BAŞKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
MUHASEBE VE FİNANSAL YÖNETİM ANABİLİM DALI
ULUSLARARASI FİNANSAL RAPORLAMA VE DENETİM
TEZLİ YÜKSEK LİSANS PROGRAMI

ÖDEME VE ELEKTRONİK PARA KURULUŞLARI İÇİN BİR İÇ KONTROL MODEL ÖNERİSİ

HAZIRLAYAN

İPEK GÜNEŞTEPE

YÜKSEK LİSANS TEZİ

TEZ DANIŞMANI

PROF.DR. ÖZGE SEZGİN ALP

ANKARA -2023

BAŞKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

Tarih: 27 / 07 / 2023

Öğrencinin Adı, Soyadı: İpek GÜNEŞTEPE
Öğrencinin Numarası: 22020080
Anabilim Dalı: Muhasebe ve Finansal Yönetim
Programı: Uluslararası Finansal Raporlama ve Denetim Tezli Yüksek Lisans
Danışmanın Unvanı/Adı, Soyadı: Prof. Dr. Özge Sezgin Alp
Tez Başlığı: Ödeme ve Elektronik Para Kuruluşları İçin Bir İç Kontrol Model Önerisi

Yukarıda başlığı belirtilen Yüksek Lisans tez çalışmamın; Giriş, Ana Bölümler ve Sonuç Bölümünden oluşan, toplam 108 sayfalık kısmına ilişkin, 22 / 06 / 2023 tarihinde tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı %9'dur. Uygulanan filtrelemeler:

1. Kaynakça hariç
2. Alıntılar hariç
3. Beş (5) kelimeden daha az örtüşme içeren metin kısımları hariç

"Başkent Üniversitesi Enstitüleri Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Usul ve Esaslarını" inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Öğrenci İmzası:

ONAY

Tarih: 27/07/2023

Öğrenci Danışmanı Unvan, Ad, Soyad, İmza:

Prof. Dr. Özge Sezgin Alp

TEŞEKKÜR

Bu tezin hazırlanmasında tecrübeleri ve bilgi birikimiyle bana yol gösteren, ilgisini ve desteğini esirgemeyen tez danışmanım kıymetli hocam Prof. Dr. Özge Sezgin Alp'e, çalışmamız süresince yardımlarını esirgemeyen sevgili hocam Prof. Dr. Deniz Umut Doğan'a teşekkür ve saygılarımı sunarım.

Hayatım boyunca beni hep destekleyen, her koşulda yanımda olan beni hiç yalnız bırakmayan kendilerinden çok beni düşünen canım babam Ömer Ayan'a ve canım annem Sevgi Ayan'a sonsuz teşekkür ederim.

Gelişmemde ve ilerlememde katkısı olan, zorluklar karşısında pes etmemeyi öğreten ve yoluma devam edebilme gücünü sağlayan ve beni hep destekleyen biricik eşim Kutay Güneştepe'ye ve kıymetli oğlum Gökay Güneştepe'ye tüm kalbimle teşekkür ederim.

ÖZET

GÜNEŞTEPE, İpek. Ödeme ve Elektronik Para Kuruluşları İçin Bir İç Kontrol Model Önerisi. Başkent Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası Finansal Raporlama ve Denetim Tezli Yüksek Lisans Programı, 2023.

Finansal kuruluşlar için etkin bir iç kontrol modelinin kurgulanması ve uygulamaya geçirilmesi oluşabilecek hata, hile ve suiistimalleri engelleyerek finans sektörünün öngörülebilir olması, verilen hizmetlerin niteliğinin artması ve dolayısıyla ekonomik gelişimin sağlanması açısından hayati önem taşımaktadır. Yazında farklı finans kuruluşlarının iç kontrol yapısını etkileyen belirli başlıklara odaklanmış akademik çalışmalar bulunmaktadır. Ancak dayandığı bilgi teknolojileri ve kanuni düzenlemeler ile kendine has dinamikleri olan ve finans kuruluşlarının özel bir çeşidi olarak karşımıza çıkan Ödeme ve Elektronik Para Kuruluşlarına yönelik yeterli sayıda çalışma bulunmamaktadır. Ayrıca iç kontrol sürecinin dayandığı farklı bileşenlerin etkileşimini bütüncül olarak ele alan bir çerçeveye ihtiyaç vardır. Bu kapsamda yapılan tez çalışması ile Ödeme ve Elektronik Para Kuruluşlarına için bir iç kontrol model önerisi geliştirilmiştir. Bu modeli oluşturan bileşenler arası ilişkiler ve etkileşimler ayrıntılarıyla sunulmuştur. Bu sayede hem yazındaki boşluğa katkıda bulunulmuş hem de uygulayıcılar için rehber olabilecek bir genel bakış açısı geliştirilmiştir. Bunun yanı sıra gelecekte yapılacak araştırmalara da zemin hazırlanmıştır.

Anahtar Kelimeler: Finans Sektörü, Ödeme ve Elektronik Para Kuruluşları, İç Kontrol, Bilgi Teknolojileri, Risk Yönetimi

ABSTRACT

GÜNEŞTEPE, İpek. An Internal Control Model Proposal for Payment and Electronic Money Institutions. Baskent University, Institute of Social Sciences, Master in International Financial Reporting And Auditing with Thesis, 2023.

