuzluklar sonrasında da öngörülen süre için erişilebilir olmaları sağlanmalıdır.

Dış kaynak hizmeti alınan kuruluşlar, müşteriler ve personel, bilgi sistemleri üzerindeki aktivitelerinin kaydının tutulduğu konusunda bilgilendirilmelidir. Denetim izlerinin tutulması, mevzuatın diğer hükümleri gereği işletmenin belge saklamasına ilişkin yükümlülüklerini değiştirmez.

p. Zaman Senkronizasyonu

İşletme bilgi sistemlerinde zaman kaynağı olarak atomik saatleri kullanmalıdır.

r. Bilgi Güvenliği İhlali

İşletme, bünyesinde gerçekleşen her türlü bilgi güvenliği ihlalinin ve bilgi sistemlerine ilişkin ortaya çıkan zayıflıkların yönetilmesini sağlayacak aşağıdaki asgari hususları içeren kontrolleri oluşturmalıdır:

- Gerçekleşen ihlal veya ortaya çıkan zayıflığın mümkün olan en kısa sürede kayda alınması ve çözülmesi için gerekli mekanizmaların kurulması, sorumlulukların belirlenmesi ve tüm personelin bilgilendirilmesi,
- İhlali veya zayıflığı bildiren kişinin, işlemin sonucu hakkında bilgilendirilmesi,
- Bildirimi yapılan tüm ihlal ve zayıflıkların kök sebebinin bulunması ve düzeltici faaliyetlerin uygulanması,
- Kritik ihlal veya zayıflıkların üst yönetime raporlanması,
- Tüm ihlal ve zayıflıkların; türü, ortaya çıkış zamanı, etkilediği bilgi sistemleri, iş süreçleri ve etki alanı ile buna karşı gerçekleştirilen düzeltici faaliyetler, harcanan zaman, maliyet ve işgücü miktarının kayda alınması,
- Tekrarlayan veya benzer ihlal veya zayıflıklara organizasyonun hazırlıklı olmasının sağlanması.

s. Bilgi Sistemleri Edinimi, Geliştirilmesi ve Bakımı

İşletme, bilgi sistemleri edinimi, geliştirilmesi ve bakımı için asgari olarak aşağıdaki hususları içeren kontrolleri oluşturmalıdır:

- İşletme kendi bünyesinde geliştirilecek, değiştirilecek veya dış kaynak hizmeti yoluyla edinilecek her türlü bilgi sisteminin fonksiyonel gereksinimleri ile tasarım, geliştirme ve test aşamalarının her biri için teknik ve güvenlik gereksinimlerinin yazılı hale getirilmesi,
- Temin edilecek bilgi sistemlerinin, işletme ölçeği, faaliyetleri ve sunulan ürünlerin niteliği ve karmaşıklığı ile uyumlu olması,
- Bilgi sistemlerinin geliştirme, değişiklik veya edinimi faaliyeti boyunca, işin gelişimini takip edebilmek için proje gelişim raporlarının hazırlanması ve işletme yönetim kurulu tarafından onaylanması,

- Bilgi sistemlerinde yapılacak önemli güncellemelerin veya değişikliklerin iş süreçlerini aksatmaması ve bilgi güvenliği riski oluşturmaması için güncelleme veya değişikliklere ilişkin planlama, test ve uygulama adımlarının detaylı olarak ele alınması,
- Uygulamalarda veri girişlerinin tam, doğru ve geçerli şekilde yapılmasını, veri üzerindeki işlemlerin doğru sonuçları üretmesini sağlayacak, veri ve işlem kaybını, verinin yetkisiz değiştirilmesini ve kötüye kullanımını önleyecek uygun kontrollerin oluşturulması,
- Uygulama güvenliği ve erişilebilirlik gereksinimleri belirlenirken organizasyonun belirlemiş olduğu veri sınıflandırması ve risk önceliklerinin göz önünde bulundurulması,
- Bilgi sistemleri gerçek ortamda kullanıma alınmadan önce kabul kriterlerinin belirlenmesi, hazırlanacak bir plana göre fonksiyonel, teknik ve güvenlik gereksinimlerinin teste tabi tutulması, test verilerinin özenle seçilerek korunması ve kontrol edilmesi,
- Gerekli hallerde değiştirilmiş veya yeni geliştirilmiş sistemin, gerçek ortamda kullanıma alınmadan önce, belirli bir olgunluk seviyesine ulaşana kadar eski sistemle beraber çalıştırılması; bu şekilde paralel işletimin mümkün olmadığı durumlarda ise, değiştirilmiş veya yeni geliştirilmiş sistem belirli bir olgunluk seviyesine ulaşana kadar eski sistemin veri kayıpsız olarak devreye alınabilir halde tutulması,
- Bilgi sistemlerinin kullanımı ile ilgili gerekli eğitim materyallerinin oluşturulması,
- Geliştirme, test ve gerçek ortamdaki işlemler ile bu işlemlerin gerçekleştiği ortamların, yetkisiz erişim ve değişim riskine karşı birbirinden ayrılması.

t. Bilgi Sistemleri Sürekliliği

İşletme birincil ve ikincil sistemlerini yurt içinde bulundurmakla yükümlüdür.

İşletme faaliyetlerini destekleyen bilgi sistemlerinin sürekliliğini sağlamak üzere iş sürekliliği planının bir parçası olan bilgi sistemleri süreklilik planını hazırlamalı ve bu plan kapsamında ikincil sistem tesis edilmeli veya bu hizmeti destek hizmeti kuruluşlarından tedarik etme hususunda güvence sağlayan anlaşmalar yapılmalıdır. İkincil sistemde, işletmenin veri ve sistem yedekleri kullanıma hazır bulundurulmalıdır.

Söz konusu plan, iş süreklilik planında belirlenen hedefleri de dikkate alacak şekilde, kritik iş süreçlerini destekleyen bilgi sistemleri hizmetlerine yönelik hazırlanarak, hizmetlerin tekrar kullanıma açılmasını sağlayacak alternatifli kurtarma süreç ve prosedürleri tesis edilmeli ve gerekli önlemler alınmalıdır. Plan kapsamında, performans takibi ve kapasite planlaması yapılarak, sistem kaynaklarının kullanımı izlenmelidir.

Bilgi sistemleri altyapısından kaynaklanabilecek kesintilere, işlem performansını düşürecek veya iş sürekliliğini aksatacak durumlara karşı gerekli tedbirler alınmalıdır. Bilgi sistemlerinin sürekliliğini sağlamak amacıyla, risk değerlendirmesi, risk azaltma ve risk izleme faaliyetleri gerçekleştirilmelidir.

Plan, iş süreçlerini veya bilgi sistemlerini etkileyecek değişikliklerden sonra gözden geçirilerek güncellenmelidir. Planın etkinliğini ve güncelliğini temin etmek üzere testler yapılmalı, testlere varsa dış kaynak yoluyla hizmet alınan kuruluşlar da dâhil edilmeli ve test sonuçları üst yönetime raporlanmalıdır. Testler, her yıl tekrarlanmalıdır.

Bilgi sistemleri, iş sürekliliği planındaki önceliklere uygun olarak yedeklenmeli ve yedekten geri dönülmesi için gerekli süreçler bilgi sistemleri sürekliliği planı ve testine dâhil edilmelidir. İşletme, bilgi güvenliği politikasının, bilgi sistemleri süreklilik planının, ağ topolojisinin, bilgi sistemleri varlık envanteri ile iş sürekliliği ve güvenliği açısından önem arz eden diğer dokümanların güncel sürümlerini ve bilgi sistemleri yönetimine ilişkin parolalarını güvenli ortamlarda saklamalıdır.

Kurul bilgi sistemleri yönetimine ilişkin yükümlülük ve muafiyetleri kısmen veya tamamen kaldırmaya, bunların kapsam ve içeriğini işletmeler bazında değiştirmeye yetkilidir. Nitekim, Kurul 08.03.2018 tarih ve 2018/10 sayılı Bülteni'nde kamuya açıklanan 01.03.2018 tarih ve 9/327 sayılı Kararı

ile, BSY Tebliğ'in 28/3 maddesinin verdiği yetki kapsamında bilgi sistemleri bağımsız denetim yükümlülüğü bulunmayan halka açık ortaklıkların bu aşamada birincil sistemlerini yurtiçinde bulundurma zorunluluğunu kaldırmıştır. Kurul, halka açık ortaklıkların bilgi sistemleri bağımsız denetim yükümlülüğünün kademeli olarak genişletilmesinin planlandığını belirtmiş olup bu çerçevede halka açık ortaklıklar bilgi sistemleri bağımsız denetim yükümlülüğüne tabi olacakları tarih itibariyle birincil sistemlerini yurtiçinde tutmak zorunda olacaklardır.

u. Değişiklik Yönetimi

İşletme, bilgi sistemlerini oluşturan her türlü yazılım, donanım ve altyapı bileşenlerine, dokümantasyona ve bilgiye yapılan değişiklikleri yönetebilmek amacıyla, en az aşağıdaki hususları içeren kontroller geliştirmekle yükümlüdür:

- Yapılacak her türlü değişiklik için; değişikliğin sebebini, kapsamını, etkisini, içerdiği riskleri, beklenen faydasını, değişikliği yapacak kişileri, maliyetini, gerekli test ve eğitim faaliyetlerini tanımlayan kayıtlar oluşturulması,
- Planlanan değişiklikler onay sürecinden geçmedikçe işleme konulmaması,
- Planlanan değişikliklerin, devreye alınma tarihleri, test ve eğitim faaliyetleriyle ilgili düzenlemelerin ilgili tüm taraflara önceden duyurulması,
- Değişikliğin uygulanmasında ortaya çıkan hatalar ve öngörülemeyen durumlarda devreye alınacak geri dönüş prosedürleri ve bunlarla ilgili sorumlulukların önceden belirlenmesi,
- Gerçekleştirilen değişikliklerin sonuçlarının gözden geçirilmesi,
- Gerçekleştirilen, iptal edilen veya reddedilen tüm değişikliklerin gerekçeleriyle birlikte kayda geçirilmesi ve saklanması.

1.3.2.6. Muafiyetler

BSY Tebliği kapsamında yer alan işletmelerin heterojen bir yapıda olması nedeniyle yükümlülüklerde farklılaşmaya gidilmiş ve muafiyetler tanımlanmıştır. Ancak Kurul, belirlenen muafiyetleri kısmen veya tamamen kaldırmaya, bunların kapsam ve içeriğini işletme türü bazında değiştirmeye yetkilidir. Muafiyetlerde aşağıda verildiği üzere kademeli bir düzenlemeye gidilmiştir. Bu kapsamda,

a) Asgari özsermaye yükümlülüğü 5 milyon TL (*)[10] ve daha az olan portföy yönetim şirketleri ve Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş. (SPL), BSY Tebliğ'in bilgi güvenliğine ilişkin 24'üncü maddesi ile değişiklik yönetimine ilişkin 27'nci maddelerini uygulamak zorunda değildir.

b) Dar yetkili aracı kurumlar, varlık kiralama şirketleri, ipotek finansmanı kuruluşları, Türkiye Sermaye Piyasaları Birliği (TSPB), Türkiye Değerleme Uzmanları Birliği (TDUB), bağımsız denetim, derecelendirme ve değerleme kuruluşları, halka açık ortaklıklar, varlık finansmanı fonları, kolektif yatırım kuruluşları, emeklilik yatırım fonları, konut finansmanı fonları,

- BSY Tebliği'nin 7'inci maddesinin beşinci fıkrasında yer alan,

"*Bilgi sistemleri güvenliğine ilişkin süreç ve prosedürlerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetilmesi hususunda üst yönetime rapor veren ve yeterli teknik bilgi ve tecrübeye sahip bir bilgi sistemleri güvenliği sorumlusu belirlenir.*",

- BSY Tebliği'nin 8'inci maddesinin dördüncü, beşinci ve altıncı fıkralarında yer alan,

"*(4) Bilgi sistemlerinin teknik açıklarına ilişkin bilgi, zamanında elde edilir ve kuruluşun bu tür*

[10] *(*)Portföy yönetim şirketlerine ilişkin asgari özsermaye yükümlülük tutarları için, 2/7/2013 tarihli ve 28695 sayılı Resmî Gazete'de yayımlanan Portföy Yönetim Şirketleri ve Bu Şirketlerin Faaliyetlerine İlişkin Esaslar Tebliği (III-55.1)'nin 28 ve 41 inci maddeleri kapsamında Kurulca yeniden değerleme kapsamında belirlenen ve ilan edilen tutarlar esas alınır.*

açıklara karşı zafiyeti değerlendirilerek, riskin ele alınması için uygun tedbirler alınır.

(5) Kurum, Kuruluş ve Ortaklıkların bilgi sistemleri, bilgi güvenliği gereklerinin yerine getirilmesi hususunda herhangi bir görevi bulunmayan ve sızma testi konusunda ulusal veya uluslararası belgeye sahip gerçek veya tüzel kişiler tarafından en az yılda bir kez sızma testine tabi tutulur.

(6) Sızma testinde bu Tebliğin 1 numaralı ekinde yer alan usul ve esaslar uygulanır.",

- BSY Tebliği'nin 14'üncü maddesinin üçüncü fıkrasında yer alan,

"*Kullanılan kimlik doğrulama verilerinin tutulduğu ortamların ve bu amaçla kullanılan araçların güvenliğini sağlamaya yönelik gerekli önlemler alınır. Bu önlemler asgari olarak kimlik doğrulama verilerinin şifreli olarak saklanması, bu veriler üzerinde yapılacak her türlü değişikliği algılayacak sistemlerin kurulması, yeterli denetim izlerinin tutulması ve güvenliğinin sağlanması hususlarını içerir. Kimlik doğrulama verilerinin aktarımı sırasında gizliliğinin sağlanmasına yönelik önlemler alınır.*",

- BSY Tebliği'nin 15'inci maddesinin üçüncü fıkrasında yer alan,

"*Yetkilendirme verilerinin güvenliği sağlanır ve bu veriler üzerinde yapılacak her türlü değişikliği algılayacak sistemler kurulur. Yetkilendirme verilerinin tutulduğu ortamlara yetkisiz erişim teşebbüsleri kayıt altına alınır ve düzenli olarak gözden geçirilir.*",

- BSY Tebliği'nin 17'nci maddesinin ikinci fıkrasında yer alan,

"*Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri faaliyetleri kapsamında gerçekleşen işlemlere ilişkin iletilen, işlenen ve saklanan önem derecesi yüksek verilerin kasten veya yanlışlıkla kurum dışına sızmasını önlemeye yönelik olarak gerekli önlemleri alır.*",

- BSY Tebliği'nin 18'inci maddesinin dördüncü fıkrasında yer alan,

"*Kurum, Kuruluş ve Ortaklıkların üst yönetimi, dış kaynak yoluyla gerçekleştirilen hizmetler için hizmetin erişilebilirliğini, performansını, kalitesini, bu hizmet kapsamında gerçekleşen güvenlik ihlali olayları ile dış kaynak yoluyla hizmet sağlayan kuruluşun güvenlik kontrollerini, finansal koşullarını ve sözleşmeye uygunluğunu yakından takip etmek için yeterli bilgi ve tecrübeye sahip sorumluları belirler.*"

- BSY Tebliği'nin 22'nci maddesinin ikinci fıkrasında yer alan,

"*Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli teknikler kullanılır. Denetim izlerinin bütünlüğü düzenli olarak gözden geçirilir ve olağandışı durumlar üst yönetime raporlanır.*",

- BSY Tebliği'nin bilgi güvenliği ihlaline ilişkin 24'üncü maddesini,

- BSY Tebliği'nin 25'inci maddesinin birinci fıkrasının (b), (d) ve (ğ) bentlerinde yer alan,

"*b) Temin edilecek bilgi sistemleri yapısının Kurum, Kuruluş ve Ortaklıkların ölçeği, faaliyetlerinin ve sunulan ürünlerin niteliği ve karmaşıklığı ile uyumlu olması zorunludur.*

...

d) Uygulamalarda veri girişlerinin tam, doğru ve geçerli şekilde yapılmasını, veri üzerindeki işlemlerin doğru sonuçları üretmesini sağlayacak, veri ve işlem kaybını, verinin yetkisiz değiştirilmesini ve kötüye kullanımını önleyecek uygun kontroller tesis edilir,

...

ğ) Bilgi sistemlerinin kullanımı ile ilgili gerekli eğitim materyalleri oluşturulur,",

- BSY Tebliği'nin 26'ncı maddesinin üçüncü fıkrasında yer alan,

"*Plan kapsamında ikincil sistem tesis edilir ya da bu hizmeti destek hizmeti kuruluşlarından tedarik etme hususunda güvence sağlayan anlaşmalar yapılır. İkincil sistemde, Kurum, Kuruluş ve Ortaklıkların veri ve sistem yedekleri kullanıma hazır bulundurulur.*",

- BSY Tebliği'nin değişiklik yönetimine ilişkin 27'nci maddesi

hükümlerini uygulamak zorunda değillerdir. Anılan hükümlerden muaftırlar.

1.3.3. Bilgi Sistemleri Bağımsız Denetim Tebliği III-62.2

SPKn'nun "*Kurulun görev, yetki ve sorumlulukları*" başlıklı 128'inci maddesinin birinci fıkrasının (h) bendinde "*Sermaye piyasası kurumlarının, halka açık şirketlerin, borsaların ve öz düzenleyici kuruluşların bilgi sistemlerinin işletimine ve bu Kanun çerçevesindeki denetimine ilişkin usul ve esasları belirlemek*" hükmü bulunmaktadır. Anılan SPKn'dan önceki kanunlarda, Kurul'un görev ve yetkileri arasında işletmelerin bilgi sistemleri denetimine ilişkin usul ve esas belirleme yetkisi bulunmamaktaydı. Yeni SPKn ile Kurul'a verilen bu görev çerçevesinde, sermaye piyasasında bilgi sistemleri bağımsız denetimine ilişkin esaslar, Seri:X, No:22 Tebliği ile konuya ilişkin BDDK düzenlemeleri dikkate alınarak III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği (BSBD Tebliği) ile düzenlenmiştir.

BSBD Tebliği, SPKn'nun 62/2, 72/3 ve 128/1-(c) ve (h) maddelerine dayanılarak 05.01.2018 tarih 30292 sayılı Resmi Gazete'de yayımlanıp, yürürlüğe girmiştir. BSBD Tebliği ile sermaye piyasasında bilgi sistemleri bağımsız denetimi faaliyetlerinin genel esasları, bu faaliyette bulunacak kuruluşların yetkilendirilmesi, denetim metodolojisi ve denetim sonuçlarının raporlanmasına ilişkin usul ve esaslar belirlenmiştir. BSBD Tebliği, benzer hususlar içermesi nedeniyle bazı konularda Seri:X, No:22 Tebliği ile muhtelif BDS'lerin kıyasen uygulanacağına ilişkin hükümler içermektedir.

BSBD Tebliği'nin dört bölümden oluşan hükümlerine devam eden bölümde yer verilmekte olup, Tebliğin tamamı ve güncellenecek hallerine Kurul'un internet sitesinin mevzuat bölümünden erişim sağlanabilir.

Diğer taraftan, 02.07.2024 tarihli ve 32590 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 7518 sayılı "*Sermaye Piyasası Kanunu'nda Değişiklik Yapılmasına Dair Kanun*" ile ülkemizde faaliyet gösteren veya gösterecek olan kripto varlık hizmet sağlayıcılarının bilgi sistemleri denetimine ilişkin düzenleme ve denetim yapma yetkisi Kurul'a verilmiştir. SPKn'nun 99/B maddesinin ikinci fıkrasında, kripto varlık hizmet sağlayıcılarının mali denetimi ve **bilgi sistemleri bağımsız denetiminin** Kurulca ilan edilen listede yer alan bağımsız denetim kuruluşlarınca yapılacağı; bilgi sistemleri denetimine ilişkin ilave usul ve esaslar TÜBİTAK ya da gerekli görülen diğer kurum ve kuruluşların görüşü alınarak Kurulca belirleneceği; Kurul personeli ve görevlendirilen diğer personel, Kurulca belirlenecek program çerçevesinde yetkili kuruluşlar tarafından yapılacak bilgi sistemleri denetimlerinin her aşamasına, denetçi bağımsızlığı ilkesini zedelemeksizin izleyici sıfatı ile eşlik edebileceği; bu şekilde denetime katılanlar bağımsız denetim kuruluşlarının ulaştığı denetim sonuçlarıyla ilgili bir sorumluluk taşımayacağı ve yetkili kuruluşun bilgi birikimini şahsına veya bir başka yetkili kuruluşa çıkar sağlamak için kullanamayacağı hüküm altına alınmıştır. Kripto hizmet sağlayıcılarının tabi olacağı bilgi sistemleri bağımsız denetimine ilişkin ikincil düzenleme çalışmaları devam etmektedir.

1.3.3.1. BSBD Tebliğ Kapsamına Giren İşletmeler

Bu Tebliğ'in kapsamına halka açık ortaklıklar, sermaye piyasası kurumları ve öz düzenleyici kuruluşlar girmektedir. Öz düzenleyici kuruluşlardan kapsama girenler tek tek sayılmıştır. Bu kapsamda Tebliğ kapsamına girenler:

a) Borsa İstanbul A.Ş.,

b) Borsalar ve piyasa işleticileri ile teşkilatlanmış diğer pazar yerleri,

c) Emeklilik yatırım fonları,

d) İstanbul Takas ve Saklama Bankası A.Ş.,

e) Merkezi Kayıt Kuruluşu A.Ş.,

f) Portföy saklayıcısı kuruluşlar,

g) Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş. (SPL),

h) Sermaye piyasası kurumları[11],

i) Halka açık ortaklıklar,

j) Türkiye Sermaye Piyasaları Birliği (TSPB),

k) Türkiye Değerleme Uzmanları Birliği (TDUB).

BSBD Tebliğ'i borsaları, ihraççıları, sermaye piyasası kurumları ve öz düzenleyici kuruluşlar (bundan sonra işletme olarak kullanılacak) kapsama alınmasına karşın, bilgi sistemleri denetim yükümlülüğü tamamı için getirilmemiştir. Tebliğ'in "*Yükümlülük ve muafiyetler*" başlıklı 30'uncu maddesinde, periyodik bilgi sistemleri bağımsız denetim yükümlülüğü kademeli olarak düzenlenmiştir. Bilgi sistemleri bağımsız denetimi Ocak-Aralık dönemini kapsayan 1 yıllık dönemi kapsamakta olup, denetim yükümlülüğünün bulunduğu dönem (yıl) için yaptırılır. Bu kapsamda:

a. Her Yıl Bilgi Sistemleri Denetimi Yaptıracaklar

Borsa İstanbul A.Ş., İstanbul Takas ve Saklama Bankası A.Ş., Merkezi Kayıt Kuruluşu A.Ş., borsalar ve piyasa işleticileri, teşkilatlanmış diğer pazar yerleri, merkezi takas kuruluşları, merkezi saklama kuruluşları ve veri depolama kuruluşları ilki 2018 yılında olmak üzere her yıl bilgi sistemleri bağımsız denetimi yaptırma zorundadır.

b. Her 2 Yılda Bilgi Sistemleri Denetimi Yaptıracaklar

Kısmî ve geniş yetkili aracı kurumlar ve asgari özsermaye yükümlülüğü 5 Milyon TL'den (*)[12] fazla olan portföy yönetim şirketleri ilki 2019 yılında olmak üzere 2 yılda bir bilgi sistemleri bağımsız denetimi yaptırmakla yükümlüdürler.

TSPB'nin talebi kapsamında Kurul 02.05.2019 tarihli Kararı ile kısmi yetkili aracı kurumlar ile asgari özsermaye yükümlülüğü 5 milyon TL'den (*) fazla olan portföy yönetim şirketlerinin ilk bilgi sistemleri denetimi 2020 yılına ertelenmiştir.

2019 yılı için geniş yetkili aracı kurumlar bilgi sistemleri bağımsız denetim raporu düzenlemiştir.

c. Her 3 Yılda Bilgi Sistemleri Denetimi Yaptıracaklar

Asgari özsermaye yükümlülüğü 5 Milyon TL (*) ve az olan portföy yönetim şirketleri ve SPL ilki 2020 yılında olmak üzere 3 yılda bir bilgi sistemleri bağımsız denetimi yaptırmakla yükümlüdürler.

TSPB'nin talebi kapsamında Kurul 14.11.2019 tarihli Kararı ile asgari özsermaye yükümlülüğü 5 milyon TL (*) ve az olan portföy yönetim şirketlerinin ve SPL'nin başvurusu üzerine Kurul 30.04.2020 tarihli Kararı ile SPL'nin ilk bilgi sistemleri denetimi 2021 yılına ertelenmiştir.

d. Bilgi Sistemleri Denetim Yükümlülüğü Bulunmayanlar

Dar yetkili aracı kurumlar, halka açık ortaklıklar, kolektif yatırım kuruluşları, varlık kiralama şirketleri, emeklilik yatırım fonları, konut finansmanı fonları, varlık finansmanı fonları, ipotek finansmanı kuruluşları, bağımsız denetim, derecelendirme ve değerleme kuruluşları, TSPB ve TDUB ve kuruluş ve faaliyet esasları Kurul'ca belirlenen diğer sermaye piyasası kurumları periyodik olarak bilgi sistemleri bağımsız denetimi yaptırmak zorunda değildir.

Denetim yükümlülüğü bulunmayan işletmeler isteğe bağlı olarak bilgi sistemleri denetimi yaptırabilir.

---

[11] SPKn'nun 35'inci maddesinde sermaye piyasası kurumları olarak, yatırım kuruluşları, kolektif yatırım kuruluşları, sermaye piyasasında faaliyette bulunacak bağımsız denetim, değerleme ve derecelendirme kuruluşları, portföy yönetim şirketleri, ipotek finansmanı kuruluşları, konut finansmanı ve varlık finansmanı fonları, varlık kiralama şirketleri, merkezî takas kuruluşları (İstanbul Takas ve Saklama A.Ş.), merkezî saklama kuruluşları (Merkezi Kayıt Kuruluşu A.Ş.), veri depolama kuruluşları ve kuruluş ve faaliyet esasları Kurulca belirlenen diğer sermaye piyasası kurumları sayılmıştır.

[12] (*) Portföy yönetim şirketlerine ilişkin asgari özsermaye yükümlülük tutarları için, 2/7/2013 tarihli ve 28695 sayılı Resmî Gazete'de yayımlanan Portföy Yönetim Şirketleri ve Bu Şirketlerin Faaliyetlerine İlişkin Esaslar Tebliği (III-55.1)'nin 28 ve 41 inci maddeleri kapsamında Kurulca yeniden değerleme kapsamında belirlenen ve ilan edilen tutarlar esas alınır.

Kurul bilgi sistemleri denetimine ilişkin yükümlülük ve muafiyetleri kısmen veya tamamen kaldırmaya, bunların kapsam ve içeriğini işletmeler bazında değiştirmeye yetkilidir. Nitekim, Kurul 08.03.2018 tarih ve 2018/10 sayılı Bülteni'nde kamuya açıklanan 01.03.2018 tarih ve 9/327 sayılı Kararı ile Tebliğ'in 30/5 maddesinin verdiği yetkiye istinaden bilgi sistemleri bağımsız denetim kapsamına girecek kurum, kuruluş ve ortaklıkların tedrici (kademeli) olarak genişletilmesinin planlandığı kamuya duyurulmuştur. Bu durum, halka açık ortaklıklara kademeli olarak, bu ortaklıkların büyüklük ve tabi olduğu pazarlar dikkate alınarak, bilgi sistemleri bağımsız denetim yükümlülüğü getirileceğini göstermektedir.

Benzer şekilde, faaliyet izni verilerek dar, kısmî veya geniş yetkili aracı kurum statsünde yetkilendirilecek aracı kurumların, BSDB Tebliği uyarınca bilgi sistemleri bağımsız denetimlerini hangi dönem için yaptıracaklarının belirlenmesine yönelik olarak Kurul'un 24.08.2023 tarih ve 49/1017 sayılı İlke Kararı'nda[13];

- İlk defa faaliyete geçerek kısmi veya geniş yetkili aracı kurum statüsünde yetkilendirilen aracı kurumlar, geçici kapalı durumdan tekrar faaliyete geçerek kısmi veya geniş yetkili aracı kurum statüsünde yetkilendirilen aracı kurumlar, dar yetkili aracı kurum statüsünden kısmi veya geniş yetkili aracı kurum statüsünde yetkilendirilen aracı kurumlar ilk bilgi sistemleri bağımsız denetimlerini Kurulca kendilerine konuya ilişkin izin verildiği tarihten sonraki yıl için; izleyen bilgi sistemleri bağımsız denetimlerini ise kısmi yetkili aracı kurum statüsünde yetkilendirilen aracı kurumların çift, geniş yetkili aracı kurum statüsünde yetkilendirilen aracı kurumların ise tek yıllarda yaptırmaları,

- Kısmi veya geniş yetkili aracı kurumların statüsünü daraltarak dar yetkili aracı kurum olduğu tarihte, o yıl için kısmi veya geniş yetkili aracı kurum statüsünden kaynaklanan bilgi sistemleri bağımsız denetimi yaptırma zorunluluğu bulunması halinde, Kurulca statü değişikliğine izin verildiği tarihte o yıl için bilgi sistemleri bağımsız denetimi yaptırmaları; dar yetkili aracı kurum statüsünde faaliyetlerine devam etmeleri halinde periyodik olarak bilgi sistemleri bağımsız denetimi yaptırma zorunluluğunun bulunmadığı,

- Kısmi yetkili aracı kurumların statüsünü genişleterek geniş yetkili aracı kurum olduğu tarihte, o yıl için kısmi yetkili aracı kurum statüsünden kaynaklanan bilgi sistemleri bağımsız denetimi yaptırma zorunluluğu bulunması halinde, Kurulca statü değişikliğine izin verildiği tarihte o yıl için bilgi sistemleri bağımsız denetimi yaptırmaları; kısmi yetkili aracı kurum statüsünden kaynaklanan bilgi sistemleri bağımsız denetimi yaptırma zorunluluğu bulunmaması halinde izleyen yıl için bilgi sistemleri bağımsız denetimi yaptırmaları; sonraki bilgi sistemleri bağımsız denetimlerini ise geniş yetkili aracı kurum statüsünde faaliyetlerine devam etmeleri halinde tek yıllarda yaptırmaları,

- Geniş yetkili aracı kurumların statüsünü daraltarak kısmi yetkili aracı kurum olduğu tarihte, o yıl için geniş yetkili aracı kurum statüsünden kaynaklanan bilgi sistemleri bağımsız denetimi yaptırma zorunluluğu bulunması halinde, Kurulca statü değişikliğine izin verildiği tarihte o yıl için bilgi sistemleri bağımsız denetimi yaptırmaları; geniş yetkili aracı kurum statüsünden kaynaklanan bilgi sistemleri bağımsız denetimi yaptırma zorunluluğu bulunmaması halinde izleyen yıl için bilgi sistemleri bağımsız denetimi yaptırmaları; sonraki bilgi sistemleri bağımsız denetimlerini ise kısmi yetkili aracı kurum statüsünde faaliyetlerine devam etmeleri halinde çift yıllarda yaptırmaları

şeklinde uygulamanın yürütülmesine karar verilmiştir. Söz konusu kararın uygulamasına aşağıdaki tabloda yer verilmektedir.

Mevcut Durumdaki Statüsü	**Kurul İzni İle Geçtiği Statü**	**Bilgi Sistemleri Bağımsız Denetimi Yaptıracağı Dönem**	**İzleyen Bilgi Sistemleri Bağımsız Denetimlerini Yaptıracağı Dönemler**
- İlk defa faaliyete geçecek aracı kurum	Kısmı veya geniş yetkili aracı kurum	İzin verilen tarihten sonraki yıl için yaptırılmalıdır.	Kısmi yetkili aracı kurumlar çift yıllarda yaptırmalıdır.

[13] *Türkiye Sermaye Piyasaları Birliği'nin 28.08.2023 tarih ve 880 sayılı Genel Mektup'u ile internet sitesinde kamuya duyurulmuştur.*

- Geçici kapalı aracı kurum - Dar yetkili aracı kurum			Geniş yetkili aracı kurumlar tek yıllarda yaptırmalıdır.
- Kısmi yetkili aracı kurum - Geniş yetkili aracı kurum	Dar yetkili aracı kurum	İzin verilen yıl yükümlülüğü var ise o yıl için yaptırmalıdır.	Muaf
- Kısmi yetkili aracı kurum	Geniş yetkili aracı kurum	İzin verilen yıl yükümlülüğü var ise o yıl için yaptırmalıdır.	Geniş yetkili aracı kurumlar tek yıllarda yaptırmalıdır.
		İzin verilen yıl yükümlülüğü yoksa sonraki yıl yaptırmalıdır.	
- Geniş yetkili aracı kurum	Kısmi yetkili aracı kurum	İzin verilen yıl yükümlülüğü var ise o yıl için yaptırmalıdır.	Kısmi yetkili aracı kurumlar çift yıllarda yaptırmalıdır.
		İzin verilen yıl yükümlülüğü yoksa sonraki yıl yaptırmalıdır.	

Diğer taraftan, bilgi sistemleri yönetim ilkelerine ve finansal raporlamaya ilişkin yükümlülüklerde olduğu gibi Tebliğ kapsamına giren bankalar, sigorta şirketleri, finansal kiralama, faktöring ve finansman şirketleri kendi özel mevzuatlarına göre bilgi sistemleri bağımsız denetimi yaptırmaları durumunda Tebliğ'deki yükümlülük yerine getirilmiş sayılacaktır.

1.3.3.2. Bilgi Sistemleri Bağımsız Denetim Faaliyetlerine İlişkin Genel Esaslar

a. Bilgi Sistemleri Bağımsız Denetiminin Amacı ve Kapsamı

Bilgi sistemleri bağımsız denetimi, bilgi sistemleri yönetimi ve işletimi kapsamında yer alan faaliyet, yazılım ve donanım gibi bilgi sistemi unsurları ile bu sistem dâhilinde tesis edilen kontrollerin, BSY Tebliği'nde düzenlenen bilgi sistemleri yönetim ilkeleri doğrultusunda değerlendirilmesi sonucunda görüş oluşturulması ve rapora bağlanması aşamalarından oluşan süreçtir.

Bilgi sistemleri bağımsız denetiminin temel amacı, işletmelerin bilgi sistemlerinin ve bu sisteme ilişkin iç kontrollerinin bilgi sistemleri yönetim ilkeleri doğrultusunda uyumluluk, etkinlik ve yeterliliği hakkında görüş oluşturulmasıdır.

Bilgi sistemleri denetçisi, bilgi sistemleri kapsamında inceleyeceği sistem, faaliyet ve kontrol mekanizmalarını, risk odaklı bir bakış açısıyla ve önemlilik kriterini esas alarak yazılı bir plan dahilinde belirler. Bilgi sistemleri denetçisi, önemlilik kriteri çerçevesinde belirlediği denetimlerin kapsamının, denetim görüşüne makul güvence sağlamak için yeterli denetim kanıtı elde edecek şekilde olmasını sağlar.

b. Önemlilik ve Denetim Riski

Önemlilik, mesleki bilgi ve tecrübeye dayalı bir mütalaa konusu olup; kontrol zayıflıkları sonucu ortaya çıkan ya da çıkabilecek hataların, ihmallerin, prosedürlere aykırılıkların ve hukuka aykırı fiillerin, işletmelerin finansal verilerini raporlamalarına, güvenli ve kesintisiz hizmet sağlamalarına olan ya da olabilecek etkisinin değerlendirilmesidir.

Önemlilik, denetimin planlanması, gerekli alanlarda yoğunlaştırılması, bulguların değerlendirilmesi ve raporlanması için kullanılabilir. Başta finansal veriler olmak üzere denetlenen açısından hassasiyet arz eden verilerin bütünlüğü, tutarlılığı, güvenilirliği, gereken durumlarda gizliliği ve faaliyetlerin sürekliliği önemlilik kavramı kapsamında dikkate alınması gereken temel unsurlardır. Finansal raporları etkileyen kontrollerin değerlendirilmesinde, süreç veya sistem tarafından yürütülen finansal işlemin değeri, işlem sıklığı gibi öğeler kullanılırken, finansal işlemlere ilişkin olmayan kontrollerin değerlendirilmesinde ise iş sürecinin kritikliği, sistem ve operasyonların maliyeti, hataların muhtemel sonuçlarının büyüklüğü, bir zaman aralığında gerçekleşen işlem/sorgu sayısı, tutulan

dosyaların ve üretilen raporların niteliği, zamanlaması ve kapsamı, hizmet seviyesi anlaşmalarının gerekleri ve ceza maddelerindeki para cezası tutarları gibi öğeler kullanılır.

Denetim riski, bilgi sistemleri denetçisinin aşağıdaki risklere bağlı olarak doğru görüş vermemesi olasılığıdır.

1) Yapısal Risk: Kontrolün olmaması nedeniyle, en azından kayda değer olan bir kontrol eksikliğinin var olması riskini,

2) Kontrol Riski: Kontrolün layıkıyla çalışmaması sebebiyle, en azından kayda değer olan bir kontrol eksikliğini önleyememesi, ortaya çıkaramaması veya zamanında düzeltememesi riskini,

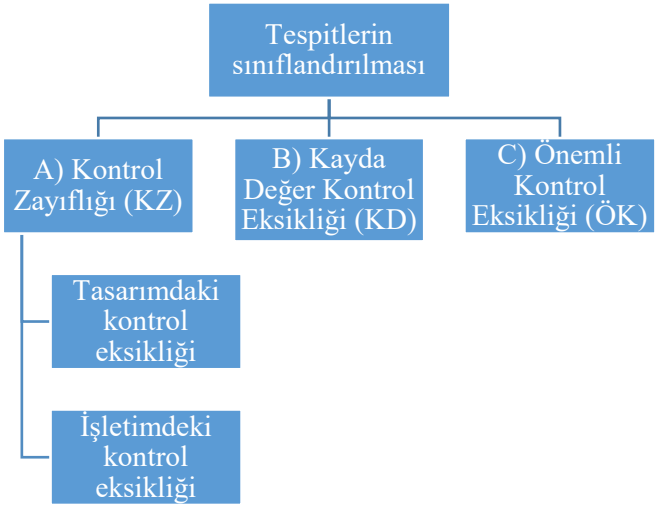
3) Tespit Riski: Bilgi sistemleri denetçisinin, denetlenen işletmenin bilgi sistemlerinde yer alan en azından kayda değer olan bir kontrol eksikliğini ortaya çıkaramaması riskini,

ifade eder.

Önemli veya kayda değer kontrol eksikliği riski, işletmenin bilgi sistemlerinde en azından kayda değer olan bir kontrol eksikliğinin bulunması riskini ifade eder. Önemli ya da kayda değer kontrol eksikliği riski, yapısal risk ve kontrol riskinden kaynaklanır. Bilgi sistemleri denetçisi, denetim riskini makul düzeye indirebilmek için, önemli veya kayda değer kontrol eksikliği riskinin yüksek olduğu alanlarda tespit riskini düşürecek şekilde uygun denetim tekniklerini kullanmalıdır.

c. Kriterler

Bilgi sistemleri denetçisi, incelemeleri neticesinde ulaştığı tespitlere konu kontrol zayıflıkları ve eksikliklerini önemlilik kavramına göre tasnif etmede aşağıda belirtilen kriterleri kullanır.



Şekil 21: Tespitlerin Sınıflandırılması

1) Kontrol Zayıflığı: Bir kontrolün tasarımı veya işletilmesinin, hataları zamanında önleme ve tespit etmeye olanak sağlamaması durumudur.

- Tasarımdaki kontrol eksikliği, bir kontrol hedefinin gerçekleşmesini sağlayacak kontrolün bulunmaması ya da var olan bir kontrolün tasarlandığı şekilde çalışıyor olsa bile tasarımındaki hatalardan dolayı kendisinden beklenen kontrol hedefini gerçekleştirememesi durumudur.
- İşletimdeki kontrol eksikliği, düzgün tasarlanmış bir kontrolün tasarlandığı şekilde çalışmaması ya da kontrolü gerçekleştiren personelin, kontrolün etkin bir şekilde yerine getirilmesi için gerekli yetki ve yeterliliğe sahip olmaması durumudur.