Establishing and implementing an effective internal control model for financial institutions is vital in preventing errors, fraud, and abuses that may occur, making the financial sector predictable, increasing the quality of the services provided, and thus ensuring economic development. In the literature, studies focus on specific topics that affect the internal control structure of different financial institutions. However, Payment and Electronic Money Institutions, a particular type of financial institution with unique dynamics counting on information technologies and regulations, are understudied. There is also a need for a framework that holistically addresses the interaction of the different components on which the internal control process is based. Accordingly, this thesis proposes an internal control model that has been developed for Payment and Electronic Money Institutions. The relationships and interactions between the components that make up this model are presented in detail. In this way, a framework is introduced that can contribute to the literature gap and guide practitioners in developing an efficient internal control system. In addition, this thesis provides a fruitful research ground for future studies.

Keywords: Finance Sector, The Payment and Electronic Money Institutions, Internal Control, Information Technology, Risk Management

İÇİNDEKİLER

TABLOLAR LİSTESİ

Sayfa

ŞEKİLLER LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR LİSTESİ

API	Application Programming Interface
BT	Bilgi Teknolojileri
COBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations
FİNTEK	Finansal Teknoloji
IFAC	Uluslararası Muhasebeciler Federasyonu
IIA	The Institute of Internal Audit
INTOSAI	Yüksek Denetim Kurumları Örgütü
IPFC	Dünya Bankalararası Finansal Telekomünikasyon Birliği
ISO	International Organization for Standardization
ITIL	Information Technologies Infrastructure Library
LIBOR	London Interbank Offered Rate
MASAK	Mali Suçları Araştırma Kurulu
NASDAQ	National Association of Securities Dealers Automated Quotations
NIST	The Nationak Institute of Standarts and Technology
PSD	Payment Services Directive
RSO	Robotik Süreç Otomasyonu
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCMB	Türkiye Cumhuriyet Merkez Bankası
TİDE	Türkiye İç Denetim Enstitüsü
UMUÇ	Mesleki Uygulama Çerçevesi
UBS	Union de Banques Suisses

GİRİŞ

Finans sektöründe iç kontrol yapılarının kurulmaması ya da verimli işlememesi şirketleri hata, hile ve suiistimallere açık hale getirmektedir. Bu nedenle finans kuruluşları ile ilgili tüm sektörü sarsacak skandallar da ortaya çıkmaktadır. Örneğin 2012 yılında İsviçre bazlı bir banka olan UBS'deki personellerin LIBOR belirlemede piyasaya dayalı nesnel verilerdense öznel verileri kullandıkları bu kapsamda yanıltıcı veriler sundukları, bunlarla yöneticilerin alım satımlarda pozisyonlardan fayda sağlayabilmek adına işlem yapmaya devam ettikleri ve çalışanların bu işlemleri kendi çıkarları için kullandıkları ortaya çıkmıştır (Kaya, 2022). Benzer skandallara diğer bir örnek olarak da Amerika Birleşik Devletleri merkezli Wells Fargo adlı banka gösterilebilir. Uygun koşullarda faiz vererek kart, hesap açılışı, çek hesabı gibi hizmetler sunan bu banka çalışanlarının hedeflerine çok hızlı bir şekilde ulaştığı bunun arkasındaki nedenin de binlerce müşteriye rızaları dışında yapılan hesap açılışlarının olduğu anlaşılmıştır (Witman, 2018).

Bu skandallar finans kuruluşlarında etkin bir iç kontrol ve risk yönetim mekanizmasının varlığının ne kadar önemli olduğunu göstermektedir. Diğer yandan gelişen bilgi teknolojileri (BT) ve değişen düzenlemelerle beraber yeni bir finans kuruluşu türü olarak *Ödeme ve Elektronik Para Kuruluşları* Türkiye'de hızla yaygınlaşmakta ve büyüyen finans kuruluşları haline gelmektedir. TCMB verilerine göre Türkiye'de 2023 yılı itibariyle 27 adet ödeme kuruluşu, 48 adet elektronik para kuruluşu bulunmaktadır. Bu kuruluşların BT ve düzenleme bazlı kendine has dinamiklerini de içeren etkili bir iç kontrol yapısının kurulması olası hata, hile ve suiistimallerin önüne geçilmesi açısından elzemdir. Dolayısıyla yaygınlaşmakta olan bu kuruluşlar için rehber nitelikte yol gösterecek akademik çalışmalara ihtiyaç duyulmaktadır.

Mevcut iç kontrol sistemlerine yönelik çalışmalar genel yapıda çerçeve çizmektedir. Örneğin, Korga ve Aslanoğlu (2020) çalışmasında iç kontrol sistem unsurları ve risk yönetiminden bankacılık sektörü kapsamına genel bir çerçeve çizilerek içerik belirlendiği görülmektedir. Demir ve diğerleri (2018)'in çalışmasında ise iç kontrole yönelik işletmeler genelinde bir bakış açısı sunulduğu görülmektedir. Bu tip yaklaşımlar sadece iç kontrol yapılarına odaklanmakta ancak bunların karar mekanizmalarıyla olan ilişkisini, BT altyapılarıyla olan etkileşimini, organizasyon içerisinde yaygınlaştırılması ve iletişiminin yapılması ile ilgili süreçleri bütüncül olarak ele almamaktadır. Ayrıca yapılan çalışmalar

Ödeme ve Elektronik Para Kuruluşlarının kendine has dinamiklerini anlamada ve bunların iç kontrol sistemi ile olan ilişkisini inceleme de yeterli çerçeveyi sağlamamaktadır.