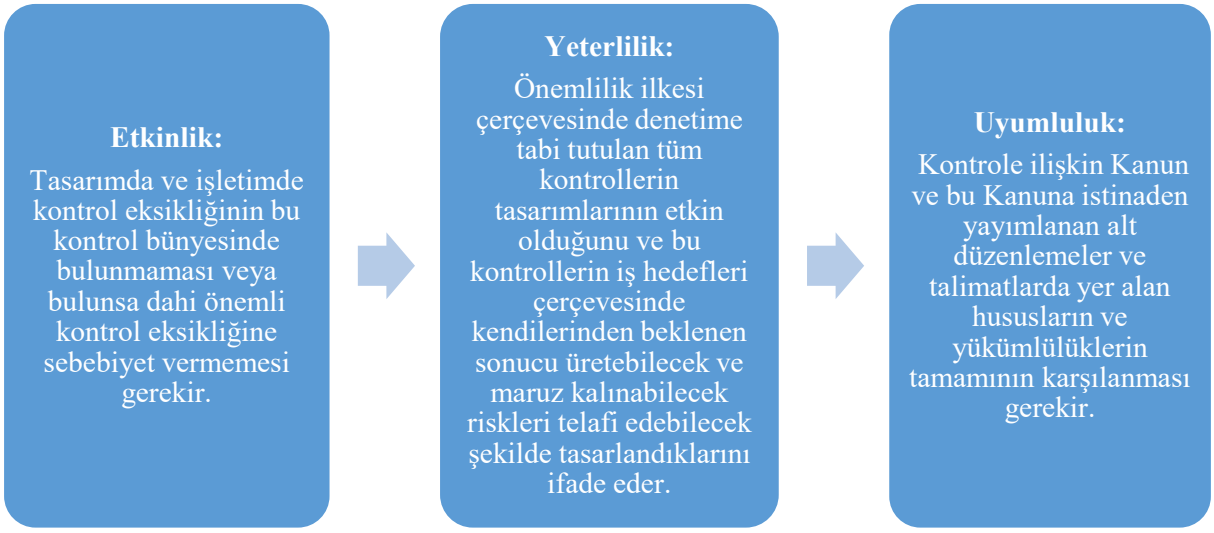
2) Kayda Değer Kontrol Eksikliği: İşletme verilerinin bütünlüğünün, tutarlılığının, güvenilirliğinin ve gereken durumlarda gizliliğinin sağlanmasına, faaliyetlerinin devamlılığının teminine olumsuz etki yapması muhtemel bir kontrol zayıflığı veya birkaç kontrol zayıflığının bir araya gelmesi sonucu oluşan önemsiz sayılamayacak eksikliktir. İşletmenin finansal verilerinin güvenilir bir

şekilde genel kabul görmüş muhasebe standartlarına uygun olarak kaydedilmesi, kayıtların yetkilendirilmesi, işlenmesi veya raporlanması sırasında oluşan hataların ve ihmallerin önlenmesine olumsuz etki yapması muhtemel eksiklikler de bu kapsamda değerlendirilir.

3) Önemli Kontrol Eksikliği: İşletmenin dönemsel olarak yaptığı finansal raporlamalarda önemli bir yanlışlığın önlenmesi veya düzeltilmesini engelleyecek veya işletme bünyesinde yürütülen faaliyetlere ilişkin bilgilerin bütünlüğünün, tutarlılığının, güvenilirliğinin, devamlılığının ve gereken durumlarda gizliliğinin sağlanmasına önemli olumsuz etki yapması kuvvetle muhtemel bir veya birkaç kontrol zayıflığının bir araya gelmesidir.

d. Etkinlik, Yeterlilik ve Uyumluluk

Bir kontrolün tasarımının etkin, yeterli ve uyumlu olarak kabul edilebilmesi için:



Şekil 22: Etkinlik, Yeterlilik ve Uyumluluk

Bilgi sistemleri kontrollerinin etkin olması, önemlilik ilkesi çerçevesinde denetime tabi tutulan tüm kontrollerin işletimlerinin etkin olduğunu ve bu kontrollerin, kendilerinden beklenen işlevleri ve kontrol hedeflerini yerine getirdiklerini; uyumlu olması ise, önemlilik ilkesi çerçevesinde denetime tâbi tutulan tüm kontrollerin uyumlu olduğunu ifade eder.

e. Bilgi Sistemleri Bağımsız Denetimi İle Bağımsız Denetim İlişkisi

Bağımsız denetim ile bilgi sistemleri bağımsız denetimi, birbirlerinin kapsam ve sonucunu etkileyecek hususlar ihtiva etmeleri nedeni ile etkileşimli bir yaklaşım içinde planlanıp, uygulanmalıdır. Bu kapsamda;

- Bilgi sistemleri denetçisi, bilgi sistemleri bağımsız denetiminin kapsamını belirlerken ve çalışmalarını yürütürken; denetim görüşünü destekleyecek düzeyde yeterli denetim kanıtı elde edilmesinin yanı sıra, bağımsız denetime ilişkin denetim riski değerlendirmelerini desteklemek için de denetim kanıtı elde edilmesini gözetir.
- Bilgi sistemleri bağımsız denetimine ilişkin görüşün "*şartlı*", "*olumsuz*" ya da "*görüş bildirmekten kaçınma*" şeklinde olması durumunda; görüş ve görüşe esas teşkil eden tespitler bağımsız denetçiye yazılı olarak iletilir. Bu hususlaki sorumluluk denetlenen işletme yönetim kuruluna aittir.
- Bağımsız denetçi tarafından, bağımsız denetim çalışmalarında kullanılmak üzere bilgi sistemleri ve denetimine ilişkin talep edilen bilgi ve belgelerin, bilgi sistemleri denetçisi tarafından bağımsız denetçiye iletilmesi esastır.

f. İç Kontrol ve İç Denetime İlişkin Değerlendirme

Bilgi sistemleri denetçisinin bilgi sistemleri kontrolleriyle sınırlı olmak üzere denetlenen işletmenin iç kontrol ve iç denetim sistemleri bünyesinde önemlilik kriteri çerçevesinde yürüttüğü

çalışmalara ilişkin olarak BDS 315 İşletme ve Çevresini Tanımak Suretiyle Önemli Yanlışlık Risklerinin Belirlenmesi Standardı[14] (BDS 315) ile BDS 610 İç Denetçi Çalışmalarının Kullanılması Standardında (BDS 610) yer alan hükümler kıyasen uygulanır. Burada, bilgi sistemleri denetçisinden beklenen, her ne kadar anılan BDS'ler finansal tabloların denetimine ilişkin olsa da, anılan BDS hükümlerinin bilgi sistemleri denetiminin planlanması, yürütülmesi ve raporlanmasına uyarlanmasıdır. Uygun olan prosedür ve yöntemlerin esas alınarak bilgi sistemleri denetiminin gerçekleştirilmesidir. Anılan standartlara ilişkin açıklamalara aşağıda yer verilmektedir.

BDS 315, denetçinin işletmenin iç kontrolü dâhil işletme ve çevresini tanımak suretiyle, finansal tablolardaki "*önemli yanlışlık*" risklerini belirleme ve değerlendirme sorumluluğunu düzenler. Burada amaç, finansal tablo ve yönetim beyanı düzeylerinde hata veya hile kaynaklı "*önemli yanlışlık*" risklerini belirlemek ve değerlendirmek;böylece "*önemli yanlışlık*" riski olarak değerlendirilen risklere karşı yapılacak işlerin tasarlanması ve uygulanması için bir dayanak oluşturmaktır.

BDS 315'in yeni versiyonunda, bilgi sistemleri konusu iç kontroldeki önemi nedeniyle yoğun bir şekilde ele alınmıştır. Yeni versiyonda, bilgi işleme kontrolleri, işletmenin bilgi sistemindeki bilgi teknolojisi uygulamalarında veya manuel bilgi süreçlerinde bilginin işlenmesiyle ilgili olan ve doğrudan bilginin bütünlüğüyle (diğer bir ifadeyle; işlemlerin ve diğer bilgilerin tamlığı, doğruluğu ve geçerliliğiyle) ilgili riskleri ele alan kontroller olarak tanımlanmıştır. Bilginin bütünlüğüne yönelik riskler, işletmenin bilgi politikalarının (işletmenin bilgi sistemindeki bilgi akışları, kayıtlar ve raporlama süreçlerini tanımlayan politikalardır) etkin olmayan bir şekilde uygulanmaya olan açıklığından kaynaklanır. Bilgi işleme kontrolleri, işletmenin bilgi politikalarının etkin bir biçimde uygulanmasını destekleyen prosedürlerdir. Bilgi işleme kontrolleri otomatik ya da manuel olabilir ve diğer bilgi işleme kontrolleri veya genel bilgi teknolojileri kontrolleri dâhil olmak üzere diğer kontrollere bağlı olabilir.

Denetçi finansal tablo ve yönetim beyanı düzeylerinde, "*önemli yanlışlık*" risklerinin belirlenmesi ve değerlendirilmesine bir dayanak oluşturmak amacıyla risk değerlendirme prosedürlerini uygular. Denetçinin risk belirleme ve değerlendirme süreci, yinelenen ve dinamik bir süreçtir. Ancak, tek başına risk değerlendirme prosedürleri, denetim görüşüne dayanak oluşturacak yeterli ve uygun denetim kanıtı sağlamaz. Risk değerlendirme prosedürleri olarak, işletme yönetiminin, varsa iç denetim fonksiyonundaki uygun kişilerin ve denetçi tarafından uygun görülen diğer kişilerin sorgulanması, analitik prosedürlerin uygulanması ile gözlem ve tetkik kullanılır.

BDS 315'in kıyasen uygulanması, bilgi sistemleri denetçisinin, işletmenin iç kontrolünün (bileşenleriyle birlikte) anlaşılması, önemli kontrol eksikliklerinin belirlenmesine ilişkin prosedürlerin uygulanması ve önemli kontrol eksikliği olabilecek alanların belirlenmesine yönelik olacaktır.

BDS 610, denetim sırasında denetçinin iç denetçilerin çalışmasını kullanması durumunda sorumluluklarını düzenlemektedir. İç denetçilerin çalışmasının kullanılması; ya denetim kanıtının elde edilmesinde iç denetim fonksiyonunun çalışmasının kullanılmasını ya da denetçinin yönlendirmesi, gözetimi ve gözden geçirmesi altında doğrudan yardım sağlaması için iç denetçilerin kullanılmasını içerir. İşletmenin iç denetim fonksiyonu yoksa, bu standart uygulanmaz. Buradaki amaç:

- İç denetim fonksiyonunun çalışmasının veya iç denetçilerden doğrudan yardımın kullanılıp kullanılmayacağına ve kullanılacaksa, hangi alanlarda ve ne düzeyde kullanılabileceğine karar vermek, ve bu kararı verdikten sonra:
- İç denetim fonksiyonunun çalışmasını kullanması hâlinde, bu çalışmanın denetimin amaçları açısından yeterli olup olmadığına karar vermek ve,
- Doğrudan yardım sağlaması için iç denetçileri kullanması hâlinde, iç denetçilerin çalışmasını uygun bir biçimde yönlendirmek, gözetimini yapmak ve gözden geçirmektir.

BDS 610'da işletmenin iç fonksiyonunun değerlendirilmesi kapsamında bu fonksiyonun hangi çalışmasının kullanılıp kullanılmayacağı, hangi alanlarda ne düzeyde kullanılabileceğine karar verilmesi; iç denetçilerin doğrudan yardım sağlaması için kullanılıp kullanılmayacağı, hangi alanlarda

[14] *Standardın adı "Önemli Yanlışlık" Risklerinin Belirlenmesi ve Değerlendirilmesi olarak değiştirilmiştir.*

ne düzeyde kullanılabileceğine karar verilmesi ve bu hususların belgelendirilmesine ilişkin esaslar düzenlenmiştir.

BDS 610'un kıyasen uygulanması, bilgi sistemleri denetçisinin, denetim kanıtı için iç denetim fonksiyonunun çalışmalarının kullanılması ya da denetim kanıtı temini için iç denetçiden yardım alınması hususlarına yönelik olacaktır.

1.3.3.3. Bilgi Sistemleri Bağımsız Denetim Faaliyetlerinde Bulunma Şartları

a. Yetkilendirilecek Kuruluşlarda Aranan Şartlar

Sermaye piyasasında bilgi sistemleri bağımsız denetimi faaliyetinde bulunacak kuruluşların belirli şartları sağlaması gerekmektedir. Bu şartlar:

a) Sermaye piyasasında bağımsız denetimle yetkili kuruluşlar listesinde yer almak. Bağımsız denetim kuruluşları, Seri:X, No:22 Tebliği kapsamında Kurul'ca yetkilendirilmektedir.

b) Bilgi sistemleri bağımsız denetimi faaliyetlerini yürütecek düzeyde yeterli sayı ve nitelikte bilgi sistemleri denetçisi istihdam etmek.

c) Yeterli teknik donanım, belge ve kayıt düzenine sahip olmak.

Her bir bilgi sistemleri bağımsız denetimi için en az biri asil ve biri yedek olmak üzere iki kişiden oluşan bir denetim ekibi oluşturulması gerektiğinden, denetim kadrosunda en az iki sorumlu bilgi sistemleri başdenetçisinin bulunması gerekir. Denetimlerin en az bir kişi olmak üzere işin gerektirdiği sayı ve nitelikte denetçilerden oluşan ekip tarafından gerçekleştirilir. Denetçilerin taşıması gerekli koşullar ayrıca düzenlenmiştir.

Yeterli teknik donanım, belge ve kayıt düzeni koşulu kapsamında, yetkilendirilecek kuruluşlarda fiziksel olarak yeterli donanım (ofis, demirbaş vb.) ve imkanlara sahip olunması; bilgi sistemleri denetimi için denetim metodolojisinin bulunması ve yeterli bir belge ve kayıt düzeninin bulunması gerekmektedir.

b. Bilgi Sistemleri Denetçi Unvanları ve Denetçilere İlişkin Şartlar

Bilgi sistemleri denetçileri, kıdem sırasına göre sorumlu bilgi sistemleri başdenetçisi, bilgi sistemleri başdenetçisi, bilgi sistemleri kıdemli denetçisi, bilgi sistemleri denetçisi ve bilgi sistemleri denetçi yardımcısı unvanlarını alırlar. Bilgi sistemleri denetim kadrosunda yer alacak bilgi sistemleri denetçilerinin taşımaları gereken nitelikler ile görev ve sorumluluklarına aşağıdaki tabloda yer verilmektedir.

Unvan	Tecrübe, Lisans ve Diğer Şartlar	Genel Şartlar	Görev ve Sorumluluklar
Bilgi Sistemleri Denetçisi	- Bilgi Sistemleri Denetçisi Sertifikası (CISA) veya Bilgi Sistemleri Bağımsız Denetim Lisansı (BSBDL) - 3 yıllık mesleki tecrübe - 4 yıllık lisans mezunu	- Müflis olmamaları, yüz kızartıcı ve bilişim alanındaki bir suçtan mahkûm bulunmamaları - Bağımsız denetim faaliyetinde bulunmaktan sürekli olarak yasaklanmamış ve bağımsız denetim faaliyetinde bulunması süreli olarak yasaklananların ise yasaklarının süresi sonunda Kurul'ca kaldırılmış olması - Faaliyet yetki belgelerinden biri veya birden fazlası iptal edilmiş yahut borsa üyeliği iptal edilmiş kuruluşlarda iptalde sorumluluğu bulunan kişilerden olmaması	Denetim programının hazırlanması gibi işin ayrıntılı çalışmalarından sorumludur. Bilgi sistemleri denetçisi, denetçi yardımcılarını işe tahsis etmek, onların çalışmalarına nezaret etmek ve hazırladıkları çalışma kağıtlarını incelemek, işin daha karmaşık ve zor bölümlerini bizzat yürütmek, çalışma programında gereken değişiklikleri, yapmak ve çalışmaları süresince işletme ile olan görüşmeleri yürütmek
Bilgi Sistemleri Kıdemli Denetçisi	- CISA veya BSDL - 6 yıllık mesleki tecrübe - 4 yıllık lisans mezunu		Denetim faaliyetlerinin planlanması, yürütülmesi, çalışma kağıtlarının incelenmesi, gereken

Bilgi Sistemleri Başdenetçisi	- CISA veya BSDL - 10 yıllık mesleki tecrübe - 4 yıllık lisans mezunu	- Sermaye piyasası mevzuatına muhalefetten dolayı haklarında verilmiş mahkûmiyet kararının bulunmaması - Türkiye'de yerleşik olmaları - İlgili mevzuat çerçevesinde sermaye piyasalarında işlem yapmalarının yasaklanmış olmaması - Tam zamanlı çalışma	revizyonların yapılması ve denetlenen işletme yetkilileri ile görüşülmesi gibi konularda denetçilerin sorumluluklarını paylaşır
Sorumlu Bilgi Sistemleri Başdenetçisi	- CISA veya BSBDL - 10 yıllık mesleki tecrübe - Denetim raporlarını yetkili kuruluş adına imzalama yetkisi ve sorumluluğu olduğuna dair beyan ve taahhütleri içeren yönetim kurulu kararı - Kurul onayı - 4 yıllık lisans mezunu		Denetçilerin görev, yetki ve sorumluluklarına ilave olarak, bilgi sistemlerinin BSY Tebliği'ne uygunluğu konusunda karar vermek
Bilgi Sistemleri Denetçi Yardımcısı	- 4 yıllık lisans mezunu		-

Mesleki tecrübe koşulunun sağlanmasında;

- Bilgi sistemleri bağımsız denetimi,

- Profesyonel bilgi sistemleri kontrolü veya güvenliği,

- Bilgi sistemleri geliştirme ve işletimi

faaliyetlerinin herhangi birinde ya da birkaçında geçirilen sürelerin toplamı dikkate alınır.

CISA, İç Denetçi Sertifikası (CIA) ve bilgi sistemleriyle ilgili alanlarda alınan yüksek lisans derecesi ilave 1 yıl, bilgi sistemleriyle ilgili alanlarda alınan doktora derecesi ilave 2 yıl bilgi sistemleri bağımsız denetimi tecrübesi olarak sayılır.

Sorumlu bilgi sistemleri başdenetçiliği unvanı haricindeki diğer unvanlara yapılan terfiler, yetkili kuruluşlar tarafından yapılır. Bilgi, yetenek ve liyakatleri bir üst kıdemin gerektirdiği nitelikte olmayanlar tecrübe şartını sağlasalar dahi bir üst unvana terfi ettirilemezler.

Yetkili kuruluşların bilgi sistemleri bağımsız denetiminde görevlendirilmiş mensuplarının tümünün, yılda en az 20 saat, 3 yılda en az 80 saat bilgi sistemleri bağımsız denetimi alanında sürekli eğitim almaları veya vermeleri zorunludur.

c. Yetkili Kuruluşlar ve Denetçilerin Uyacakları Etik İlkeler

Yetkili kuruluşlar ve bilgi sistemleri denetçileri için KGK tarafından yayınlanan Etik Kurallar kıyasen uygulanır. Söz konusu Etik Kurallar bağımsız denetçiler için oluşturulmuş olmakla birlikte; bilgi sistemleri denetim faaliyetinin finansal tabloların bağımsız denetimi faaliyetine benzer nitelik taşıması nedeniyle büyük ölçüde bilgi sistemleri denetçilerinin de bu kurallara uyması gerekmektedir.

Temel etik ilkeler:

1) Dürüstlük

2) Objektif Olma (Tarafsızlık)

3) Mesleki Yeterlilik ve Özen

4) Sır Saklama

5) Mesleğe Uygun Davranış

Temel etik ilkeler ve uygulaması Çalışma Notu'nun 1.3.6 kısmında detaylı olarak yer almaktadır.

1.3.3.4. Denetim Faaliyetine İlişkin Yükümlülük ve Denetim Metodolojisi

a. Denetlenen İşletmelerin Yükümlülükleri

Denetlenen işletmeler, bilgi sistemleri dokümantasyonunu ve bu dokümantasyonla ilgili her türlü kayıt, bilgi, belge, yapı ve sistemlerini denetime uygun ve hazır hale getirmek ve denetçinin bağımsız denetime yönelik talep ettiği her türlü bilgi ve belgeyi vermekle yükümlüdür. İşletmeler, varsa bilgi sistemleri denetçisi tarafından talep edilen iç denetim raporlarının bir örneğini denetçiye iletmek ve bilgi sistemleri denetçisi ile iç denetçileri arasındaki işbirliğinin sağlanması için gerekli tedbirleri almakla yükümlüdür. İşletme, iç denetçilerin bilgi sistemleri denetçileri tarafından yöneltilen soruları zamanında yanıtlamalarını ve açıklık getirmelerini sağlamalıdır.

Bilgi sistemleri denetçilerince yapılacak tespitler hakkında denetlenen işletme yönetim kurulunun bilgilendirilmesi ile denetçiler ile işletme yönetim kurulu üyeleri ve personeli arasında koordinasyonun sağlanması yönetim kurulunun sorumluluğundadır.

İşletmeler, bilgi sistemlerine ilişkin iç kontrolleri hakkında denetim dönemi itibariyle güvence veren ve yönetim kurulu tarafından onaylanmış olan yönetim beyanını bilgi sistemleri denetçisine sunmakla yükümlüdür. Yönetim beyanı;

1) Amaç (Yönetim beyanının amacı, işletme yönetim kurulunun, bilgi sistemlerine ilişkin iç kontrollerinin bilgi sistemleri bağımsız denetim dönemi açısından etkinlik, yeterlilik ve uyumluluğuna ilişkin değerlendirmede bulunarak, bu çerçevedeki mevcut durum ve yürütülen çalışmalara ilişkin güvence sunmasıdır.),

2) Kapsam (İşletme, yönetim beyanı çerçevesinde bilgi sistemlerine ilişkin iç kontrollerin etkinlik, yeterlilik ve uyumluluğuna ilişkin kanaat oluştururken, bilgi sistemleri bağımsız denetim kapsamını dikkate alır. Bilgi sistemleri dâhilinde değerlendirilecek alanlar, risk odaklı bir bakış açısıyla ve önemlilik kriteri esas alınarak belirlenir. Bu değerlendirme kapsamı, yönetim beyanında bilgi sistemlerinin bütünü için verilecek görüşe makul güvence sunacak ölçüde yeterli denetim kanıtının temin edilmesine imkân sağlayacak şekilde belirlenir. Yönetim beyanı sadece bilgi sistemlerine ilişkin iç kontroller hakkında düzenlenir. Yönetim beyanı oluşturulurken alınan destek hizmetleri de göz önünde bulundurulur.),

3) Dönem (İşletme yönetim kurulu, yönetim beyanını, cari bilgi sistemleri denetim dönemine ilişkin yürütülen çalışmalar ve değerlendirmeler neticesinde oluşturur. Bu kapsamda, esas alınacak dönem 1 Ocak -31 Aralık dönemi olup, yönetim kurulu bu dönemin sonu itibariyle, bilgi sistemleri bağımsız denetim raporu tarihi ile uyumlu olarak beyanda bulunur.),

4) İçerik (Yönetim beyanında açık ve kesin ifadelerle asgari olarak;

a) İşletmenin BSY Tebliği'ne istinaden etkin, yeterli ve uyumlu bir iç kontrol sistemi kurma ve işletme yükümlülüğünün bulunduğu,

b) İlgili birimlerce, iç kontrol sisteminin incelenmiş ve bu sistem hakkında bütün önemli kontrol eksikliklerini ortaya koymak üzere bir değerlendirme yapılmış olduğu,

c) İlgili birimlerce, iç kontrol sistemi hakkında yapılan değerlendirmede bağımsız denetim kuruluşu tarafından gerçekleştirilen çalışmaların kullanılmadığının taahhüt edildiği,

d) İç kontrol sistemi üzerinde -varsa- tespit edilen önemli kontrol eksiklikleri,

e) İç kontrol sisteminin, BSBD Tebliği'nin 10'uncu ve BSY Tebliği'nde belirtilen usul ve esaslar açısından etkinliği, yeterliliği veya uyumluluğuna engel teşkil edecek ve beyan edilenlerin haricinde herhangi bir önemli kontrol eksikliğinin olmadığı,

f) İç kontrol sistemi üzerinde yapılan değerlendirmelerde -dönem sonu itibariyle düzeltilmiş olsa dahi- tespit edilen iç kontrol sistemine ilişkin tüm kontrol zayıflıklarının, kayda değer ve önemli kontrol eksikliklerinin sınıflandırılarak bilgi sistemleri denetçisine sunulduğu,

g) Finansal tablolarda önemli yanlış beyana sebep olan veya başta finansal veriler olmak üzere işletme açısından hassasiyet arz eden verilerin bütünlüğü, tutarlılığı, güvenilirliği, gereken durumlarda gizliliği ve faaliyetlerin sürekliliğini önemli ölçüde etkileyen ya da önemli seviyede olmasa da

yöneticilerin veya iç kontrol sisteminde kritik görevleri bulunan diğer görevlilerin dâhil olduğu tüm suiistimal veya yolsuzluklar,

h) Daha önceki bilgi sistemleri bağımsız denetimlerinde tespit edilip işletmeye sunulmuş ve yetkili kuruluş tarafından çözüldüğü onaylanmamış olan bulguların çözülüp çözülmediğine ilişkin mevcut durumuna yönetim beyanı ekinde yer verildiği,

i) İç kontrol sisteminde gerçekleştirilen incelemeleri takiben, önemli ve kayda değer kontrol eksiklikleri konularında işletme tarafından alınmış olan düzeltici önlemleri de içerecek şekilde, iç kontrol sisteminde veya iç kontrol sistemini önemli derecede etkileyebilecek diğer hususlarda meydana gelmiş olan değişiklikler,

beyan edilir.)

kısımlarından oluşur.

Denetlenen işletme, denetim raporunda ortaya konulan tespitlerin çözümlerine ilişkin taahhütlerini bir aksiyon planı ile karara bağlar ve uygular. Aksiyon planının yürütülmesinin ve bu planda yer alan taahhütlerin zamanında ve eksiksiz olarak yerine getirilmesinin sağlanmasından denetlenen işletmenin yönetim kurulu sorumludur.

b. Yetkili Kuruluş ve Denetçilerin Yükümlülükleri

Bilgi sistemleri denetçileri, mesleğin zorunlu kıldığı mesleki ilkelere ve etik ilkelere uymak, bilgi sistemleri içerisinde yer alabilecek riskleri ve zayıflıkları dikkate alarak mesleki şüphecilik çerçevesinde bir denetim planı hazırlamak, denetlenene sunmak ve uygulamak, yöneticilerin açıklamalarını yeterli denetim kanıtı olarak kabul etmemek ve denetim raporunu oluşturmakla yükümlüdür.

Seri:X, No:22 Tebliği hükümleri uyarınca bağımsız denetim kuruluşlarınca tesis edilmesi gerekli olan kalite güvence sistemi, yetkili kuruluşlar tarafından yapılan bilgi sistemleri bağımsız denetim çalışmalarını ve bilgi sistemleri bağımsız denetim raporlarını da kapsayacak şekilde yürütülmelidir.

Bilgi sistemleri denetçisi, ortaya çıkan hata ve suistimaller hakkında denetlenen işletmenin yöneticilerine ve denetimden sorumlu komitesine her aşamada yazılı olarak bilgi vermek zorundadır.

Yetkilendirmeye ilişkin koşullara ilişkin sunulan belge ve beyanlardaki değişikliklerin, 6 işgünü içerisinde Kurul'a bildirilmesi zorunludur. Denetim kadrosunda meydana gelen değişiklikler, gerekçeleri ile birlikte Kurul'a bildirilmelidir.

Yetkili kuruluşlar, istihdam ettikleri bilgi sistemleri denetçilerinin süreklilik arz edecek şekilde eğitim programlarına katılmalarını sağlamakla yükümlüdür.

Bilgi sistemleri bağımsız denetim faaliyeti sırasında, esas alınan mevzuat hükümlerine uymayan işlemlerin veya olumsuz görüş oluşturmaya veya görüş vermemeye yol açabilecek herhangi bir gelişmenin tespit edilmesi durumunda; denetlenen işletme bunları gidermiş olsa dahi, bu hususun öğrenildiği tarihten itibaren 10 işgünü içinde bilgi sistemleri denetçisi tarafından Kurul'a yazılı olarak bildirilmesi zorunludur. Kanun'a ve diğer kanunlara göre konusu suç teşkil eden hallerde durumun ivedi olarak yetkili mercilere intikali sağlanır ve ayrıca Kurul'a yazılı olarak bilgi verilir.

Bilgi sistemleri denetçisi, bilgi sistemleri bağımsız denetimi sırasında ortaya çıkan, aşağıda belirtilen konular dâhil olmak üzere, önemli bulduğu her konuda denetlenen işletme veya yöneticilerini, yazılı veya sözlü olarak derhal bilgilendirir:

a) Muhtemel kısıtlamalar ve ilave çalışmalar da dâhil olmak üzere bilgi sistemleri bağımsız denetiminin genel yaklaşımı ve kapsamı,

b) Bilgi sistemleri üzerinde önemli bir etkisi olan ya da olabilecek politika oluşturma süreci ile ilgili aksaklıklar, politika uygulamalarındaki sorunlar ya da politika uygulamalarındaki değişiklikler,

c) Denetlenen işletme faaliyetlerinin sürekliliği üzerinde şüphe uyandırabilecek belirsizlikler,

d) Bilgi sistemlerine veya denetim raporuna önemli etkisi olabilecek konularda denetlenen işletme yöneticileri ile olan görüş ayrılıkları,

e) Bilgi sistemleri içerisinde yer alan önemli zayıflıklar ve riskler.

Sözlü olarak bilgilendirmenin yapıldığı durumlarda; bilgi sistemleri denetçisi, bildirilen hususlara ve alınan cevaplara çalışma kâğıtlarında yer vermesi gerekir.

Bilgi sistemleri denetçileri, bilgi sistemleri bağımsız denetimi çerçevesinde ilgililerce kendilerine tevdi edilen dokümantasyon ve belgeleri işlerinin gerektirdiği süre içinde iyi niyetle ve değiştirmeden muhafaza etmekle ve işin bitiminde iade etmekle yükümlüdürler. Denetim kanıtı oluşturan dokümanların kopyaları yetkili kuruluş tarafından saklanabilir.

Yetkili kuruluşlar ve bilgi sistemleri denetçileri, bilgi sistemleri bağımsız denetimi faaliyetleri dolayısıyla öğrendikleri ve ilgili düzenlemelere göre sır kapsamında bulunan bilgilerin kendi nezdlerinde korunmasına ilişkin tedbirleri alır, bu bilgileri kanunen açıkça yetkili kılınanlardan başkasına açıklayamaz ve doğrudan veya dolaylı şekilde kendilerinin veya başkalarının yararına kullanamazlar.

İşletmeler tarafından bilgi sistemleri bağımsız denetimine ilişkin bilgi ve belgelerin bilgi sistemleri denetçilerine verilmemesi halinde, bu durum yetkili kuruluş tarafından Kurul'a ivedilikle bildirilmelidir.

Yetkili kuruluş, bilgi sistemleri denetiminden kaynaklanabilecek riskleri de karşılayabilecek kapsamda mesleki sorumluluk sigortası yaptırmakla yükümlüdür.

Yetkili kuruluş, istihdam ettiği bilgi sistemleri denetçileri tarafından düzenlenecek çalışma kağıtlarını ve denetime ilişkin her türlü bilgi ve belgeyi istenildiğinde Kurul'a göndermek ya da Kurul'un denetime yetkili personeline sunmak zorundadır.

Yetkili kuruluşlar, Seri:X No:22 Tebliği veya BDS'lerin kıyasen uygulanacak hükümleri için yönetim kurulu onayından geçirilmiş uygulama yönergeleri hazırlamakla yükümlüdür. Kıyasen uygulanacak hükümlerde uygulamanın yönlendirilmesinde Kurul yetkilidir.

Bilgi sistemleri denetçileri, son 2 yıl içinde fiilen bilgi sistemleri bağımsız denetim sürecine katıldıkları işletmenin yönetim kurulu başkan ve üyeliği, genel müdür, müdür ve yardımcılığı ile önemli karar, yetki ve sorumluluğu taşıyan pozisyonlarda görev alamazlar.

c. Bilgi Sistemleri Bağımsız Denetim Sözleşmesi

Bilgi sistemleri bağımsız denetimi, denetlenen işletme ile yetkili kuruluş arasında imzalanan denetim sözleşmesi kapsamında gerçekleştirilir. İşletmeler, bilgi sistemleri bağımsız denetimini gerçekleştirecek yetkili kuruluş ile denetim sözleşmesini denetime tabi dönemin ilk 4 ayı içerisinde imzalamakla yükümlüdür. Denetlenecek dönemi izleyen Nisan ayı sonuna kadar denetim sözleşmesinin imzalanması gerekir. Denetim sözleşmesinin kapsamı, BDS 210 hükümleri kıyasen uygulanarak belirlenir. BDS 210 uyarınca yetkili kuruluş;

- Bilgi sistemleri bağımsız denetimin ön şartlarının mevcut olup olmadığını tespit ederek,
- Müşteri işletmenin denetim sözleşmesinin şartlarının aynı şekilde anladığını teyit ederek

denetim sözleşmesini kabul etmeli veya mevcut denetim sözleşmesini devam ettirmelidir. Denetim ön şartlarının sağlanmaması durumunda yetkili kuruluş, bilgi sistemleri bağımsız denetim teklifini kabul etmez.

Yetkili kuruluş, işletme yönetiminin denetim sözleşmesinde bilgi sistemleri denetiminin kapsamını sınırlandıracak şartlar teklif etmesi ve bu sınırlamanın bilgi sistemleri hakkında görüş vermekten kaçınmayı gerektirmesi durumunda, mevzuatla aksi zorunlu kılınmadıkça, bu kapsam sınırlamalarını kabul etmez. Denetim sözleşmesi aşağıdaki hususları içerir:

- Bilgi sistemleri denetiminin amacı ve kapsamı,
- Yetkili kuruluş ve bilgi sistemleri denetçilerinin sorumlulukları,

- İşletme yönetimin sorumlulukları,
- Denetimde esas alınacak bilgi sistemleri yönetimi çerçevesini belirten açıklama,
- Düzenlenecek raporların şekli ve içeriği.

Müteakip denetimler için denetim sözleşmesi şartlarının içinde bulunulan durum ve şartlara göre revize edilmesinin gerekli olup olmadığını ve denetim sözleşmesinin mevcut şartlarının işletmeye tekrar hatırlatılmasına ihtiyaç olup olmadığını değerlendirilmelidir. Yetkili kuruluşun, makul bir gerekçe olmadıkça denetim sözleşmesinin şartlarında değişiklik yapılmasını kabul etmemelidir. Denetimin şartlarında değişiklik olması hâlinde yetkili kuruluş ve denetlenen işletme, bu şartlar üzerinde anlaşmaya varıp, denetimin yeni şartlarını yeni bir denetim sözleşmesiyle veya ilk sözleşmeye ek yapmak suretiyle kayıt altına almalıdır.

Yetkili kuruluş, denetim sözleşmesi şartlarında yapılan bir değişikliği kabul etmesinin mümkün olmaması ve işletme yönetimin geçerli olan denetim sözleşmesine göre denetimin devam etmesine izin vermemesi hâlinde, mevzuatla izin verilmesi hâlinde denetimden çekilmeli ve sözleşme gereğince veya diğer sebeplerle bu durumu, işletmenin üst yönetimden sorumlu olanları, sahipleri veya düzenleyici kurumlar gibi diğer taraflara rapor etme yükümlülüğünün olup olmadığı değerlendirmelidir.

Bilgi sistemleri bağımsız denetim sözleşmesinin herhangi bir nedenle imzalanamaması halinde, konu en geç durumun ortaya çıktığı tarihi izleyen ilk iş gününde Kurul'a bildirilmelidir.

Bir yetkili kuruluşun, işletmeye vereceği bilgi sistemleri bağımsız denetim hizmetinin azami süresinin belirlenmesinde TTK'nın 400'üncü maddesinin ikinci fıkrası hükmü uygulanır. Bu kapsamda, her yıl bilgi sistemleri bağımsız denetimi hizmeti alacak işletmeler için, 10 yılda en çok 7 yıl üst üste bilgi sistemleri bağımsız denetim hizmeti verilebilir ve 3 yıllık ara geçmeden tekrar bilgi sistemleri bağımsız denetim hizmeti verilemez.

Yetkili kuruluşların imzaladıkları bilgi sistemleri bağımsız denetim sözleşmelerini en geç 6 iş günü içinde Kurul'a göndermeleri zorunludur.

Yetkili kuruluş ile işletme anlaşarak bilgi sistemleri bağımsız denetim sözleşmesini sona erdiremezler. Ancak işletmeler ve yetkili kuruluşlar Kurul tarafından onaylanacak haklı gerekçelerin varlığı halinde, yazılı gerekçe göstermek koşuluyla bilgi sistemleri bağımsız denetim sözleşmesini Kurul'dan izin alarak sona erdirebilirler. Sona erme durumunda, yetkili kuruluş çalışma notlarını ve gerekli tüm bilgileri, yerine geçecek olan yetkili kuruluşa devredilmek üzere Kurul'a teslim etmesi zorunludur.

d. Denetim Planı

Bilgi sistemleri bağımsız denetiminin planlanması bakımından BDS 300 hükümleri kıyasen uygulanır. BDS 300 uyarınca denetimin planlaması, denetimin etkin bir şekilde yürütülmesi için denetime yönelik genel denetim stratejisinin oluşturulması ve denetim planının geliştirilmesini içerir. Yeterli bir planlama aşağıdaki hususlarda bilgi sistemleri denetçisine yardımcı olur:

- Denetimin önemli alanlarına dikkatin yoğunlaşması,
- Muhtemel problemlerin zamanında belirlenmesi ve çözüme kavuşturulması,
- Denetimin etkin ve verimli biçimde yürütülmesi için denetimin düzgün biçimde düzenlenmesi ve idare edilmesi,
- Öngörülen risklere karşılık verecek kabiliyet ve yetkinlik sahibi denetim ekibi üyelerinin seçilmesi ve bu kişiler arasında uygun bir iş dağılımı yapılması,
- Denetim ekibi üyelerinin yönlendirilmesi, gözetimi ve yaptıkları çalışmanın gözden geçirilmesini kolaylaştırmak,
- Uygun hâllerde, işletme birimleri denetçileri ile uzmanlar tarafından yapılan çalışmanın koordinasyonunda yardımcı olmak.

Bilgi sistemleri denetçisi, denetimin kapsamını, zamanlamasını ve yönünü belirleyen ve denetim planının geliştirilmesine yönelik rehberlik sağlayan genel denetim stratejisini oluşturmalıdır. Genel denetim stratejisini oluştururken:

- Denetimin kapsamını tanımlayan denetimin özellikleri belirlenir.
- Denetimin zamanlaması ve kurulması gereken iletişimlerin niteliğini planlamak amacıyla denetimin raporlama amaçları belirlenir.
- Mesleki muhakeme kullanılarak, denetim ekibinin çalışmalarının yönlendirilmesinde önemli faktörler değerlendirilir.
- Ön denetim çalışmaları sonuçlarını ve varsa işletme için yürütülen diğer denetimlerden elde edilen bilgilerin ilgili olup olmadığı değerlendirilir.
- Denetimin yürütülmesi için ihtiyaç duyulan kaynakların niteliğini, zamanlamasını ve kapsamı belirlenir.

Denetim planında;

- Planlanan risk değerlendirme prosedürlerinin niteliği, zamanlaması ve kapsamı,
- Planlanan denetim prosedürlerinin niteliği, zamanlaması ve kapsamı
- Planlanan diğer denetim prosedürlerini

tanımlanır. Denetim sırasında gerekmesi durumunda genel denetim stratejisi ve denetim planı güncellenmeli ve değiştirilmelidir. Ayrıca, bilgi sistemleri denetim ekibi üyelerinin yönlendirilmesinin, gözetiminin ve denetim ekibi üyelerinin yaptığı çalışmaların gözden geçirilmesinin niteliği, zamanlaması ve kapsamı da planlanır.

Bilgi sistemleri denetçisi, genel denetim stratejisi, denetim planı ve denetim sırasında bunlarda yapılan her türlü önemli değişiklik ve bunların sebeplerini çalışma kağıtlarında belgelendirmelidir.

e. Denetim Kanıtı, Teknikleri, Örneklemesi ve Kontrol Testi

Bilgi sistemleri bağımsız denetiminde denetim kanıtları, denetim teknikleri ve örneklemesi bakımından BDS 500, BDS 520 Analitik Prosedürler Standardı (BDS 520) ve BDS 530 Bağımsız Denetimde Örnekleme Standardı (BDS 530) hükümleri kıyasen uygulanır.

BDS 500, finansal tablo denetiminde nelerin denetim kanıtlarını oluşturduğunu açıklar ve denetçinin, görüşüne dayanak oluşturan makul sonuçlara ulaşabilmesi amacıyla yeterli ve uygun denetim kanıtı elde etmek için denetim prosedürlerini tasarlama ve uygulama sorumluluğunu düzenler. Aynı zamanda denetim sırasında temin edilen tüm denetim kanıtlarına uygulanır. Diğer standartlar, denetimin belirli yönlerini, belirli bir konuya ilişkin elde edilecek denetim kanıtlarını, denetim kanıtı elde etmek için uygulanan belirli prosedürleri ve yeterli ve uygun denetim kanıtı elde edilip edilmediğine ilişkin değerlendirmeleri kapsar.

Bu BDS'de amaç, denetçinin görüşüne dayanak oluşturan makul sonuçlara ulaşabilmek amacıyla yeterli ve uygun denetim kanıtı elde etmesini sağlayacak denetim prosedürlerini tasarlaması ve uygulamasıdır. Denetim kanıtı, denetçinin, görüşüne dayanak oluşturan sonuçlara ulaşırken kullandığı bilgiler olarak tanımlanmıştır. Denetçi, yeterli ve uygun denetim kanıtı elde etmek amacıyla içinde bulunulan şartlara uygun olan denetim prosedürlerini tasarlamak ve uygulamakla yükümlüdür. Denetim prosedürleri, kontrol testleri ile detay testlerini ve analitik maddi doğrulama prosedürlerini içeren maddi doğrulama prosedürlerinden oluşur. Maddi doğrulama prosedürleri:

- Tetkik: İşletme içinden veya dışından elde edilen, basılı veya elektronik ortamda ya da başka bir depolama ortamında bulunan kayıt veya belgelerin incelenmesini ya da varlıkların fiziki olarak incelenmesini içerir.
- Gözlem: Başkaları tarafından uygulanan bir süreç veya prosedürün izlenmesidir (örneğin, işletme personeli tarafından yapılan stok sayımının veya kontrollerin uygulanmasının denetçi tarafından gözlemlenmesi). Gözlem, bir süreç veya prosedürün işleyişiyle ilgili denetim kanıtı sağlar fakat yapıldığı zamanla sınırlıdır.

- Dış teyit: Üçüncü bir tarafın (teyit eden taraf) doğrudan denetçiye basılı, elektronik ortamda ya da başka bir depolama ortamında verdiği yazılı yanıttan elde edilen denetim kanıtını ifade eder.
- Yeniden hesaplama: Belge veya kayıtların matematiksel doğruluğunun kontrolüdür. Yeniden hesaplama, manuel veya elektronik olarak yapılabilir.
- Yeniden uygulama: Esas olarak işletmenin iç kontrolünün bir parçası olarak uygulanmış olan prosedür veya kontrollerin, denetçi tarafından bağımsız bir şekilde yürütülmesidir.
- Analitik prosedürler: Finansal ve finansal olmayan veriler arasındaki anlamlı ilişkilerin analiz edilmesi yoluyla finansal bilgilerin değerlendirilmesidir. Analitik prosedürler, beklenen değerlerden önemli miktarda farklılık arz eden veya diğer ilgili bilgilerle tutarsızlık gösteren belirlenmiş dalgalanma ya da ilişkilerin gerektiğinde araştırılmasını da kapsar.
- Sorgulama: İşletme içindeki veya dışındaki bilgili kişilerden, finansal ve finansal olmayan konularda bilgi alınmasıdır. Sorgulama, diğer denetim prosedürlerine ek olarak denetim sırasında yoğun bir şekilde kullanılır. Sorgulamalar, resmi olarak yapılan yazılı sorgulamalardan resmi olmayan sözlü sorgulamalara kadar çeşitli şekillerde yapılabilir. Sorgulamalara verilen cevapların değerlendirilmesi, sorgulama sürecinin ayrılmaz bir parçasıdır.

BDS 520, denetçinin analitik prosedürleri maddi doğrulama prosedürü olarak kullanmasını düzenler. Ayrıca, denetimin sonuna doğru, finansal tablolarla ilgili genel bir sonuç oluştururken denetçiye yardımcı olan analitik prosedürleri uygulama sorumluluğunu da ele alır. Denetçinin amacı, analitik prosedürler kullanıldığında ihtiyaca uygun ve güvenilir denetim kanıtları elde etmek ve finansal tabloların denetçinin işletmeye ilişkin anlayışı ile tutarlı olup olmadığına dair genel bir sonuç oluştururken kendisine yardımcı olan analitik prosedürleri denetimin sonuna doğru tasarlamak ve uygulamaktır.

BDS 500 ve 520'nin kıyasen uygulanması, bilgi sistemleri denetçisinin, denetim sırasında uygulayacağı denetim prosedürleri ile elde ettiği denetim kanıtlarının değerlendirilmesine yönelik olacaktır.

BDS 530, denetçinin, denetim prosedürlerinin uygulanmasında denetim örneklemesi kullanmaya karar vermesi durumunda uygulanır. Denetçinin, denetim örneklemini tasarlarken ve seçerken, kontrol testlerini ve detay testlerini uygularken ve örneklemden çıkarılan sonuçları değerlendirirken, istatistiki ve istatistiki olmayan örnekleme yöntemlerini kullanmasını düzenler. BDS 500'ü tamamlayıcı nitelik taşır. Burada denetim örneklemesi kullanırken denetçinin amacı, örneklemin seçildiği anakitle hakkında sonuçlara varmak için makul bir dayanak oluşturmaktır.

BDS 530'un kıyasen uygulanması, bilgi sistemleri denetçisinin, denetim sırasında denetim örnek örneklemesine yönelik olacaktır.

Bilgi sistemleri denetçisi, test edeceği kontrollerin kapsamını, önemlilik ilkesini gözeterek ve test edeceği kontrol kümesinin bilgi sistemleri ile bu sistem üzerindeki kontrollerin bütününün etkinliği, yeterliliği ve uyumluluğu hakkında makul bir güvence sağlayacak şekilde belirlemelidir. Bilgi sistemleri kontrollerinin etkin, yeterli ve uyumlu olduğuna dair görüş verilebilmesi için, incelemeye tâbi tutulan tüm kontrollerin, tasarım ve işletiminin etkinlikleri ve uyumluluklarının test edilmesi gerekir.

Bilgi sistemleri denetçisi, denetim riskini makul düzeye indirebilmek için, test ettiği kontrolle ilişkili önemli veya kayda değer kontrol eksikliği riskinin yüksek olduğu alanlarda tespit riskini düşürecek şekilde testlerini detaylandırır, örneklem hacmini genişletir ve kanıtlarının yeterlilik ve güvenilirlik seviyesini artırmalıdır.

Bilgi sistemleri denetçisi kontrole ilişkin test kapsamını belirlerken ilgili kontrolün uygulanma sıklığı, faal olma durumu açısından güvenilen süre, kontrollerdeki sapma beklentisi gibi kontrol karakteristiklerini dikkate almalıdır.

Bilgi sistemleri denetçisi sadece bilgi toplama tekniğini kullanarak elde ettiği denetim kanıtıyla bir kontrolün etkinlik, yeterlilik ve uyumluluğuna ilişkin görüş oluşturamaz.

Bilgi sistemleri denetçisi, bir kontrolü test ederken dikkate alacağı zaman boyutunu denetim döneminin bütününe ilişkin görüş oluşturacak şekilde belirlemelidir.

1.3.3.5. Bilgi Sistemleri Bağımsız Denetim Raporu

Bilgi sistemleri bağımsız denetim raporu, bilgi sistemleri denetçisinin denetlediği bilgi sistemleri hakkında oluşturduğu görüşünü içerir. Denetim görüşünde bilgi sistemleri ile bu sistem üzerindeki kontrollerin bütününün etkin, yeterli ve uyumlu olup olmadığı hususuna açıkça yer verilir. Bilgi sistemleri denetçisi bu hususstaki kanaatini BSY Tebliği çerçevesinde oluşturur.

a. Görüş Türleri

Bilgi sistemleri bağımsız denetim raporunda aşağıda yer verilen 4 türde görüş belirtilir:

- Olumlu Görüş,
- Olumsuz Görüş,
- Şartlı Görüş,
- Görüş Bildirmekten Kaçınma Görüşü.

Olumlu Görüş: Sorumlu bilgi sistemleri başdenetçisi, yapılan denetim sonucunda herhangi bir önemli kontrol eksikliğinin bulunmaması ve denetim kapsamında herhangi bir kısıtlama ya da engelleme ile karşılaşılmaması durumunda, olumlu görüş bildirir. Olumlu görüş örneği BSBD Tebliği'nin 3 numaralı ekinde yer almaktadır.

Şartlı Görüş: Sorumlu bilgi sistemleri başdenetçisi;

a) Yapılan denetim sonucunda en az bir önemli kontrol eksikliğiyle karşılaşmalarına rağmen, bu eksikliklerin denetlenen işletmenin bilgi sistemlerinin bütününü veya büyük bir kısmını etkilemediğini düşünmesi,

b) Görüş bildirmekten kaçınmayı gerektirecek önemde olmamakla birlikte, denetim faaliyetlerini sınırlayan herhangi bir hususun varlığı veya yeni tesis edilmiş bir sistem hakkında yeterince bilgi edinememesi veya

c) Denetim görüşünün oluşturulması için yeterli ve uygun denetim kanıtının elde edilememesi

durumlarında şartlı görüş bildirir. Şartlı görüş örneği BSBD Tebliği'nin 4 numaralı ekinde yer almaktadır.

Olumsuz Görüş: Sorumlu bilgi sistemleri başdenetçisi, yapılan denetim sonucunda rastlanılan önemli kontrol eksikliklerinin tek başlarına veya beraber değerlendirildiğinde;

a) İşletmenin bilgi sistemlerinin bütününü veya büyük bir kısmını etkilediğine ilişkin kanaat edinmesi veya

b) Yönetim beyanı ile bilgi sistemleri denetçisinin denetlen işletmenin bünyesinde gerçekleştirdiği denetim sonrasında önemli bir kontrol eksikliğinin bütün önemli taraflarıyla eksik veya yanlış aktarılmasından kaynaklanan bir farklılık bulunması

durumlarında olumsuz görüş bildirir. Olumlu görüş örneği BSBD Tebliği'nin 5 numaralı ekinde yer almaktadır.

Görüş Bildirmekten Kaçınma: Sorumlu bilgi sistemleri başdenetçisi, denetim çalışmalarında karşılaşılan belirsizlik ve sınırlamaların görüş belirtilmesini engelleyecek derecede önemli olduğunu düşündüğü durumlarda, bilgi sistemleri hakkında görüş bildirmekten kaçınabilirler. Görüş bildirmekten kaçınma görüş örneği, BSBD Tebliği'nin 6 numaralı ekinde yer almaktadır. Bu tür raporda, görüş bildirmekten kaçınmaya yol açan nedenlere ilişkin denetçi görüşlerine yer verilmesi şarttır.

Olumlu görüş dışındaki görüş türlerinin verilmesi durumunda, BDS 705 Bağımsız Denetçi Raporunda Olumlu Görüş Dışında Bir Görüş Verilmesi Standardı (BDS 705) hükümleri kıyasen uygulanır. Sorumlu bilgi sistemleri denetçisinin olumlu görüş dışında (şartlı, olumsuz veya görüş bildirmekten kaçınma) bir görüş vermesinin gerekmesi durumunda, içinde bulunan şartlara uygun rapor düzenleme sorumluluğu hususunda BDS 705 hükümleri kıyasen uygulanır. BDS 705 kapsamında bilgi sistemleri denetçisi, elde edilen denetim kanıtlarına dayanarak, herhangi bir kontrol eksikliğinin bulunması ve denetim kapsamında herhangi bir kısıtlama ya da engelleme ile karşılaşılması durumunda verilmesi gereken, olumlu görüş dışında uygun bir görüşü, açık bir biçimde raporunda yer verir.

Bilgi sistemleri denetçisi, denetim sözleşmesinin kabulünden sonra, işletme yönetimin bilgi sistemlerine ilişkin şartlı görüş verilmesine veya görüş vermekten kaçınılmasına yol açması muhtemel şekilde denetimin kapsamını sınırladığının farkına varırsa, yönetimden söz konusu sınırlamayı kaldırmasını talep etmelidir. Yönetimin söz konusu sınırlamayı kaldırmayı reddetmesi durumunda, konuyu üst yönetimden sorumlu olanlara iletir ve yeterli ve uygun denetim kanıtı elde etmek için alternatif prosedürleri uygulamanın mümkün olup olmadığına karar verir. Bilgi sistemleri denetçisi, yeterli ve uygun denetim kanıtı elde edemezse, şartlı görüş veya bu görüşün ciddiyetinin iletilmesinde yetersiz kalacağı sonucuna varırsa, mevzuatın izin vermesi ve uygulanabilir olması durumunda, denetimden çekilir veya denetim raporu düzenlenmeden önce denetçinin denetimden çekilmesinin mümkün veya uygulanabilir olmadığı durumda, finansal tablolara ilişkin görüş vermekten kaçınır. Denetimden çekilinmesi durumunda, denetimden çekilmeden önce, denetim sırasında belirlenen ve olumlu görüş dışında bir görüş verilmesine sebep olan hususlara, üst yönetimden sorumlu olanlara iletilir. Olumlu görüş dışında bir görüş verilmesi durumunda, görüş bölümünde duruma göre "*Şartlı Görüş*", "*Olumsuz Görüş*" veya "*Görüşten Kaçınma*" başlıklarından birini kullanır. Yeterli ve uygun denetim kanıtı elde edilemediği için şartlı görüş verilmesi durumunda; verilen görüşte, bu duruma uygun olarak *"... hususunun (veya hususlarının) muhtemel etkileri hariç olmak üzere..."* ifadesini kullanır. Yeterli ve uygun denetim kanıtı elde edilemediği için görüş vermekten kaçınılması durumunda, işletmenin bilgi sistemlerine yönelik görüş bildirilemediği (verilemediği) belirtilir ve dayanak bölümünde tanımlanan hususun (veya hususların) öneminden dolayı, görüşe dayanak teşkil edecek yeterli ve uygun denetim kanıtı elde edilemediği belirtilir. Görüş türlerine ilişkin rapor örnekleri, bu Çalışma Notu ekinde yer almaktadır.

b. Bilgi Sistemleri Bağımsız Denetim Raporunun Temel Unsurları

Bilgi sistemleri bağımsız denetim raporu aşağıdaki unsurları içerecek şekilde düzenlenir:

a) Başlık,

b) Raporun sunulduğu merci,

c) Giriş paragrafı,

d) Denetim çalışmasına ilişkin bilgi,

e) Denetlenen işletmenin bilgi sistemleri hakkında genel bilgi,

f) Denetlenen işletmenin bilgi sistemlerine ilişkin iç kontrol ve iç denetim yapısına ilişkin genel değerlendirme,

g) Denetçi görüşü,

h) Kısaltmalar ve sözlük,

i) Ek veya dipnot dizini.

c. Bilgi Sistemleri Bağımsız Denetim Raporunun Kesinleşmesi ve Bildirim

Bilgi sistemleri bağımsız denetim raporu, sorumlu bilgi sistemleri başdenetçisi tarafından imzalandığında kesinleşir. Bilgi sistemleri bağımsız denetim raporu kesinleşme tarihini izleyen ilk işgünü mesai bitimine kadar denetlenen işletme yönetim kurulu başkanlığına teslim edilmelidir. Yönetim kurulu başkanlığı teslim alınan bilgi sistemleri raporu, en geç 5 işgünü içerisinde raporun kabulüne yönelik yönetim kurulu kararıyla birlikte Kurul'a göndermelidir.

Bilgi sistemleri bağımsız denetim raporu, ilgili denetim döneminin bitimini izleyen 30 gün içinde tamamlanarak Kurul'a gönderilmelidir. Bilgi sistemleri raporlarının son bildirim gününün resmi tatil gününe denk gelmesi halinde, resmi tatil gününü takip eden ilk iş günü, son bildirim tarihidir.

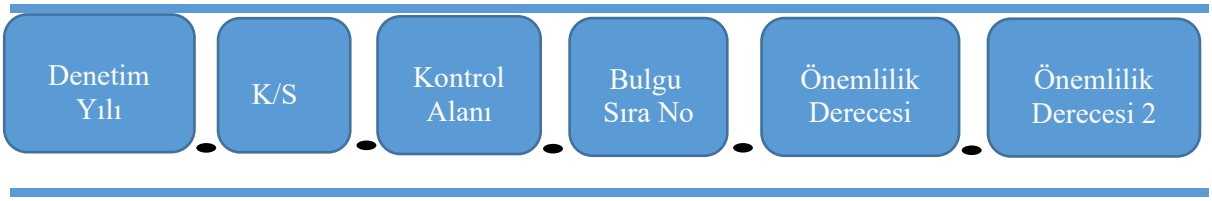
Bu aşamada, bilgi sistemleri bağımsız denetim raporları sadece Kurul'a bildirilmekte olup, başka ortamlarda kamuya açıklanmamaktadır. Bilgi sistemleri bağımsız denetim raporlarının bildiriminde, haklı gerekçelerin varlığı halinde Kurul'a başvurularak ek süre almak mümkündür.

1.3.3.6. Bilgi Sistemleri Bağımsız Denetim Sonuçlarının Raporlanması

a. Tespitler

Bilgi sistemleri denetçisi, yeterli ve uygun denetim kanıtlarıyla desteklemek suretiyle kayda değer kontrol eksikliklerini ve önemli kontrol eksikliklerini sınıflandırarak raporlamalıdır. Tespitler raporlanırken, denetim amaçlarının gerektirdiği kadarıyla, bu tespitlerin kriter ve durumlarına ilişkin bilgilere yer verilmelidir.

Kontrol zayıflığı olarak tanımlanan tespitler, bilgi sistemleri denetçisi tarafından denetlenen işletme yöneticilerine yazılı olarak iletilmelidir. Bilgi sistemleri denetçisi böyle bir yazının yöneticilere iletildiği ifadesi ve kontrol hedefleri bazında tespit ettiği kontrol zayıflıklarının sayısına, raporda yer vermelidir. Geçmiş dönemlerde tespit edilmiş ve bir önceki dönem raporunda halen giderilmediği ifade edilmiş olan tüm kontrol zayıflığı ve eksiklikleri raporda değerlendirilmelidir. Ayrıca, bu kontrol zayıflığı ve eksikliklerinin son durumlarına, devam edip etmediklerine ve işletmenin taahhüt ettiği aksiyon planına uyumuna ilişkin açıklamalara da raporda yer verilmelidir. Bilgi sistemleri denetçisi, denetimlerinde tespit ettiği bulguları aşağıdaki şekilde kodlar:



Şekil 23: Bulgu Kodlama Sistematiği

Denetim yılı alanına, bulgunun tespit edildiği denetim yılı dört hane olarak (2020, 2021, …) yazılır. K/S alanına, konsolide bilgi sistemleri denetimi bulguları için "*K*", solo bilgi sistemleri denetimi bulguları için "*S*" harfi kullanılır. Kontrol alanına bulgunun tespit edildiği kontrol alanının aşağıdaki tabloda yer verilen kısaltması yazılır.

Kontrol Alanı	**Kısaltma**
Bilgi Sistemlerinin Yönetilmesi	BSY
Bilgi sistemleri yönetiminin oluşturulması ve hayata geçirilmesi	BSY-1
Bilgi güvenliği politikası	BSY-2
Üst yönetimin gözetimi ve sorumluluğu	BSY-3
Bilgi sistemleri risk yönetimi	BSY-4
Güvenlik testi	BSY-5
Diğer	BSY-DGR
Bilgi Sistemleri Kontrollerine İlişkin Esaslar	BSK
Bilgi sistemleri kontrollerinin tesisi ve yönetilmesi	BSK-1
Varlık yönetimi	BSK-2
Görevler ayrılığı prensibi	BSK-3
Fiziksel ve çevresel güvenlik	BSK-4

Ağ güvenliği	BSK-5
Kimlik doğrulama	BSK-6
Yetkilendirme	BSK-7
İşlemlerin, kayıtların ve verilerin bütünlüğü	BSK-8
Veri gizliliği	BSK-9
Bilgi sistemlerine ilişkin dış kaynak yoluyla alınan hizmetlerin yönetimi	BSK-10
Müşteri bilgilerinin gizliliği	BSK-11
Müşterilerin bilgilendirilmesi	BSK-12
Üçüncü taraflarla bilgi değişimi	BSK-13
Denetim izlerinin oluşturulması	BSK-14
Zaman Senkronizasyonu	BSK-15
Bilgi Güvenliği İhlali	BSK-16
Bilgi sistemleri edinimi, geliştirilmesi ve idamesi	BSK-17
Bilgi sistemleri sürekliliği	BSK-18
Değişiklik yönetimi	BSK-19
Diğer	BSK-DGR

Bulgu sıra no alanı, solo bilgi sistemleri denetimi raporunda yer alan tüm bulgular, tespit edildiği süreç ve denetim alanından bağımsız olarak, her yıl için 1'den başlayacak şekilde numaralandırılır. Konsolide bilgi sistemleri denetimi raporundaki bulgular da, tespit edildiği ortaklık, süreç ve denetim alanından bağımsız olarak, her yıl için 1'den başlayacak şekilde numaralandırılır. Numaralandırma sonrasında bulguya ait sıra no bilgisi üç haneli olarak girilir (001, 162, … gibi).

Önemlilik derecesi analına bulgu ilk tespit edildiğinde, bulguya verilen önemlilik derecesi girilir. Bu bilgi takip eden dönemlerde değiştirilmez. Kontrol zayıflığı olarak sınıflandırılan bulgular için "*KZ*", kayda değer kontrol eksikliği olarak sınıflandırılan bulgular için "*KD*" ve önemli kontrol eksikliği olarak sınıflandırılan bulgular için "*ÖK*" kısaltmaları kullanılır.

Önemlilik derecesi 2 alanına, önceki dönem bulgularının önemlilik derecesinde, cari dönem itibariyle değişiklik oluştuğu durumlarda, bulgunun yeni önemlilik derecesi girilir. Bulgunun önemlilik derecesinin birden fazla değiştirildiği durumlarda, bu alana bulguya son durum itibariyle verilen önemlilik derecesi girilir. Bulgunun önemlilik derecesinde bir değişiklik yoksa bu bölüm boş bırakılır.

Örnek kodlamalar;

2020.S.BSY-1.003.ÖK.KD

2021.S.BSK-2.152.ÖK

2022.K.BSY-3.045.KD

Bilgi sistemleri denetçisi, topladığı denetim kanıtlarına dayanarak sahtecilik, kanuna aykırı uygulamalar, sözleşme ihlali, suiistimal, çift kayıt sistemi veya mükerrer bilgi sistemleri gibi hallerden bir veya birkaçının bulunduğu kanaatine varırsa, bu hususlara raporunda yer vermelidir. Bu hususlar ayrıca sorumlu bilgi sistemleri başdenetçisi tarafından yazılı olarak Kurul'a ivedilikle bildirilmelidir.

b. Denetlenen İşletme Görüşleri

Bilgi sistemleri denetçisi, tespit edilen eksiklikler, varsa bunlara ilişkin olarak yapılması planlanan düzeltme çalışmaları ve bu çalışmaların olası sonuçları hakkında denetlenen işletmenin görüşlerine raporunda yer vermelidir. Bilgi sistemleri denetçisi, geçmiş dönemlerde tespit edilmiş ve bir önceki dönem raporunda halen giderilmediği ifade edilmiş kontrol zayıflığı ve eksikliklerine ilişkin denetlenen işletmenin görüşlerine ve denetlenenin söz konusu zayıflık ve eksikliğin giderilmesine ilişkin yaptığı çalışmalara raporunda yer vermelidir. Raporda, denetlenen işletmenin görüş bildiremediği veya görüş bildirmeyi reddettiği durumlarda, nedenleriyle birlikte yer verilmelidir.

c. Tespitlere İlişkin Sonuç Değerlendirmesi

Bilgi sistemleri denetçisi, denetim amaçları, denetim tespitleri ve varsa denetlenen işletmenin görüşlerini yorumlayarak kendi çıkarımları ve görüşleri doğrultusunda değerlendirmelere raporunda yer vermelidir. Raporda denetimde tespit edilen hususların nasıl anlaşılması gerektiği hakkında yorum yapmalıdır. Denetlenen işletme görüşlerine katılmadığı veya planlanan düzeltme çalışmalarının uygun olmadığını düşündüğü takdirde buna sonuç değerlendirmesinde ayrıca yer vermelidir. Denetlenen işletmenin görüşlerini haklı bulması halinde, bunlara ilişkin düzeltmeleri raporunda yapmalıdır.

Herhangi bir kontrol zayıflığının ve eksikliğinin düzeltildiğine dair bir beyanın rapor tarihinden önce denetlenen tarafından bilgi sistemleri denetçisine ulaştırılması durumunda, tespit edilen her bir husus için birer defaya mahsus olmak koşuluyla, bilgi sistemleri denetçisi denetlenenin beyanını doğrulamak için bu tespitin son durumunu tahlil eder, kontrol zayıflığının ve eksikliğinin ortadan kalktığı kanaatine ulaşırsa, düzeltme yapıldığı bilgisine raporun tespite ilişkin sonuç değerlendirmesi bölümünde yer vermelidir.

Bilgi sistemleri denetçisi, geçmiş dönemlerde tespit edilmiş ve bir önceki dönem raporunda halen giderilmediği ifade edilmiş olan kontrol zayıflığı ve eksikliğine ilişkin tespitlere ait sonuç değerlendirmesi bölümünde konunun çözümüne ilişkin denetlenen tarafından aksiyon planına uyumla birlikte, zayıflık ve eksikliğin devam durumunu;

- devam etmektedir,
- kısmen düzeltilmiştir veya
- düzeltilmiştir

şeklinde raporunda ifade etmelidir.

1.3.4. Bilgi Sistemleri Denetimi İle İlgili Diğer Mevzuat

Ülkemizde bilgi sistemleri denetimi ile ilgili diğer mevzuata bakıldığında, bilgi sistemlerinin öneminden dolayı birçok kamu kurumu tarafından mevzuatlarla düzenlendiği görülmektedir. Bu bölümde, belirli başlı mevzuatlar ele alınacaktır.

1.3.4.1. Bankacılık Düzenleme ve Denetleme Kurumu (BDDK)

Ülkemizde bilgi sistemleri bağımsız denetimine ilişkin ilk düzenleme BDDK tarafından yapılmıştır. BDDK düzenlemesinin temelde üç ayağı olduğu görülmektedir. Birincisi, bilgi sistemleri denetimi, ikincisi bilgi sistemleri denetiminin raporlaması ve üçüncüsü ise bilgi sistemleri yönetim ilkeleridir. Konuya ilişkin ilk olarak düzenleme geçmişine yer verildikten sonra, son düzenlemeler hakkında kısaca açıklama yapılacaktır.

BDDK'nın bankalar için ilk düzenlemesi, 16.05.2006 tarih ve 26170 sayılı Resmi Gazete'de yayımlanan "*Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik*"tir. Bu Yönetmelik ile bankaların bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemlerinin denetimi, bağımsız denetim kuruluşlarının yetkilendirilmesi, tarafların yükümlülükleri ve bilgi sistemleri denetiminin raporlanmasına ilişkin esaslar belirlenmiştir. Yönetmelik ile uygulama kontrollerinin her yıl, genel kontrol alanlarının ise 2 yılda bir kez denetlenmesi zorunlu kılınmıştır. Bu Yönetmelik, 13.01.2010 tarih ve 27461 sayılı Resmi Gazete'de yayımlanan "*Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik*" ile yürürlükten kaldırılmıştır. Bu Yönetmelik ile, bilgi sistemleri ve bankacılık süreçlerinin denetimine ilişkin genel ilkeler ve esaslar ile denetim raporlarına ilişkin esaslar düzenlenmiştir. Yönetmelik'te, genel kontroller, tesis edilmelerinde esas alınan çerçeve, standart ya da metodolojiden bağımsız olarak bankalarda bilgi sistemleri yönetiminde esas alınacak ilkelere ilişkin BDDK tarafından yapılan düzenlemelerdeki hükümler gözetilerek, COBIT'e göre denetim yapılacağı hüküm altına alınmıştır. Benzer şekilde Yönetmelikte hüküm bulunmaması durumunda uluslararası denetim standartları ile COBIT'in esas alınacağı belirtilmiştir. Son olarak bu Yönetmelik de 31.12.2021 tarih ve 31706 6. Mükerrer sayılı Resmi Gazete'de yayımlanan "*Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Hakkında Yönetmelik*" ile yürürlükten kaldırılmıştır.

BDDK'nın bankalar için ikinci düzenlemesi, 05.12.2006 tarih ve 26367 sayılı Resmi Gazete'de yayımladığı "*Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri*

Denetimine İlişkin Rapor Formatı Hakkında Tebliğ"i ile bilgi sistemleri denetiminin raporlanması ve rapor formatlarına ilişkin esasları belirlemiştir. Bu Tebliğ, 13.01.2010 tarih ve 27461 sayılı Resmi Gazete'de yayınlanan "*Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimine İlişkin Rapor hakkında Tebliğ*" ile, bu Tebliğ ise 25.03.2022 tarih ve 31789 sayılı Resmi Gazete'de yayımlanan "*Bilgi Sistemleri ve İş Süreçleri Bağımsız denetimine İlişkin rapor Hakkında Tebliğ*" ile yürürlükten kaldırılmıştır.

BDDK'nın bankalar için üçüncü düzenlemesi 14.09.2007 tarih ve 26643 sayılı Resmi Gazete'de yayımlanan "*Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ*"i ile bankaların, faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetiminde esas alınacak asgari usul ve esasları düzenlenmiştir. Bu Tebliğ, 15.03.2020 tarih ve 31069 sayılı Resmi Gazete'de yayınlanan "*Bankalarda Bilgi sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğin Yürürlüktün Kaldırılmasına Dair Tebliğ*" ile yürürlükten kaldırılmıştır. Son olarak 15.03.2020 tarih ve 15.03.2020 tarihli Resmi Gazete'de yayımlanan "*Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik*" ile bankaların bilgi sistemleri yönetimine ilişkin usul ve esaslar belirlenmiştir.

1.3.4.1.1. Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Hakkında Yönetmelik

Bu Yönetmelik ile BDDK gözetimi altındaki tüm kuruluşlar (bankalar, finansal kiralama şirketleri, faktöring şirketleri, finansman şirketleri, tasarruf finansman şirketleri, risk merkezi, bilgi alışverişi kuruluşları vb.) ile bilgi sistemleri bağımsız denetimine ilişkin rapor oluşturulması amacıyla sınırlı olmak üzere bankaların konsolidasyon kapsamındaki ortaklıkların bilgi sistemleri ve iş süreçlerinin bilgi sistemleri denetimi ile bu denetimi gerçekleştiricek yetkilendirilmiş bağımsız denetim kuruluşlarına ilişkin usul ve esaslar belirlenmiştir. Yönetmelik ile düzenlenen bilgi sistemleri bağımsız denetimine ilişkin kavramlar ve esaslar önemli ölçüde BSD Tebliği ile uyumludur.

Yönetmelik ile daha önceki yönetmelikte düzenlenen bilgi sistemleri ve iş süreçlerinin denetimine ilişkin genel kavramlar, yetkilendirilecek bağımsız denetim kuruluşları ve bilgi sistemleri denetçilerinde aranacak koşullar, yetkinin kaldırılması, tarafların yükümlülükleri, bilgi sistemleri ve iş süreçleri denetimine ilişkin esaslar, denetim metodolojisine ilişkin esaslar, bilgi sistemleri denetim sözleşmesine ilişkin esaslar ve denetim raporu ve bildirimine ilişkin esaslar geliştirilmiş ve bilgi sistemleri bağımsız denetim siciline ilişkin esaslar ilk olarak düzenlenmiştir. Önceki yönetmelikte bilgi sistemleri denetiminin COBIT'e göre yapılacağı ile hüküm bulunmaması durumunda uluslararası denetim standartlarının yanında COBIT'in esas alınacağı hususuna, bu Yönetmelik'te yer verilmeyerek, bilgi sistemleri denetiminde COBIT referansı kaldırılmış ve bilgi sistemleri denetiminin bu Yönetmelik'teki hükümler kapsamında yapılacağı hüküm altına alınmıştır.

Yönetmelik ile bilgi sistemleri bağımsız denetiminin, yetkilendirilmiş bağımsız denetim kuruluşları ve bilgi sistemleri bağımsız denetimi yapmak için dış hizmet alınan kuruluşlar[15] tarafından gerçekleştirileceği hüküm altına alınmıştır. Tanımlar kısmında, "*bilgi sistemleri bağımsız denetimi*", bilgi sistemleri yönetimi kapsamında yer alan süreç, faaliyet, yazılım ve donanım gibi bilgi sistemi unsurları ve denetlenenin faaliyetlerine ilişkin süreçler ile bu sistem ve süreçler dâhilinde tesis edilen iç kontrollerin değerlendirilmesi sonucunda görüş oluşturulması ve rapora bağlanması aşamalarından oluşan süreç olarak; genel kontroller, bilgi sistemlerinden beklenen fonksiyonların doğru bir şekilde yerine getirilmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli güven ortamının oluşturulmasını ve iş süreçleri üzerindeki kontrollerin işlevselliği için güvenilir bir ortamın sağlanmasını hedefleyen, bilgi sistemlerini oluşturan sistemler, bileşenler, süreçler ve verinin tamamına veya büyük bir bölümüne tatbik edilen kontroller ile bu kontrollerin tatbik edilmesini sağlayan politika ve prosedürler olarak; iş süreçleri, bankaların faaliyetlerine ilişkin tesis edilen iş süreçleri ile risk merkezi ve bilgi alışverişi kuruluşlarının ilgili mevzuatı çerçevesinde yürüttükleri faaliyetler kapsamındaki iş süreçleri olarak; kontrol, iş hedeflerinin gerçekleştirilmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli derecede güvenceyi oluşturma amacı güden politikalar, prosedürler, uygulamalar ve organizasyonel yapıların tamamı olarak;

[15] *Bankaların Bağımsız denetimi Hakkında Yönetmelik kapsamında bankalarda bağımsız denetim yapma yetkisini haiz bağımsız denetim kuruluşlarının bu Yönetmelik kapsamında izin alarak bilgi sistemleri denetim faaliyetini gerçekleştirmek için hizmet aldığı dış hizmet kuruluşudur.*

kontrol hedefi ise belirli bir bilgi sistemleri aktivitesi içinde kontrol prosedürleri oluşturarak istenen bir sonucun veya bir amacın gerçekleştirilmesini sağlayan hedefler olarak tanımlanmıştır. Yönetmelikte, önemlilik, kontrol zafiyetlerinin sınıflandırılması, etkinlik, yeterlilik ve uyumluluk, denetim risk türleri gibi pek çok kavram BSD Tebliğ'indekine benzer şekilde tanımlanmıştır.

Bilgi sistemleri bağımsız denetimi, "*BSD*" olarak kısaltılmış ve bankalar, risk merkezi ve bilgi alışverişi kuruluşlarının bilgi sistemleri ve iş süreçlerinin denetime tabi olduğu; diğer kuruluşların ise sadece bilgi sistemlerinin denetime tabi olduğu düzenlenmiştir. Bu kapsamda, yetkilendirilecek kuruluşlar için üç koşul getirilmiştir. Bankalar, risk merkezi ve bilgi alışverişi kuruşularında bilgi sistemleri ve iş süreçleri denetimi yapacak yetkili kuruluşlar için bankalarda bağımsız denetim yapma yetkisine sahip bağımsız denetim kuruluşu olma koşulu getirilirken ; diğer kuruluşların bilgi sistemleri denetimi yapacak yetkili kuruluş için sadece KGK yetkilendirilmesi yeterli görülmüştür. Aynı olan diğer iki koşuldan birincisi, yeterli sayı ve nitelikte denetçi ve etkin bir bilgi sistemine sahip olma; ikincisi ise kalite kontrol sistemine ilişkin yapı ve yazılı politikalara sahip olmadır.

Bankalarda bağımsız denetim yapma yetkisini bulunan bağımsız denetim kuruluşları, BDDK'dan izin alarak bilgi sistemleri denetim faaliyetini dış hizmet alımı yoluyla gerçekleştirebilir. Bağımsız denetim kuruluşunun bilgi sistemleri denetim hizmetlerini dış hizmet alımı yoluyla gerçekleştirmesi durumunda, ilgili faaliyetler ve bu Yönetmelik kapsamındaki yükümlülüklerden kendisi ve dış hizmet kuruluşu adına nihai olarak sorumludur. Dış hizmet kuruluşu birden fazla bağımsız denetim kuruluşuna hizmet verebilir. Bir bağımsız denetim kuruluşu, bir seferde en fazla üç dönem için dış hizmet alımı ile bilgi sistemleri denetimi yapma izni başvurusunda bulunabilir. İzin süresi dolduğunda tekrar başvuruda bulunabilir. Dış hizmet kuruşulu bilgi sistemleri bağımsız denetimi gerçekleştirebilmesi için bu Yönetmelik kapsamında, bağımsız denetim kuruluşu ile sözleşme yapmış olması gereklidir. Dış hizmet kuruluşunun;

- Denetçilerinin bu Yönetmelikte tanımlanan denetçi niteliklerini haiz olması,

- Denetim ekipleri içerisinde yeterli sayıda ve nitelikte denetçi istihdam etmesi,

- Denetçisinin, geçmişte görev aldığı bilgi sistemleri bağımsız denetim faaliyetlerinde, denetim ilkelerine bağlı ve denetçi bağımsızlığı ilkesini zedelememiş olması,

- Denetim faaliyetlerinde rotasyona ilişkin hükümlere uyulması,

şarttır.

Yönetmelik'te, denetçi unvanları kıdem sırasına göre bilgi sistemleri bağımsız başdenetçisi, bilgi sistemleri bağımsız kıdemli denetçisi ve bilgi sistemleri bağımsız denetçisi olarak düzenlenmiştir. Bunların dışındaki unvanlar ve şartları yetkili kuruluşun takdirine bırakılmıştır. Mesleki tecrübe sayılacak hususlar BSBD Tebliği ile aynı şekilde düzenlenmesine karşın; bilgi sistemleri bağımsız denetçisinin 3 yıllık mesleki tecrübesinin en az 1 yılının fiilen bilgi sistemleri denetimi; kıdemli bilgi sistemleri bağımsız denetçisinin 6 yıllık mesleki tecrübenin en az 2 yılını fiilen bilgi sistemleri denetimi, bilgi sistemleri bağımsız başdenetçisinin ise 10 yıllık mesleki tecrübenin en az 3 yılının fiilen bilgi sistemleri denetimi tecrübesi olması gerektiği hüküm altına alınmıştır. Ayrıca, bilgi sistemleri bağımsız başdenetçilik unvanı için BDDK uygun görüşünün alınması gerekmektedir. BSD Tebliğ'inde sadece sorumlu bilgi sistemleri başdenetçisinin Kurul onayını alması gerekmektedir. Bilgi sistemleri bağımsız başdenetçileri, son iki yıl içinde denetim sürecine katıldıkları denetlenenlerde ve bağlı ortaklıklarında görev alamazlar.

Bu Yönetmelik ile, CISA ve CIA belgelerinin mesleki tecrübe olarak değerlendirilmesindeki ayrıcalıkları ve bilgi sistemleri başdenetçileri için zorunlu unsurlar arasında yer alan CISA sahibi olma şartı kaldırılmıştır. Bilgi sistemleri bağımsız denetim kuruluşları ve denetçiler için sicil uygulaması getirilmiştir. Bu kapsamda yetkili bağımsız denetim kuruluşları ile bilgi sistemleri bağımsız başdenetçisi unvanına sahip olan denetçiler, sicil numarası verilerek BDDK tarafından sicile kaydedilmektedir. Bilgi sistemleri bağımsız denetim kuruluşlarına veri güvenliği konusunda yeni yükümlülükler getirilmiştir. Destek hizmeti kuruluşları ifadesi dış hizmet kuruluşu şeklinde düzenlenerek kapsamı genişletilmiştir. Bağımsız denetim terminolojisinin standardizasyonunun sağlanabilmesi adına KGK tarafından yayımlanan standartlara referans verilmiştir.

Yönetmelik uyarınca, bankalar, risk merkezi ve bilgi alışverişi kuruluşlarında iş süreçleri bağımsız denetimi her yıl, bilgi sistemleri bağımsız denetimi ise 2 yılda bir kez yapılacaktır. Bilgi sistemleri denetimi yapılmayan yıllarda bilgi sistemleri denetçisi tarafından, geçmiş dönemden gelen bulguların değerlendirmesi gerekir ve ayrıca denetçi bilgi sistemi ortamında meydana gelen önemli değişiklikleri ve önemlilik kriteri kapsamında incelenmesini gerekli gördüğü süreçleri denetim kapsamına alabilir. Süreçlerin kapsama alınma sebeplerine ilişkin değerlendirmelere raporda yer verilmelidir. Diğer finansal kuruluşların, 3 yılda bir bilgi sistemleri bağımsız denetimi yaptırma yükümlülüğü bulunmaktadır. BDDK gerekli gördüğü hallerde denetlenenlerden herhangi biri ya da tüm denetlenenler için, bu denetimlerin kapsamını ve sıklığını farklılaştırabilir.

Bankalar için konsolide bilgi sistemleri bağımsız denetimi kapsamında bağımsız denetime tâbi tutulacak kuruluşlar, denetlenenin konsolide finansal tablolarının oluşturulmasına ilişkin BDDK tarafından yapılan düzenlemelerde yer alan ve konsolide finansal tabloların oluşturulmasına dahil edilecek kredi kuruluşu veya finansal kuruluş niteliğine sahip kuruluşların tespitinde esas alınan hükümler doğrultusunda belirlenir. Bu kapsamda, denetçi bağımsız denetime tâbi tutacağı ortaklıklarda gerçekleştireceği bilgi sistemleri bağımsız denetiminin kapsamını, önemlilik kriterini kullanarak, konsolidasyona esas finansal bilgiyi üreten bilgi sistemleri ve süreçler üzerindeki kontrollerin etkinlik, yeterlilik ve uyumluluğunun tespit edilmesini sağlayacak şekilde yazılı olarak belirler.