Bu tez kapsamında sayıları hızla artan ve büyüyen finansal teknoloji firmaları içerisinde yer alan Ödeme ve Elektronik Para Kuruluşlarının iç kontrol yapılarının kurulmasına dair bir model önerisi geliştirilmiştir. Bu model kapsamında kanuni düzenlemeler, yönetimin kararları ve risk iştahı çerçevesinde belirlenen organizasyon yapısının BT destekli ilgili kontrol yapıları ile ilişkisi ve oluşan mekanizmanın izleme, faaliyet, iletişim, eğitim ve raporlama gibi süreçler ile etkileşimi bütüncül bir bakış açısıyla sunulmuştur. Ayrıca ilgili modeldeki etkileşimler Ödeme ve Elektronik Para Kuruluşlarına özgü dinamikleri içerecek şekilde detaylandırılmıştır. Böylece etkin bir iç kontrol sisteminin kurulması için gerekli olan tüm parçalar bir araya getirilerek Ödeme ve Elektronik Para Kuruluşları özelinde hem akademik çalışmaları destekleyecek ve yeni araştırmaların yapılmasını tetikleyecek hem de finans sektöründeki uygulayıcıların karar süreçlerine destek olacak bir akademik çalışma ortaya konmuştur.

Tezin akışı şu şekildedir: giriş bölümünü takip eden birinci bölümde finansal teknoloji (fintek) firmalarının gelişimi, kullandıkları bilgi teknolojileri alt yapılarına ve yasal düzenlemelerine yer verilmiştir. İkinci bölümde iç kontrol sistemlerine yönelik tanım, modeller, politika ve prosedürlere değinilmiştir. Bununla beraber risk tanımları yapılarak risk iştahının belirlenmesi ve risk değerlendirme çalışmalarına yer verilmiştir. Üçüncü bölümde model önerisi yapılarak bu model ile ilgili detaylı bilgi aktarılmıştır. Sonuç bölümünde ise yapılan çalışmanın ve sonuçlarının akademik yazına ve uygulayıcılara katkısı sunulmuş, çalışmanın kısıtlarından ve zemin hazırladığı olası gelecek çalışmalardan bahsedilmiştir.

BİRİNCİ BÖLÜM
1. FİNANSAL TEKNOLOJİ (FİNTEK)

Finans alanının uzun bir tarihi geçmişi olsa bile teknolojinin finans alanına müdahil olması buna nazaran daha yeni bir olgudur. Finansal teknoloji, 1990'lı yılların başında Citigorup tarafında teknolojik işbirliklerini kolaylaştırmak amacıyla kullanılmaya başlandı (Arner, ve diğerleri. 2016).

Fintek, finansal operasyonel faaliyetleri düzenlemek ve geliştirmek maksadıyla teknoloji destekli yeni bir finans sektörüdür (Shueffele, 2016). Oxford sözlüğünde ise finansın, bankacılık gibi sektörlere fayda sağlayan yazılım ve teknolojileri tanımlamak için kullanılan bir terim olduğundan bahsedilmektedir.

Finansal teknoloji, finans hizmetleri ve bilgi teknolojilerinin birleşimi olarak görülen, çözüm sunabilmek adına finans teknolojisinin kullanıldığı bir alan olarak da ifade edilebilir (Arner ve diğerleri, 2016).

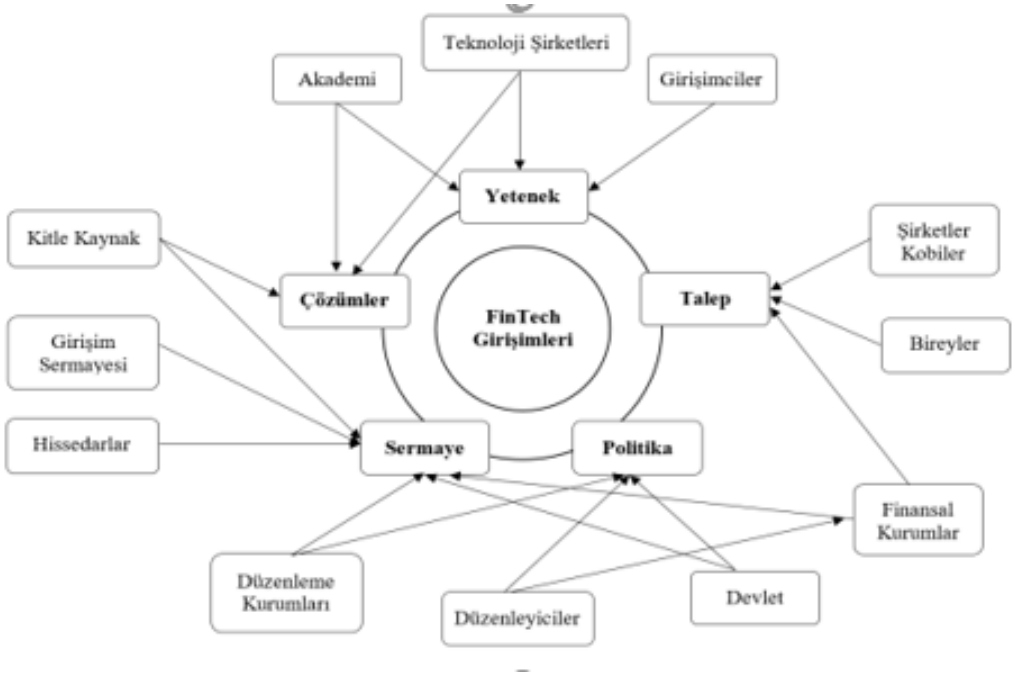
Fintek firmaları müşterilere elektronik para transferi, kripto işlemler, varlık yönetimi, ödeme hizmetleri, bankacılık hizmetleri gibi pek çok alanda hizmet vermektedir. Bu hizmetler güvenli ve kolay erişimin yanı sıra prosedür anlamında daha kolay hizmet sağlamaktadırlar. Fintek firmaları zamanla teknolojik gelişmelerin beraberinde geleneksel yapıda olan finansal kuruluşları ile yarışır hale gelmişlerdir.