Yönetmelik ile denetçinin denetim çalışmasının sonunda, tespit ettiği her bir kontrol zayıflığını ayrı ayrı incelemesi ve bu zayıflıkları hem tek başlarına, hem de birlikte oluşturacakları farklı kombinasyonlarla değerlendirerek bunların kayda değer kontrol eksikliği veya önemli kontrol eksikliği olarak sınıflandırılmasını nitel ve nicel yöntemler kullanarak gerçekleştirmesi yükümlü kılınmıştır. Denetçi, denetim esnasında aşağıdaki alanlardan herhangi birinde kontrol zayıflığı ile karşılaşması durumunda bunları en azından kayda değer kontrol eksikliği olarak kabul etmelidir:

- Türkiye Muhasebe Standartlarının uygulanmasına ilişkin politikalar,

- Denetlenenin tabi olduğu mevzuata istinaden yayımlanan alt düzenlemeler ve talimatların gereğinin yerine getirilmesine ilişkin kontroller,

- Sahteciliği önleyen kontroller veya programlar,

- Rutin veya sistematik olmayan işlemler,

- Yılsonu finansal raporlama süreci.

Yönetmelik ile denetçi, aşağıdaki durumlardan herhangi biriyle karşılaşması halinde bunları en azından kayda değer kontrol eksikliği olarak kabul etmeli ve önemli kontrol eksikliğine güçlü birer işaret olarak algılamalıdır:

- Hata veya suistimal nedeniyle, denetlenenin varlık ve yükümlülüklerinin farklı şekilde yansıtılarak mevzuatta tanımlanan ve yasal yükümlülükler bakımından denetlenen ile ilgili alınması gereken kararları veya sağlıklı bir finansal değerlendirme yapılmasını etkileyecek şekilde, önceden yayımlanmış olan finansal tablolar üzerinde düzeltmeler yapılması,

- Cari döneme ait finansal tablolarda veya verilerde denetlenenin iç kontrol ve/veya iç denetim faaliyetleri sırasında önceden fark edilmemiş olan önemli bir yanlış beyanın denetim esnasında denetçi tarafından tespiti,

- Denetlenenin farklı birimlerinden aynı hususa ilişkin olarak gelen bilgi, belge ve veriler arasında tutarsızlık olduğunun tespit edilmesi,

- Denetlenenin yönetimi tarafından denetçiye verilen beyanlarda kasıt içermese dahi önemli bir yanlış beyanın tespit edilmesi,

- Aksiyon planında yer verilen taahhütlerin yerine getirilmemiş olması,

- Bankanın büyüklüğü dikkate alınarak iç denetim ve risk yönetim fonksiyonlarının etkin bir iç kontrol ortamının tesis edilmesi için gerekli olduğunun düşünüldüğü durumlarda, bilgi sistemlerine yönelik söz konusu fonksiyonların bulunmaması veya etkin olmaması,

- Bilgi sistemleri ile denetlenenin faaliyetlerine ilişkin süreç ve sistemler kapsamında mevzuata uyum kontrolünü sağlayacak bir birimin/fonksiyonun bulunmaması veya etkin olmaması,

- Yönetici veya yöneticilerin dâhil olduğu küçük dahi olsa bir sahteciliğin tespit edilmesi,

- Yöneticilere iletilmiş olan kayda değer bir kontrol eksikliğinin makul bir süre geçmesine rağmen hala düzeltilmemiş olması,

- Etkin bir iç kontrol ortamının tesis edilmemiş olması,

- Bankalarda denetim komitesince, muhasebe, finansal raporlama ve iç kontrol sistemi üzerinde etkin bir gözetimin tesis edilmemiş olması.

Yönetmelik uyarınca, bilgi sistemleri denetim raporları, BDDK tarafından aksi belirtilmedikçe denetlenenin finansal tablolarının bağımsız denetim raporuyla birlikte tamamlanır. Bu raporlar, bankalar, risk merkezi ve bilgi alışverişi kuruluşlarında denetimden sorumlu bilgi sistemleri bağımsız başdenetçisi ile yetkili kuruluşun sorumlu denetçisi; diğer finansal kuruluşlarda bilgi sistemleri bağımsız başdenetçisi tarafından imzalanması gerekmektedir. Düzenlenen raporlar, bankalar, risk merkezi ve bilgi alışverişi kuruluşlarında yetkili kuruluşu temsil ve ilzama yetkili olanların imzasını taşıyan bir yazı ekinde denetlenenin yönetim kuruluna, bankalarda ayrıca denetim komitesine ve risk merkezinde risk merkezi yönetimine iletilmelidir. Diğer finansal kuruluşlarda düzenlenen rapor, yetkili kuruluşu temsil ve ilzama yetkili olanların imzasını taşıyan bir yazı ekinde denetlenenin yönetim kurulu başkanlığına iletilmelidir. Bu raporlar içeriği gizli bilgi niteliği taşır ve herhangi bir ortamda yayımlanmaz. Denetlenenler, denetim sonuçlarını içerecek beyanatlar veremezler ve bu hususları reklam amaçlı kullanamazlar.

Bu Yönetmelikte hüküm bulunmayan hallerde KGK tarafından yayınlanan BDS 300, BDS 402, BDS 500, BDS 530 ile ilgili paragrafları bilgi sistemleri bağımsız denetimine kıyasen uygulanacağı belirtilmiştir.

1.3.4.1.2. Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik

Bu Yönetmelik ile bankaların faaliyetlerini yürütürken kullandıkları bilgi sistemlerinin yönetimi ile elektronik bankacılık hizmetlerinin sunulmasında ve bunlara ilişkin risklerin yönetiminde esas alınacak asgari usul ve esaslar ile tesis edilmesi gereken bilgi sistemleri kontrollerini düzenlemektir.

a. Kavramlar

Yönetmelikte, daha çok Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmeliği'ne atıflar yaparak kavramlar tanımlanmıştır. Bu kapsamda, bilgi sistemleri, bilginin toplanması, işlenmesi, saklanması, dağıtımı ve kullanımına yönelik insan kaynağı, operasyonel faaliyetler ve süreçler ile bunlarla etkileşim içinde bulunan bilgi teknolojileri olarak; bilgi teknolojileri, herhangi bir biçimdeki verinin, girişinin yapılması, saklanması, işlenmesi, iletilmesi ve çıktılarının alınması için kullanılan donanım, yazılım, iletişim altyapısı ve ilgili diğer teknolojiler olarak; bilgi sistemleri yönetimi, bankaca gerçekleştirilen faaliyetlerin ve verilen hizmetlerin etkin, güvenilir ve kesintisiz bir şekilde yürütülmesine; mevzuattan kaynaklanan yükümlülüklerin yerine getirilmesine; muhasebe ve finansal raporlama sisteminden sağlanan bilgilerin bütünlüğünün, tutarlılığının, güvenilirliğinin, zamanında elde edilebilirliğinin ve gereken durumlarda gizliliğinin sağlanması amacıyla uygun bilgi sistemleri ortamının tesis edilmesine; bilgi sistemleri kaynaklarının verimli olarak kullanılmasına; bilgi sistemlerinin kullanılmasından kaynaklanan risklerin kontrolünün ve izlenmesinin sağlanmasına; bu amaçla gerekli sistemsel ve yönetsel önlemlerin alınmasına ilişkin faaliyetler olarak; bilgi varlığı ise, bankacılık faaliyetlerinin yürütülmesinde kullanılan veriler ile bu verilerin taşındığı, saklandığı, iletildiği veya işlendiği sistem, yazılım, ağ cihazları, bilg teknolojileri donanımları, iş süreçleri gibi banka için değeri olan varlık olarak tanımlanmıştır.

b. İçerik

Yönetmelik'in "*Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi*" başlıklı ikinci kısmının bilgi sistemleri yönetişimi bölümünde yönetim gözetimi, roller ve sorumluluklar ile bilgi sistemleri politika, prosedür ve süreç dökümanları; bilgi sistemleri risklerinin yönetilmesi bölümünde bilgi varlıkları envanteri ve sınıflandırılması ile bilgi sistemleri risk yönetim süreci; bilgi güvenliği

yönetimi bölümünde bilgi güvenliği organizasyonu, roller ve sorumluluklar, veri gizliliği, verilerin paylaşılması, kimlik ve erişim yönetimi, bütünlük kontrolleri, iz kayıtlarının oluşturulması ve takibi, ağ güvenliği, güvenlik konfigürasyonu yönetimi, güvenlik açıkları ve yama yönetimi, fiziksel güvenlik kontrolleri, siber olay yönetimi, sızma testi ve siber istihbarat paylaşımı ile bilgi güvenliği farkındalığını artırma; sistem geliştirme ve değişikliği yönetimi bölümünde bilgi mimarisinin tanımlanması, proje yönetimi, sistem geliştirme, taşıma ve kurulum, uygulama kontrolleri ile değişiklik yönetimi; bilgi sistemleri sürekliliği ve erişilebilirlik yönetimi bölümünde birinci ve ikincil sistemler, bilgi teknolojileri operasyon yönetimi, erişilebilirlik ve yedekleme ile bilgi sistemleri sürekliliğinin sağlanması; dış hizmet alımı bölümünde dış hizmet alımı sürecinin yönetimi; bilgi sistemleri iç kontrol ve iç denetim faaliyetleri bölümünde bilgi sistemleri iç kontrol faaliyetleri, bilgi sistemleri iç denetim faaliyetleri, bulguların takibi ve güvence sağlama ile personelin eğitilmesi ve kaynak tahsisi; "*Elektronik Bankacılık Hizmetleri*" başlıklı üçüncü kısmının ortak hükümler bölümünde kimlik doğrulama ve işlem güvenliği, inkar edilemezlik ve sorumluluk atama, işlemlerin takibi ile müşterilerin bilgilendirilmesi; internet bankacılığı bölümünde internet bankacılığında kimlik doğrulama ve işlem güvenliği; mobil bankacılık bölümünde mobil bankacılıkta kimlik doğrulama ve işlem güvenliği; telefon bankacılığı bölümünde telefon bankacılığında kimlik doğrulama, işlem güvenliği ve hizmet kalitesi; açık bankacılık servisleri bölümünde açık bankacılık servislerinde kimlik doğrulama ve işlem güvenliği; ATM bankacılığı bölümünde ATM'lerde kimlik doğrulama ve işlem güvenliği hususları düzenlenmiştir.

c. Komiteler

Yönetmelik uyarınca banka yönetim kurulunun bilgi sistemleri strateji komitesi ve bilgi sistemleri yönlendirme komitesi kurması gerekmektedir. Banka yönetim kurulu bankanın ölçeği, bilgi sistemlerine bağımlılığı, personel sayısı ve bilgi sistemleri konusunda alınan dış hizmetler gibi kriterleri esas alarak strateji ve yönlendirme komitelerini birleştirebilir. Bu komitelerin görev tanımları ve çalışma esasları yönetim kurulu tarafından onaylanır. Bilgi sistemleri strateji komitesi, yönetim kurulu adına, bilgi sistemleri strateji planı doğrultusunda bilgi sistemleri yatırımlarının uygun bir şekilde kullanılıp kullanılmadığının ve bankanın iş hedefleri ile bilgi sistemleri hedeflerinin birbiriyle uyumluluğunun gözetimini yürütmek; bu hususlarda yönetim kuruluna doğrudan ve düzenli olarak raporlama yapmak; bilgi sistemleri strateji planını yılda en az bir defa olmak üzere gözden geçirerek gerekli olduğu durumlarda revize ederek yönetim kurulu onayına sunmak ve bilgi sistemleri yönlendirme komitesinin faaliyetlerini gözetmekle sorumludur. Bu komitede en az bir yönetim kurulu üyesinin bulunması ve bilgi sistemlerinden sorumlu üst düzey yönetici ile bankanın ilgili iş birimlerinden üst düzey yöneticilerin bu komiteye üye olması gerekmektedir. Komitenin, bilgi sistemleri strateji planının düzgün bir şekilde uygulanıp uygulanmadığını gözden geçirmek ve önemli bilgi sistemleri yatırım kararlarını değerlendirmek üzere yılda en az iki defa bir araya gelmek ve yılda en az bir defa yönetim kuruluna rapor sunmakla yükümlüdür.

Bilgi sistemleri stratejisinin yönetim kurulu onayı doğrultusunda uygulanmasında, bilgi sistemleri strateji komitesine ve üst düzey yönetime yardımcı olmak amacıyla bilgi sistemleri yönlendirme komitesi oluşturulmalıdır. Bu komite, bilgi sistemleri yatırımlarının ve projelerinin öncelik sırasını belirlemek, devam eden bilgi sistemleri projelerinin durumunu takip etmek, projeler arasındaki kaynak çatışmalarını çözüme kavuşturmak, bilgi sistemleri mimarisi ve projelerinin mevzuata uyumluluğunu sağlamak üzere gerekli yönlendirmeleri yapmak ve bilgi sistemleri servislerine ilişkin hizmet seviyelerini izlemekten sorumludur. Komitede, bilgi sistemleri, insan kaynakları, bankanın ilgili iş birimlerinden temsilcilerin ve banka organizasyonunda bulunması durumunda uyum ve hukuk ile ilgili birim ya da pozisyonlardan temsilcilerin bulunmalıdır. Bu komite, yılda en az iki defa bir araya gelmeli ve yılda en az bir defa bilgi sistemleri strateji komitesine rapor sunmalıdır.

Yönetmelik uyarınca, banka bünyesinde bilgi güvenliğinin sağlanmasında nihai sorumluluk yönetim kuruluna aittir. Yönetim kurulu, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi hususunda gerekli kararlılığı göstermekle ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis etmekle yükümlüdür. Bu sorumluluk kapsamında yönetim kurulu, banka genelinde uygulanmasını gözetmekle yükümlü olduğu bir bilgi güvenliği yönetim sistemi tesis etmelidir. Bilgi güvenliği yönetim sisteminin ulusal veya uluslararası standartları ya da en iyi uygulamaları referans alması ve aşağıdaki faaliyetleri içermesi esastır:

- Bilgi varlıklarına yönelik olarak düzenli bir şekilde tehdit ve risk değerlendirme çalışmalarının yapılması,

- Bilgi varlıklarının sınıflandırılarak varlık sahipliklerinin belirlenmesi ve varlık sınıflarına uygun güvenlik önlemlerinin alınması,

- Bilgi güvenliği ihlaline ilişkin olayların izlenmesi ve raporlanması,

- Banka genelinde verilen bankacılık hizmetlerinde, görevler ayrılığı prensibi ile tutarlı etkin bir kimlik doğrulama ve erişim yönetimi tesis edilmesinin sağlanması,

- Bilgi güvenliğinin sağlanmasına ilişkin kontrollerin ve tesis edilen yapıların test edilmesi ve test sonuçlarının takip edilerek raporlanması,

- Bilgi varlıklarına yönelik güncel güvenlik açıklarının takip edilmesi ve gerekli aksiyonların alınmasının sağlanması,

- Üst yönetim de dâhil olmak üzere banka çalışanları, dış hizmet sağlayıcılar ve müşteriler gibi bankanın bilgi güvenliğini ilgilendiren paydaşlara yönelik, bilgi güvenliği farkındalığını artıracak çalışmaların yapılması,

- İş sürekliliği yönetimi kapsamında bilgi güvenliğini ilgilendiren hususların da yer almasının sağlanması,

- Dış hizmet alımlarının yönetimi kapsamında bilgi güvenliğini ilgilendiren hususların da yer almasının sağlanması.

Yönetmelik uyarınca bilgi güvenliği politikasının oluşturulması ve uygulanması faaliyetleri yönetim kurulu adına bilgi güvenliği komitesi tarafından gerçekleştirilir. Bu komiteye, belirlenen bir yönetim kurulu üyesi veya genel müdür başkanlık eder ve komitenin koordinasyonunu bilgi güvenliği sorumlusu yerine getirir. Komite toplantılarına bilgi sistemlerinden sorumlu üst düzey yöneticinin, bankanın ilgili iş birimlerinden üst düzey yöneticilerin, insan kaynakları, risk yönetimi birimlerinden ve banka organizasyonunda bulunması durumunda uyum ve hukuk ile ilgili birim ya da pozisyonlardan temsilcilerin de katılması esastır. Komitenin görev tanımları ve çalışma esasları, yönetim kurulu tarafından onaylı olacak şekilde yazılı hale getirilmeli, yılda en az iki defa toplanmalı ve yılda en az bir defa yönetim kuruluna rapor sunmalıdır.

Yönetmelik uyarınca banka bünyesinde, bilgi sistemlerinden sorumlu üst düzey yönetici ve ona bağlı birimlerden meydana gelen bilgi sistemleri fonksiyonundan ayrı ve bağımsız olacak şekilde bir bilgi sistemleri güvenlik fonksiyonu oluşturulmalıdır. Bilgi sistemleri güvenlik fonksiyonunun doğrudan yönetim kuruluna veya genel müdüre bağlı olmalıdır. Bankanın bilgi sistemleri güvenlik fonksiyonu, bilgi güvenliği sorumlusu tarafından yönetilir. Bilgi güvenliği sorumlusu aşağıdaki görevleri yerine getirmelidir:

- Bilgi güvenliği politikası, prosedürleri ve süreç dokümanlarının oluşturulması, bunların güncellenmesi ve onaya sunulması,

- Bilgi güvenliği bakış açısıyla, bilgi varlıklarının sınıflandırılması ve bilgi varlıklarına yönelik gizlilik, bütünlük, erişilebilirlik kriterleri bakımından bilgi sistemleri risk yönetimi çalışmalarına aktif katkı sunulması ve yardımcı olunması,

- İlgili birimlerle uyum içinde, iş gereksinimleri ve iş hedefleriyle uyumlu banka genelinde bilgi güvenliğinin tesis edilmesi,

- Bilgi güvenliği ile ilgili mevzuat hükümlerine, standartlara, politika, prosedür ve süreç dokümanlarına uyumun takip edilmesi,

- Bilgi güvenliği faaliyetlerinin ve testlerinin yürütülmesinin sağlanması ve bunların takip edilmesi,

- Önemli projeler ve değişiklikler için bilgi güvenliği gereksinimlerinin belirlenmesi çalışmalarına katkıda bulunulması,

- Bankanın bilgi güvenliğini ilgilendiren paydaşlara yönelik bilgi güvenliği farkındalık programının yürütülmesi.

Yönetmelik uyarınca bankacılık faaliyetlerinin yürütülmesinde kullanılan bilgi istemleri servislerinin sürekliliğini sağlamak üzere iş sürekliliği yönetiminin ve planının bir parçası olan bilgi sistemleri süreklilik yönetimi süreci ve yönetim kurulu onaylı bir bilgi sistemleri süreklilik planı hazırlanmalı, bilgi sistemleri süreklilik yönetimi süreci sorumlusu atanır ve bilgi sistemleri süreklilik komitesi kurulmalıdır. Bu komite, bankanın insan kaynakları, ilgili iş birimleri, bilgi sistemleri güvenlik fonksiyonu, ilgili bilgi sistemleri birimlerinin temsilcileri ve organizasyonda bulunması durumunda uyum ve hukuk ile ilgili birim ya da pozisyonların temsilcilerinden oluşmalıdır. Bilgi sistemleri süreklilik yönetimi süreci sorumlusu bu komiteye başkanlık eder. Komite, meydana gelen olaylarla ilgili bütün faktörleri göz önünde bulundurarak kriz durumu olduğunu ilan etmek, bilgi sistemleri planın devreye alınmasına karar vermek ve diğer kurtarma, süreklilik ve müdahale ekipleriyle koordinasyonu sağlamakla yükümlüdür. Bilgi sistemleri süreklilik yönetimi sürecinin ulusal veya uluslararası standartları ya da en iyi uygulamaları referans alınmalıdır.

d. Siber Olaylar

Yönetmelik uyarınca, banka, siber olaylardan sonra bankacılık faaliyetlerini en az etkileyecek şekilde ve mümkün olan en kısa sürede bilgi sistemleri hizmetlerini normal işleyişine döndürmek üzere gerçekleşen siber olayların ele alınması ve takibine yönelik siber olay yönetimi ve siber olaylara müdahale süreci oluşturmalıdır. Yeterli teknik ve operasyonel becerilere sahip bir kurumsal siber olaylara müdahale ekibi kurulmalı, bu ekibe ilişkin güncel iletişim bilgilerinin BDDK'ya iletilmeli ve siber olayların BDDK ve ilgili yönetim birimlerine raporlanması sağlanmalıdır. Bu ekip, siber olay öncesinde, bilgi işlem varlıkları üzerinde rutin sızma testi çalışması yapmak veya yaptırmak, kayıt yönetimi sistemi arayüzünden rutin olarak iz kayıtlarını takip etmek, iz kayıtları arasında anlamlı sonuçlar doğurabilecek korelasyonları kontrol etmek; siber olay esnasında ise, bilgi sistemleri fonksiyonunun yapacağı müdahaleyi yönetmek ve bilgi sistemleri fonksiyonunda görevli ilgili personeli koordine etmekle sorumludur.

Banka, yaşanan bir siber olayın büyüyerek bir krize dönüşmesi, verilerin sızması ya da ifşası ile sonuçlanması, bilgi sistemleri süreklilik planının ya da ikincil merkezin[16] devreye alınması gibi hallerde derhal sektörel siber olaylara müdahale ekibini[17] bilgilendirmelidir. Hassas verilerin ya da kişisel verilerin sızmasına ya da ifşasına yol açan bir siber olayın yaşanması halinde banka tarafından yapılacak değerlendirme sonrasında müşterilerin bilgilendirilmesi sağlanmalıdır. Banka, bilgi sistemleri hizmetlerinde ciddi kesintilere veya bozulmalara yol açan önemli siber olaylar için bir kök neden ve etki analizi yapmak ve benzer olayların tekrarını önlemek için iyileştirici önlemleri almakla ve yapılan çalışmaları sektörel siber olaylara müdahale ekibini bildirmekle yükümlüdür.

Yönetmelik uyarınca, banka, bilgi sistemleri aracılığıyla sunduğu hizmetlerin tasarımı, geliştirilmesi, uygulanması veya yürütülmesinde görevi bulunmayan bağımsız ekiplere yılda en az bir

[16] *İkincil sistemlerin kullanıma hazır olacak şekilde tesis edildiği ve birincil sistemlerde herhangi bir kesinti yaşanması durumunda personelin çalışmasına imkân tanıyacak ve birincil merkez ile aynı riskleri taşımayacak şekilde oluşturulmuş yapıyı ifade eder.*

[17] *Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğin 7 nci maddesinde ifade edilen BDDK bünyesinde teşkil edilmiş sektörel siber olaylara müdahale ekibini (Sektörel SOME) ifade etmektedir.*
Sektörel SOME'lerin görev ve sorumlulukları
MADDE 7 – (1) Sektörel SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini USOM'la koordineli şekilde yürütürler.
(2) Sektörel SOME'ler birlikte çalıştıkları SOME'lerde yaşanan siber olayları gecikmeksizin USOM'a bildirirler.
(3) Sektörel SOME'ler siber olaylara ilişkin USOM tarafından iletilen alarm, uyarı ve duyuruları dikkate alarak birlikte çalıştıkları SOME'lerde gerekli tedbirlerin alınmasına yönelik çalışmaları yürütürler.
(4) Sektörel SOME'ler birlikte çalıştıkları SOME'lerin yapılanması konusunda düzenleyici faaliyetleri yürütürler.
(5) Sektörel SOME'ler ilgili oldukları sektörde, bilgilendirme, bilinçlendirme ve eğitim faaliyetleri ile siber güvenlikle ilgili kabiliyetlerinin geliştirilmesi ve önlemlerin alınması konusunda gerekli düzenleyici faaliyetleri yürütürler.
(6) Sektörel SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştıkları SOME'lere ve USOM'a bildirirler.
(7) SOME'ler 7/24 erişilebilir olan iletişim bilgilerini Sektörel SOME'lere ve USOM'a bildirirler.
(8) Sektörel SOME'ler birlikte çalıştıkları SOME'lerde yaşanan siber olaylarda imkânları ölçüsünde gerekli desteği sağlarlar. Sektörel SOME'ler, imkânlarının yetersiz olması durumunda USOM'dan destek alırlar.
(9) Sektörel SOME'ler siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaştıklarında gecikmeksizin durumu kanunen yetkili makamlara bildirirler. Durumu gecikmeksizin USOM'a da bildirirler.
(10) Sektörel SOME'ler gerekmesi durumunda birlikte çalıştıkları SOME'ler arasındaki işbirliğini koordine ederler.

defa sızma testi yaptırır. BDDK sızma testlerine ilişkin usul ve esasları 24.07.2012 tarih BSD.2012/1 sayılı genelge ile belirlemiştir. Anılan genelgede sızma testlerinin amacı, banka bilgi sistemlerinde yetkisiz erişim elde edilmesi veya hassas bilgilere ulaşılmasına neden olabilecek güvenlik açıklarının istismar edilmeden önce tespit edilmesi ve düzeltilmesi olarak; kapsamı da sızma testleri, temel sızma testleri ile bu testler sonrası uygulanacak detaylı sızma testleri olarak belirlenmiştir. Ayrıca, sızma testleri olarak asgari olarak gerçekleştirilecek testler:

- İletişim altyapısı ve aktif cihazlar,
- DNS servisleri,
- Etki alanı ve kullanıcı bilgisayarları,
- E-posta servisleri,
- Veritabanı sistemleri,
- Web uygulamaları,
- Mobil uygulamalar,
- Kablosuz ağ sistemleri,
- ATM sistemleri,
- Dağıtık servis dışı bırakma testleri,
- Sosyal mühendislik testleri.

Banka, BDDK'nın belirleyeceği usul ve esaslar çerçevesinde, tespit ettiği ya da haber aldığı yeni siber tehditler, zararlı yazılımlar, siber olaylar ya da bankacılık sektöründe ortaya çıkan yeni dolandırıcılık yöntemleri hakkında bilgilendirmeleri yapmakla ve dolandırıcılıkla mücadelede erken müdahaleyi sağlamak amacıyla 7/24 irtibat kurulabilecek bir irtibat görevlisi atamakla yükümlüdür.

e. Birincil ve İkincil Sistemler

Yönetmelik uyarınca, bankaların birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur. Birincil sistemlerin kaçıncı yedeği olduğuna bakılmaksızın birincil sistemlerin her türlü yedeği ikincil sistemler olarak kabul edilir ve yurtiçinde bulundurulması zorunludur. Bankacılık faaliyetlerinin yürütülmesi veya mevzuatta tanımlanan sorumlulukların yerine getirilmesi amacını taşımayan banka içi mesajlaşma sistemleri, piyasa izleme platformları gibi sistemler birincil sistemler kapsamında yer almaz. Bankanın kullanmakta olduğu herhangi bir sistem ya da uygulamanın birincil sistemler kapsamına girmemesi için sistem veya uygulama üzerinden herhangi bir iş sürecinin yürütülmemesi, hassas veri ya da sır kapsamına girebilecek verilerin işlenmemesi, iletilmemesi ve saklanmaması gereklidir. İşlemlerin doğası gereği yurt dışı ile etkileşimin gerekli olduğu ödeme veya mesajlaşma sistemleri gibi bankacılık işlemleri hariç olmak üzere, bankanın yurt dışında kurulu bir sistemden herhangi bir onay sürecine tabi olmaksızın bankacılık işlemlerini gerçekleştirebilmeli ve yurt dışı iletişim ağlarıyla bağlantılarının kesildiği durumlarda dahi yurt içinde kurulu bulunan birincil ve ikincil sistemleri aracılığıyla ülke içerisinde bankacılık faaliyetlerini sunmaya devam edebilmelidir.

Birincil veya ikincil sistemler kapsamında olan bir faaliyet için dış hizmet ya da bulut bilişim hizmeti alınması halinde, dış hizmet sağlayıcının sunduğu hizmete ilişkin faaliyetleri yürütmede kullandığı bilgi sistemleri ve bunların yedekleri de birincil ve ikincil sistemler kapsamındadır ve yurt içinde bulundurulmalıdır. Birincil veya ikincil merkez için dış hizmet alınması ya da başka kuruluşlarla paylaşılan bir veri merkezinde barındırılması halinde, veri merkezlerinin bulunduğu konumda veya bölgesel olarak yaşanacak gerçek bir felaket anında birincil ve ikincil merkezdeki çalışma ortamının ve dış hizmet sağlayıcıların bankaya ayıracağı kaynağın, bankanın iş sürekliliğini sağlamayı garanti edecek nitelikte olmalıdır.

f. Bilgi Sistemleri İç Kontrol Faaliyetleri

Yönetmelik uyarınca banka ve bankanın dış hizmet sağlayıcıları nezdindeki bilgi sistemleri yönetimine ilişkin faaliyetler, bu faaliyetleri destekleyen süreçler ve tesis edilen bilgi sistemleri kontrollerinin mevzuata ve banka içi politika, prosedür ve standartlara uyumlu olduğunu kontrol etmek

üzere bilgi sistemleri iç kontrol fonksiyonu oluşturulmalıdır. Bu fonksiyon için bilgi sistemleri iç kontrol sorumlusu atanmalı ve bilgi sistemleri iç kontrol faaliyetleri bu kişinin sorumluluğunda yürütülmelidir. Bilgi sistemleri iç kontrol sorumlusunun bilgi sistemleri iç kontrol, bilgi sistemleri denetimi, bilgi sistemleri yönetişimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarının herhangi birinde ya da birkaçında toplamda en az 5 yıllık mesleki tecrübesinin bulunması şarttır. Bilgi sistemleri iç kontrol fonksiyonunda görev alacak personelin de, ilgili alanlarda öğrenim durumları itibarıyla veya aldıkları sertifikalarla kanıtlanabilir asgari bilgi ve beceriye sahip olmaları zorunludur. Bilgi sistemleri iç kontrol fonksiyonu ilave olarak aşağıdaki faaliyetleri de yerine getirir:

- Kontroller sonucunda belirlenen eksikliklerin giderilmesi ve aksiyon alınması amacıyla ilgili birimlere ve üst yönetime bildirimde bulunulması,

- Kontroller sonucunda gerekli olduğu anlaşılan süreçsel veya sistemsel iyileştirme önerilerinin ilgili birimlere ve üst yönetime bildirilmesi,

- Talep halinde bankanın ürünlerinde ve süreçlerinde planlanan değişiklikler, yenilikler veya banka içi politika, prosedür ve süreç dokümanları hakkında görüş oluşturulması,

- Görev alanına giren kritik süreçlerle ilgili proje ve çalışma gruplarına, kurul ve komitelere katılım sağlanması ve ilgili toplantılarda riski en aza indirmeye yönelik öneriler getirilmesi,

- Bilgi teknolojileri yönetimi ve dış hizmet alımından kaynaklı risklerin takibinin sağlanmasına yönelik üst yönetim, denetim komitesi ve iç kontrol birimi yöneticisine periyodik olarak raporlama yapılması,

- Bir sonraki yıl yapılacak planlı incelemeleri gösterecek şekilde her yıl bilgi sistemleri iç kontrol inceleme planları oluşturulması ve bunların banka denetim komitesinin onayından geçirilmesi.

g. Bilgi Sistemleri İç Denetim Faaliyetleri

Yönetmelik uyarınca banka ve bankanın dış hizmet sağlayıcıları nezdindeki bilgi sistemleri yönetimine ilişkin faaliyetler, bu faaliyetleri destekleyen süreçler ve tesis edilen bilgi sistemleri kontrollerinin mevzuata ve banka içi politika, prosedür ve standartlara uyumlu olduğu ve bilgi sistemlerine ilişkin iç kontrol ve risk yönetimi faaliyetlerinin etkinliği ve yeterliliği hususunda yönetim kuruluna güvence sağlamak üzere bilgi sistemleri iç denetim fonksiyonu oluşturulmalıdır. Bu fonksiyon için bilgi sistemleri iç denetim sorumlusu atanmalı ve bilgi sistemleri iç denetim faaliyetleri bu kişinin sorumluluğunda yürütülmelidir. Bu sorumlunun, bilgi sistemleri iç kontrol, bilgi sistemleri denetimi, bilgi sistemleri yönetişimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarının herhangi birinde ya da birkaçında toplamda en az 5 yıllık mesleki tecrübesinin bulunması şarttır. Bilgi sistemleri iç denetim fonksiyonunda görev alacak personelin de, ilgili alanlarda öğrenim durumları itibarıyla veya aldıkları sertifikalarla kanıtlanabilir asgari bilgi ve beceriye sahip olmaları zorunludur.

Bilgi sistemleri iç denetimlerinin kapsamının kritik bilgi sistemleri servisleri, süreçleri ve kritik varlıkları içerecek ve bunlara ilişkin güvence verecek derinlikte ve detayda olmalıdır. Yıllık olarak denetlenebilir bilgi sistemleri alanlarından oluşan bir denetim planı oluşturularak banka denetim komitesinin onayından geçirilmelidir. Bankanın bilgi sistemleri iç denetimlerinin sıklığı ve denetim döngülerinin; bilgi sistemleri servislerinin, süreçlerinin ve varlıklarının kritikliği ve riski ile orantılı olmalıdır. Bu Yönetmelik'te yer alan hükümlerin tamamının banka tarafından yerine getirildiği konusunda güvence vermek üzere yapılacak bilgi sistemleri iç denetimleri için denetim döngüsü 2 yılı aşmayacak şekilde belirlenmelidir.

Yönetmelik uyarınca, bilgi istemleri iç kontrol ve bilgi sistemleri iç denetim faaliyetlerinin etkin bir biçimde yerine getirilmesini sağlamak üzere, yeterli nitelik ve sayıda personel istihdam edilmeli ve banka tarafından yeterli kaynak tahsis edilmelidir. Bu faaliyetler, karşılıklı iş birliği ve bilgilendirmeye dayalı olarak koordineli bir şekilde yürütülmelidir. Önemlilik arz eden sistem, süreç ve alanların zamanında ve öncelikli olarak değerlendirilmesini sağlayacak şekilde iç kontrol ve iç denetim faaliyetleri planlanmalı ve gerekli kaynaklar sağlanmalıdır.

h. Bilgi Sistemleri Risk Yönetim Süreci

Yönetmelik uyarınca banka, bankacılık faaliyetlerinde bilgi teknolojilerini kullanıyor olmasından kaynaklanan riskleri analiz etmek, azaltmak, takip etmek ve raporlamak üzere bir bilgi sistemleri risk yönetim süreci kurmalıdır. Bilgi sistemleri risk analizi kapsamında aşağıdaki faaliyetler yerine getirilmelidir:

- Varlık envanterindeki bilgi varlıklarına ilişkin tehdit ve güvenlik açıklarının tespit edilmesi suretiyle risklerin belirlenmesi,

- Tespit edilen tehditlere ve güvenlik açıklarına göre bilgi varlıklarının riske maruz kalma olasılıklarının belirlenmesi,

- Risklerin gerçekleşmesi durumunda ilişkili bilgi varlığının gizliliği, bütünlüğü, erişilebilirliği gibi kriterlerine olan etkilerin belirlenmesi suretiyle ilgili bilgi varlığına yönelik etki hesaplaması yapılması,

- Bilgi varlıklarını tehdit eden risklerin belirlenen olasılık ve etki değerlerine göre risk derecelendirmesinin yapılması,

- Risk analizinde gerçekleştirilen çalışmaların bütününü temsil eden özet risk değerlendirme raporunun hazırlanarak üst yönetime sunulması.

Risk analizi sonuçlarına göre tespit edilen her bir bilgi sistemleri riskine ilişkin, bu risklerin ilişkili olduğu bilgi varlıklarının değerine ve bankanın risk limitlerine uygun olacak şekilde risklere ilişkin aksiyonlar belirlenmelidir. Risk aksiyonlarının belirlenmesi aşamasında, riskin ilgili olduğu iş biriminin temsilcileriyle beraber risk analizi sonucunda, riskin azaltılması, riskten kaçınma, riskin kabulü ve riskin transferi gibi yöntemlerle nasıl ele alınacağına karar verilmelidir. Her bir risk için belirlenen aksiyonlar risk aksiyon planına dönüştürülmelidir. Alınacak aksiyonlar için yapılacak kaynak aktarımında ve aksiyonların tamamlanma tarihlerinin önceliklendirilmesinde, risk analizi aşamasında belirlenen risk dereceleri dikkate alınmalıdır. Aksiyon planının uygulanması sonucunda kalacak artık riskler için de alınacak aksiyonlar planlanmalı ve güncellenmelidir.

Riskin kabul edilebilmesi için bilgi sistemlerinden sorumlu üst düzey yöneticinin onayının bulunması, riskin bilgi sistemleri stratejisine ve mevzuata aykırılık teşkil etmemesi şarttır. Kabul edilecek riskin aynı zamanda bir iş süreci veya iş uygulamasıyla ilgili olması durumunda ilgili iş biriminin üst düzey yöneticisinin de riskin kabul edildiğine ilişkin onayının bulunması gerekir. Sonradan telafi edici yeni kontrol tekniklerinin ya da yeni güvenlik çözümlerinin ortaya çıkmış olması veya riskin eskiye nazaran artıp artmadığı yönünde koşulların değişmiş olması ihtimaline karşı, önceden kabul edilmiş olan riskler periyodik olarak gözden geçirilmelidir.

Risk analizleri sonucu hazırlanan güncel risk değerlendirme raporu ve güncel risk aksiyon planı birleştirilerek bankanın bilgi sistemleri risk envanteri oluşturulmalıdır. Banka, yılda en az bir defa olmak üzere veya bilgi sistemlerinde meydana gelecek önemli değişikliklerden önce risk analizlerini tekrarlamalıdır. Tekrarlanan risk analizi sonuçlarına göre risk aksiyon planı ve bilgi sistemleri risk envanteri güncellenmelidir. Bankanın kurumsal risk yönetimi süreci, bilgi sistemleri risklerini de kapsamalıdır. Bilgi sistemleri risklerinin bankacılık faaliyetlerinden kaynaklanan diğer risklerin de bir çarpanı olabileceği dikkate alınarak banka genelinde, bilgi sistemlerinden kaynaklanan riskleri de içerecek şekilde, bütünleşik bir risk yönetim metodolojisi uygulanmalıdır. Bilgi sistemleri risk yönetim süreci çıktılarından elde edilen verilerin bankanın bütünsel risk yönetim çerçevesinin bir parçası haline gelmesi sağlanmalıdır. Bilgi sistemlerinden kaynaklanan riskler ele alınırken gelişen yeni teknolojilerin getireceği riskler ayrıca değerlendirilmelidir. Bilgi sistemleri risk envanteri kapsamında riskler takip edilerek yönetim kurulu ve üst düzey yönetime yılda en az bir defa raporlanmalıdır.

1.3.4.1.3. Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimine İlişkin Rapor Hakkında Tebliğ

Bu Tebliğ'in amacı, bilgi sistemleri bağımsız denetim raporunun içerik ve şekline ilişkin usul ve esasları belirlemektir. Tebliğ, Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Hakkında Yönetmelik uyarınca çıkarılmıştır.

Tebliğ'de bilgi sistemleri denetim raporu hazırlanırken uyulacak ilkeler, bulgular, denetlennin görüşleri, bulgularla ilgili sonuçların değerlendirilmesi, rapor içeriği, yönetici özeti, denetim

çalışmasına ilişkin bilgi, denetlenenin bilgi sistemleri hakkında genel bilgi, denetlenenin iç kontrol ve iç denetim yapısına ilişkin değerlendirme, iş süreçleri bağımsız denetimi, bilgi sistemleri bağımsız denetimi ve konsolide denetim raporuna ilişkin hususlar düzenlenmiştir.

1.3.4.1.4. Diğer Düzenlemeler

BDDK tarafından, 04.12.2013 tarih ve 28841 sayılı Resmi Gazete'de yayınlanan "*Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ*" ile risk merkezi, bilgi alışverişi, takas ve mahsuplaşma kuruluşlarının faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetiminde esas alınacak asgari usul ve esaslar ile bilgi sistemleri ve iş süreçlerinin, yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesi ile ilgili esaslar düzenlenmiştir. Bu Tebliğ, 19.08.2021 tarih ve 31573 sayılı Resmi Gazete'de yayımlanan "*Bilgi Alışverişi Kuruluşları İle Risk Merkezinin Bilgi Sistemleri Yönetimine ve Denetimine İlişkin Tebliğ*" ile yürürlükten kaldırılmıştır. Bu Tebliğ ile risk merkezi ve bilgi alışverişi kuruluşlarının uyacakları bilgi sistemleri yönetim ilkeleri bakımından Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmeliği; bilgi sistemleri denetimi bakımından ise Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Hakkında Yönetmelik hükümlerinin esas olduğu düzenlenmiştir.

BDDK tarafından 06.04.2019 tarih ve 30737 sayılı Resmi Gazete'de yayınlanan "*Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ*" kapsamında, ilgili şirketlerin faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetimine ve yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesine ilişkin usul ve esaslar belirlenmiştir. Finansal kiralama, faktöring ve finansman şirketleri için 3 yılda bir bilgi sistemleri denetim yükümlülüğü getirilmiştir.

Yine BDDK tarafından 27.06.2014 tarih ve 29043 sayılı Resmi Gazete'de yayınlanan "*Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ*"i ile ödeme kuruluşları ve elektronik para kuruluşlarının faaliyetlerinin yürütülmesi sırasında kullandıkları bilgi sistemlerinin yönetimine ve yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesine ilişkin usul ve esasları düzenlenmiştir. Ödeme kuruluşları ve elektronik para kuruluşları için 2 yılda bir bilgi sistemleri denetim yükümlülüğü getirilmiştir.

BDDK 2023/1 sayılı genelge ile "*Elektronik Bankacılık Hizmetlerinde ve Elektornik Ortam Sözleşme İlişkisinin Kurulmasında Kimlik Doğrulama ve İşlem Güvenliği için Sağlanması Gereken Kriterler*", BSD.2010/1 sayılı genelge ile "*Bağımsız Denetim Takip Sistemi (BADES)*" ve BSD.2012/1 sayılı genelge ile "*Bilgi Sistemlerine İlişkin Sızma Testleri*"ne ilişkin esaslar belirlemiştir.

1.3.4.2. Gelir İdaresi Başkanlığı (GİB)

Ticari hayatın bir gereği olarak, vergi mevzuatının elektronik belge oluşturulması ve kullanımına izin vermesiyle birlikte, söz konusu elektronik belgelerin kullandığı bilgi sistemlerinin belirli esaslar çerçevesinde oluşturulup yönetilmesi önem arz etmiştir. Bu kapsamda da GİB tarafından söz konusu alanın düzenlenmesi gerekmiştir. GİB 19.11.2019 tarihinde, e-Belge entegratörlerinin faaliyetlerini gerçekleştirmede kullandıkları bilgi sistemlerinin yönetimi ile yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmelerine ilişkin usul ve esasları içeren "*E-Belge Özel Entegratörleri Bilgi Sistemleri Denetimi Kılavuzu*"nu yayınlamıştır. Anılan kılavuz, 509 Sıra No.lu Vergi Usul Kanunu Genel Tebliğinde belirtilen e-Belge uygulamaları kapsamında, GİB'den izin alan/alacak olan özel entegratör kuruluşlarının e-Belge uygulamaları ile ilgili özel entegratörlük faaliyet ve süreçlerine ilişkin bilgi sistemleri bağımsız denetim faaliyetinin gerçekleştirilmesine ve sonuçlarına ilişkin usul ve esasları belirlemek üzere hazırlanmıştır.

Kılavuzda, bağımsız denetim bankacılık ve sermaye piyasası mevzuatı kapsamında bilgi sistemlerine ilişkin bağımsız denetim faaliyetleri olarak tanımlanmış ve yine anılan mevzuatlar kapsamında yetkilendirilmiş kuruluşlar tarafından gerçekleştirileceği belirtilmiştir. Özel entegratör kuruluşları, vergi mevzuatı kapsamında elektronik ortamda oluşturulmasına imkan verilen belgelerin (e-Belgeler) oluşturulma, imzalanma, iletilme veya saklanmasına ilişkin hizmetlerin tamamı veya bir

kısmını verebilir. Özel entegratör kuruluşları, bilgi sistemleri denetimini, ilk denetim tarihini[18] takip eden 2 yılda bir yaptırmak zorundadır. Bakanlık ya da GİB'in gerek görmesi durumunda, bu kuruluşların altyapı sistemlerini dilediği anda ve dilediği şekilde denetleyebilir ya da denetletebilir[19]. Bu kapsamda, GİB'e sunulan bilgi sistemleri bağımsız denetim raporları, rapor tarihinden itibaren en fazla 2 yıl süre ile geçerlidir. Söz konusu sürenin bitiminden önce yeni bilgi sistemleri bağımsız denetim raporunun GİB'e ibrazı zorunludur. Denetim raporu, rapor tarihinden itibaren en geç 15 gün içinde GİB'e yazılı olarak gönderilmelidir. GİB, yetkilendirilmiş özel entegratörler veya ilk başvuru aşamasında olanlara ilişkin denetim sonuçlarını ebelge.gib.gov.tr adresinde yayınlayabilir. Belirlenen süreler içerisinde denetim raporu GİB'e ulaşmamış olan özel entegratörler ile özel entegratör adaylarının izinleri/başvuruları önce askıya alınır ve bu durum ebelge.gib.gov.tr adresinden duyurulur. Bunun üzerine özel entegratöre denetim raporlarını teslim etmesi için 6 ay ek süre verilir. Bu süre zarfında da denetim raporlarını teslim etmeyen ya da edemeyen özel entegratörün izni iptal edilir.

Kılavuzda, kritik varlıklar ve aktörler, fiziki güvenlik şartları ve tedbirleri, sızma testleri, risk yönetimi, iş sürekliliği ve FKM yönetimi, değişiklik yönetimi, denetim izlerinin oluşturulması ve saklanması, dış hizmet alımı, personelin niteliğine ilişkin gereksinimler, uluslararası standartlara ilişkin sertifikasyonlar, özel entegratörün denetime ilişkin sorumlulukları, denetim raporunun içeriği ve oluşturulması, denetim raporuna bağlı olarak GİB tarafından uygulanacak yaptırımlar ve denetim değerlendirme sınıfları hususlarına; ekinde ise denetim değerlendirme sınıfları kontrol tabloları, denetçinin görüşünü oluşturması için kılavuz, denetim rapor formatı ve görüş yazısı şablonlarına yer verilmiştir.

Özel entegratör kuruluşlarının, yılda en az bir kez sızma testi yaptırmakla yükümlüdür. Bu testlerde, varsa tespit edilen açıklara ilişkin alınan tedbirler ve bir takvime bağlanmış eylem planı kayıt altına alınmalıdır. Özel entegratör kuruluşu, ilk denetim dışında, bilgi sistemleri bağımsız denetimi sırasında son iki sızma testi raporlarını ve alınan tedbirlerin yer aldığı kayıtları denetçiye bildirmelidir. Özel entegratör kuruluşları, bilgi sistemlerinin tamamını içerecek bir kapsamdan daha dar olmamak üzere, aşağıdaki sertifikasyon belgelerine sahip olmalıdır:

- ISO/IEC 20000:1 2011 Bilgi Teknolojileri Hizmet Yönetim Sistemi Belgesi,
- ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Belgesi,
- ISO 22301 İş Sürekliliği Yönetim Sistemi Belgesi.

Kılavuz uyarınca, GİB, denetim raporunun sonuçlarına göre uygulayacağı yaptırımlar:

- Rapor sonucunun olumlu olması halinde özel entegratör kuruluşu, varsa kendisine tebliğ edilen eksikliklerin veya iyileştirmelere ilişkin alacağı tedbirleri içeren eylem planını ve buna ilişkin faaliyetleri ve tamamlama sürelerini GİB'e 15 gün içinde bildirmelidir. Buna uymayanlar yazıyla uyarılır. GİB, eylem planına ilişkin tamamlama sürelerinde değişiklik yapmaya yetkilidir.
- Şartlı görüş veya görüşten kaçınma halinde, özel entegratör kuruluşu ivedilikle yazıyla uyarılır ve denetimi en geç 90 gün içinde tekrarlaması istenir. Üst üste 2 kez şartlı görüş veya görüşten kaçınma olması durumunda, özel entegratörün faaliyeti, olumlu görüş alacağı yeni bir denetim sonucuna kadar askıya alınır. Faaliyetin askıya alınması nedeninin 2 kez üst üste görüşten kaçınma olması durumunda, faaliyetin askıya alınma süresi 3 aydan daha kısa olamaz.
- Rapor sonucunun olumsuz olması halinde özel entegratörün faaliyeti ivedilikle geçici süreyle durdurulur. 6 ay içinde olumlu görüş bildiren yeni bir denetim raporunun GİB'e

[18] Bu Kılavuz'un yayım tarihinden (Kasım 2019) itibaren yapılacak özel entegratörlük başvurularında, özel entegratör kuruluş adaylarının bu Kılavuzda belirtilen bilgi sistemleri bağımsız denetimini yaptırmış olması ve başvuru dosyasına denetim raporunu eklemiş olması zorunludur. Ayrıca hali hazırda bu Kılavuz'un yayım tarihi itibariyle özel entegratör kuruluş yetkisi almış olanlar ile test ve değerlendirme süreçleri devam edenler; bilgi sistemleri bağımsız denetimi yaptırmaları için bu Kılavuz'un yayım tarihinden başlamak üzere ilk denetimlerini yaptırmak üzere 31/12/2020 tarihine kadar süre verilmiştir.

[19] Bilgi sistemleri bağımsız denetimi 2 yılda bir gerçekleştirilir. GİB dilediği zaman kendi personeliyle yerinde denetim yapabileceği veya yazıyla bilgi talep edebileceği gibi, son denetimin üzerinden 2 yıl geçmemiş olmasına karşın özel entegratörden denetim yaptırmasını isteyebilir.

ibraz edilmemesi halinde özel entegratörün yetkisi iptal edilir. Özel entegratör, 6 ay içinde yaptıracağı her yeni denetime ilişkin, denetim öncesinde ve sonrasında GİB'i bilgilendirmekle mükelleftir.

1.3.4.3. Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumu (SEDDK)

SEDDK tarafından 25.11.2021 tarih ve 31670 sayılı Resmi Gazete'de "*Sigortacılık ve Özel Emeklilik Sektörlerinde İç Sistemlere Dair Yönetmelik*" yayınlanmıştır. Bu Yönetmelik'in amacı, sigorta, reasürans ve emeklilik şirketlerinin, sigortacılık ve özel emeklilik sektörlerinde faaliyet gösteren özellikli kuruluşların ve tüzel kişiliği haiz sigorta ve reasürans brokerlerinin kuracakları iç kontrol, risk yönetimi, aktüerya ve iç denetim sistemlerine ve bunların işleyişine ilişkin usul ve esasları düzenlemektir. Yönetmelik, kuruluşların gerçekleştirilen faaliyetlerin veya verilen hizmetlerin etkin, güvenilir ve kesintisiz bir şekilde yönetilmesi, mevzuattan kaynaklanan yükümlülüklerin yerine getirilmesi, muhasebe ve finansal raporlama ile ana faaliyetlerin yürütüldüğü sistemlerden sağlanan bilgilerin bütünlüğü, tutarlılığı, güvenilirliği, zamanında elde edilebilirliği ve gereken durumlarda gizliliğinin sağlanmasına elverişli ve aynı zamanda bilgi sistemlerinin kullanılmasından kaynaklı risklerin izlenmesini, kontrolünü ve gerekli önlemlerin alınmasını sağlayan iş süreçlerinin ve bilgi sistemlerinin tesisini zorunlu kılmıştır. Bilgi sistemleri tanımı, BDDK'nın Yönetmeliği ile aynı şekilde tanımlanmıştır. Ayrıca tesis edilecek asgari bilgi sistemleri altyapısı unsurları ve bilgi sistemleri kontrollerine yer vermiştir. Yönetmelik'e göre bilgi sistemlerinden beklenen fonksiyonların doğru bir şekilde yerine getirilmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli derecede güvence oluşturulmasını sağlamak üzere bilgi sistemlerinin kontrolü amacıyla COBIT kapsamında genel bilgi sistemi kontrolünün yapılması beklenmektedir.

Yönetmelik uyarınca, iç kontrol fonksiyonu kapsamında birim yöneticisi ile en az bir denetim komitesi üyesi tarafından imzalanmış aşağıdaki raporların her yıl hazırlanıp, Nisan ayı sonuna kadar SEDDK'ya gönderilmesi gerekmektedir:

- İş süreçleri ve bu süreçlerde yıl içinde yapılan değişikliklerin açıklandığı ve güncel iş akış şemaları ile bu şemalarda yıl içinde yapılan değişikliklerin verildiği iş süreçleri raporu,

- Bilgi sistemlerinin yapısı, bilgi sistemleri kapsamında yapılan hizmet alımları, iş sürekliliğinin sağlanması konusunda alınan tedbirler ve bu konularda planlanan ve yürütülen çalışmalar ile yapılan testlere ilişkin bilgi sistemleri raporu,

- İç kontrol fonksiyonuna ilişkin yıl içinde yapılan kontroller ve sonuçları raporu.

1.3.4.4. Türkiye Cumhuriyet Merkez Bankası (TCMB)

TCMB, 27.06.2014 tarih ve 29043 sayılı Resmi Gazete'de yayınlanan "*Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ*" ile ödeme kuruluşları ve elektronik para kuruluşlarının faaliyetlerinin gerçekleştirilmesi sırasında kullandıkları bilgi sistemlerinin yönetimi ve denetimine ilişkin usul ve esasları düzenlemiştir. Daha sonra bu Tebliğ 01.12.2021 tarih ve 31676 sayılı Resmi Gazete'de yayımlanan "*Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ*" ile yürürlükten kaldırılmıştır. Yeni Tebliğ ile ödeme kuruluşları ve elektronik para kuruluşlarının faaliyetlerinin yürütülmesinde kullandıkları bilgi sistemlerinin yönetimi ve yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesinin yanı sıra ödeme hizmeti sağlayıcılarının ödeme hizmetleri alanındaki veri paylaşım servislerine ilişkin usul ve esaslar düzenlenmiştir.

Tebliğ'in "*Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler*" bölümünde bilgi sistemleri, ödeme hizmetine ilişkin faaliyetlerin yürütülmesi amacıyla ödeme hizmeti sağlayıcısının bilgi ve verilerle ilgili olarak mevzuatla belirlenmiş sorumluluklarının yerine getirilmesini sağlayan donanım, yazılım, veri, süreç ve insan kaynağından oluşan yapının tamamı olarak tanımlanmıştır. Tebliğ ile bilgi sistemlerinin yönetimine ilişkin genel hükümler, bilgi sistemlerine ilişkin risk yönetimi, bilgi sistemlerinin işletimi, olay yönetimi ve siber olaylar, bilgi güvenliği ve bilgi güvenliği yönetimi, veri güvenliği ve mahremiyeti, kimlik doğrulama, erişim yönetimi, güvenlik açıkları ve ihlalleri, denetim izlerinin oluşturulması, bilgi sistemleri süreklilik planı, ikincil merkez, ikincil sistem ve veri yedekleme merkezi, bilgi sistemlerine ilişkin dış hizmet alım sürecinin yönetimi, müşterilerin bilgilendirilmesi ve

internet sitesi, elektronik sertifikalar, yüksek riskli işlemlerin takibi, işyerleri, temsilciler ve insansız hizmet noktaları, bilgi sistemlerine ilişkin sınırlamalar ve uzaktan iletişim aracı ile yürütülecek süreçler; "*Ödeme Hizmetlerinde Kullanılan Veri Paylaşım Servisleri*" bölümünde veri paylaşım servisi, veri paylaşım servisine ilişkin HHS'nin yükümlülükleri, oturum özellikleri ve denetim izleri, veri paylaşım servislerinde kimlik doğrulama ve işlem güvenliği ve veri paylaşım servislerine ilişkin olağanüstü durum önlemlerine ilişkin esaslar düzenlenmiştir.

Tebliğ uyarınca ödeme ve elektronik para kuruluşlarında bilgi sistemleri denetimi iki yılda bir yapılır. Yeni faaliyet izni alan bir kuruluşa ilişkin ilk bilgi sistemleri denetimi, kuruluşa faaliyet izni verilmesini takip eden yılı kapsayacak şekilde yürütülür. TCMB, gerekli gördüğü hallerde bilgi sistemleri denetiminin kapsamını ve sıklığını farklılaştırabilir. Bilgi sistemleri denetimi ise, BDDK tarafından yayımlanan Bankalarda Bilgi Sistemleri Denetimi Yapmaya Yetkili Bağımsız Denetim Kuruluşları listesinde yer alan bağımsız denetim kuruluşları tarafından yapılır. TCMB, gerek görmesi durumunda kuruluş tarafından, bu listede yer alan bir bağımsız denetim kuruluşundan bağımsız denetim hizmeti alınmamasına veya bu listede yer almayan bir bağımsız denetim kuruluşunun kuruluş nezdinde bilgi sistemleri denetimi yapabilmesine karar vermeye yetkilidir. Bilgi sistemleri denetim raporu, denetim dönemini izleyen yılın Şubat ayı sonuna kadar kuruluşlar tarafından TCMB'ye bildirilmelidir. TCMB, talep üzerine gerekli gördüğü hallerde ilave süre vermeye yetkilidir.

Tebliğ uyarınca, kuruluşlar bilgi sistemlerinin, bilgi güvenliği gereklerinin yerine getirilmesi hususunda herhangi bir görevi bulunmayan ve sızma testi konusunda ulusal veya uluslararası belgeye sahip gerçek veya tüzel kişiler tarafından, gerçekleşebilecek iç ve dış tehditleri kapsayan senaryolar doğrultusunda yılda en az 1 defa düzenli olarak sızma testine tabi tutulmasını sağlamakla yükümlüdür. Sızma testlerine ilişkin usul ve esaslar Tebliğ'in ekinde düzenlenmiştir. Kuruluşlar, gerçekleşen güvenlik ihlalleri, sızma testinin sonuçları ve tespit edilen kritik güvenlik açıkları, bunların giderilmesine yönelik alınan tedbirleri ve sonuçlarını içeren raporu yılda en az bir defa TCMB'nin uygun gördüğü yöntemle TCMB'ye sunma yükümlülükleri bulunmaktadır.

TCMB, 09.01.2016 tarih ve 29588 sayılı Resmi Gazete'de yayınlanan "*Ödeme ve Menkul Kıymet Mutabakat Sistemlerinde Kullanılan Bilgi Sistemleri Hakkında Tebliğ*"i ile ödeme ve menkul kıymet mutabakat sistemlerine ilişkin faaliyetlerin yürütülmesinde kullanılan bilgi sistemleri ile ilgili usul ve esasları düzenlemiştir.

1.3.4.5. Sayıştay Başkanlığı

Ülkemizde özellikle son yıllarda kamu kurumlarının bilgi sistemlerinden ve bu sistemlerin sunduğu imkânlardan yararlanmak amacıyla başta finansal süreçleri olmak üzere tüm iş süreçlerinde giderek daha yaygın bir şekilde bilgi sistemlerini kullanmaları, Sayıştay denetimlerinin bilgi sistemleri alanını da kapsayacak şekilde yeniden yapılandırılmasını sağlamıştır. Bu kapsamda Sayıştay tarafından denetlenen kurumların mali (finansal) denetiminin etkin bir şekilde yapılmasına katkı sağlamak amacıyla, 2013 yılında Bilişim Sistemleri Denetim Rehberi yayımlanmıştır. Bu Rehber ile Sayıştay, kamu kurumlarında yürütmüş olduğu mali denetim sürecine destek vermeyi, bilgi sistemlerinin kontrol zayıflıklarının tespit edilmesini ve kamuoyuna ve parlamentoya bilgi sunulmasını amaçlamaktadır. Rehber, denetimin planlanması, yürütülmesi ve raporlanmasında yol göstermek amacıyla hazırlanmıştır.

Söz konusu rehberin hazırlanmasında Bilgi Güvenliği Standartları, INTOSAI (The International Organisation of Supreme Audit Institutions-Uluslararası Sayıştaylar Birliği) rehberleri ve standartları, ISACA standartları ve çerçeveleri ile diğer ülkelerin uygulamalarından yararlanılmıştır. Rehberde, Sayıştay'ın mali denetim için hazırlamış olduğu Mali Denetim Rehberi'nde belirtilen süreçler dikkate alınarak, denetçinin hangi aşamada hangi işleri yapacağını gösteren süreç odaklı bir yaklaşım benimsenmiş olup genel olarak bilgi sistemleri genel kontrollerinin nasıl değerlendirileceği düzenlenmiştir. Rehber, denetimin planlanması, sistem kontrollerinin değerlendirilmesi ve denetim sonuçlarının raporlanması ve izlenmesine olmak üzere üç temel bölümden oluşmakta olup, Rehber'in önemli bir kısmın genel ve uygulama kontrollerine ilişkin sistem kontrollerinin değerlendirilmesinden oluşturmaktadır.

1.3.5. Uluslararası Düzenlemeler

Günümüzde yalnızca bilgi sistemleri denetimine özgü olmayan, ancak bilgi sistemleri denetimi kapsamına giren risk, yönetim, kontrol ve bilgi güvenliği alanlarında uluslararası kuruluşlar tarafından geliştirilmiş standartlar ve çerçeveler bulunmaktadır. Bu standart ve çerçeveler içerdikleri usul ve esaslar itibarıyla birbirleri arasında sürekli geçişmekte ve güncellenerek daha da kapsamlı bir hale gelmektedir.

Uluslararası kuruluşlar ve ülke otoriteleri, gelişen teknolojilere ve bu teknolojilerin işletmelerin iş süreçlerinde ve finansal raporlamalarında kullanımının artması ile birlikte yükselişe geçen denetim ihtiyacının, daha objektif ve daha güvenilir bir şekilde karşılanabilmesi için uluslararası alanda kabul gören standartlar ve uygulamalar geliştirerek, kamunun yapılan denetimlere olan güvenini sağlamaya ve bu denetimlerin objektifliğini artırmaya çalışmaktadır. Söz konusu standart ve iyi uygulama örneklerinden bazıları yalnızca bilgi sistemleri tarafından üretilen bilginin güvenliği üzerinde yoğunlaşırken, bazıları tüm bilgi sistemlerinin işletme ve kullanıcılar açısından az riskli olmasını ve işletmelerin yürüttüğü iş süreçlerine uygun olmasını amaçlamıştır. Bu kapsamda bilgi teknolojileri standart ve çerçevelerinin, bilgi sistemleri denetçileri tarafından en çok kullanılanları COBIT, ISO/IEC 27000 Standart Serisi, COSO, ITAF, ITIL olarak sayılabilir.

BSBD Tebliği'nde, hüküm bulunmayan durumlarda BDS'ler ve mesleki en iyi uygulamalarda yer alan usul ve esasların uygulanacağı belirtildiğinden, konuya ilişkin uluslararası standart ve çerçevelerin bilinmesi gerekmektedir.

1.3.5.1. COBIT (The Control Objectives for Information and Related Technology)

COBIT'in Türkçe karşılığı "*Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri*" olarak ifade edilebilir. BDDK tarafından yayınlanan ve daha sonra yürürlükten kaldırılan "*Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik*" uyarınca bankalara getirilen COBIT'te yer alan usul ve esasların uygulanması zorunluluğu ile ülkemizde de yaygınlaşan COBIT, iş ihtiyaçlarına göre bilgi sistemlerinin ne kadar hizmet verdiğinden emin olunmasını sağlayan öneriler bütününden oluşan bir çerçevedir.

İşletmelerin operasyonlarına ve hizmetlerine fayda sağlayacak bilgilerin üretimi ve aktarımının hızlı, sürekli ve güvenli olarak sağlanabilmesi için kullandıkları bilgi sistemlerinden kaynaklanan risklerin belirlenmesi, yönetimi ve kontrolünün etkin ve verimli olarak yapılması gerekmektedir. Bu kapsamda, bilgi sistemlerinden kaynaklanan risklerin nasıl yönetileceği ve bu sistemleri nasıl daha güvenli hale getirecekleri sorularına yanıt arayan yalnızca bilgi işlem birimlerinin yöneticilerine değil, bilgi sistemlerini iş süreçlerine entegre etmiş tüm yöneticilerin sorularına sistematik bir şekilde yanıt verecek şekilde oluşturulmuş bir çerçeve yöntem olan COBIT, aynı zamanda bilgi sistemlerinin maruz kaldığı riskleri, bu risklerin değerlendirilmesi, yönetilmesi ve ortadan kaldırılmasına yönelik kontrolleri ve bu kontrollerin denetlenme yöntemlerini de ele alan bir bakış açısı ile oluşturulmuş bir mimariye sahiptir.

İşletmenin iş hedefleri doğrultusunda hizmet vermesini sağlamak amacıyla bilgi işlem kaynaklarını kullanmasını amaçlayan COBIT, verilen hizmetlerin istenilen kalite, güvenlik ve hukuksal ihtiyaçlara cevap vermesini sağlayan kontrol esaslı bir yaklaşımdır. Dolayısıyla, işletmelerin neler yapması gerektiği ile yetinir, bunların nasıl yapılması gerektiği ile ilgilenmez.

COBIT, Information Systems Audit and Control Foundation (ISACF) tarafından ilk kez 1996 yılında oluşturulmuştur. İkinci versiyonu 1998'de, üçüncü versiyonu 2000 yılında, üçüncü versiyonu 2003 yılında elektronik olarak, dördüncü versiyonu 2005 yılında ve 4.1 versiyonu 2007 yılında yayımlanmıştır. Son olarak teknolojik gelişmelere bağlı olarak son sürümü COBIT 5 ISACA nezdinde kurulan ITGI tarafından 2012 yılında yayınlanmıştır. Daha sonra, bu versiyon bilgi ve teknolojideki dijitalleşme başta olmak üzere, yeni teknoloji ve iş trendlerini içerecek şekilde 2019 yılında güncellenmiştir. Yeni sürümde COBIT açık mimarisi, çekirdek model yapısını değiştirmeden, kullanıcıların yeni odak alanları eklemelerini ve mevcut olanları değiştirmelerini mümkün kılar. En güncel bilgi teknolojileri standartları ve uyumluluk yönetmelikleri başta olmak üzere tüm yeni kavramlarla uyumludur. Kavramsal modeli, somutlaştırılmış bir bilgi teknolojileri yönetişim sistemi için kullanılmaya uygun şekilde yapılandırılmıştır. Capability Maturity Model Integration (CMMI) ile daha iyi uyum gösterecek olgunluk ve yetenek kavramları çerçeveye dahil edilmiştir. Performans yönetimi, yetenek ve olgunluk seviyelerinin 0 ile 5 arasında ölçüldüğü CMMI Performans Yönetim Planı'na dayanır.

COBIT, ISACF tarafından bir denetim aracı olarak tasarlanmış olmasına rağmen, teknolojik gelişmelere bağlı olarak zamanla kontrol ve yönetim odaklı hale gelmiş, daha sonra ise bilgi teknolojilerinin yönetimi ve yönetişim odaklı kullanılan bir çerçeve olarak sunulmuştur.

COBIT, önceleri denetim, kontrol ve daha sonra yönetim odaklı çerçeve iken daha sonraları risk ve katma değer ile ilgili standartları da bünyesine katmış ve zamanla bir bilgi sistemleri yönetişim çerçevesi haline gelmiştir. Her versiyonunda kendisini yenilemeye devam eden COBIT, son olarak sadece bilgi sistemleri değil diğer iş süreçlerini de kapsayarak kapsamlı bir model haline gelmiştir (ISACA, 2012: 13).

COBIT 5, sistem teorisinin temel varsayımlarını kullanarak birbiriyle etkileşim içerisindeki bileşenleri dikkate alarak bütüncül bir yaklaşım sergilenmesi gerektiğini ortaya koyar. Buna göre, gerçekleştiriciler kurumsal yönetişim ve yönetim açısından birbirini bütünleyen, diğer çerçeve ve standartların eksikliklerini tamamlayan, işletmenin varlığını sürdürmesi için gerekli olan alt sistemlerden oluşan canlı bir sistemin birliğini tamamlamaktadır (ISACA, 2012: 13).

COBIT'ın altı temel ilkesi:

1- Paydaşa değer sağlama (Provide stakeholder value),

2- Bütüncül yaklaşım (Holistic approach),

3- Dinamik yönetişim (Dynamic governance system),

4- Yönetimden ayrı yönetişim (Governance distinct from management),

5- Uçtan uca yönetişim (End-to-end governance system),

6- Kurumsal ihtiyaçlara uyarlama (Tailored to enterprise needs).

Bu ilkeler, aşağıdaki yedi alt kolaylaştırıcı ilkeye dayanır:

1- İlkeler, politikalar ve çerçeveler (Principles, policies, procedures),

2- Süreçler (Processes),

3- Bilgi (Information)

4- Örgütsel yapılar (Organizational structure),

5- Kültür, etik ve davranış (Culture, ethics and behavior),

6- Hizmetler, altyapı ve uygulamalar (Servies, infrastructure and applications),

7- İnsanlar, beceriler ve yetkinlikler (People, skills and competencies).

1.3.5.2. ISO/IEC 27000 Standart Serisi

ISO 27000 standartları her geçen gün büyüyen ISO/IEC ISMS standart ailesinin bir parçasıdır. ISO 27000 standart serisi; ISO 27001, ISO 27002, ISO 27003 vb. uluslararası standartları içeren bir standart ailesidir. ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı, ISO 27000 Bilgi Güvenliği Yönetim Sistemi standartlar ailesinin ana standardı olup diğer standartlar ise bu standardın uygulanmasına yardımcı sözlük, rehber, metrik ve ölçümler, belgelendirme ve bazı farklı sektörlere uyarlanması olarak birbirinden ayrışmıştır.

ISO/IEC 27001 standardının tarihi gelişimi, 1992 yılında İngiltere'de kamu ve özel sektörde yer alan birçok kuruluşun bilgi güvenliği standardı oluşturulmasına yönelik isteği dikkate alınarak, İngiliz Standartları Enstitüsü (BSI) desteği ile oluşturulan çalışma grubu tarafından BS (British Standart) 7779 adında bir rehber oluşturulması ve söz konusu rehberin BSI tarafından BS 7779 İngiliz Standardı olarak kabul edilmesi ile başlamıştır. İlgili standart BS 7779 – 1 ve BS 7779 – 2 olarak iki kısımdan oluşmuştur. BSI tarafından 1999 yılında BS 7779 – 2 Bilgi Güvenliği Yönetim Sistemi Gereksinimleri adı altında yayımlanmış ve ISO (International Organization for Standardization – Uluslararası Standardizasyon Kuruluşu) tarafından 2000 yılında ISO/IEC 17799 Standardı olarak kabul görmüştür. İlgili standart ülkemizde de 2002 yılında Türk Standartları Enstitüsü (TSE) tarafından referans alınmıştır. Daha sonra ISO tarafından 2005 yılında ISO 27001 Bilgi Güvenliği Yönetim Sistemi Gereklilikleri adı altında

yayımlanmıştır. 2006 yılında ISO/IEC 27001:2005 sürümü ve 2014 yılında ISO/IEC 27001:2013 sürümü TSE tarafından Türkçe olarak yayımlanmıştır (Haklı, 2012: 16).

Vural ve Sağıroğlu (2008:5), ISO 27001 Bilgi Güvenliği Yönetim Sistemi Gereklilikleri'nin en iyi uluslararası uygulama ve standart olarak kabul gördüğünü ifade etmektedir. Bu standart, bilgi güvenliği yönetim sistemi için gereklilikleri ortaya koyar ve bilgilerin düzenli olarak maruz kaldığı tehditlerin tanımlanmasına, yönetilmesine ve bunların minimize edilmesine yardımcı olur. Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır ve "*gizlilik*", "*bütünlük*" ve "*süreklilik (erişilebilirlik/kullanılabilirlik)*" olarak isimlendirilen üç temel unsurdan meydana gelir. Bu üç temel güvenlik öğesinden herhangi biri zarar görürse güvenlik zaafiyeti oluşur. Bilgi güvenliği yönetim sistemi, işletmenin gizli veya hassas kurumsal bilgilerini yönetmek için sistematik bir yaklaşım sunar ve böylece bilginin erişilebilirliğini, gizliliğini ve bütünlüğünü koruyarak bilginin güvenliğini sağlar. Yalnızca bilgi sistemlerini değil, süreçleri ve hatta insanları da kapsar. Bir işletme bu standarda göre bilgi güvenliği yönetim sistemini uygulayacaksa, bilgi güvenliği yönetim sistemi gereklerini anlamalı ve bu alanlara dikkat etmelidir. ISO 27001'e göre bilgi güvenliği yönetim sistemi aşağıdaki 10 alanda güvenliğin gerekli olduğuna odaklanmıştır.

Güvenlik Politikası: İşletmenin iş hedefleri ve bilgi güvenliğine bağımlılığının kapsamlı bir şekilde anlaşılması ve ilk olarak bilgi sistemleri güvenlik politikasının oluşturulmasıyla başlanır. Bu politika üst yönetimin bilgi güvenliği yönetimi ile ilgili taahhüdü ve kurumsal yaklaşımını yansıtmalıdır. Bu son derece önemli bir görevdir ve üst yönetimin tamamı tarafından onaylanmalıdır.

Organizasyonel Güvenlik: İşletme içinde bilgi güvenliğini başlatmak, uygulamak ve kontrol etmek için bir yönetim çerçevesinin oluşturulması gerekir. Yönetim çerçevesinin oluşturulması ise, bilgi güvenliği politikasının onaylanması, güvenlik rollerinin atanması ve güvenliğin işletme içindeki koordinasyonu için uygun prosedürlere ihtiyaç duyar. Yönetim işletme içinde uygulanacak güvenlik tedbirlerini aktif olarak desteklemeli, bilgi güvenliği ile ilgili hedefler belirlenmeli ve sorumluların atanması yapılmalıdır. Ayrıca işletme içerisindeki uygulama ile güvenlik politikası esaslarının aynı, güvenlik politikasının etkin ve uygulanabilir olduğu düzenli bir şekilde gözden geçirilmelidir.

Varlık Sınıflaması ve Kontrolü: En zahmetli, ancak zorunlu görevlerden biri, bilgi varlıkları, yazılım varlıkları, fiziksel varlıklar veya benzeri diğer hizmetler olmak üzere tüm bilgi sistemlerinin varlıklarının envanterini yönetmektir. Tüm bilgi varlıklarını içeren bir varlık envanteri tutulmalıdır. Bu envanter hazırlanırken bilgi (veri tabanı, sözleşme ve anlaşmalar, sistem dokümantasyonu vb.), yazılım varlıkları (uygulama yazılımları, sistem yazılımları ve yazılım geliştirme araçları), fiziksel varlıklar (bilgisayarlar ve iletişim araçları), hizmete dönük varlıklar (bilgisayar ve iletişim hizmetleri, ısıtma, aydınlatma, güç vb.), personel (nitelik ve tecrübeleri ile birlikte) ve soyut varlıklar (işletmenin itibarı ve imajı gibi) varlık türleri dikkate alınır.

Personel Güvenliği: Hırsızlık, dolandırıcılık veya tesislerin kötüye kullanılmasından insan hataları, ihmal ve açgözlülük sorumludur. Alınması gereken çeşitli proaktif önlemlerden önemli olanları ise, personele düşen güvenlik rol ve sorumlulukları belirlemek, personel tarama politikalarını belirlemek, gizlilik anlaşmaları yapmak, istihdam şartlarını ve koşullarını oluşturmak, bilgi güvenliği eğitimini almak ve bu konuda personeli sürekli eğitmektir. İşletme çalışanlarının güvenlik politika ve prosedürlerine uymaması durumunda devreye girecek bir disiplin süreci olmalıdır. Güvenlik konusunda nelere dikkat edeceğinin farkında olan iyi eğitim almış çalışanlar, gelecekteki güvenlik ihlallerini önlemekte kilit rol oynayabilir.

Fiziksel ve Çevresel Güvenlik: Bilgi sistemlerini korumak amacıyla fiziksel güvenlik ortamı oluşturulmalıdır. Fiziksel güvenlik ortamı, fiziksel giriş kontrolü, güvenli ofisler, odalar, tesisler, fiziksel erişim kontrolleri, ateşten elektromanyetik radyasyona kadar çeşitli riskleri en aza indiren ve güç kaynaklarına ve veri kablolarına koruma cihazları sağlayan bazı faaliyetlerden oluşur. Yangın, sel, deprem, patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınmalıdır. Bu faaliyetlerin uygun maliyetlerle tasarlanması ve sürekli izlenmesi, yeterli derecede fiziksel güvenlik denetimini korumanın iki temel özelliğidir.

İletişim ve Operasyon Yönetimi: Tüm bilgi işlem tesislerinin yönetimi ve işletilmesi için doğru dokümante edilmiş prosedürler oluşturulmalıdır. Buna ayrıntılı çalışma talimatları ve olaylarla ilgili müdahale prosedürleri dâhildir.

Erişim Kontrolü: Bilgi ve iş süreçlerine erişim, iş ve güvenlik gereklilikleri çerçevesinde kontrol edilmelidir. Erişim kontrolü hem fiziksel, hem işlevsel boyutları ile değerlendirilmeli ve erişim kontrol politikası bütün kullanıcılar veya kullanıcı grupları için erişim kurallarını ve haklarını açıkça belirtmelidir. Erişim haklarının "*Yasaklanmadıkça her şey serbesttir*" değil "*İzin verilmedikçe her şey yasaktır*" prensibine göre verilmesine dikkat edilmelidir.

Sistem Geliştirme ve Bakım: Yeni sistemlerin geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır. Güvenlik, bir sistemin başlangıcında ideal bir şekilde oluşturulmalıdır. Bu nedenle güvenlik düzenlemeleri, bilgi sistemlerinin geliştirilmesinden önce belirlenmeli ve üzerinde anlaşmaya varılmalıdır. Güvenlik düzenlemeleri, güvenlik ihtiyaçlarının analizi ve spesifikasyonu ile başlar ve her aşamada, veri girişi, veri işleme, veri saklama, veri alma ve veri çıkışı gibi kontroller sağlar. Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmalı; doğru girilmiş bilginin işlem sırasında hatalı veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmelidir. Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmalıdır. Bilginin korunması için kriptografik kontrollerin kullanılmasını düzenleyen politika geliştirilmiş ve uygulamaya alınmış olmalıdır. Örnek vermek gerekirse, bir işletmede şifreleme denetimleri ile uygulamalar oluşturmak gerekebilir. Şifreleme, dijital imza, şifreleme anahtarlarının korunması ve kriptografi için kullanılacak standartların kullanılabileceği bu kontrollerin kullanımı hakkında tanımlanmış bir politika olmalıdır.

İş Sürekliliği Yönetimi: Felaketlerden kaynaklanan ve güvenlik arızalarının neden olduğu aksaklıkları azaltmak için bir iş sürekliliği yönetim süreci tasarlanmalı, uygulanmalı ve periyodik olarak test edilmelidir. Bu iş sürekliliği yönetim süreci, iş sürekliliği ile ilgili olarak işletmenin riskleri, kritik iş süreçleri ile ilgili varlıkları, bilgi güvenliği olayları yüzünden gerçekleşebilecek kesintilerin etkisini, ilave önleyici tedbirlerin belirlenmesi ve uygulanmasını, bilgi güvenliğini de içeren iş sürekliliği planlarının belgelenmesi konularını içermelidir.

Uyum: Fikri mülkiyet hakları, yazılım telif hakları, kurumsal kayıtların korunması, kişisel bilgilerin korunması ve gizliliği, bilginin kötüye kullanımının önlenmesi gibi hususlara ilişkin ulusal ve uluslararası bilgi teknolojileri yasalarına sıkı sıkıya bağlı kalınması gerekir. Bilgi sistemileri için ilgili tüm yasal, düzenleyici ve sözleşmeye bağlı gereksinimler ve gereksinimleri sağlamak için kullanılacak kurumsal yaklaşım açık şekilde tanımlanmalı ve belgelendirilmelidir. Bu gereksinimleri karşılamak için kontroller ve bireysel sorumluluklar tanımlanmalı ve belgelenmelidir.

ISO 27001'de ortaya konulan şartlar geneldir ve türleri, büyüklükleri ve doğalarından bağımsız olarak tüm işletmelere uygulanabilir olması hedeflenmiştir. Ayrıca, ISO 27001, teknik ve teknoloji bağımlı bir standart değildir ve belli bir ürün veya bilgi teknolojisi ile ilgilenmez. Hatta bilgi teknolojileri güvenliği de söz konusu standart içerisinde yer almaz. Tek ilgi alanı vardır, o da bilgi güvenliğidir. Teknik detaylara inmeden kuruluşların bilgi güvenliği hususunda neler yapması gerektiğini açıklar. ISO 27001'in öngördüğü sistem kurmak işletmelere aşağıdaki faydaları sağlar (Yılmaz:2014-2015:55):

- İşletmenin güvenlik politikaları ve buna bağlı olarak bilgi güvenliğini yönetir.
- Bilgi varlıklarının farkına varılıp korunmasını sağlar.
- Böylece işletmenin para, zaman ve itibar kayıplarının önüne geçer.
- Bilginin, gizlilik, erişilebilirlik ve bütünlüğünün korunması sayesinde bilgi güvenliğini sağlar.
- Tehdit ve riskleri yöneterek iş sürekliliğini sağlar.
- İlgili mevzuata uyum sayesinde yasal takipleri önler.
- İşletmenin, çalışanlarının ve birlikte iş yaptığı taraflarının güvenlik risklerini asgariye indirir.
- Çalışanların ve üçüncü kişilerin bilgi güvenliği farkındalıklarını arttırır.

- İşletmenin itibarını yükseltir, rekabet avantajı sağlar.

- Bilgi sistemlerin kötü amaçlar için kullanımını engeller.