1.1. Fintek Sektörü Ekosistemi ve Aktörleri

Sektör içerisinde bulunulan çevre ekonomik açıdan ekosistem olarak nitelendirilmektedir. Ekosistem, birbirleriyle bağlantılı ve bağımlı, aralarında bilgi ve kaynak akışı olan aktörlerden, kurum ve kuruluşlardan oluşur (Mars ve Bronstein, 2017).

Ekosistem içerisindeki aktörlerin birbirleriyle bağlantılı olmasından kaynaklı olarak birbirleri üzerinde etkiye sahiptirler. Aktörler arası rekabet işbirlikçi olabildiği gibi rekabetçi de olabilir (Peltoniemi, 2006). Aktörler, kuruluşlar, müşteriler ve şirketlerin haricinde devlet ve kamu gibi kural koyuculardan oluşabilir bu farklılık aktörlerin amaç, sorumluluk ve mevcut içerisindeki durumlarının yerini belirler ve belli hareket alanları yaratır.

Fintek sisteminde yer alan aktörler ve aralarındaki ilişkiler bazı çalışmalarda belirtilmiş ve modellenmiştir. Örneğin Nicoletti (2017), tarafından önerilen modelde (Şekil 1.1.) hissedarlardan başlayarak buna bağlı alt sistemler arası ilişki gösterilmiştir. Talep alt sistemi bireylerden oluşan müşteriler, finansal kurumlar ve şirketler/kobiler arasında oluşturulan işbirliğinin sonucudur. Yetenek başlığı akademi ve diğer eğitim kurumlarına, teknoloji şirketlerine ve işlerini finansal teknolojilere dayalı olarak yürüten girişimcilere bağlıdır. Çözümler ise teknoloji şirketlerine, akademiye ve kitle kaynak kullanımına dayalıdır. Sermaye özelliği ise melek yatırımcılar, girişim sermayesi ve kitle fonlamasından oluşan üç ana yatırımcı kategorisine bağlıdır. Son olarak politika ise politik ortamın yanı sıra vergi teşvikleri ve hükümet programlarının etkinliğini kapsar dolayısıyla düzenleme kurumları, düzenleyiciler ve devlet ile ilişkilidir.



Şekil 1. 1. Fintek Ekosistemi Aktörleri ve Arasındaki İlişki

Kaynak: Nicoletti, B. (2017), The Future of Fintech: Integrating Finance anf Technology in Financial Services, Palgrave Macmillanss

1.2. Fintek Tarihçesi ve Gelişimi

Fintekleri tarihçesi açısından ele alınacak olursa ilk örneklerin eskilere dayandığı görülmektedir. Bu süreçteki gelişim incelendiğinde 1866 yılından 1913 yılına kadar süren

finansal altyapıyı sağlayacak olan transatlantik kablo süreci ile başladığı düşünülmektedir (Arner ve diğerleri, 2015). Bu gelişmenin beraberinde 1918'de telgraf ve mors alfabesiyle gelişime devam eden ilk transfer sistemi ortaya çıkmış olup Fedwire olarak adlandırılmaktadır (Federal Reserve Bank, 2014). 1950 yılında ise Frank McNamara Dinners Club Kredi kartını çıkarmıştır (IPFC Online Web Agency, 2018). 1967 yılında Barclays Bank'a ait ilk ATM hizmete sunulmuştur (Wulan, 2017).

Fintek 1.0 dönemi Arner'ın bölümlendirmesi dikkate alınacak olursa 1866 ve 1967 yılları arası dönem olarak adlandırılmaktadır.

Fintek 2.0 döneminde 1967 yılı sonrası ve 2008 yılı global krize kadarki dönemi içerecek şekilde kullanılmaktadır. Bu dönemde ise 1971 yılında NASDAQ tarafında elektronik ticaretin icat edildiği 1973 yılında yurtiçi ve yurtdışı banka hesaplarına döviz transferi işlemlerini gerçekleştirmek amacıyla SWIFT sistemi kurulduğu, 1993 yılında ise Citigroup tarafından Finansal Hizmetler Konsorsiyumu kurularak 1998 yılında PAYPAL hizmetine başlandığı görülmektedir (IPFC Online Web Agency, 2018).

Fintek 3.0 döneminde Arners'in bölümlendirmesinde ekonomik krizden sonraki dönemin günümüze kadar devam etmesidir. Bu dönemde 2009 yılında Bitcoin, 2011 yılı içinde Google Cüzdan tanıtımı, 2014 yılı içinde Apple Pay'in başlaması, 2016 yılında ise Fintek lisansına dair programın belirlenmesi ile devam etmektedir (IPFC Online Web Agency, 2018).

1.3. Fintek Sektörü Teknolojik Altyapısı

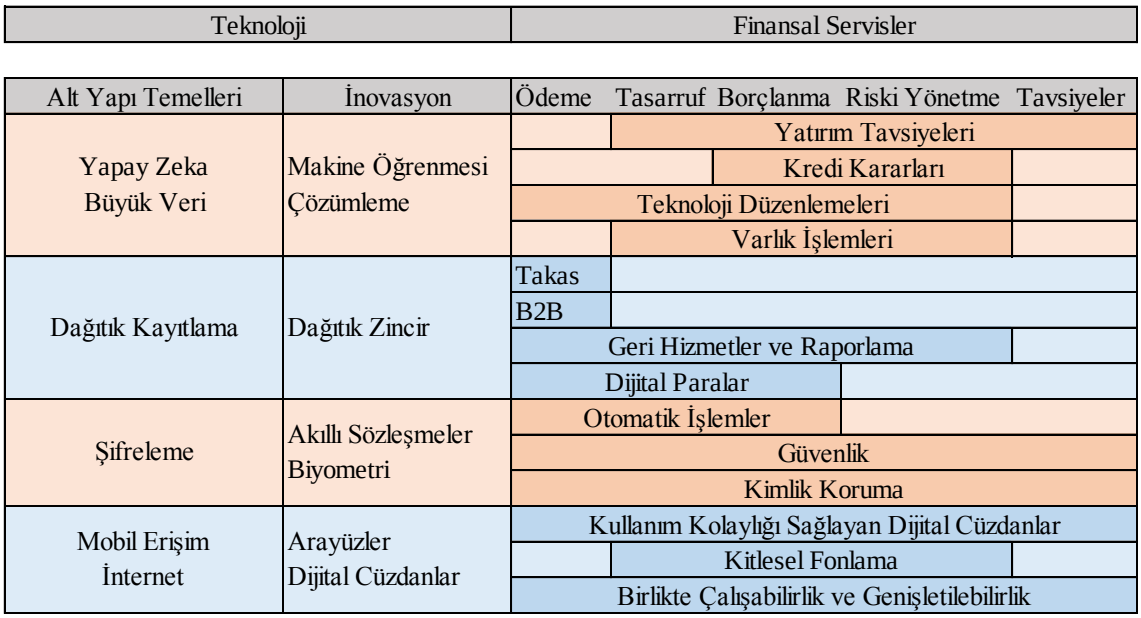
Fintek sektörü müşterilerine ödemeye ilişkin hizmetleri sunmak ve kolay yapılabilecek işlemler sağlamak, paylaşımı geliştirmek, işlem maliyetlerini azaltarak hızlı ve kaliteli hizmet vermeyi sağlayarak gelişen teknolojiyi kullanan sürekli gelişmeyi önemsemektedir (Haddad ve Hornuf, 2016).

Bilgi teknolojileri alt yapısının gelişimiyle işletmelerin yenilikçi teknolojilere vermesi gereken önem artmaktadır. Bu gelişim birçok avantaj sağlarken beraberinde bilgi güvenliği yönetimi, hassas veri yönetimi gibi pek çok hassas konuyu beraberinde getirmektedir. Bu doğrultuda Fintekler bilgi teknolojileri anlamında yatırımlar yaparak ve

iç kontrol sistemler oluşturarak bilgi teknoloji varlıklarını korunmalı ve güvenilirliğinin sağlamalı aynı zamanda kural koyucu otoritelerin getirdiklerine de uyum sağlamalıdırlar.

Şirketler verimliliği arttırmak ve rekabetçi koşullarda hız, maliyet, kalite ve bunun gibi konularda başarı elde edebilmek için bilişim teknolojilerine yatırımlar yapmaktadırlar. Sistemlerin gelişmesi ile birlikte teknolojik maliyetler azalmasına rağmen sistemlerin gelişmesi, yenilenmesi ve var olan sistemin devamlılığının sağlanabilmesi gerekliliği ortaya çıkmaktadır. Bu durum şirketler açısında ek maliyetler yaratmaktadır. Maliyetleri azaltıp verimliliği arttırmak için yeni modeller üzerinde şirketler çalışma yapmaktadırlar.

Şirketler özellikle Fintek firmaları bulut bilişimi, büyük veri, yapay zeka, makine öğrenmesi, şifre bilim, biyometrik tanıma, robotik süreç otomasyonu gibi teknolojileri kullanmaktadırlar. Bu uygulamaların kullanımı ve bilgi güvenliğine etkileri hususu işletmelerin ve kural koyucunun önemsediği konular arasında yer almaktadır. He ve diğerleri (2017) finansal servislerin dönüşümünü sağlayan teknolojileri özet bir şekil ile (Şekil 1.2.) sunmuştur. Bu teknolojiler sayesinde ortaya çıkan finansal serviseler son kullanıcıların zaman tasarrufu yapmasını, sundukları analitik yaklaşımlar ile karar vericilerin daha doğru kararlar almasını ve riskleri daha iyi yönetmelerini sağlamaktadır.



Şekil 1. 2. Finansal Servislerin Dönüşümü Sağlayan Teknolojiler

Kaynak: He ve Diğerleri (2017). Fintech and Financial Services: Initial Considerations.International Monetary Fund

1.3.1. Yapay zeka

Yapay zeka terimi ilk defa 1956 yılında Darthmouth College tarafından düzenlenen konferansta ortaya atıldı ve yapay zekanın oluşum aşamalarını, gelişimini eleştiren birçok rapor yayımlandı. Bu raporlamalar sonucunda yapay zekaya verilen destek ve ilgide azalma yaşandı. 1980'li yıllarda bu alan Japonlarla yarışabilmek için İngiliz devleti tarafından fonlanmasıyla yeniden canlanmaya başladı (Lewis, 2014).