- İş sürekliliği kontrolleri ile işletmenin iş ve finansal kaybını asgariye indirir.

- Bilgi güvenliği ihlallerini yöneterek işletmenin her türlü tehditlerden zarar görme risklerini düşürür.

- Mevzuata uyumu sağlayarak işletmeyi hukuki yaptırımlara karşı korur.

Bu sistemin kurulması; varlık envanterinin yapılması, bu varlıklara karşı muhtemel risklerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun çözümlerin geliştirilerek sistemin iyileştirilmesi gibi birbirini izleyen ve tamamlayan denetimlerin gerçekleştirilmiş olması demektir (Yılmaz:2014-2015:55).

1.3.5.3. ITAF (The Information Technology Assurance Framework)

ITAF, bilgi sistemleri denetim ve güvence uzmanlarının rol ve sorumluluklarına, bilgi ve becerilerine, gayret, davranış ve raporlama gereksinimlerine yönelik standartlar oluşturan, bilgi sistemleri güvencesine özgü terim ve kavramları tanımlayan, bilgi sistemleri denetim ve güvence raporlarının planlanması, tasarlanması, yürütülmesi ve raporlanması konularında gerekli araçları, teknikleri ve rehberliği sağlayan kapsamlı ve iyi uygulama odaklı bir referans modelidir.

ITAF, ISACA'nın bilgi sistemleri denetim ve güvence standartları üzerine yoğunlaşmıştır ve bilgi sistemleri denetim ve güvence uzmanlarının rehberlik, araştırma politikaları ve prosedürleri talep edebilmesi, denetim ve güvence programları edinebilmesi ve etkili raporlar geliştirebilmesi için tek bir kaynak sunmaktadır.

ITAF metni; "*Bilgi Sistemleri Denetim ve Güvence Standartları*", "*Bilgi Sistemleri Denetim ve Güvence Kılavuzları*" ve "*Bilgi Sistemleri Denetim ve Güvence Araç ve Teknikleri*" ana başlıklarını içeren üç bölümden oluşmaktadır. İlk iki bölüm genel, performans ve raporlama olarak yine üç bölüme ayrılmıştır. Birinci bölüm bilgi sistemleri denetimi ve güvencesi alanlarında olması gereken standartları tanımlarken, diğer iki bölüm standartların uygulanmasına ilişkin rehberleri, araç ve teknikleri sunmaktadır.

ITAF, bilgi sistemleri denetim ve güvence uzmanları tarafından uygulanan bilgi sistemleri uygulamaları ve altyapısının bileşenleri üzerinde güvence sağlayan bir standartlar bütünüdür. Söz konusu standartların, bu standartlara yol gösterici rehber, araç ve tekniklerin tasarlanmasında bilgi sistemlerinin denetim ve güvence raporlarının kullanıcıları da dâhil olmak üzere, daha geniş bir yelpazeye fayda sağlayacak şekilde olmasına bilhassa dikkat edilmiştir. Çerçevenin uygulanması, bilgi sistemleri denetim ve güvence işinin yürütülmesi için bir önkoşuldur. Denetimlerinde ITAF'ı uygulayan bilgi sistemleri denetçisi, ITAF içerisinde yer alan bilgi sistemleri denetim ve güvence standartlarını uygulamak zorundadır. Rehberler, araçlar ve teknikler denetim ve güvence raporlaması sürecinde zorunlu olmayan bir destek sağlaması için tasarlanmıştır (ITAF, 2014:5).

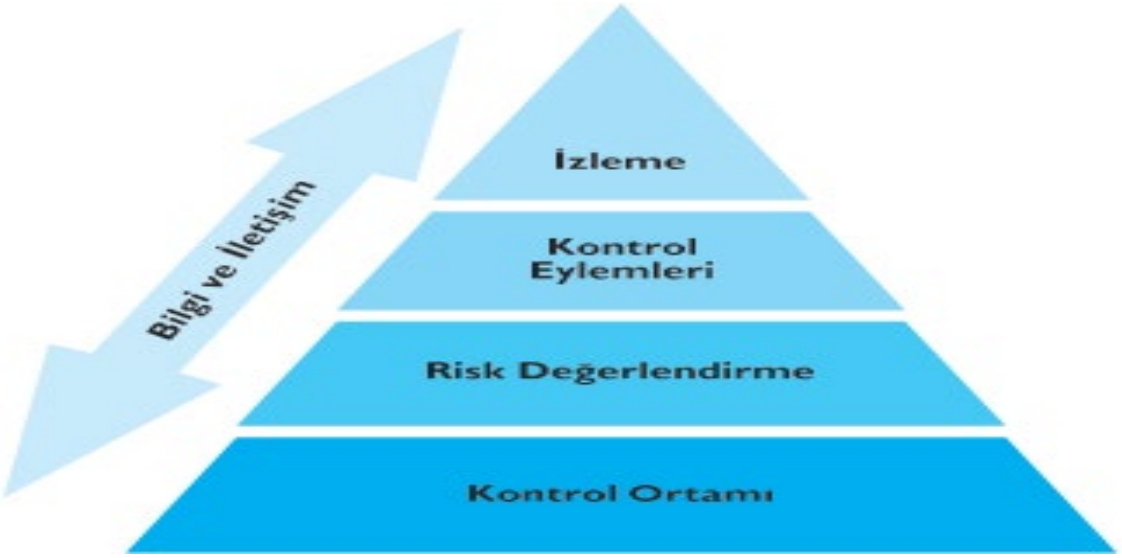
1.3.5.4. COSO (Committee of Sponsoring Organizations)

1980'li yılların başında ortaya çıkan muhasebe skandalları nedeniyle Hileli Finansal Raporlamalar Komisyonu (Treadway Komisyonu) tarafından bugün halen aktif faaliyet gösteren COSO kurulmuştur (Karakaya, 2016: 160). COSO gönüllü bir kuruluştur. Amerikan Mali Müşavirler Enstitüsü (American Institute of Certified Public Accountants-AICPA), Amerikan Muhasebe Derneği (American Accounting Association-AAA), Yönetim Muhasebecileri Enstitüsü (Institute of Management Accountants-IMA) ve Finans Yöneticileri Enstitüsü'nün (Financial Executives International-FEI) içinde bulunduğu bu yapının amacı, finansal raporlamanın kalitesinin artırılması amacıyla iç kontrol kavramının net olarak anlaşılmasını sağlamak ve işletmelerde uygulanabilmesi için yol gösterici önerilerde bulunmaktır.

COSO tarafından 1992 yılında yayınlanan ve 2013 yılında revize edilen İç Kontrol-Entegre Çerçevesi (Internal Control-Integrated Framework) ve 2004 yılında yayınlanan ve 2017 ismi de değiştirilerek güncellenen Kurumsal Risk Yönetimi-Riskin Strateji ve Performansla Uyumlaştırılması

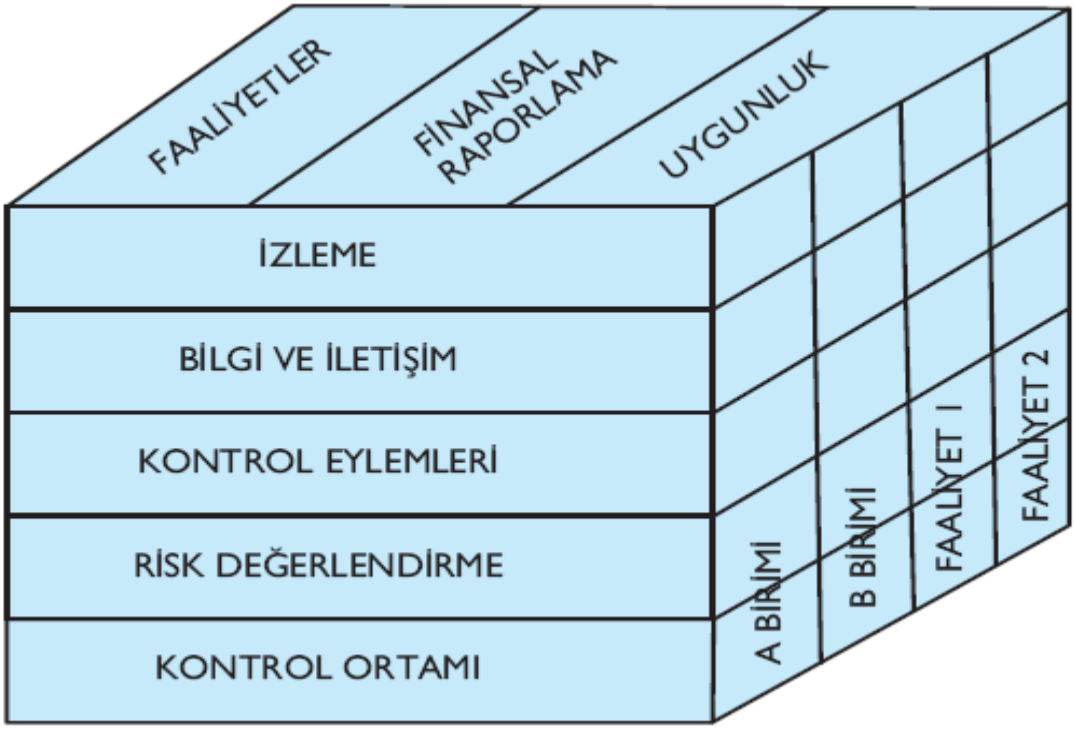
(Enterprise Risk Management—Aligning Risk with Strategy and Performance) olmak üzere iki çerçeve vardır.

İlk çerçeve, iç kontrole yönelik COSO iç kontrol modelini ortaya koyar. COSO tanımına göre iç kontrol, yönetim kurulu, üst düzey yönetim ve işletmenin diğer çalışanlarınca etkilenen ve işletme operasyonlarının etkinliği ve verimliliği, finansal raporlamanın güvenilirliği ve yasal düzenlemelere uyum hedeflerinin yerine getirildiğine dair makul bir güvence sağlamak amacıyla tasarlanan bir süreçtir. COSO modeli, iç kontrolün amaçlarının ve bileşenlerinin belirlendiği bütünleşik bir çerçeve sunar. Bu kapsamda, işletmelerde iç kontrol yapısının var olması birlirleriyle ilişkili beş iç kontrol bileşenleri ve 17 ilke ile mümkündür. Bu bileşenler, "*Kontrol Ortamı*", "*Risklerin Değerlendirilmesi*", "*Kontrol Faaliyetleri*", "*Bilgi Paylaşımı ve İletişim*" ve "*İzleme*"dir (Moeller, 2014: 36). COSO'nun ilk baştaki tasarımında iç kontrol unsurları, yukarıda bahsedilen beş ana unsurdan oluşan bir piramit olarak tasvir edilmiştir.



Şekil 24: COSO Piramidi

Yenilenmiş COSO'da ise, iç kontrol yapısı üç boyutlu bir küp şeklinde tasvir edilmiştir. Küpün üzerinde üç boyut bulunmaktadır; bunlar "*unsurlar*", "*iç kontrol amaçları*" ve "*örgüt yapısı*"dır. Unsurlar, yukarıda bahsedilen beş ana kategoriden oluşmaktadır. İç kontrol amaçları üç ana kategoride incelenmektedir: "*faaliyetler*", "*mali raporlama*" ve "*uygunluk*". Küpün üçüncü boyutundaki örgüt yapısında ise, işletmenin genel kurumsal yapısı, alt bölümleri, varsa iştirakleri ve detay fonksiyonları yer almaktadır.



Şekil 25: COSO Küpü

COSO piramidine ve COSO küpüne yukarıdaki şekillerde yer verilerek; COSO modelinin yukarıda sayılan beş unsuru aşağıda özetlenmiştir.

a. Kontrol Ortamı

Kontrol ortamı, iç kontrolün ne kadar başarılı olabileceğini belirleyen temel unsur olup, diğer dört unsur için temel oluşturur. İşletmenin faaliyetlerini yapma biçimini ifade eder. İşletmedeki iç kontrol ortamının sağlıklı ve etkin çalışabilmesi için üst yönetim ve çalışanların sorumluluk ve yetkilerinin sınırını iyi bilmesi gereklidir. Bir işletmenin çalışma disiplinin oluşumunda esas belirleyici olan yönetim kurulu ile üst yöneticilerdir. Dolayısıyla kontrol ortamının ana belirleyicisi olan çalışanlarının kontrol bilincinin üst yönetim tarafından etkilenebilme derecesidir (McNally, 2013: 5). Bu bileşene ilişkin ilkeler:

- Dürüstlük ve meslek ahlakı,
- Gözetim sorumluğu uygulamaları,
- Görev ve yetki dağılımların oluşturulması,
- Yetkinlik bağlılığının gösterilmesi,
- Hesap verebilirliği uygulanması.

b. Risklerin Değerlendirilmesi

İşletmeler, kendilerine tahsis edilen kaynakları amaç ve hedeflerine ulaşmak için kullanırlar. Bu kaynakların kullanımı için alınan kararlar yürütülen faaliyet, süreç ve projeler beraberinde riskleri de getirir. Risk yönetimi, işletmelerin amaç ve hedeflerine ulaşmalarına yardımcı olan bir araçtır. Risk yönetimi, risk stratejisinin belirlenmesi, risklerin tespit edilmesi, değerlendirilmesi, risklere cevap verilmesi, risklerin gözden geçirilmesi ve raporlanması aşamalarını kapsar (McNally, 2013: 5). Bu bileşene ilişkin ilkeler:

- Uygun hedefleri belirlenmesi,
- Risklerin belirlenmesi ve analiz edilmesi,
- Hile riskinin değerlendirilmesi,

- Risklerde meydana gelebilecek değişimlerin izlenmesi.

c. Kontrol Faaliyetleri

Kontrol faaliyetleri, öngörülen bir riskin etki ve/veya olasılığını azaltmayı ve böylece işletmenin amaç ve hedeflerine ulaşma olasılığını artırmayı amaçlayan eylemlerdir. Kontrol faaliyetlerinin belirlenmesi, risk değerlendirmesinin tamamlanmasına bağlıdır. Yönetim, görevlerin ve hedeflerin gerçekleştirileceğine dair makul güvence elde etmek için risk yönetimini esas almak suretiyle kontrol faaliyetlerini planlamalı, bunları organize etmeli ve yönlendirmelidir. Kontrol faaliyetleri finansal olan ve olmayan kontrolleri kapsamakta olup, işletmenin tüm faaliyetleri için bir bütün olarak tasarlanıp uygulanmalıdır (McNally, 2013: 5). Bu bileşene ilişkin ilkeler:

- Kontrol faaliyetlerinin seçilmesi ve uygulamaya konulması,
- Teknoloji genel kontrollerin uygulanmaya konulması,
- Politika ve süreçler yoluyla kontrol aktivitelerinin dağıtılması.

d. Bilgi Paylaşımı ve İletişim

İç kontrol yapısı, diğer dört unsur arasındaki ilişkiyi bilgi paylaşımı ve iletişim yoluyla sağlar. İşletme genelinde bilgi akışının düzenlenmesi, kurumsal amaç ve hedeflere ulaşma yolunda bir araç olarak görülen iç kontrol yapısının işlerliği ve uygulanma kabiliyetinin artmasında önemli bir role sahiptir. İletişim, bilginin işletme içinde gerek yatay ve dikey olarak, gerekse işletme dışında uygun mekanizmalarla ilgili kişi ve mercilere iletilmesini ve dönüşümünü ifade eder (McNally, 2013: 5). Bu bileşene ilişkin ilkeler:

- İlgili bilgileri kullanılması,
- İç iletişimin kurulması,
- Dış iletişimin kurulması.

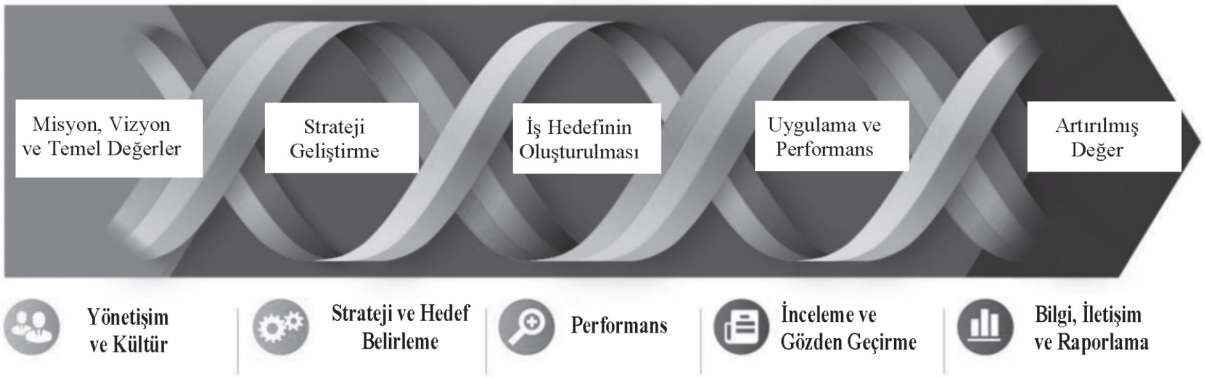
e. İzleme

İzleme, işletmenin amaç ve hedeflerine ulaşma konusunda iç kontrol yapısının beklenen katkıyı sağlayıp sağlamadığının, iç kontrol standartlarına uyum çerçevesinde değerlendirilmesi ve sistemin iyileştirmeye açık alanlarına yönelik eylemlerin belirlenmesidir. İzleme ile, işletmenin faaliyetlerinin misyon doğrultusunda, hedeflerle uyumlu olarak yürütülüp yürütülmediği, risk yönetimi esasları çerçevesinde gerekli kontrollerin öngörülüp öngörülmediği, söz konusu kontrollerin uygulanıp uygulanmadığı, iletişimin açık ve yeterli olup olmadığı gibi hususlar tespit edilip değerlendirilir (McNally, 2013: 5). Bu bileşene ilişkin ilkeler:

- Sürekli ve/veya ayrı değerlendirmeler yürütülmesi,
- Eksikliklerin değerlendirilmesi ve iletilmesi.

COSO iç kontrol modelinin, içeriğinin kapsayıcılığı, işletmelere uygulama rehberi sunması ve çağın gereklerine göre yenilenerek yaşayan bir model olması gibi nedenlerle dünya çapında en yaygın olarak kabul görmüş model olduğu görülür.

İkinci çerçeve, kurumsal risk yönetimine yönelik COSO risk yönetim modelini ortaya koyar. COSO tanımına göre kurumsal risk yönetimini, bir işletmenin hedeflerine ulaşmasını etkileyebilecek potansiyel olayları tanımlayan, risk alma istekliliği sınırları içinde yöneten ve işletme hedeflerinin başarılması konusunda makul derecede güvence sağlayan, işletme genelinde yapılandırılmış ve yönetim kurulundan, yönetimden ve diğer çalışanlardan etkilenen bir süreçtir. COSO modeli, kurumsal risk yönetiminin amaçlarının ve bileşenlerinin belirlendiği bütünleşik bir çerçeve sunar. Bu çerçeve 5 bileşen ve 20 ilkeden oluşmaktadır. Bu bileşenler, "*yönetişim ve kültür*", "*strateji ve hedef oluşturma*", "*perfomans*", "*gözden geçirme ve düzeltme*" ile "*bilgi, iletişim ve raporlama*"dır. Kurumsal risk yönetimi, işletmenin tüm aktivite ve süreçlerine entegre edilmesi; organizasyonun yönetişim, strateji, hedef belirleme ve günlük operasyonlarına ilişkin karar alma süreçlerini iyileştireceği, performansı artıracağı ve değerin oluşturulması, korunması ve sürdürülmesine katkı sağlayacağı belirtilmiştir.



Şekil 26: COSO Kurumsal Risk Yönetim Bileşenleri

COSO kurumsal risk yönetim bileşenlerine yukarıda yer verilerek; COSO modelinin yukarıda sayılan beş unsuru aşağıda özetlenmiştir.

a. Yönetişim ve Kültür

Yönetişim ve kültür, kurumsal risk yönetimin diğer unsurlarının temelini oluşturur. Yönetişim, işletmenin tonunu belirler. Yönetişim genel anlamda; rol, yetki ve sorumlulukların, paydaşlar, yönetim kurulu ve yönetim arasındaki dağılımına işaret eder. Yönetişim organizasyonun tarzını belirler, gözetim sorumluluklarını oluşturur. Kültür, yönetimin ve personelin kararlarını etkileyen tutum, davranış ve riski anlama şeklidir ve organizasyonun visyon, misyon ve temel değerlerini yansıtır. Bu bileşene ilişkin ilkeler:

- Yönetim kurulunun risk gözetimini uygulaması,
- Operasyonel yapının oluşturulması,
- Arzu edilen kültürün tanımlanması,
- Temel değerlere bağlılığın gösterilmesi,
- Yetenekli bireylerin kazanılması, geliştirilmesi ve elde tutulması.

b. Stareji ve Hedef Belirleme

Strateji planlama sürecinde, kurumsal risk yönetimi, strateji ve hedef belirlemeyle birlikte hareket ederler. Stratejiyle uyumlu, yönetim kurulu seviyesinde bir risk iştahı belirlenir. İş hedefleri; risklerin belirlenmesi, değerlendirilmesi ve cevap verilmesine esas oluşturur. İş hedefleri, stratejinin uygulamaya konulmasını sağlar ve kurumun günlük operasyonlarını ve önceliklendirmelerini şekillendirir. Bu bileşene ilişkin ilkeler:

- İş ortamının analiz edilmesi,
- Risk iştahının belirlenmesi,
- Alternatif stratejilerin değerlendirilmesi,
- İş hedeflerinin oluşturulması.

c. Performans

Strateji ve iş hedeflerine ulaşmayı etkileyebilecek riskler belirlenmeli ve değerlendirilmelidir. Riskler, risk iştahına göre önceliklendirilmelidir. Organizasyon daha sonra, riske vereceği cevabı seçer ve yükleneceği risklerin miktarını portföy (işletmenin her seviyesinde) bakış açısıyla belirler. Alternatif stratejiler ve/veya iş hedefleri için değerlendirilmesi gereken risk profilindeki değişiklikler, risklere cevaplar bir risk portföyü oluşturacağı ve bu portföyün izlenmesi, alternatif stratejiler ve/veya iş hedefleri ile portföyün çeşitlendirilmesi, tüm bu süreç ile entegre çalışacak bir kurumsal risk yönetimi anlayışı ile kurumun performansına bağlı oluşacak değerinin arttırılması ve sürdürülebilir kılınması için çalışılabilecektir. Bu bileşene ilişkin ilkeler:

- Risklerin tanımlanması,

- Risk şiddetlerinin değerlendirilmesi,
- Risklerin önceliklendirilmesi,
- Risk yanıtlarının uygulanması,
- Portföy bakış açısının geliştirilmesi.

d. İnceleme ve Revizyon

Organizasyon, önemli değişmeler ışığında, hedeflere göre performansın nasıl sonuçlandığını, kurumsal yönetim uygulamalarının iyi çalışıp çalışmadığını, işletmeye değer katıp katmadığı, değer katmaya devam edip etmediğini ve düzeltilmesi gereken hususlar bulunup bulunmadığını gözden geçirir. Bu bileşene ilişkin ilkeler:

- Önemli değişikliklerin değerlendirilmesi,
- Risk ve performansın incelenmesi,
- Kurumsal risk yönetiminde gelişmelerin takip edilmesi.

e. Bilgi, İletişim ve Raporlama

İletişim, bilginin elde edilmesi, kurum genelinde paylaşılmasıdır ve sürekli tekrar eden bir süreçtir. Yönetim, kurumsal risk yönetimini desteklemek için; hem içerden, hem de dışarıdan uygun olan bilgileri kullanır. Organizasyon, bilgi ve veriyi tutmak, işlemek ve yönetmek için bilgi sistemlerinden yararlanır. Tüm bileşenlere ilişkin bilgiyi kullanarak, organizasyon kültür, risk ve performansa ilişkin raporlama yapar. Bu bileşene ilişkin ilkeler:

- Bilgi ve teknolojiden yararlanılması,
- Riske ilişkin bilginin iletilmesi,
- Risk, kültür ve performans ile ilgili raporlama yapılması.

COSO tarafından yayınlanan yukarıda bahsedilen çerçeveler birbirlerinin yerine geçer nitelikte değildir. Kurumsal risk yönetimi çerçevei, iç kontrol çerçevesini genişleterek risk yönetimi ile birleştirmiştir. Kurumsal risk yönetimi işletmenin yönetim yapısını desteklemee iç kontrolden daha geniş bir role sahiptir.

1.3.5.5. ITIL (Information Technologies Infrastructure Library)

ITIL (Bilgi Teknolojisi Altyapı Kütüphanesi-Information Technologies Infrastructure Library) servis yönetim metodolojisi, bilgi teknolojileri servislerini eksiksiz ve en iyi kalitede yönetmek için geliştirilmiştir. ITIL, servis yönetimini en iyi şekilde sürdürmek için kullanıcılarına rehberlik etmektedir.

ITIL, 1980'li yıllarda İngiltere Ticaret Bakanlığı tarafından başlatılmış, bilgi teknolojileri altyapı ve hizmet süreçlerinin standartlaştırılmasını hedefleyen bir yaklaşımdır. ITIL'ın ilk versiyonu 1985 yılında yayınlanmıştır ancak bu yayınlar hakkında o döneme ait pek fazla bir bilgi bulunmaz. ITIL'ın, ikinci versiyonu ise 2001 yılında 8 kitap olarak yayınlanmış olup, bu versiyonda servis disiplinini ön plana çıkarmıştır. Son versiyonu olan ITIL v3 ise, 2007 yılında yayımlanmış ve bahse konu versiyonda bir önceki sürüme göre modülerden yaşam döngüsü yapısına geçilmiştir. Özetle, bir servisin planlanmasından sonlandırılmasına kadar ki süreci kapsamaktadır (ICAI, 2017: 4). Son olarak 2019 yılında ITIL v4 versiyonu yayınlanmıştır. Yeni versiyon, hizmet yönetimine yönelik daha bütünsel bir yaklaşımla ITIL'ı modern bilgi teknolojileri ortamı için daha geniş ve kapsayıcı hale getirmiştir.

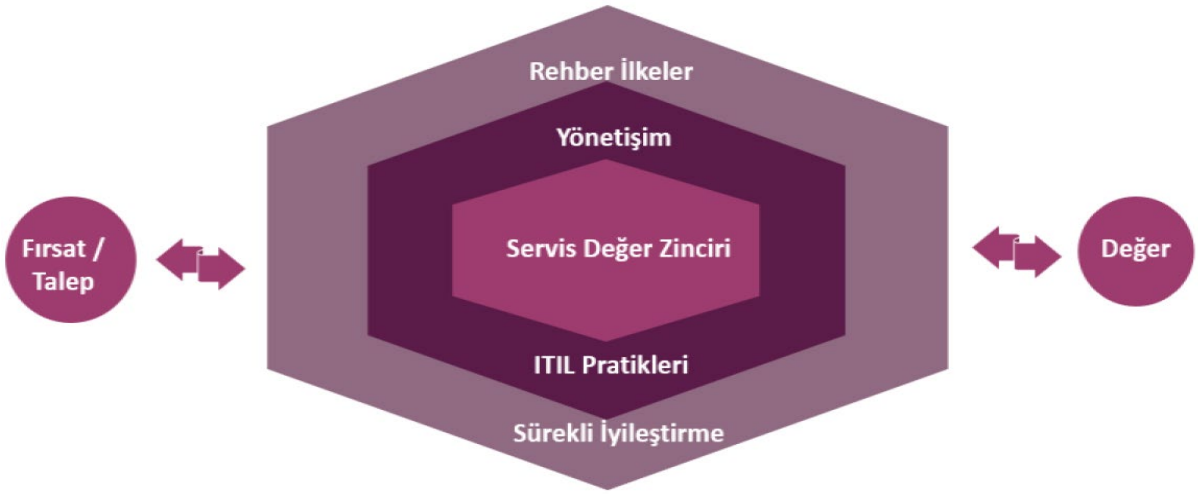
Bilgi sistemleri hizmet yönetimi, iş ihtiyaçlarına uygun bilgi sistemleri hizmetlerini planlama, tedarik etme, tasarlama, uygulama, işletme, destekleme ve geliştirme ile ilgilidir. ITIL, bilgi sistemleri hizmet yönetimi ve ilgili süreçler için kapsamlı ve tutarlı bir en iyi uygulama çerçevesi sağlamakta ve bilgi sistemleri hizmet yönetiminde etkinlik ve verimlilik sağlamak için yüksek kaliteli bir yaklaşım sunmaktadır. ITIL uygulayan işletmeler, maliyetleri düşürmeyi, erişilebilirliği artırmayı, kapasiteyi ayarlamayı, iş gücünü artırmayı, kaynakların verimli kullanılmasını sağlamayı ve ölçeklenebilirliği

artırmayı hedeflemektedir. ITIL'ın işletmelerin sistemlerine başarılı bir şekilde entegre edilmesi durumunda bu hedeflerin kendiliğinden gerçekleşmesi beklenmektedir.

Bu kapsamda ITIL'ın bilgi sistemleri hizmetleri için oluşturduğu bir yaşam döngüsü mevcuttur. Aşağıdaki şekilde yer verildiği üzere, ITIL bu hizmet yaşam döngüsünü 5 aşamada açıklar. Bu aşamalar, hizmet stratejisi, hizmet tasarımı, hizmet geçişi, hizmet operasyonu ve devamlı hizmet iyileştirme olarak belirlenmiştir. Özetlemek gerekirse, ITIL ile servis yönetim metodolojisi gerçekleştiren işletmeler, bir hizmet stratejisi ile uzun dönem hedeflerini belirlemiş olur. İşletmeler, bu doğrultuda bilgi sistemleri hizmetlerini tasarlar ve bu hizmetin canlı ortama geçişini gerçekleştirir. Daha sonra bu servisin sürekli ayakta kalması ve daha iyi hizmet verebilmek için daha iyiye doğru yol alması yönünde çalışmalar yapar.

Şekil 26: ITIL Yaşam Döngüsü

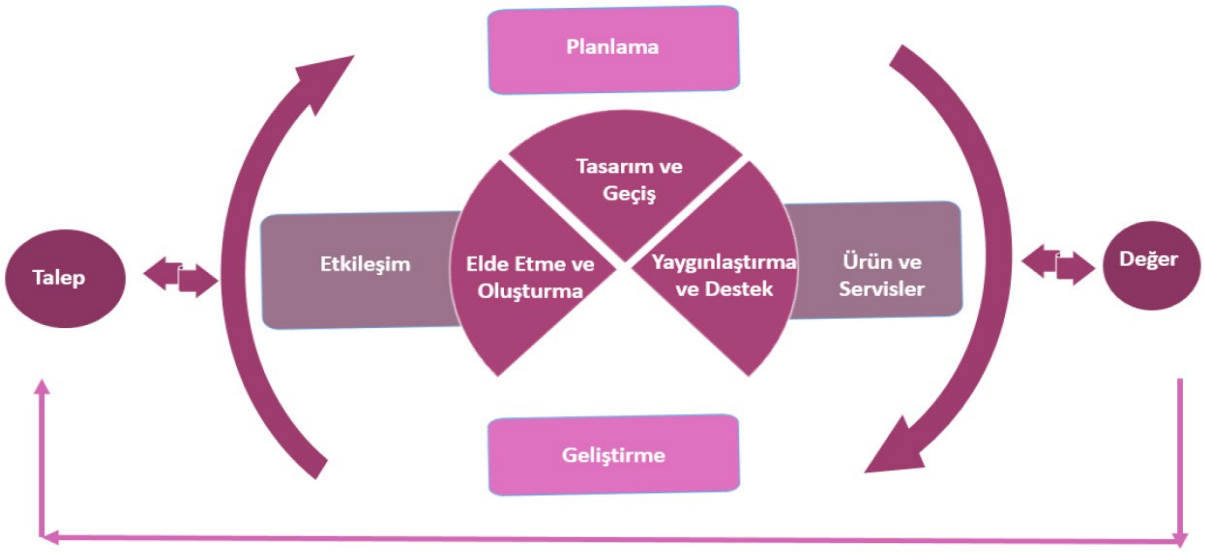
ITIL 4'de bilgi sistemleri yönetimi ve organizasyonel gereksinimlerin karşılanmasını temel alan 5 stratejik unsur yer alır. ITIL servis değer sistemini oluşturan bu 5 unsur; aşağıdaki Şekil-27'de verildiği üzere servis değer zinciri ve dört boyut modeli olarak adlandırılan ITIL pratikleri, rehber ilkeler, yönetişim ve sürekli iyileştirmedir



Şekil 27: ITIL Değer Sistemi

Servis değer sisteminin temel amacı, müşteri için değer üretimi için işletmenin bir bütün halinde çalışmasını sağlamaktır. Servis değer sisteminin ana girdileri fırsat ve talepler iken çıktısı değerdir. Fırsatlar, organizasyonu her alanda iyileştirebilecek seçeneklerdir. Talepler, organizasyonun tüm müşterilerinin sunulan ürün ve servislere duyduğu ihtiyaçtır. Değer ise ürün ve servisin algılanan faydasıdır. Servis değer sistemine göre fırsat ve taleplerin değere dönüştürülmesi için rehber ilkeler, yönetişim, servis değer zinciri, ITIL pratikleri ve sürekli iyileştirmenin organizasyonda doğru anlaşılması ve uygulanması gerekir.

Servis değer zinciri, ürün ve servislerin etkin yönetimi için ihtiyaç duyulan tüm faaliyetleri kapsayan bir işletim modelidir. Tüm servis sağlayıcı organizasyonlar iç-dış taleplerini müşterileri için değerli ürün ve servislere dönüştürebilmek amacıyla Şekil 28'de gösterilen 6 adet faaliyetin işletimine ihtiyaç duyar. Bu faaliyetler, planlama, geliştirme, etkileşim, tasarım ve geçiş, elde etme ve oluşturma, yaygınlaştırma ve destekten oluşur.



Şekil 28: ITIL Servis Değer Sistemi

ITIL, bir işletmenin iş süreçlerini desteklemeyi amaçlamakla birlikte dikte etmeyi amaçlamaz. ITIL çerçevesinin rolü, işletmelerin kendi uygulamalarını temel alabilecekleri yaklaşımları, işlevleri, rolleri ve süreçleri tanımlamaktır. ITIL'ın rolü, genel olarak uygulanabilir olan en düşük seviyede rehberlik vermektir (ITGI, 2008: 5). ITIL'in sağlayacağı yararlardan en önemlisi, hizmet geliştirme yaşam döngüsü boyunca boşa harcanan zaman ve para miktarını azaltırken, son ürünün kalitesini yükseltmesidir. Bu da, bir hizmet veya ürün uygulandıktan sonra müşteri memnuniyetini ve üzerinde çalışan personelin moralini büyük oranda artırır.

İşletmeye değer katılması, iş ve bilgi sistemleri stratejilerinin hizalanması, bilgi sistemleri servislerinin performansının sürekli takibi-iyileştirilmesi ve optimize edilmesi, bilgi sistemleri yatırım ve bütçesinin etkin yönetimi, risklerin takibi ve yönetimi, kaliteli servis sunumu için kabiliyet ve kaynakların yönetimi, işletme genelinde bilgi sistemleri yönetimi için ortak bir kültürün benimsenmesi ve tüm paydaşlarla etkin iletişim konusunda sağladığı faydalar dolayısıyla ITIL işletmeler tarafından sıklıkla tercih edilen bir yönetim çerçevesidir.

1.3.5.6. ISA (Uluslararası Denetim Standartları-International Standards on Auditing)

IAASB (Uluslararası Denetim ve Güvence Standartları Kurulu-International Auditing and Assurance Board), bağımsız denetim, sınırlı bağımsız denetim (inceleme), kalite kontrol ile diğer güvence ve ilgili hizmetler için uluslararası düzeyde kamu yararını dikkate alarak genel kabul gören ve yüksek kalitede standartlar oluşturan uluslararası bağımsız bir standart yapıcıdır. IAASB diğer uluslararası standartların yanında Uluslararası Denetim Standartlarını (UDS-ISA) yayınlamakta ve uluslararası yaygınlaştırılmasını desteklemektedir. ISA, genel olarak finansal tabloların denetiminde kullanılmakla birlikte, işletmenin kontrol ortamına yönelik hususlar içermesi ve bağımsız denetiminin planlanması, raporlanması, denetim örneklemesi ve uygulanan denetim prosedürleri bakımından bilgi sistemleri denetimine benzerlik göstermesi nedeniyle kıyasen uygulanması mümkündür. Nitekim, gerek Kurul'un gerekse BDDK'nın bilgi sistemlerine ilişkin düzenlemelerinde, ISA'lardan alınmış ifadeler veya ISA'lara atıflar bulunur.

ISA altında yer alan bazı standartlarda bilgi sistemleri denetimine ilişkin kontroller yer almaktadır. Bu maddelerin bazıları denetçinin işletmenin finansal raporlamasında yer alan bilgi sistemleri yapısı hakkında bilgi sahibi olması gerektiğine vurgu yaparken, bazıları ise risk değerlendirmesinde bilgi sistemi uzmanlığına ihtiyaç duyulduğunu ve denetim kanıtları elde edilirken

bilgi sistemleri genel kontrollerine bakılması gerektiğini ifade eder. Bilgi sistemleri denetimine ilişkin hükümler bulunan veya bilgi sistemleri bağımsız denetiminde kıyasen uygulanabilecek ISA'ları aşağıda özetlenmiştir.

ISA 240: Bu standart finansal tabloların denetiminde, denetçinin hileye ilişkin sorumlulukları ile hile kaynaklı önemli yanlışlık risklerine ilişkin olarak ISA 315 ve ISA 330'un nasıl uygulanacağını detaylı olarak ele almaktadır. Bu standartta, yanlışlıkların hata veya hile kaynaklı olabileceği; hileyi hatadan ayıran unsurun ise kasıtlı yapılması olduğu belirtilmektedir. Denetçi, hileli finansal raporlamadan kaynaklanan yanlışlıklar ve varlıkların kötüye kullanılmasından kaynaklanan yanlışlıklar olmak üzere iki tür kasıtlı yanlışlıkla ilgilenmelidir. Yönetim tarafından yapılan hile (yönetim hilesi) kaynaklı önemli yanlışlığı tespit edememe riski, çalışanların yaptığı hileyi tespit edememe riskinden daha yüksektir. Hilenin önlenmesi ve tespit edilmesine ilişkin esas sorumluluk, işletme yönetimine aittir. Yönetimin, imkân veren fırsatları azaltarak hileyi önleme ve hilenin tespit ve cezalandırılma ihtimali sebebiyle kişileri hileye teşebbüsten caydırma konusunda güçlü bir tutum sergilemesi önemlidir. Bu tutum, yönetimin aktif gözetimiyle güçlendirilebilecek bir dürüstlük ve etik davranış kültürü oluşturulmasını gerektirir.

Burada denetçinin sorumluluğu, denetim standartlarına uygun olarak denetimi planlayarak yürütmek ve bir bütün olarak hata veya hile kaynaklı önemli bir yanlışlığın bulunmadığına ilişkin makul güvence sağlamaktır. Ancak, denetimin yapısal kısıtlamaları sebebiyle kaçınılmaz olarak bazı önemli yanlışlıkların tespit edilememe riski bulunur.

Anılan standardın A35'üncü paragrafında özetle, denetçinin, denetim sırasında adli bilişim ve bilgi sistemleri gibi teknik bilgi ve beceri gerektiren alanlarda, bu alanda bilgi ve deneyim sahibi kişi veya kişileri görevlendirerek finansal raporlama denetimlerinde karşılaşılan hile kaynaklı önemli risklere karşılık verilebileceği ifade edilmektedir.

ISA 265: Bu standart. denetçinin finansal tabloların denetimi sırasında tespit ettiği iç kontrol eksikliklerini uygun bir biçimde işletmenin yönetimden sorumlu kişilere bildirmesine yönelik sorumluluğunu düzenler. Bu standart denetçiye, işletmenin iç kontrol sisteminin anlaşılması ve kontrol testlerinin tasarlanması ve uygulanması bakımından, BDS 315 ve BDS 330 hükümlerinde yer alan sorumluluklara ilâve sorumluluklar yüklemez. "*Önemli yanlışlık*" risklerinin belirlenmesi ve değerlendirilmesi sırasında denetçinin işletmenin iç kontrol sistemini anlaması gerekir.

Denetçinin, denetim sırasında tespit edilen önemli iç kontrol eksikliklerini üst yönetimden sorumlu olanlara zamanında ve yazılı olarak bildirmesi gerekmektedir.

ISA 300: Bu standart, hem ilk denetimin hem de yinelenen denetimin planlanmasında denetçinin sorumluluklarını ele almaktadır. Bu standart, BSBD Tebliğ'inde de bilgi sistemleri bağımsız denetiminin planlanması bakımından kıyasen uygulanacağı hüküm altına alınmıştır. Denetimin planlanması, denetime yönelik genel denetim stratejisinin oluşturulması ile denetim planının geliştirilmesini kapsar. Bu standartta, denetim stratejisinin oluşturulması aşamasında verilerin erişilebilirliği ve bilgisayar destekli denetim tekniklerinin kullanımı dâhil olmak üzere, bilgi sistemlerinin planlanan denetim metodolojisi üzerindeki etkisi ile bilgi teknolojisi ve iş süreçlerindeki değişiklerin dikkate alınması gerektiği ifade edilmektedir.