Nabiyev (2012) tanımına göre yapay zeka; bilgisayar veyahut bilgisayar destekli bir makinenin kişiye has özelliklerle anlamlandırma, çözüm üretme, önceki tecrübelerle öğrenme gibi süreçlerle alakalı vazifeleri yerine getirebilme yetisidir. Popov (1990)'a göre insan görevlerini bilgisayara yaptırabilme süreci olarak tanımlanırken Charniak ve McDermot (1985)'a göre doğada görülen akılcı davranışların yapay olarak üretilmesi sürecidir.

Yapay zeka kavramının ortaya çıkışına yönelik çeşitli bilgiler mevcuttur. Bunlar ele alındığında (Öztürk ve Şahin, 2018);

- Tarih öncesi dönem olarak mitolojide rüzgar tanrısı olarak nitelendirilen Daedelus ilk yapay-insan girişimidir. 1769 yılında ise Osmanlı sarayı için yaptırılan satranç oynaya adam otomatı geliştirilmiştir.
- Karanlık dönem (1965-1970); Bilgisayarlar sadece veri yükleyen ve düşünen bir mekanizma olarak geliştirildi. Bu dönem bekleme dönemi olarak yaşandı
- Rönesans dönem (1975-1980); Yapay zeka geliştirenler sağlık alanında yeniliklerle ilgilendir.
- Ortaklık dönemi (1975-1980); Yapay zeka geliştirenler bilim alanlarından faydalanmaya başladı.
- Girişimcilik dönemi (1980-..); Laboratuvar dışına çıkılarak gerçek ortamın ihtiyaçlarına yönelik daha detaylı uygulamaların düşünüldüğü ve geliştirmelerin yapıldığı dönemdir.

Yapay zeka ile pek çok ülkede finansal verilerin değerlendirilmesine amacıyla terörün önlenmesine yönelik işaretlemeler ve yüz tanıma sistemlerinden faydalanmaktadır (Scherer, 2016). Yapay zeka, finansal işlemlerin dijital hale gelmesi, otomasyonu ve geliştirilmesi amacıyla fintek sektöründe kullanılmaktadır. Bunlara örnekler verecek

olursak yapay zeka algoritmaları ile sahtekarlıkların tespitinin yapılması, sanal asistanlar kullanılarak müşteri hizmetlerinde anlık destekler sağlanabilmesi, kredi başvurularının değerlendirilmesi için risk analizlerinin yaptırılması gibi firmalara ve müşterilere zaman ve süreç yönetimi anlamında fayda sağlayabilecek uygulamalardan bahsedilebilir.

1.3.2. Büyük Veri Analizi

Büyük veri terimi M. Cox ve D. Ellsworth aracılığıyla ilk defa 1997 yılında düzenlenen bir konferansta verilerin büyüklüğünün bilgisayar sistem hafızasını, diskler ve harici disklerin kapasitesini doldurması olarak ele aldığı Büyük Veri Problemi adı altında değinmiştir (Aktan, 2018). Çelik (2017)'ye göre büyük veri, veri tabanları ile analizi zor olan ve yönetiminde güçlük yaşanan büyük ölçekli veri kümeleridir.

Ohlhorst (2013)'e göre büyük veri, veri işleme araçları ile analizlerin yapılması ve yönetilmesi güç olan büyük verileri içeren setlerdir. Büyük veriyi 5V kavramı ile nitelemiştir. Bunlar; Volume (Hacim), Velocity (Hız), Variety (Çeşitlilik), Verification (Doğrulama), Value (Değer). Veri kaynak ve çeşitlerindeki artışla beraber bu adet 7'ye çıkmıştır. Bunlara ek olarak gelen 2 adet kavram ise Volatility (Oynaklık), Validity (Geçerlik) şeklindedir (Khan ve diğerleri, 2014). Bu 7 kavrama Vulnerability (Hassaslık), Variability (Değişkenlik), Visualization (Görselleştirme) eklenerek 10V kavramına ulaşılmıştır (Firican, 2017).

Büyük veri bilimi pek çok avantaj sahiptir. Bunlardan bazıları (Satyanarayara, 2015);

- Karar verme yetisini yükseltme,
- Müşteri davranışları anlama,
- Hilenin ve risklerin tespit edilmesi,
- Operasyonel etkinlik,
- İş süreçlerini anlama,
- Güvenliği arttırmak.

Yukarıda sıralanan avantajlar düşünüldüğünde büyük veri, işletmelerin karar vermelerine fayda sağlayacak verilerin toplanması saklanması ve sonuç elde edilmesi süreçlerinde kullanılan dijital bir teknolojidir.

1.3.3. Makine öğrenmesi

Oxford Learner's Dictionaries'e göre makine öğrenimi bilgisayarların görevleri yerine getirmelerinin öğretildiği büyük verilerin kullanıldığı yapay zeka türüdür. Bilgisayar sistemlerinin verileri analiz etme, gelecekteki kararları veya tahminleri yapma adına algoritmaların geliştirilmesidir. Makine öğrenimi genellikle örneklerden bir yol öğrenerek mantıksal işlemlere dayalı hesaplama yöntemidir.

1.3.4. Robotik süreç otomasyonu (RSO)

Robotik süreç otomasyonu, (Institute for Robotic Process Automation & Artifical Intelligence (IRSOAI) tarafından bir işletmede yazılım veya robot yapılandırmasıyla hali hazırdaki uygulamalarda işlemleri devam ettirmeyi, yorumlamayı, diğer sistemlerle iletişim kurmayı hedefleyen uygulama olarak tanımlanmaktadır. UiPath'e göre teknolojik sistemlerde insan hareketlerini taklit ederek iş süreçlerini bütünleştiren yazılım robotlarıdır.

RSO'nun bankacılık sistemine çeşitli faydaları dokunmaktadır. Pavaloiu (2016)'ya göre hilelerin azalmasında, sistem sıkıntılarının tahmininde maliyet tasarrufuna sebep olacaktır. Robotik süreçlerde operasyonel işlemlerin dijital kanallara yönlendirilmesi ile insan gücüne olan ihtiyaç azalmakta ve verimlilik artmaktadır. Bunun yanı sıra müşteri hizmet hızı ve kalitesinin de arttığı söylenebilmektedir. Bankacılık sektörü dışında Fintek firmalarında da RSO kullanılarak benzeri faydalar sağlanabilecektir.

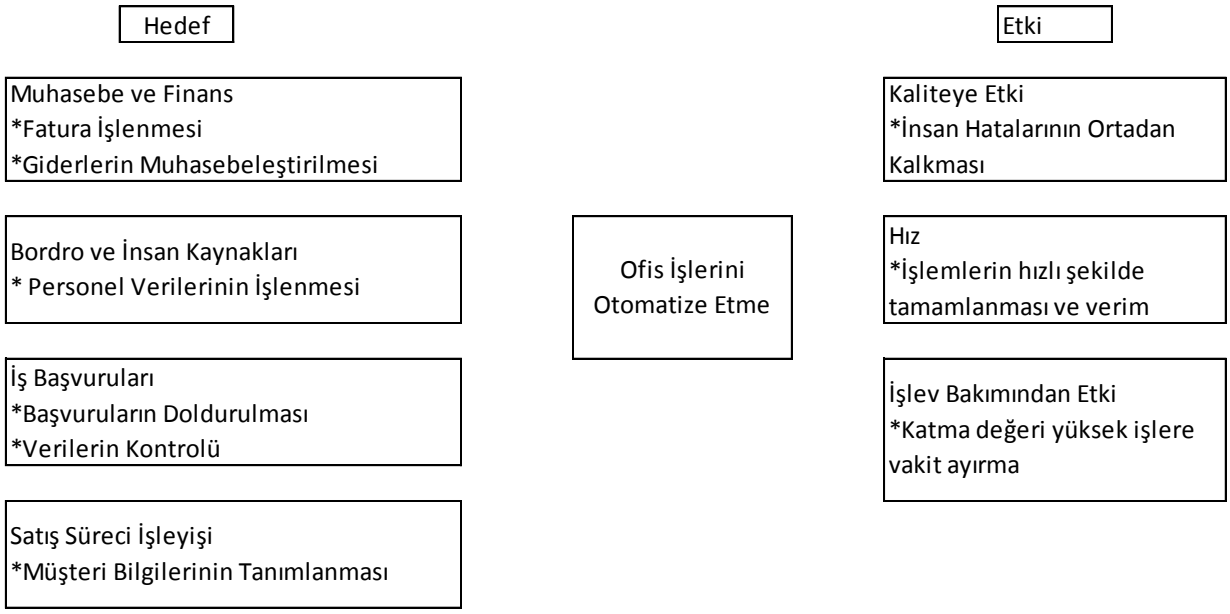
RSO, Huang ve Vasarhelyi (2019)'a göre yaptıkları araştırmada denetçiler açısında tekrarlı görevlerde ve muhakeme sürecinin etkin olmadığı süreçlerde kullanımının verimli olduğu ve muhakeme gerektiren süreçlere odaklanmalarını kolaylaştıran bir teknoloji olduğu kanısına varmışlardır.

RSO, iş süreçlerinde, denetim ve kontrol alanlarında verimli, etkin ve zamanın iyi kullanıldığı bir teknolojik sistem olduğu görülmektedir. Bu sistemin Fintek firmalarında insan gücü ve muhakeme gerektirmeyen süreçlerde kullanılmasının etkin, verimli, müşteriler açısından hızlı ve kaliteli hizmet verilmesine fayda sağladığı görülmektedir.

RSO robotlar dijital asistanlar olarak da isimlendirilirken teknik destekler sağlanarak 7/24 çalışabilmektedirler. KPMG Türkiye (2018) raporuna göre RSO standart işlerin

dijital çalışanlara yaptırılması, insan gücüne olan ihtiyacın daha karmaşık ve özel işlerde kullanılmasıdır şeklinde tanımlanmıştır. Bu tanımdan yola çıkarak dijital asistanların tamamıyla tüm işlerde kullanılamayacağı, insan gücüne ve muhakemesine olan ihtiyacın halen devam edeceğini söylemek mümkündür. Özellikle denetim alanından robotik süreçler veri almayı ve işlemeyi kolaylaştırsa da insana özgü muhakeme, akıl yürütmeye ihtiyaç her zaman mevcuttur.