ISA 315: Bu standart, denetçinin işletmenin iç kontrolleri dâhil olmak üzere, işletme ve çevresini tanımak suretiyle finansal tablolardaki önemli yanlışlık risklerini belirleme ve değerlendirme sorumluluğunu düzenler. Burada amaç, finansal tablo ve yönetim beyanı düzeylerinde hata veya hile kaynaklı "*önemli yanlışlık*" risklerini belirlemek ve değerlendirmek ve böylece "*önemli yanlışlık*" riski olarak değerlendirilen risklere karşı yapılacak işlerin tasarlanması ve uygulanması için bir dayanak oluşturur. Yönetim beyanı düzeyindeki "*önemli yanlışlık*" riskleri, yapısal risk ve kontrol riski olmak üzere iki bileşenden oluşur ve ayrı ayrı değerlendirilmelidir. Yapısal risk faktörleri nitel ya da nicel olabilir. Nitel yapısal risk faktörleri:

- Karmaşıklık,
- Subjektiflik,
- Değişiklik,

- Belirsizlik veya
- Yapısal riski etkiledikleri ölçüde, yönetimin taraflılığı veya diğer hile riski faktörleri nedeniyle yanlışlığa olan açıklık.

Bu standartta, bilgi sistemleri konusu iç kontroldeki önemi nedeniyle yoğun bir şekilde ele alınmıştır. Burada, bilgi işleme kontrolleri, bilgi teknolojisi çevresi, bilgi teknolojisi uygulamaları, bilgi teknolojisi altyapısı, bilgi teknolojisi kullanımından kaynaklanan riskler ve genel bilgi teknolojisi kontrollerine ilişkin tanımlamalar yapılmıştır. Bilgi işleme kontrolleri, işletmenin bilgi sistemindeki bilgi teknolojisi uygulamalarında veya manuel bilgi süreçlerinde bilginin işlenmesiyle ilgili olan ve doğrudan bilginin bütünlüğüyle (işlemlerin ve diğer bilgilerin tamlığı, doğruluğu ve geçerliliğiyle) ilgili riskleri ele alan kontrollerdir. Bilgi teknolojisi çevresi, işletmenin, faaliyetlerini desteklemek ve iş stratejilerini başarıyla uygulamak için kullandığı bilgi teknolojisi uygulamaları ve destekleyici bilgi teknolojisi altyapısının yanı sıra bilgi teknolojisi süreçleri ve bu süreçlerde yer alan personeldir. Bilgi teknolojisi uygulaması, işlem veya bilgilerin başlatılması, işlenmesi, kaydedilmesi ve raporlanması için kullanılan bir program veya program setidir. Bilgi teknolojisi altyapısı, ağ, işletim sistemleri, veri tabanları ile bunlarla ilgili donanım ve yazılımlardan oluşur. Bilgi teknolojisi süreçleri, bilgi teknolojisi çevresine erişimi yönetme, program değişikliklerini veya bilgi teknolojisi çevresinde meydana gelen değişiklikleri yönetme ve bilgi teknolojisi operasyonlarını yönetmeye ilişkin işletme süreçleridir. Bilgi teknolojisi kullanımından kaynaklanan riskler, işletmenin bilgi teknoloji süreçlerindeki kontrollerin etkin olmayan tasarımı veya işleyişi nedeniyle; işletmenin bilgi sistemi içinde bilgi işleme kontrollerinin etkin olmayan tasarım ve işleyişe olan açıklığıdır veya bilgilerin bütünlüğüne yönelik risklerdir. Genel bilgi teknolojisi kontrolleri, işletmenin bilgi sistemi içinde bilgi işleme kontrollerinin etkin biçimde işlemeye devam etmesi ve bilginin bütünlüğü dâhil olmak üzere, işletmenin bilgi teknolojisi çevresinin sürekli doğru biçimde çalışmasını destekleyen, işletmenin bilgi teknolojisi süreçleri üzerindeki kontrollerdir.

Bu standartta, önemli yanlışlık risklerinin belirlenmesi ve değerlendirilmesine yönelik risk değerlendirme prosedürlerinin uygulanacağı; risk belirleme ve değerlendirme sürecinin yinelenen ve dinamik bir süreç olduğu; ancak, tek başına risk değerlendirme prosedürleri denetim görüşüne dayanak oluşturacak yeterli ve uygun denetim kanıtı sağlayamayacağı ve risk değerlendirme prosedürleri olarak, işletme yönetiminin, varsa iç denetim fonksiyonundaki uygun kişilerin ve denetçi tarafından uygun görülen diğer kişilerin sorgulanması, analitik prosedürlerin uygulanması ile gözlem ve tetkikin kullanılacağı belirtilmiştir.

Standartta, iç kontrol sistemi, finansal raporlamanın güvenilirliği, faaliyetlerin etkinliği ve verimliliği ile ilgili mevzuata uygunluk açısından işletmenin amaçlarına ulaştığına dair makul güvence sağlamak amacıyla üst yönetimden sorumlu olanlar, yönetim ve diğer personel tarafından tasarlanan, uygulanan ve sürekliliği sağlanan sistem olarak tanımlanmıştır. Denetçi iç kontrol bileşenleri olan, kontrol çevresi, risk değerlendirme süreci, iç kontrol sistemini izleme süreci, bilgi sistemi ve iletişim ile kontrol faaliyetleri hakkında kanaat edinmelidir.

Bu standarda göre, denetçi işletmenin ilgili iş süreçleri dâhil finansal raporlamayla ilgili bilgi sistemi ve işletmenin bu bilgi sistemlerinden kaynaklanan risklere nasıl karşılık verdiği hakkında bilgi edinmelidir. Standardın açıklayıcı hükümler ve uygulama örnekleri kısmında, denetçinin işletmenin bilgi sistemleri ve bilgi sistemleri kontrollerinin anlışılması ile bilgi sistemleri risklerinin tespiti ve değerlendirilmesine yönelik rehberlik sağlayan kapsamlı açıklama içeren hükümler yer almaktadır.

ISA 330: Bu standart, finansal tabloların denetimi sırasında, ISA 315'e uygun olarak belirlenen ve değerlendirilen önemli yanlışlık riski barındıran alanlara karşı uygulanacak denetim prosedürlerini tasarlamak ve uygulamakla yükümlü olan denetçinin sorumluluğunu açıklar. Denetçinin amacı, önemli yanlışlık risklerine karşı uygun denetim prosedürlerini tasarlayıp, uygulayarak yeterli ve uygun denetim kanıtı elde etmektir. Denetim prosedürleri, kontrol testleri veya maddi doğrulama prosedürleri olarak ikiye ayrılmıştır. Bu standartta, kontrollerin testine ilişkin esaslarda düzenlenmiştir. Kontrol testi, yönetim beyanı düzeyindeki önemli yanlışlıkları önleme veya tespit edip düzeltmede kontrollerin işleyiş etkinliğini değerlendirmek üzere tasarlanmış denetim prosedürü olarak tanımlanmıştır.

Bu standarda göre, denetçi önceki denetimlerden elde edilen denetim kanıtlarının kullanılmasının uygun olup olmadığına karar verirken genel bilgi sistemleri kontrollerinin halen etkin

olup olmadığına bakması gerekmektedir. Ayrıca, bu standardın açıklamalarında, bilgisayar destekli denetim teknikleri kullanılmasının, elektronik işlemlerin ve hesapların daha kapsamlı test edilebilmesini sağlacağı ve ana elektronik dosyalardan örnek işlemler seçmek, belirli özellikleri olan işlemleri sınıflandırmak veya bir örneklem yerine ana kitlenin tamamını test etmek için kullanılabileceği belirtilmiştir.

ISA 402: Bu standart, dışarıdan hizmet alan bir işletmenin bir veya daha fazla hizmet kuruluşu kullanması halinde, denetçinin bu hizmet sağlayıcılar hakkında da yeterli ve uygun denetim kanıtı elde etme sorumluluğunu düzenler. Burada amaç, "*önemli yanlışlık*" risklerinin belirlenmesi ve değerlendirilmesi için uygun bir dayanak sağlamaya yetecek ölçüde, hizmet kuruluşundan sağlanan hizmetlerin niteliği ve önemi ile bu hizmetlerin hizmet alan işletmenin iç kontrol sistemi üzerindeki etkisini anlamak ve bu risklere karşı denetim prosedürlerini tasarlamak ve uygulamaktır.

Bu standarda göre, işletmenin finansal raporlamaya ilişkin bilgi sistemleri faaliyetleri destek hizmeti kapsamında dışarıdan bir kuruluş tarafından sağlanıyorsa, söz konusu kuruluşun sağladığı hizmete yönelik kontrollerinin, denetim kapsamında değerlendirilmesi gerekir.

1.3.6. Etik İlke ve Kurallar (Bağımsız Denetçiler İçin Etik Kurallar ve ISACA'nın Etik Kuralları)

Bilgi sistemleri denetçilerine yönelik uygulanacak etik ilkelere bakıldığından, mevzuatla KGK'nın Etik Kuralları'nın zorunlu kılındığı görülmektedir. Uluslararası düzenleyici kuruluş olarak ISACA tarafından yayınlanan etik kurallar da bulunmaktadır. Bu kısımda, bu iki etik kural seti ele alınacaktır.

1.3.6.1. Bağımsız Denetçiler İçin Etik Kurallar

BSBD Tebliği'nin 17'nici maddesi uyarınca, sermaye piyasasında bilgi sistemleri denetimi yapmak üzere yetkilendirilen bağımsız denetim kuruluşları ile bunların bünyesinde çalışan bilgi sistemleri denetçileri için etik kurallar bakımından KGK tarafından yayınlanan "*Bağımsız Denetçiler İçin Etik Kurallar*" (bundan sonra Etik Kurallar) kıyasen uygulanmaktadır. Etik Kurallar, Uluslararası Etik Standartları Kurulu (International Ethics Standards Board for Accountants-IESBA) tarafından oluşturulmuş Uluslararası Etik Kodu'nun Türkçe tercümesinden oluşmaktadır. Etik Kurallar'ın giriş bölümünde denetçilik mesleği ve denetçinin sorumluluğu hususunda aşağıdaki ifade yer almaktadır:

"Denetçilik mesleğinin ayırt edici özelliklerinden biri, kamu yararına hareket etme sorumluluğunu kabul etmesidir. Dolayısıyla bir denetçinin sorumluluğu, yalnızca tek bir müşterinin veya işverenin ihtiyaçlarını karşılamak değildir. Denetçi, kamu yararı doğrultusunda hareket ederken Bağımsız Denetçiler İçin Etik Kurallar'ı (Etik Kurallar veya Kurallar) gözetir ve bu Kurallara uygunluk sağlar."

Etik Kurallar, "*Etik Kurallara Uyum, Temel İlkeler ve Kavramsal Çerçeve*", "*Bağımsız Denetçiler*" ve "*Bağımsızlık Standartları (Kısım 4A ve 4B)*" olmak üzere üç kısımdan oluşur. Bağımsızlık Standartları, bağımsız denetim ve sınırlı bağımsız denetimde bağımsızlığa ilişkin hususları içeren A bölümü ile bağımsız denetim ve sınırlı bağımsız denetim dışında kalan güvence denetiminde bağımsızlığa ilişkin hususları içeren B bölümünden oluşur. Burada, ilk kısım ile bağımsızlığa ilişkin standartların A bölümü (bilgi sistemleri bağımsız denetimi ile bağımsız denetim ilişkisi ve özellikleri dikkate alınarak) ele alınacaktır.

1.3.6.1.1. Etik Kurallara Uyum, Temel İlkeler ve Kavramsal Çerçeve

Denetçi, Etik Kurallar'a uymakla yükümlüdür. Mevzuatın Etik Kurallar'da yer alan hükümlerden daha kısıtlayıcı hükümler öngörmesi durumunda, denetçi söz konusu mevzuata uymak zorundadır. Etik Kurallar'ın bazı hükümlerine uyulmasının mevzuatla kısıtlandığı durumlar olabilir. Böyle durumlarda denetçi, başta söz konusu mevzuat olmak üzere Etik Kurallar'ın diğer hükümlerine uymakla yükümlüdür. Mesleğe uygun davranış ilkesi, denetçinin mevzuata uymasını zorunlu kılar.

Etik Kurallar, denetçilerden beklenen yüksek kaliteli etik davranış standartlarını belirler ve uyulması denetçilerin kamu yararına hareket etme sorumluluklarını yerine getirmelerini sağlar. Bağımsızlık ihlali dışındaki Etik Kurallar'ın ihlalinin tespit edilmesi durumunda, denetçi söz konusu ihlalin ciddiyetini ve denetçinin temel ilkelere uyma kabiliyetine olan etkisini değerlendirmelidir.

Ayrıca, denetçi ihlalin sonuçlarını tatminkâr bir şekilde ele alabilecek tüm adımları, en kısa sürede atmak ve ihlalin ilgili taraflara bildirilip bildirilmeyeceğine karar vermekle yükümlüdür.

1.3.6.1.1.1. Temel Etik İlkeler

Denetçiler için beş temel etik ilke bulunmaktadır. Bunlar:

1. Dürüstlük,
2. Tarafsızlık,
3. Mesleki yeterlilik ve özen,
4. Sır saklama,
5. Mesleğe uygun davranış.

Denetçinin söz konusu beş temel etik ilkenin her birini uyması gerekmektedir. Bu ilkeler, denetçiden beklenen standart davranışları belirleyerek, sınırlarını çizer.

Dürüstlük: Dürüstlük, bütün mesleki ve iş ilişkilerinde dürüst, açık, doğru ve güvenilir olmaktır. Dürüstlük doğru iş yapmayı, güvenilir olmayı ve bu şekilde hareket etmek olumsuz kişisel veya kurumsal sonuçlara yol açabilecek olsa ya da aksi şekilde hareket etme baskısıyla karşı karşıya kalınsa dahi uygun şekilde davranma gücüne sahip olmayı içerir. Buna göre denetçi, elde ettiği bilgilerin önemli düzeyde yanlış veya yanıltıcı beyan içerdiğini, dikkatsizce sunulmuş beyan veya bilgi içerdiğini veya içermesi gereken bilgileri göz ardı ettiğini veya gizlediğini, dolayısıyla yanıltıcı mahiyette olduğunu düşündüğü durumlarda bu bilgileri içeren raporlar, beyannameler, yazışmalar veya diğer bilgiler ile bilerek ilişkilendirilmemesi gerekir. Denetçinin, bu tür bilgilerle ilişkilendirildiğini fark etmesi durumunda; söz konusu bilgilerle ilişkilendirilmesini sonlandırmak için gerekli adımları atması zorunludur. Böyle bir hususla ilgili olumlu görüş dışında bir görüş içeren rapor sunan denetçi, dürüstlük ilkesini ihlal etmiş sayılmaz.

Tarafsızlık: Tarafsızlık, önyargıların, temayüllerin, çıkar çatışmalarının veya başkalarının nüfuzlarını kötüye kullanarak meslek veya işle ilgili muhakemelerini ve kararlarını etkilemesine izin vermemektir. Tarafsızlık ilkesi, denetçiye, önyargıların, temayüllerin, çıkar çatışmalarının veya başkalarının nüfuzlarını kötüye kullanarak meslek veya işle ilgili yargıları ve kararlarını etkilemesine izin vermeme yükümlülüğü getirir. Denetçi, tarafsızlığa zarar verebilecek, tarafsızlığı zedeleyebilecek durumlara maruz kalabilir. Bu tür durumların hepsinin tanımlanması ve öngörülmesi mümkün değildir. Herhangi bir durum veya ilişkinin, mesleki hizmeti veya faaliyetiyle ilgili muhakemesinin tarafsızlığını bozması veya uygunsuz şekilde etkilemesi durumunda denetçi, söz konusu mesleki hizmeti veya faaliyeti yürütmez.

Mesleki yeterlik ve özen: Mesleki yeterlik ve özen, güncel teknik ve mesleki standartlar ile mevzuata uygun olarak, müşterilerin yeterli mesleki hizmetleri almalarını temin edecek mesleki bilgi ve beceriyi elde etmek ve korumak ile uygulamadaki teknik ve mesleki standartlara uygun bir şekilde ve özen içinde hareket etmektir. Bu ilke denetçiye, güncel teknik ve mesleki standartlar ile mevzuata uygun olarak, müşterilerin yeterli mesleki hizmetleri almalarını temin edecek mesleki bilgi ve beceriyi elde etme ve koruma yükümlülüğü ile uygulamadaki teknik ve mesleki standartlara uygun bir şekilde ve özen içinde hareket etme yükümlülüğü getirir.

Yeterli mesleki hizmet, hizmet yerine getirilirken mesleki bilgi ve becerinin uygulanması sırasında doğru yargılarda bulunulmasını gerektirir. Mesleki yeterlik, mesleki yeterliğin kazanılması ve mesleki yeterliğin sürdürülmesi olmak üzere iki aşamaya ayrılabilir. Mesleki yeterliğin sürdürülmesi; ilgili teknik, mesleki ve iş hayatına ilişkin gelişmelerin anlaşılmasını ve bunlara yönelik sürekli bir farkındalığı gerektirir. Sürekli mesleki gelişim, denetçinin mesleki çevrede yeterli bir şekilde faaliyet gösterebilmesi için gerekli kabiliyetleri geliştirebilmesine ve sürdürebilmesine imkân sağlar.

Özen, bir görevin gereklilikleri uyarınca dikkatli, derinlemesine ve zamanında hareket etme sorumluluğunu kapsar. Denetçi, mesleki faaliyet kapsamında, maiyetinde çalışan kişilerin uygun hizmet içi eğitim almasını ve gözetime tabi olmasını temin etmek üzere gerekli adımları atmalıdır. Denetçi,

uygun hallerde, müşterilerin ve denetçinin mesleki hizmetlerinden veya faaliyetlerden faydalanan diğer tarafların, bu hizmetlerde bulunan yapısal kısıtlamalardan/kısıtlardan haberdar olmasını sağlamalıdır.

Sır saklama (gizlilik): Sır saklama, mesleğin icrası sırasında elde edilen bilgilerin gizliliğine riayet etmektir. Sır saklama ilkesi, denetçiye, mesleğin icrası sırasında edindiği gizli bilgileri, bu bilgilerin açıklanması için yasal veya mesleki bir hak veya görev ya da uygun ve belirli bir yetki olmaksızın denetim şirketi dışında bir tarafa açıklama ve mesleğin icrası sırasında edindiği gizli bilgileri, kendisinin veya üçüncü kişilerin çıkarlarına kullanma durumlarından kaçınma yükümlülüğü getirir.

Denetçi:

- Bulunulan sosyal ortamlar da dâhil olmak üzere, başta çekirdek ailesinin bir üyesine, aile yakınlarından birine veya yakın bir iş arkadaşına, kasıtsız bir şekilde bilgi verme, açıklama ihtimaline karşı dikkatli olmalıdır.
- Sır saklama yükümlülüğü denetim şirketi bünyesinde de sürdürmelidir.
- Potansiyel bir müşteri tarafından açıklanan bilgilere ilişkin sır saklama yükümlülüğünü sürdürmelidir.
- Mesleki faaliyetler sırasında edindiği gizli bilgileri, bu bilgilerin açıklanması için yasal veya mesleki bir görev veya hak ya da uygun ve belirli bir yetki olmaksızın denetim şirketi dışında bir tarafa açıklayamaz.
- Mesleki faaliyetler sırasında edindiği gizli bilgileri, kendisinin veya üçüncü kişilerin menfaatlerine kullanamaz.
- Mesleki veya iş ilişkileri kapsamında edindiği veya aldığı herhangi bir gizli bilgiyi söz konusu ilişki sona erdikten sonra kullanamaz veya açıklayamaz.
- Denetçi, gözetimi altındaki çalışanlar ile danışmanlık ve yardım aldığı kişilerin, sır saklama yükümlülüğüne uymalarını sağlamak üzere uygun adımları atmalıdır.

Temel bir ilke olarak sır saklama; bilginin, müşteriden denetçiye serbestçe aktarılmasına imkân sağladığından kamu yararına hizmet eder. Bununla birlikte, denetçinin gizli bir bilgiyi açıklamasının gerektiği veya gerekebileceği ya da bu tür bir açıklamanın uygun olabileceği durumlar aşağıda yer almaktadır:

- Hukuki takip sürecinde belge ve diğer kanıtların toplanması veya ortaya çıkan mevzuat ihlallerinin kamu yetkililerine açıklanması gibi mevzuatın açıklama yapmayı zorunlu tutması,
- Mevzuat tarafından açıklamaya izin verilmesi ve müşteri tarafından açıklama yapmak üzere yetkilendirilmesi,
- Hukuki takip sürecinde belgelerin ve diğer kanıtların toplanması veya ortaya çıkan mevzuat ihlallerinin yetkililere açıklanması gibi mevzuat tarafından açıklama yapmanın zorunlu tutulması,
- Mevzuatla yasaklanmadığı sürece, yetkililerce kalite inceleme sürecine uygunluk sağlama, yetkililerce yapılan bir sorgulamaya veya araştırmaya/incelemeye cevap verme, hukuki takip sürecindeki bir denetçinin mesleki çıkarlarını koruma veya Etik İlkeler dahil teknik ve mesleki standartlara uygunluk sağlama amaçlarıyla açıklamanın mesleki bir görev veya hak olması.

Gizli bir bilginin açıklanıp açıklanmayacağına karar verirken; müşterinin, bilgilerin denetçi tarafından açıklanmasına razı olması durumunda, çıkarları etkilenebilecek üçüncü taraflar dâhil olmak üzere, tüm tarafların çıkarlarının zarar görüp görmeyeceği, mümkün olduğu ölçüde, ilgili tüm bilgilerin bilinen ve doğrulanabilir bilgiler olup olmadığı, beklenen iletişim şekli ve bu iletişimin muhatabı olan kişi, iletişimin muhatabı olan tarafların, bilgi alması uygun kişiler olup olmadığı gibi etkenler dikkate alınmalıdır.

Denetçi, denetim ilişkinin sona ermesinden sonra da sır saklama yükümlülüğü bulunmaktadır. Yeni bir müşteri edinmesi durumunda denetçi, önceki deneyimlerini kullanma hakkı bulunmakla birlikte; mesleki veya iş ilişkileri sonucunda edindiği veya kendisine ulaşan herhangi bir gizli bilgiyi kullanamaz veya açıklayamaz.

Mesleğe uygun davranış: Mesleğe uygun davranış, ilgili mevzuata uymak ve denetim mesleğinin itibarını zedeleyici tutum ve davranışlardan kaçınmaktır. Mesleğe uygun davranış ilkesi, denetçiye, ilgili mevzuata uyma, tüm mesleki faaliyetlerde ve iş ilişkilerinde mesleğin kamu yararına hareket etme sorumluluğuyla tutarlı olacak şekilde davranma ve mesleğin itibarını zedeleyeceğini bildiği veya bilmesi gereken her tür tutum ve davranıştan kaçınma yükümlülüğü getirir. Bu kaçınma yükümlülüğü; gerekli bilgiye sahip makul üçüncü bir tarafın, denetçinin o an için erişiminde bulunan tüm özel durum ve gerçekleri değerlendirmek suretiyle mesleğin itibarını kötü yönde etkileyeceği sonucuna varmasının daha muhtemel olduğu tüm tutum ve davranışları içerir.

Denetçi, dürüstlük ve tarafsızlık ilkelerine veya mesleğin itibarına zarar veren veya verebilecek ve sonuç olarak temel ilkelerle uyumsuzluk oluşturacak herhangi bir iş, meslek veya faaliyet ile bilerek uğraşamaz. Denetçi, pazarlama ve tanıtım çalışmalarında kendisini tanıtırken mesleğin itibarına gölge düşüremezler. Denetçiler, açık sözlü ve dürüst olurlar ve sunabilecekleri hizmetler, taşıdıkları nitelikler ve edindikleri tecrübeler konusunda aşırıya kaçan iddialarda bulunamazlar veya başkalarının işleriyle ilgili kötüleyici referanslar veremezler veya mesnetsiz karşılaştırmalar yapamazlar.

Denetçi, bir temel ilkeye uyması hâlinde başka bir veya birden fazla temel ilkeyle çatışmasının söz konusu olabileceği bir durumla karşılaşabilir. Bu durumda, denetçi, gerektiğinde denetim kuruluşundaki diğer kişiler, üst yönetimden sorumlu olanlar, yetkili merciler, düzenleyici otorite veya hukuk müşavirine danışmayı değerlendirebilir. Ancak, bu tür bir danışmanlık alınması denetçinin çatışmayı çözmek için mesleki muhakemede bulunma veya gerektiğinde -mevzuatla yasaklanmadığı sürece- çatışmaya yol açan hususla ilişkisini sonlandırma sorumluluğunu ortadan kaldırmaz.

1.3.6.1.1.2. Kavramsal Çerçeve

Kavramsal çerçeve, temel etik ilkelere uyumu engelleyen tehditlerin belirlenmesi, belirlenen tehditlerin değerlendirilmesi ve tehditleri, ortadan kaldırmak veya kabul edilebilir bir düzeye indirmek suretiyle ele alınmasına yönelik esasları içerir. Denetçi, temel etik ilkelere uyumu engelleyen tehditleri belirlemek, değerlendirmek ve bunlara ilişkin önlemler almak üzere kavramsal çerçeveyi uygulamalıdır.

Denetçi, etikle ilgili bir konu yada sorunla ilgilenirken, söz konusu konu veya sorunun ortaya çıktığı veya çıkabileceği bağlamı dikkate almalıdır. Kavramsal çerçeve uygulanırken, denetçinin sorgulayıcı bir yaklaşımla hareket etmesi, mesleki yargısını kullanması ve gerekli bilgiye sahip makul üçüncü taraf testini uygulaması gerekir. Sorgulayıcı bir yaklaşımla hareket etmek, üstlenilen mesleki faaliyetin niteliği, kapsamı ve sonuçlarını dikkate alarak, elde edilen bilginin kaynağı, uygunluğu ve yeterliliğini göz önünde bulundurmayı ve daha fazla araştırma/inceleme veya başka bir adım atma ihtiyacına karşı açık ve dikkatli olmayı kapsar. Mesleki muhakeme, mesleki faaliyetlerin niteliği ve kapsamı ile çıkar ve ilişkileri dikkate alarak, durum ve gerçeklere uygun ilgili eğitim, mesleki bilgi, beceri ve deneyimin uygulanmasını içerir. Gerekli bilgiye sahip makul üçüncü taraf testi, denetçi tarafından, aynı sonuçlara başka bir tarafça ulaşılmasının muhtemel olup olmadığı hakkında yapılan bir değerlendirmedir. Bu tür bir değerlendirme, sonuçlara ulaşılan zamanda, denetçinin haberdar olduğu veya haberdar olmasının makul bir şekilde beklendiği tüm ilgili durum ve gerçekleri değerlendiren gerekli bilgiye sahip bir üçüncü tarafın bakış açısıyla yapılır. Gerekli bilgiye sahip makul üçüncü tarafın denetçi olması gerekmez, ancak denetçinin sonuçlarının uygunluğunu tarafsız bir biçimde anlamak ve değerlendirmek için ilgili bilgi ve deneyime sahip olması gerekir.

Denetçi, temel etik ilkelere uyumu engelleyen tehditleri belirlemekle yükümlüdür. Bu tehditler çok farklı durum ve olaylar sonucunda ortaya çıkabilir. Tehdit oluşturan her bir durumun belirlenmesi mümkün olamayabilmektedir. Benzer şekilde, sunulan hizmetlerin niteliklerine göre farklılık gösterebilir ve farklı tehditler ortaya çıkabilir. Temel etik ilkelere uyumu engelleyen tehditler aşağıdakilerden bir veya birkaçının kapsamına girebilir:

Kişisel çıkar tehdidi: Finansal veya finansal olmayan bir çıkarın, denetçinin yargısını veya davranışını uygun olmayan şekilde etkilemesi tehdididir.

Kendi kendini denetleme tehdidi: Denetçinin, kendisi veya çalıştığı denetim şirketindeki bir başka kişi tarafından varılmış bir yargının veya gerçekleştirilmiş bir faaliyetin sonuçlarını cari dönemde yürüttüğü faaliyetin parçası olan bir yargıya varırken dayanak olarak kullanması durumunda, söz konusu sonuçları uygun şekilde değerlendiremeyecek olması tehdididir.

Taraf tutma tehdidi: Denetçinin, bir müşterinin pozisyonunu, kendi tarafsızlığından taviz verecek şekilde desteklemesi tehdididir.

Yakınlık tehdidi: Denetçinin, bir müşteri ile uzun süreli veya yakın ilişki içerisinde bulunması nedeniyle bu kişinin çıkarları lehine fazlasıyla temayül göstermesi veya bunun çalışmalarına yönelik olarak fazlasıyla kabul eder bir yaklaşım sergilemesi tehdididir.

Yıldırma tehdidi: Denetçi üzerinde başkalarının nüfuzlarını kötüye kullanma çabaları dâhil olmak üzere, denetçinin mevcut veya hissettiği baskılardan dolayı tarafsız olarak hareket edebilmesinin engellenmesi tehdididir.

Temel etik ilkelere uyumu engelleyen bir tehdit tespit edildiğinde, söz konusu tehdidin kabul edilebilir bir düzeyde olup olmadığı değerlendirilmelidir. Kabul edilebilir düzey, gerekli bilgiye sahip makul üçüncü taraf testini kullanan bir denetçinin, temel ilkelere uyduğu sonucuna varmasının daha muhtemel olduğu düzeydir.

Bir tehdidin ortadan kaldırılıp kaldırılmadığını veya kabul edilebilir bir düzeye indirilip indirilmediğini etkileyebilecek yeni bir bilgiden veya durum ve gerçeklerdeki değişikliklerden haberdar olunması durumunda, tehdit yeniden değerlendirilerek buna göre yeniden ele alınmalıdır.

Temel etik ilkelere uyumu engelleyen tehditler, kabul edilebilir bir düzeyde olmadığına karar verilmesi durumunda, söz konusu tehditleri ortadan kaldırmak veya kabul edilebilir bir düzeye indirmek suretiyle bu tehditler ele alınmalıdır. Bu tehditleri, çıkar veya ilişkiler dâhil tehdit oluşturan durumları ortadan kaldırmak, mevcut olması ve uygulanma kabiliyetinin bulunması hâlinde, tehditleri kabul edilebilir bir düzeye indirmeye yönelik önlemler almak veya belirli mesleki faaliyeti reddetmek veya sonlandırmak suretiyle ele alınmalıdır.

1.3.6.1.2. Bağımsız Denetçiler

Etik Kurallar'ın bu kısmı, yukarıda esaslarına kavramsal çerçevenin uygulamasına yönelik temel ve uygulama esaslarını düzenler. Bu kısımda, denetçilerin karşılaşabileceği temel ilkelere uyumu engelleyen mesleki faaliyet, çıkar ve ilişkiler dâhil tehditler oluşturan veya oluşturabilecek durum ve gerçeklerin tamamı tanımlanmamaktadır. Bu sebeple, kavramsal çerçeve denetçinin bu tür durum ve gerçeklere karşı dikkatli olmasını gerektirir.

Bu kısımda, temel etik ilkelere uyumda tehdit oluşturabilecek çıkar çatışmaları, denetçinin görevlendirilmesi, ikinci görüşler, ücretler ve diğer menfaatler, hediyeler ve ağırlanma dahil teşvikler, emanet olarak tutulan müşteri varlıkları ve mevzuata aykırılıklara karşılık verilmesi hususları düzenlenmiştir. Denetçi, temel etik ilkelere uyumu engelleyen tehditleri belirlemek, değerlendirmek ve ele almak için kavramsal çerçeveyi uygulamakla yükümlüdür. Denetçinin karşılaşabileceği tehditlerin kaynaklanabileceği söz konusu durum ve gerçeklere ilişkin örnekler her bir tehdit sınıfı bazında aşağıda yer almaktadır:

a. Kişisel Çıkar Tehditleri:

- Denetçinin, müşteride doğrudan finansal çıkarının bulunması,

- Denetçinin, yeni bir iş almak için düşük fiyat teklifinde bulunması ve bu fiyatın işin teknik ve mesleki standartlara uygun olarak yürütülmesini zorlaştırabilecek kadar düşük olması,

- Denetçinin, müşterisiyle yakın bir iş ilişkisinin bulunması,

- Denetçinin, kişisel kazanç amacıyla kullanılabilecek gizli bilgilere erişiminin bulunması,

- Denetçinin, çalıştığı denetim şirketindeki bir kişinin daha önceden gerçekleştirmiş olduğu mesleki hizmetin sonuçlarını değerlendirirken önemli bir hata tespit etmesi.

b. Kendi Kendini Denetleme Tehditleri:

- Denetçinin, finansal sistemleri uyguladıktan sonra bu sistemlerin işleyiş etkinliğine ilişkin güvence raporu düzenlemesi,

- Denetçinin, güvence denetiminin konusunu teşkil eden kayıtları oluşturmak için kullanılacak olan orijinal verileri hazırlaması.

c. Taraf Tutma Tehditleri:

- Denetçinin, müşterinin çıkarlarını gözetmesi veya hisse senetlerinin lehine tanıtım yapması,

- Denetçinin, üçüncü taraflarla yaşanan hukuki bir davada veya anlaşmazlıkta, müşterisi adına bir avukat gibi hareket etmesi,

- Denetçinin, müşterinin lehine bir yasal düzenleme yapılması için çalışması.

d. Yakınlık Tehditleri:

- Denetçinin aile yakınlarından birisinin veya çekirdek ailesinin bir üyesinin, müşterinin yöneticisi veya yetkilisi olması,

- Müşterinin yöneticisinin veya yetkilisinin ya da müşteriye sunulan hizmetin konusu üzerinde önemli etkisi bulunan bir pozisyonda istihdam ettiği diğer bir çalışanının, yakın bir zamanda sorumlu denetçi olarak hizmet vermiş olması,

- Denetim ekibinin bir üyesinin, denetim müşterisiyle uzun süredir iş ilişkisi içinde olması.

e. Yıldırma Tehditleri:

- Denetçinin, mesleki bir hususstaki anlaşmazlık sebebiyle sözleşmenin veya denetim şirketindeki işinin sonlandırılmasıyla tehdit edilmesi,

- Müşterinin ilgili konu hakkında daha fazla bilgi sahibi olması nedeniyle, müşterinin vardığı yargılarla hemfikir olması konusunda, denetçinin kendisine baskı yapıldığını hissetmesi,

- Denetçinin, uygun olmayan bir muhasebe uygulamasını onaylamaması durumunda, önceden planlanmış bir terfinin olmayacağına dair bilgilendirilmesi,

- Denetçinin, müşteriden önemli bir hediye kabul etmiş olması ve bu durumun kamuya açıklanacağı hususuyla tehdit edilmesi.

Denetçi, mesleki veya işe ilişkin yargılarından taviz verdirecek hiçbir çıkar çatışmasına izin veremez. Denetçi, yeni bir müşteri ilişkisini, işi veya iş ilişkisini kabul etmeden önce, çıkar çatışması ve bu nedenle bir veya daha fazla temel ilkeye uyumu engelleyen tehditleri oluşturabilecek şartları belirlemek için uygun adımları atar. Bu tür adımlar taraflar arasındaki ilişkilerin ve ilgili çıkarların niteliği ile izmet ve bu hizmetin ilgili taraflar açısından olası sonuçları/yansımaları belirlenmesini içerir.

Denetçi, potansiyel bir müşteri tarafından diğer bir denetçinin yerine geçmesinin istenmesi, bir başka denetçinin elindeki işe teklif vermeyi düşünmesi veya başka bir denetçinin işi açısından tamamlayıcı veya ilave niteliğinde olacak bir işi üstlenmeyi düşünmesi durumlarında söz konusu işi kabul etmemesi için herhangi bir sebebin olup olmadığını belirlemelidir. Denetçi, müteakip (yinelenen) denetimlere devam edip etmeyeceğini periyodik olarak gözden geçirmelidir.

Denetçiden ikinci bir görüş isteyen işletmenin, mevcut veya önceki denetçiyle iletişim kurma konusunda kendisine izin vermeyecek olması durumunda denetçi, istenen görüşü verebilip veremeyeceğini belirlemelidir.

Denetçi, teklif verilen ücret düzeyi mesleki hizmetleri mesleki standartlara uygun olarak yürütme kabiliyetini etkileyebildiğinden, sunulacak hizmete uygun olarak nitelendirilebilecek ücret neyse onu teklif etmelidir. Başka bir denetçiden daha düşük ücret teklifi verilmesi tek başına etik ilkelere aykırı değildir. Ancak, teklif verilen ücretin düşüklüğü nedeniyle söz konusu hizmetin, uygulamadaki teknik ve mesleki standartlara uygun olarak yürütülmemesine yo açabilir.

Teşvik teklifinde bulunulması veya teşviklerin kabul edilmesi; dürüstlük, tarafsızlık ve mesleğe uygun davranış ilkeleri başta olmak üzere, temel etik ilkelere uyumu engelleyen bir kişisel çıkar tehdidi, yakınlık tehdidi veya yıldırma tehdidi oluşturabilir Birçok ülkede, belirli durumlarda teşvik teklifinde

bulunulmasını veya teşviklerin kabul edilmesini yasaklayan, rüşvet ve yolsuzlukla ilgili olanlar gibi mevzuat hükümleri bulunmaktadır. Denetçi, bu tür mevzuat hükümlerine ilişkin kanaat edinmek ve böyle bir durumla karşılaşması durumunda mevzuata uymakla yükümlüdür Denetçi, teşvik alacak kişinin veya diğer bir kişinin davranışını uygunsuz şekilde etkileme niyetiyle yapılan veya denetçinin, gerekli bilgiye sahip makul üçüncü bir tarafın bu niyetle yapıldığı sonucuna varmasının daha muhtemel olduğunu düşündüğü bir teşvik teklifinde bulunamaz/teşviki kabul edemez veya başkalarını teklifte bulunmak/kabul etmesi için destekleyemez.

Denetçi, mevzuat tarafından açıkça izin verilmedikçe ve müşterinin parasının veya diğer varlıklarının alınmasına ilişkin her türlü şarta uymadıkça, bu tür varlıkları emanet olarak tutmaz. Müşteri parasının veya varlıklarının emanete alınmasına ilişkin müşteri ve iş kabul prosedürlerinin bir parçası olarak denetçi varlıkların kaynağıyla ilgili uygun sorgulamaları yaparak yasal yükümlülükleri göz önünde bulundurulmalıdır.

Denetçinin mevzuata ilişkin bir aykırılığın veya şüphelenilen aykırılığın farkına varması durumunda, dürüstlük ve mesleğe uygun davranış ilkelerine uyumu engelleyen bir kişisel çıkar veya yıldırma tehdidi oluşabilir. Denetçi bu aykırılıkları nasıl ele alması gerektiği hakkında bazı ülkelerin mevzuatlarında hükümler bulunmaktadır. Söz konusu hükümler, Etik Kurallar'dan farklı veya daha kapsamlı olabilir. Bu tür aykırılıklarla karşılaşılması durumunda, denetçi aykırılığın yetkili bir kuruma bildirilmesine ilişkin hükümler ve müşterinin haberdar edilmesini yasaklayan hükümler de dahil olmak üzere söz konusu mevzuat hükümlerini anlamak ve bunlara uymak zorundadır.

1.3.6.1.3. Bağımsızlık Standartları

Bağımsızlık standartlarının 4A kısmında bağımsız denetim ve sınırlı bağımsız denetimde bağımsızlığa ilişkin esaslar belirlenmiştir. Bağımsızlık, Etik Kurallar ile zorunlu tutulmuş olup, kamu yararınadır. Bu kısımdaki bağımsızlık hükümleri, denetçi, denetim şirketi ve denetim ekibi üyelerine yöneliktir. Bağımsızlık, tarafsızlık ve dürüstlük ilkeleriyle bağlantılı olup aşağıdaki iki unsurdan oluşur:

Esasta bağımsızlık: Denetçinin dürüstlük, tarafsızlık ve mesleki şüphecilik içinde hareket etmesini teminen, mesleki muhakemesini olumsuz etkileyebilecek tesirlerden ari olarak görüş/sonuç açıklamasıdır.

Şekilde bağımsızlık: Denetim şirketinin, denetçinin veya denetim ekibi üyesinin; makul ve bilgi sahibi üçüncü kişilerde, dürüstlük, tarafsızlık ve mesleki şüphecilikten ödün verdiği intibaını oluşturabilecek durum ve davranışlardan sakınmasıdır.

Bu kısımda, bağımsızlığa tehdit oluşturabilecek ücretler, ödüllendirme ve değerlendirme politikaları, hediyeler ve ağırlama, fiili hukuki ihtilaflar ve hukuki ihtilaf tehditleri, finansal çıkarlar, kredi ve garantiler, iş ilişkileri, ailevi ve kişisel ilişkiler, denetim müşterisinin yöneticisi veya yetkilisi olarak denetim verilmesi, denetim müşterisi tarafından istihdam, çalışanların geçici olarak görevlendirilmesi, çalışanların denetim müşterisiyle uzun süreli ilişkisi, denetim müşterilerine güvence dışı hizmetler verilmesi ve hazırlanan raporların sınırlamasına ilişkin hususlar ayrı bölümler halinde düzenlenmiştir. Söz konusu bölümler kapsamında önemli hususlara aşağıda yer verilmektedir.

Bağımsızlık, denetim dönemi ve finansal tabloların kapsadığı dönem olmak üzere her iki dönem sürdürülmelidir. Denetim dönemi, denetim ekibinin denetime başlamasıyla başlar ve denetim raporunun yayımlanmasıyla sona erer.

Denetim müşterisinin kamu yararı olan işletme olması ve birbirini takip eden iki yıl için, bu müşteriden ve ilişkili işletmelerinden alınan ücretlerin, müşterinin finansal tabloları üzerinde görüş beyan eden denetim şirketi tarafından alınan toplam ücretlerin %15'inden fazlasını oluşturması durumunda denetim şirketi bu durum müşteri üst yönetimine açıklanmalı ve bunun yarattığı tehdide ilişkin önlemler değerlendirilmelidir. Denetim şirketi tarafından denetim işiyle ilgili doğrudan veya dolaylı olarak bir şarta bağlı ücret talep edilemez.

Denetim şirketi, bir kilit denetçiyi, kendi denetim müşterisine güvence dışı hizmetler satma konusundaki başarısına dayanarak değerlendiremez veya ödüllendiremez. Bu hüküm, denetim şirketinin ortakları veya kilit yöneticileri arasındaki normal kâr paylaşımı düzenlemelerini yasaklamaz.

Denetim şirketi, denetim ağına dâhil şirket veya denetim ekibinin bir üyesi, küçük ve önemsiz bir değerde olmadığı müddetçe, denetim müşterisinin hediyesini ve ağırlanma teklifini kabul edemez.

Denetim şirketi, ağa dâhil şirket, denetim ekibi üyesi veya bu kişinin çekirdek aile üyelerinden birisi; normal borç verme durumları dâhilinde verilmediği müddetçe, banka veya benzeri bir kuruluş olan denetim müşterisinden kredi veya kredi garantisini kabul edemez; normal ticari şartlar altında tutulmadığı müddetçe, banka, aracı kuruluş veya benzeri bir kuruluş olan bir denetim müşterisinde mevduat veya aracı kurum hesabı bulunamaz.

Finansal çıkar ve iş ilişkisi, uygun hâllerde, denetim şirketi, ağa dâhil şirket, denetim ekibi üyesi ve müşteri veya müşterinin yönetimi açısından önemsiz olmadığı müddetçe, denetim şirketi, ağa dâhil şirket veya bir denetim ekibi üyesi; denetim müşterisi veya yönetimiyle yakın bir iş ilişkisi kuramaz.

Denetim şirketinin veya ağa dâhil şirketin ortağı, kilit yöneticisi ya da çalışanı, müşterinin yöneticisi veya yetkilisi olarak hizmet vermez.

Kamu yararı bulunan şirketlerin denetiminde, sorumlu denetçi, işin kalitesine yönelik gözden geçirmeden sorumlu olarak atanan denetçi ve diğer herhangi bir kilit denetçi rolü kümülatif olarak yedi yıldan (azami denetlenebilir dönem) daha fazla üstlenemez. Sorumlu denetçi, kümülatif olarak yedi yıllık süre sonunda, beş yıl ara vermelidir. Kaliteye yönelik gözden geçirmeden sorumlu olan denetçi, kümülatif olarak 7 yıllık sürenin sonunda, üç yıl ara vermelidir. Kilit denetçi rolündekiler ise kümülatif 7 yılın ardından iki yıl ara vermelidir.

Bir denetim şirketi veya denetim ağına dâhil şirket, denetim müşterisi adına yönetim sorumluluğu üstlenmez.

1.3.6.2. ISACA'nın Etik Kuralları

ISACA, tüm bilgi sistemleri denetçilerinin (CISA belgesine sahip) ve birlik üyelerinin mesleki davranışlarını ve etiğini yöneten bir kurallar seti ortaya koymaktadır. ISACA, bilgi sistemleri denetçilerinin, bu kurallar setini uygulamak ve desteklemekle yükümlü olduğunu; aşağıda yer alan yedi maddenin, bu kurallar setinin gerçek amacını temsil ettiğini belirtmektedir. Üyeler ve ISACA sertifikası sahipleri:

- Denetim, kontrol, güvenlik ve risk yönetimi dahil olmak üzere kurumsal bilgi sistemleri ve teknolojisinin etkin yönetişimi ve yönetimi için uygun standart ve prosedürlerin uygulanmasını destekler ve bunlara uyumu teşvik eder.
- Görevlerini, mesleki standartlara uygun olarak, tarafsızlık ve gereken özen ve mesleki titizlik ile yerine getirir.
- Yüksek davranış ve karakter standartlarını korurken ve mesleğin veya birliğin itibarını zedelemeden, yasal ve dürüst bir şekilde paydaşların çıkarına hizmet eder.
- Görevleri sırasında elde ettikleri bilgilerin, yasal merci tarafından açıklanması zorunlu olmadıkça mahremiyetini ve gizliliğini korumakla yükümlüdür. Bu bilgileri kişisel çıkarları için kullanamaz veya uygunsuz taraflara veremez.
- Kendi alanlarında yetkinliği sağlayıp sürdürür ve yalnızca mesleki bilgi, beceri ve yeterlilikle tamamlamayı makul olarak bekleyebilecekleri faaliyetleri üstlenmeyi kabul eder.
- Yapılan işin sonuçları hakkında, açıklanmaması denetim sonuçlarının farklı anlaşılmasına yol açacak önemli hususlarda dahil, uygun tarafları bilgilendirir.
- Denetim, kontrol, güvenlik ve risk yönetimi dahil olmak üzere kurumsal bilgi sistemleri ve teknolojisinin yönetişim ve yönetimine ilişkin anlayışlarını geliştirmede paydaşların mesleki eğitimini destekler.

Mesleki Etik Kurallara uyulmaması, bir üyenin veya sertifika sahibinin davranışlarının soruşturulmasına ve nihayetinde disiplin cezalarına neden olabilir.

Örnek Sorular

Soru 1: Aşağıdakilerden hangisinin Bilgi Sistemleri Bağımsız Denetim Tebliği kapsamında bilgi sistemleri bağımsız denetim yükümlülüğü bulunmamaktadır?

A) Merkezi Kayıt Kuruluşu A.Ş.

B) Borsa İstanbul A.Ş.

C) Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.

D) Halka Açık Ortaklıklar

E) Geniş Yetkili Aracı Kurumlar

Cevap: D

Soru 2: Aşağıdakilerden hangisi bilgi sistemleri denetçileri için kıyasen uygulanan ve KGK tarafımdan yayınlanan Etik Kurallar'ın temel ilkelerinden değildir?

A) Dürüstlük

B) Objektif Olma (Tarafsızlık)

C) Mesleki Yeterlilik ve Özen

D) Sır Saklama

E) Meslekte En İyi Olma

Cevap: E

Soru 3) Aşağıdakilerden hangisi denetçinin gizli bir bilgiyi açıklamasının gerektiği veya gerekebileceği ya da bu tür bir açıklamanın uygun olabileceği durumlardan biri değildir?

A) Mesleki veya iş ilişkileri kapsamında edindiği veya aldığı herhangi bir gizli bilgiyi söz konusu ilişki sona erdikten sonra

B) Mevzuat tarafından açıklamaya izin verilmesi ve müşteri tarafından açıklama yapmak üzere yetkilendirilmesi

C) Hukuki takip sürecinde belgelerin ve diğer kanıtların toplanması veya ortaya çıkan mevzuat ihlallerinin yetkililere açıklanması gibi mevzuat tarafından açıklama yapmanın zorunlu tutulması

D) Mevzuatla yasaklanmadığı sürece, yetkililerce kalite inceleme sürecine uygunluk sağlama, yetkililerce yapılan bir sorgulamaya veya araştırmaya/incelemeye cevap verme,

E) Hukuki takip sürecindeki bir denetçinin mesleki çıkarlarını koruma veya Etik İlkeler dahil teknik ve mesleki standartlara uygunluk sağlama amaçlarıyla açıklamanın mesleki bir görev veya hak olması

Cevap: A

EKLER

Ek/1 Sızma Testine İlişkin Usul ve Esaslar

Bilgi Sistemleri Sızma Testleri Usul ve Esasları

1) Amaç: Sızma testlerinin amacı, Kurum Kuruluş ve Ortaklıkların bilgi sistemlerinde tespit edilen açıklıkların ve zafiyetlerin kullanılmasıyla sistemlere sızma girişimlerinin önceden tespit edilmesi ve düzeltilmesidir.

2) Kapsam: Sızma testleri kapsamında gerçekleştirilecek testler asgari olarak aşağıdaki başlıkları kapsar:

a**.** İletişim Altyapısı ve Aktif Cihazlar,

b. DNS Servisleri,

c. Etki Alanı ve Kullanıcı Bilgisayarları,

ç. E-posta Servisleri,

d. Veritabanı Sistemleri,

e. Web Uygulamaları,

f. Mobil Uygulamalar,

g. Kablosuz Ağ Sistemleri,

ğ. Dağıtık Servis Dışı Bırakma Testleri,

h. Sosyal Mühendislik Testleri.

3) Metodoloji: Sızma testleri, aşağıda detaylandırılan kullanıcı profilleri ile tanımlanan erişim noktalarından gerçekleştirilecek testlerden oluşur. Testler, sistem tespiti, servis tespiti ve açıklık taraması/araştırması adımları ile başlar ve her bir erişim noktası kapsamında uygulanacak adımlar ile devam eder. Bu testler sonrası saptanan açıklık ve bulgular, Kapsam bölümünde belirtilen ve ilişkili olduğu her bir başlık altında ayrıntılı olarak incelenerek raporlanır. Sızma testleri gerçekleştirilirken her bir test başlığı kapsamında saptanan açıklık ve bulgular, ayrı ayrı değerlendirilmenin yanında, bir araya geldiklerinde oluşturabilecekleri riskler ve açıklıklar açısından da değerlendirilir ve bu birlikte değerlendirme sonucu ortaya çıkan yeni açıklık ve bulgular da raporlanır. Bulgular, **"*Bulgu Önem Dereceleri*"** bölümünde yer verilen dereceler kullanılarak "***Bulgu Formatı***" bölümünde tariflenen formata uygun olacak şekilde sunulur. Bu kapsamda bulgu önem dereceleri belirlenirken varlığın değeri dikkate alınmaz. Varlık değerlendirmesi yapmak ve varlıkların önem derecelerine göre aksiyon almak Kurum, Kuruluş ve Ortaklıkların sorumluluğundadır. Sızma testleri gerçekleştirilirken, Kurum, Kuruluş ve Ortaklıklar faaliyetlerinin aksamasına ve hizmet kesintisine yol açmayacak yöntemler kullanılmasına dikkat edilir. Hizmet kesintisine yol açabilecek tüm testler Kurum, Kuruluş ve Ortaklıklar ile koordineli bir şekilde planlanarak gerçekleştirilir.

a. Testlerin Gerçekleştirileceği Erişim Noktaları

Sızma testlerinin gerçekleştirileceği asgari erişim noktaları aşağıda tanımlanmaktadır. Bu noktalardan sisteme erişildikten sonra, sızma testleri gerçekleştirilir.

i. İnternet: Kurum, Kuruluş ve Ortaklıkların internet üzerinden erişilebilen tüm sunucu ve servislerine İnternet üzerinden erişilerek sızma testleri gerçekleştirilir ve devamında ve detaylı sızma testleri uygulanır.

ii. Kurum, Kuruluş ve Ortaklıklar iç ağı: Kurum, Kuruluş ve Ortaklıkların iç ağında yer alan ve test kapsamında ele alınan sunuculara Kurum, Kuruluş ve Ortaklıklar iç ağı üzerinden erişilerek sızma testleri gerçekleştirilir. Ağ ve ağ trafiği üzerinde gerçekleştirilecek testler için de bu ağ kullanılır ve testi gerçekleştirecek şahıslara kullanımı en yaygın olan çalışan bilgisayarı profilinde bilgisayarlar sağlanır.

b. Testlerin Gerçekleştirileceği Kullanıcı Profilleri

Sızma testlerinin sağlıklı bir şekilde gerçekleştirilebilmesi ve testlerin gerçek hayata uygun olması için, yukarıda tanımlanan erişim noktalarına bu ortamların doğasına uyacak şekilde aşağıdaki kullanıcı profilleri ile sızma testleri gerçekleştirilir.

i. Anonim kullanıcı profili: İnternet üzerinden, Kurum, Kuruluş ve Ortaklıkların web servislerine erişebilen ancak web uygulamalarına giriş yetkilerine sahip olmayan kullanıcıyı temsil eder. Kurum, Kuruluş ve Ortaklıklara ait web uygulamalarının üyesi olmayan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.

ii. Kurum, Kuruluş ve Ortaklıklar müşterisi profili: İnternet üzerinden, Kurum, Kuruluş ve Ortaklıklar'ın web servislerine erişebilen ve web uygulamalarına giriş yetkilerine sahip olan kurumsal veya bireysel kullanıcıları temsil eder. İnternet üzerinde Kurum, Kuruluş ve Ortaklıklara ait web uygulamalarının üyesi olan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.

iii. Kurum, Kuruluş ve Ortaklıklar çalışanı profili: Kurum, Kuruluş ve Ortaklıklar personelinin çalışma ortamını kullanarak sahip olduğu yetkiler ile sistemde oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır. Kurum, Kuruluş ve Ortaklıklar çalışanı profili ile gerçekleştirilecek testlerde, Kurum, Kuruluş ve Ortaklıklarda çapında en yaygın olarak kullanılan çalışan profilinin seçilmesinin yanında, yerel yönetici (local admin) yetkisine sahip çalışan profilleri ile de sızma testleri gerçekleştirilir. Kurum, Kuruluş ve Ortaklıklar çalışanı profili ile yapılan testlerde, testi yapan kişi/kuruluşa Kurum, Kuruluş ve Ortaklıklar tarafından tanımlanan erişim yetkileri ve verilen izinler raporda açıkça ifade edilmelidir.

iv. Diğer kullanıcı profilleri: Sızma testlerinin, yukarıda tanımlanan diğer dört kullanıcı profiline uymayan bir kullanıcı profili ile gerçekleştirilmesi durumunda, kullanılan her bir profil için tanımlanan hak ve yetkiler bu başlık altında açıkça ifade edilir.

c. Sistem Tespiti, Servis Tespiti ve Açıklık Taraması

Sızma testleri aşağıda tanımlanan sistem tespiti, servis tespiti ve açıklık taraması/araştırması adımları ile başlar. Sistem tespiti, servis tespiti ve açıklık taraması/araştırması tüm bilgi sistemi varlıklarına uygulanır.

i. Sistem tespiti: Sunucu veya aktif/pasif ağ cihazlarının sistem/yapılandırma bilgilerinin tespit edilmeye çalışıldığı adımdır.

ii. Servis tespiti: Kurum, Kuruluş ve Ortaklıklar bilgi sistemlerinde yer alan varlıkların port taramasının gerçekleştirildiği ve dış dünyaya/genel erişime açık olan portların sunduğu servislerin tespit edilmeye çalışıldığı adımdır.

iii. Açıklık taraması/araştırması: Kurum, Kuruluş ve Ortaklıkların bileşenleri ve bu bileşenlerin sunduğu servislerin açıklık tarayıcıları ile güncel açıklıklara karşı tarandığı ve muhtemel güvenlik açıklıklarının belirlenmeye çalışıldığı adımdır. Bu adımda ayrıca, tespit edilen muhtemel açıklıklar için açıklık veritabanları gibi kaynaklar kullanılarak bu açıklıkların bileşenlere ve bileşenlerin etkileşimde olduğu sistemlere güvenlik açısından etkileri araştırılır.

d. Sızma Testleri

i. İnternet üzerinden gerçekleştirilecek temel sızma testleri: Kurum, Kuruluş ve Ortaklıklar ağından bağımsız bir lokasyondan, Kurum, Kuruluş ve Ortaklıklar'ın internet üzerinde sahip olduğu IP ağı taranarak sistem tespiti, servis tespiti ve açıklık taraması adımları gerçekleştirilir.

ii. Kurum, Kuruluş ve Ortaklıklar iç ağından gerçekleştirilecek sızma testleri: Kurum, Kuruluş ve Ortaklıkların iç ağında sistem tespiti, servis tespiti ve açıklık taraması adımlarının yanında aşağıdaki faaliyetlerin gerçekleştirilmesi sağlanır:

- Kurum yerel ağ haritası tespiti,

• Belirlenen açık portlar üzerinden içerik filtreleme, güvenlik duvarı atlatma ve bilgi kaçırma testlerinin gerçekleştirilmesi,

• Yerel alan ağı içerisinde zafiyet taraması yapılması,

• Kurum yerel ağında araya girme teknikleri ile hassasiyet derecesi yüksek bilgilerin elde edilmeye çalışılması,

• Elde edilen bilgiler ışığında kullanıcı bilgisayarları, sunucu sistemleri ve aktif cihazlara yönelik ele geçirme saldırılarının gerçekleştirilmesi,

• Ele geçirilen sunucu ve kullanıcı bilgisayarları üzerinden daha kritik bilgilere ulaşılmaya çalışılması.

4) Sızma Testi Sonuçlarının Takibi

Kurum, Kuruluş ve Ortaklıklar, sızma testleri bulguları, bulguların önem derecelerini, birlikte oluşturabilecekleri riskleri, tespit edildiği varlıkların değeri ve sızma testi raporlarında yer alan önerileri dikkate alarak, Kurum, Kuruluş ve Ortaklıklar yönetim kurullarınca onaylanan ve bu bulguların en kısa sürede giderilmesini amaçlayan bir aksiyon planı çerçevesinde takip eder. Sızma testleri sonucu ortaya çıkan tespitler, gerekli görülmesi halinde Kurum, Kuruluş ve Ortaklıkların teftiş kurullarının iç denetim planına da dâhil edilir. Sızma testi raporları, tamamlanmasını müteakip bir ay içinde Kurul'a gönderilir.

Bulgu Önem Dereceleri

Bulgu önem dereceleri beş kategoride ele alınır. Acil, kritik, yüksek, orta ve düşük şeklinde olan bu kategorilere ilişkin açıklamalar aşağıda yer almaktadır:

Önem Derecesi	**Açıklama**
Acil	Niteliksiz saldırgan tarafından Kurum, Kuruluş ve Ortaklıklar dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Kritik	Nitelikli saldırgan tarafından Kurum, Kuruluş ve Ortaklıklar dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Yüksek	Kurum, Kuruluş ve Ortaklıklar dış ağından gerçekleştirilen ve kısıtlı hak yükseltilmesi veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan saldırılara sebep olan açıklıklardır.
Orta	Yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan saldırılara sebep olan açıklıklardır.
Düşük	Etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan eksikliklerdir.

Bulgu Formatı

Kapsam bölümünde belirtilen başlıkların her biri altında raporlanacak bulguların sunuluş biçimi aşağıda yer almaktadır:

Bulgu Referans No	**Rapordaki her bulguyu tekil olarak niteleyen harf/rakam dizisi**
Bulgu Adı	Bulguyu özet olarak ifade eden tanımlayıcı isim
Önem Derecesi	Bulgunun, EK-1'de yer verilen önem derecesi
Etkisi	Bulguda yer verilen açıklığın/eksikliğin kötüye kullanılması durumunda oluşabilecek potansiyel sonuç
Erişim Noktası	"3.a Testlerin Gerçekleştirileceği Erişim Noktaları" bölümünde yer verilen testin gerçekleştirildiği erişim noktası
Kullanıcı Profili	"3.b Testlerin Gerçekleştirileceği Kullanıcı Profilleri" bölümünde yer verilen testin gerçekleştirildiği kullanıcı profili
Bulgunun Tespit Edildiği Bileşen/Bileşenler	Bulgunun tespit edildiği bileşeni niteleyen IP Numarası, URL, Sistem, Servis, Sunucu veya Varlık adı gibi bilgiler
Bulgu Açıklaması	Bulgunun detaylı açıklaması
Çözüm Önerisi	Bulgunun giderilmesi için testi gerçekleştiren kuruluş tarafından yapılacak çözüm önerisi

Ek/2 Rapor Örnekleri

BİLGİ SİSTEMLERİ BAĞIMSIZ DENETİM GÖRÜŞÜ

(Olumlu Görüş)

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kurum, Kuruluş ve Ortaklık Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri kontrollerinin denetlenen nezdinde VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği'nde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri kontrollerinin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.

Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

[Denetçi Görüşü]

Görüşümüze göre, bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde, VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Düzenleme Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Başdenetçisinin Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

BİLGİ SİSTEMLERİ BAĞIMSIZ DENETİM GÖRÜŞÜ

(Şartlı Görüş)

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kurum, Kuruluş ve Ortaklık Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri kontrollerinin denetlenen nezdinde VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği'nde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri kontrollerinin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.

Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Denetim faaliyetine getirilen sınırlandırma ve bu nedenle denetlenemeyen süreçler, uygulamalar, kontroller; denetlenenin bilgi sistemleriyle ilgili tespit edilen önemli kontrol eksiklikleri ve bu kontrol eksikliklerinin denetlenenin bilgi sistemleri bütününü veya büyük bir kısmını etkilememesine ilişkin görüşüne esas neden ve gerekçeler)

Görüşümüze göre, yukarıda (....ncı paragrafta) açıklanan husus(lar) nedeniyle, denetlenenin bilgi sistemleri üzerinde bu hususun/hususların muhtemel etkileri haricinde bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde, VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Düzenleme Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Başdenetçisinin Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

BİLGİ SİSTEMLERİ BAĞIMSIZ DENETİM GÖRÜŞÜ

(Olumsuz Görüş)

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kurum, Kuruluş ve Ortaklık Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri kontrollerinin denetlenen nezdinde VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği'nde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri kontrollerinin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.

Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Denetlenenin bilgi sistemleri kontrollerinin etkin, yeterli ve uyumlu bulunmama sebepleri)

[Denetçi Görüşü]

Görüşümüze göre, yukarıda (...ncı paragrafta) açıklanan husus(lar) nedeniyle, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde, VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun etkin, yeterli ve uyumlu kontroller tesis edilmemiştir.

Düzenleme Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Başdenetçisinin Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

BİLGİ SİSTEMLERİ BAĞIMSIZ DENETİM GÖRÜŞÜ

(Görüşten Kaçınma)

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kurum, Kuruluş ve Ortaklık Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri kontrollerinin denetlenen nezdinde VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği'nde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri kontrollerinin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.

(Denetçinin görüş bildirmemesinin nedenleri)

[Denetçi Görüşü]

Yukarıda (...ncı paragrafta) açıklanan husus(lar) nedeniyle ..... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleriyle ilgili tesis edilen kontrollerin etkinliği, yeterliliği ve uyumluluğu hakkında görüş bildirmiyoruz.

Düzenleme Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Başdenetçisinin Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

KAYNAKÇA

Aksoy, S. (2018, Ocak). *Denetimde önemlilik ve denetim riski.* İstanbul Ticaret Üniversitesi Dış Ticaret Enstitüsü. http://ticaret.edu.tr/wp-content/uploads/2020/921/136%20DENET%C4%B0MDE%20%C3%96NEML%C4%B0L%C4%B0K%20VE%20DENET%C4%B0M%20R%C4%B0SK%C4%B0.pdf adresinden erişildi.

Anadolu Üniversitesi. (2018). *Denetim*. Anadolu Üniversitesi. https://ets.anadolu.edu.tr/storage/nfs/ISL401U/ebook/ISL401U-12V4S1-8-0-1-SV1-ebook.pdf adresinden erişildi.

Andriole, S. (2020, 18 Eylül). *Why No One Understands Enterprise Architecture & Why Technology Abstractions Always Fail.* Kasım 2021 tarihinde *https://www.forbes.com/sites/steveandriole/2020/09/18/why-no-one-understands-enterprise-architecture--why-technology-abstractions-always-fail/?sh=76d848207eb5* adresinden erişildi.

Armour, F., Kaisler, S., Liu, S.Y. (1999). *Building an Enterprise Architecture Step-by-Step. IT Professional. 1. 31 - 39. 10.1109/6294.781623.* Aralık 2021 tarihinde https://www.researchgate.net/publication/3426367_Building_an_Enterprise_Architecture_Step-by-Step adresinden erişildi.

Avron, S. (2017, 11 Temmuz). *4 Effective Ways to Manage Resources More Efficiently.* Aralık 2021 *tarihinde https://flevy.com/blog/4-effective-ways-to-manage-resources-more-efficiently/* adresinden erişildi.

Balanced Scorecard Institute. (t.y.). *What is a Balanced Scorecard?*. 29 Ocak 2022 tarihinde *https://balancedscorecard.org/bsc-basics-overview/* adresinden erişildi.

Başaranoğlu, E. (2020, 4 Mayıs*). Bilgi Güvenliği Bakışı ile Güvenlik Kontrollerinin Sınıflandırılması*. Siber Portal. 24 Kasım 2021 https://www.siberportal.org/white-team/securing-information/bilgi-guvenligi-bakisi-ile-guvenlik-kontrollerinin-siniflandirilmasi/ adresinden erişildi.

BDDK, *Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Hakkında Yönetmelik. https://www.bddk.org.tr/Mevzuat/Liste/50* adresinden erişildi.

BDDK, *Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimine İlişkin Rapor Hakkında Tebliğ.* https://www.bddk.org.tr/Mevzuat/Liste/50 adresinden erişildi.

BDDK, *Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik*. https://www.bddk.org.tr/Mevzuat/Liste/50 adresinden erişildi.

BDDK, *Bilgi Alışverişi Kuruluşları İle Risk Merkezinin Bilgi Sistemleri Yönetimine ve Denetimine İlişkin Tebliğ*. https://www.bddk.org.tr/Mevzuat/Liste/50 adresinden erişildi.

BDDK, *Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ*. https://www.bddk.org.tr/Mevzuat/Liste/50 adresinden erişildi.

Bursa Uludağ Üniversitesi. (2019, 27 Ekim). *İç Kontrol Nedir?* Aralık 2021 tarihinde https://uludag.edu.tr/mkpasa/konu/view?id=346&title=ic-kontrol-nedir adresinden erişildi.

Cascarino, R. E. (2012). *Auditor's Guide to IT Auditing (2nd ed.).* Wiley. https://learning.oreilly.com

Çelik, O. (2021, Haziran). *Lisanslama sınavları çalışma notları - Muhasebe ve finansal raporlama*. Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu. https://www.spl.com.tr/icerik/sinav-calisma-notlari adresinden erişildi.

Chapter 7 Assessing the Risk of Material Misstatement. (t.y.). SlideToDoc. 24 Kasım 2021 tarihinde https://slidetodoc.com/chapter-7-assessing-the-risk-of-material-misstatement/ adresinden erişildi.

Clarke, I. (2018, 21 Haziran). *Control Objectives & Activities: What Are They? What's Appropriate?* Linford & Company LLP. 24 Kasım 2021 tarihinde https://linfordco.com/blog/appropriateness-of-control-objectives-and-controls adresinden erişildi.

DDO. (2021). *Bilgi ve İletişim Güvenliği Rehberi* (1st ed.). Cumhurbaşkanlığı Dijital Dönüşüm Ofisi.

Deniz, A. (2013, Kasım). *Bağımsız denetimde kullanılan kanıt toplama teknikleri ve denetçi açısından önemi.* Okan Üniversitesi Sosyal Bilimler Enstitüsü. http://abdullahcavus.com.tr/wp-content/uploads/2018/02/BA%C4%9EIMSIZ-DENET%C4%B0MDE-KULLANILAN-KANIT-TOPLAMA-TEKN%C4%B0KLER%C4%B0-ve-DENET%C3%87%C4%B0-A%C3%87ISINDAN-%C3%96NEM%C4%B0.pdf

Doshi, H. (2020). *CISA – Certified Information Systems Auditor Study Guide*. Packt Publishing. https://learning.oreilly.com. adresinden erişildi.

Farmer, D. (2021, 20 Temmuz). *5 principles of a well-designed data architecture.* 29 Ocak 2022 tarihinde https://searchdatamanagement.techtarget.com/tip/5-principles-of-a-well-designed-data-architecture adresinden erişildi.

Firebrand Training Ltd. (2017). *2017 CISA Review Course [Slides]*. Firebrand Training. https://firebrand.training/uk/pdf/learn/isaca/isaca-cisa-courseware.pdf adresinden erişildi.

Gantz, S. D. (2013). *The Basics of IT Audit: Purposes, Processes, and Practical Information* (1st ed.). Syngress. https://learning.oreilly.com/ adresinden erişildi.

Gönen, S., & Yıldırım, F. (2019). *Bağımsız Denetimde Kanıt ve BİST Uygulaması.* MANAS Sosyal Araştırmalar Dergisi, 1115–1127. https://doi.org/10.33206/mjss.492787 adresinden erişildi.

Gregory, P. H. (2019). *CISA Certified Information Systems Auditor All-in-One Exam Guide, Fourth Edition* (4th ed.). McGraw-Hill Education. https://learning.oreilly.com

Hayes, D. (2020). *Practical Guide to Digital Forensics Investigations* (2nd ed.). Pearson IT Certification. https://learning.oreilly.com/ adresinden erişildi.

Hingarh, V., & Ahmed, A. (2013). *Understanding and Conducting Information Systems Auditing.* Wiley. https://learning.oreilly.com adresinden erişildi.

Holicky, K. (2021, 4 Ağustos). *What is Resource Management?*. Ocak 2022 tarihinde *https://meisterplan.com/blog/what-is-resource-management/* adresinden erişildi.

İDKK, Kamu Bilgi Teknolojileri *Denetim Rehberi*. 2014. İc Denetim Koordinasyon Kurulu.

İSMMMO. (t.y.). *Denetim Türleri.* İstanbul Serbest Muhasebeci Mali Müşavirler Odası. 24 Kasım 2021 tarihinde https://archive.ismmmo.org.tr/docs/yayinlar/kitaplar/130/2%20denetim%20turleri.pdf adresinden erişildi.

IA COP. (2014, Nisan). *Risk assessment in audit planning*. Internal Audit Community of Practice (IA COP). https://www.pempal.org/sites/pempal/files/event/attachments/cross_day-2_4_pempal-iacop-risk-assessment-in-audit-planning_eng.pdf adresinden erişildi.

Innotas, (2012, 28 Ağustos). *The Smart Approach To IT Resource Management.* Ocak 2022 tarihinde *https://www.projectmanagement.com/pdf/innotas_wp_resourcemgmt_2012-08-28.pdf* adresinden erişildi.

Integrated test facility. (t.y.). Oxford Reference. 25 Kasım 2021 tarihinde https://www.oxfordreference.com/view/10.1093/oi/authority.20110803100005981 adresinden erişildi.

Integrated test facility. (2021, 12 Mart). Wikipedia. https://en.wikipedia.org/wiki/Integrated_test_facility adresinden erişildi.

ISACA. (2019). *CISA Review Manual, 27th Edition.* ISACA.

ISACA. (2018). *ISACA terimler sözlüğü.* ISACA. 24 Kasım 2021 tarihinde https://www.isaca.org/resources/glossary adresinden erişildi.

IOSCO. (2021, Ekim). *Principles on Outsourcing*. 7 Ocak 2022 tarihinde https://www.iosco.org/library/pubdocs/pdf/IOSCOPD654.pdf adresinden erişildi.

ISACA. (2019). *CISA Review Manual, 27th Edition.* ISACA.

Jaksic, D. (2009). *Implementation of computer assisted audit techniques in application controls testing.* Management Information Systems, 4(1), 9–12. https://www.ef.uns.ac.rs/mis/archive-pdf/2009%20-%20No1/MIS2009_1_2.pdf adresinden erişildi.

Kamal, S., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2020). *Computer-Assisted Audit Tools for IS Auditing.* Internet of Things—Applications and Future, 139–155. https://doi.org/10.1007/978-981-15-3075-3_10 adresinden erişildi.

KGK, *BDS 210 Bağımsız Denetim Sözleşmesinin Şartları Üzerinde Anlaşmaya Varılması Standardı*. http://kgk.gov.tr/ adresinden erişildi.

KGK, *BDS 300 Finansal Tabloların Bağımsız Denetiminin Planlaması Standardı*. http://kgk.gov.tr/ adresinden erişildi.

KGK, *BDS 300 Finansal Tabloların Bağımsız Denetiminin Planlaması Standardı*. http://kgk.gov.tr/ adresinden erişildi.

KGK, *BDS 315 İşletme ve Çevresini Tanımak Suretiyle Önemli Yanlışlık Risklerinin Belirlenmesi Standardı* http://kgk.gov.tr/ adresinden erişildi.

KGK, *BDS 330 Bağımsız Denetçinin Risk Olarak Değerlendirilmiş Hususlara Karşı Yapacağı İşler Standardı.* http://kgk.gov.tr/ adresinden erişildi.

KGK, *BDS 500 Bağımsız Denetim Kanıtları Standardı*. http://kgk.gov.tr/ adresinden erişildi.

KGK, *BDS 520 Analitik Prosedürler Standardı*. http://kgk.gov.tr/ adresinden erişildi.

KGK, *BDS 530 Bağımsız Denetimde Örnekleme Standardı*. http://kgk.gov.tr/ adresinden erişildi.

KGK, *Bağımsız Denetçiler İçin Etik Kurallar.* http://www.kgk.gov.tr adresinden erişildi.

Kiracı, M. (t.y.). *Muhasebe denetimi.* SlidePlayer. 24 Kasım 2021 tarihinde https://slideplayer.biz.tr/slide/1947387 adresinden erişildi.

KPI (t.y.). *What is a Key Performance Indicator (KPI)?*. 30 Ocak 2022 tarihinde https://kpi.org/KPI-Basics adresinden erişildi.

Lumen Learning. (2021). *An Introduction to Management*. Ekim 2021 tarihinde https://courses.lumenlearning.com/boundless-business/chapter/an-introduction-to-management/#:~:text=Management%20in%20all%20business%20and,available%20resources%20efficiently%20and%20effectively. adresinden erişildi.

Marr, B. (2021). *How to Develop Effective KPIs.* 30 Ocak 2022 tarihinde https://bernardmarr.com/how-to-develop-effective-kpis/ adresinden erişildi.

Miller, A. (2021, 7 Mayıs), *IT Best Practices: The Best Introduction.* Ocak 2022 tarihinde https://www.bmc.com/blogs/it-best-practices/ adresinden erişildi.

National Cyber Security Centre, (2018, 16 Kasım). *Risk management guidance.* 25 Ocak 2022 tarihinde https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/fundamentals adresinden erişildi.

Olavsrud, T. (2022, 24 Ocak). *What is data architecture? A framework for managing data.* 24 Ocak 2021 tarihinde https://www.cio.com/article/190941/what-is-data-architecture-a-framework-for-managing-data.html adresinden erişildi.

Özdemir, B. (1999). Stratejik Yönetim ve Stratejik Planlamanın Kamu Yönetiminde Uygulanabilirliği. Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek lisans Tezi. Ankara.

Polat, G. (2021a, 20 Mart). *Bilgi Sistemi Uygulama Kontrolleri.* Medium. 24 Kasım 2021 tarihinde https://medium.com/databulls/bilgi-sistemi-uygulama-kontrolleri-e646627b22f9 adresinden erişildi.

Polat, G. (2021b, 19 Mayıs). *Compliance testing vs substantive testing.* Medium. 25 Kasım 2021 tarihinde https://medium.com/databulls/compliance-testing-vs-substantive-testing-3ed95926791d adresinden erişildi.

Polat, G. (2021c, 3 Haziran). *Denetimde örneklem kullanımı.* Medium. 25 Kasım 2021 tarihinde https://medium.com/databulls/%C3%B6rneklem-denilen-%C5%9Fey-3f0f417c467e adresinden erişildi.

SAYIŞTAY, *Bilişim Sistemleri Denetim Rehberi*. 2013. T.C. Sayıştay Başkanlığı.

SEDDK, *Sigortacılık ve Özel Emeklilik Sektörlerinde İç Sistemlere Dair Yönetmelik.* https://seddk.gov.tr/tr/mevzuat/sigortacilik/yonetmelikler adresinden erişildi.

SPK, *Bilgi Sistemleri Bağımsız Denetim Tebliği (III-62.2).* https://mevzuat.spk.gov.tr adresinden erişildi.

SPK, *Bilgi Sistemleri Yönetimi Tebliği (VII-128.9).* https://mevzuat.spk.gov.tr adresinden erişildi.

SPK, *Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ (Seri:X, No:22).* https://mevzuat.spk.gov.tr adresinden erişildi.

Swanagan, M. C. (t.y.). *The 3 Types Of Security Controls (Expert Explains).* PurpleSec. 24 Kasım 2021 tarihinde https://purplesec.us/security-controls/ adresinden erişildi.

TCMB, *Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ.* https://tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Banka+Hakkinda/Mevzuat adresinden erişildi.

TCMB, *Ödeme ve Menkul Kıymet Mutabakat Sistemlerinde Kullanılan Bilgi Sistemleri Hakkında Tebliğ.* https://tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Banka+Hakkinda/Mevzuat adresinden erişildi.

TSE. (2013, Aralık). *Bilgi teknolojisi-Güvenlik teknikleri-Bilgi güvenliği için Uygulama Kodu (TS ISO/IEC 27002)*.

TSE, (2018, Kasım). *Yönetim Sistemleri Tetkik Kılavuzu (TS EN ISO 19011).* http://www.kalite.yildiz.edu.tr/login/sys/admin/subPages/img/D%C5%9E-255-TSE%20ISO%2019011.pdf adresinden erişildi.

Van der Nest, D. P., Smidt, L., & Lubbe, D. (2015). *The application of statistical and/or non-statistical sampling techniques by internal audit functions in the South African banking industry.* Risk Governance and Control: Financial Markets and Institutions, 5(1), 72–80. https://doi.org/10.22495/rgcv5i1art7 adresinden erişildi.

Wibowo, A. M. (t.y.). *Auditing computer-based information systems.* IT Governance Lab, Faculty of Computer Science, University of Indonesia. 25 Kasım 2021 tarihinde https://itgov.cs.ui.ac.id/audit/anotasi%20slide%20audit%20aplikasi.pdf adresinden erişildi.

Paşaoğlu, D., Tokgöz, N., Şakar, N., Ergun Özler, N.D., Özalp, İ. (2013), T.C. Anadolu Üniversitesi Yayınları, *Yönetim ve Organizasyon.* Kasım 2021 tarihinde https://www.ders.es/yonetim_organizasyon.pdf adresinden erişildi.

Roush, J., Hertvik J. (2020, 29 Ekim). *IT Management: Get Started with Help from Two Experienced Joes.* Ocak 22 tarihinde https://www.bmc.com/blogs/it-management/ adresinden erişildi.

Quinn, S., Ivy, N., Barrett M., Feldman L., Witte G., Gardner R.K. (2021 Kasım*). Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management.* Ocak 2022 tarihinde https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8286A.pdf adresinden erişildi.

Soucy, L. (t.y.). *Top 10 Risks of Outsourcing (and How to Manage Them).* Ocak 2022 tarihinde https://biz30.timedoctor.com/risks-of-outsourcing/ adresinden erişildi.

Stangarone, J. (2018, 18 Ağustos), *7 secrets of effective IT departments.* Ocak 2022 tarihinde https://www.mrc-productivity.com/blog/2018/08/7-secrets-of-effective-it-departments-2/ adresinden erişildi.

Stedman, C. (2021, Ağustos)**.** *What is data architecture? A data management blueprint.* 26 Ocak 2022 tarihinde https://searchdatamanagement.techtarget.com/definition/What-is-data-architecture-A-data-management-blueprint adresinden erişildi.

Townsend, S. (t.y.). *Top 12 Resource Management Best Practices.* Ocak 2021 tarihinde https://www.planview.com/resources/guide/resource-management-software/top-12-resource-management-best-practices/ adresinden erişildi.

Twin, A. (2021, 29 Ağustos). Outsourcing. 28 Ocak 2022 tarihinde https://www.investopedia.com/terms/o/outsourcing.asp adresinden erişildi.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19004&MevzuatTur=9&MevzuatTertip=5 adresinden erişildi.

Wanamaker, J. (2018, 8 Mart). *How To Build A Great IT Department.* Aralık 2021 tarihinde https://complete.network/how-to-build-a-great-it-department/ adresinden erişildi.

Yıldırım, S. (2017). *Bilgi Sistemleri Denetim Süreçleri*. Sermaye Piyasası Kurulu Yeterlilik Etüdü. İstanbul.

Yılmaz, Hasan (2014). *TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi.* Denetişim. 15.05.2023 tarihinde https://dergipark.org.tr/tr/download/article-file/208742 adresinden erişildi.