KPMG'nin Robotik süreç otomasyonun hedef etkilerini tariflediği Şekil 1.3.'de makinelerin yapabileceği düzeydeki ofis işlerinin otomatize edilmesi gösterilmektedir. Örneğin; Muhasebe ve finans birimlerine özgü faturaların işlenmesi otomatize edilirse insan hatalarının ortadan kalkacağı, hızlı bir şekilde işlemlerin gerçekleştirileceği bir süreç izlenebilir.



Şekil 1. 3. Robotik Süreç Otomasyonu Hedef ve Etkileri

Kaynak: KPMG Türkiye, (2018). Robotik Süreç Otomasyonu. https://assets.kpmg.com/content/dam/kpmg/tr/pdf/2018/11/robotik-surec-otomasyonu.pdf

1.3.5. Dağıtık Hesaplama

Dağıtık hesaplama, bir bilgisayar ağı ile birbirine bağlı bir sistemin parçalarını ayrıştırarak hesaplama açısından yoğun sorunları çözebilme sürecidir. Dağıtık hesaplama

yöntemleri ilişkin yaklaşımlar incelendiğinde bulut bilişimi, kümeli hesaplamalar, ızgara hesaplaması yaklaşımları bulunmaktadır.

- **Bulut bilişim**

Bulut bilişim, bilgisayar sistemlerinin İnternet üzerinden paylaşılan kaynaklara erişmesine izin vererek veri depolama, bilgi işlem gücü, uygulamalar ve diğer bilgi teknolojilerinin sağlanmasıdır. Bu teknoloji, işletmelerin, bireylerin ve kurumların bilgi teknolojisi altyapılarını yönetmelerini ve kullanmalarını sağlar (Bughin ve diğerleri, 2010).

Bulut bilişimin en önemli faydalarından biri maliyetinin düşük olmasıdır. Bulut bilişim sayesinde bakım, güncelleştirme, yatırım maliyetlerine katlanılmadan hizmet alınmaktadır. Bulut bilişim verilerinin birden fazla bilgisayarda saklanması ihtiyaç halinde hesaplamaların bulut üzerinden yapılması bilgisayar kapasitelerinin öneminin azalmasına etki etmiştir. Zaman ve mekan sınırı olmaksızın bulut bilişim aracılığıyla erişebilmek mümkün hale gelmiştir (Dal ve Aydın, 2013).

Bulut bilişim maliyet tasarrufu sağlarken donanım altyapı ve yazılım yatırımlarının azalmasına etki eder. Uzaktan erişim ile internet bağlantısı bulunan cihazlardan verilere ve uygulamalara erişim kolaylığı sağlar. Veri yedeklerine erişim kolaylaştırır ve veri kaybı riskini azaltır.

- **Kümeli hesaplama**

Kümeli hesaplama, verileri benzerliklerine ve ilişkilerine göre gruplara ayırmak için kullanılan veri analiz tekniğidir. Kümeli hesaplamada bir iş birden çok bölüme ayrılarak her bölümden hesaplanan sonuçlar tek bir yerde toplanırlar. Böylelikle daha kısa zamanda daha hızlı bir hesaplama yapılır (Akçay ve diğerleri, 2007).

- **Izgara hesaplama**

Izgara hesaplama, dağıtık ve paralel şekilde çalışan gücü yüksek sunucuların hesaplama güçlerinin birleştirilmesiyle maksimum kapasiteli sistemler oluşturulup tek bir yapı ile uyum sağlamasıdır (Sultan, 2011). Izgara hesaplama ile farklı konumlarda bulunan kaynakların, depolamaları, yazılımları ve altyapıları ağa bağlı tüm bilgisayarlarla paylaşılmasını sağlayan sistemdir.

1.4. Ödeme Hizmetleri ve Ödeme Sistemleri

1.4.1. Ödeme Hizmetleri

TCMB'ye göre ödeme hizmeti, kullanıcının ödeme hesabından bağımsız olarak para transferi ve bu transferlerle bağlantılı olan işlemler olarak adlandırılmaktadır. Bu çerçeveden bakıldığında para çekme, para yatırma, elektronik ödemeler ve online hizmetler yardımıyla yapılabilecek ödemeleri içermektedir.

1.4.2. Ödeme Sistemleri

TCMB'ye göre ödeme sistemi, bankaların para aktarımı sırasında kullanılan özel altyapıdır. Ödeme sistemi çalışma kuralları incelendiğinde;

1- Müşteri para transferini gerçekleştirmek adına sistem üyesi olan bankasına ödeme emri verir
2- Müşteri ödeme emrini alan banka, işlemin transferine ait emri sistem iletir
3- EFT sistemi tarafından paranın gönderen banka hesabından alan banka hesabına geçmesine katkı sağlar
4- Alıcı banka işlem detayları ile ilgili bilgilendirilir
5- Alıcı banka gelen bilgi doğrultusunda müşterisi olan alıcıya ödeme işlemini gerçekleşmesini sağlar.

Bu aktarımın gerçekleşmesini sağlayan ödeme araçları ödeme emir işlemini başlatmak için kullanılan kart, cep telefonu, şifre gibi araçlardır.

1.4.3. Ödeme ve Elektronik Para Kuruluşlarının Türkiye'deki Yeri

Türkiye'de Ödeme ve Elektronik Para Kuruluşları 28690 sayılı Resmi Gazete'de yayımlanan 6493 sayılı Kanun'un 12.maddesi uyarınca belirtilen ödeme hizmetlerine uymakla yükümlüdürler. 12. maddenin fıkraları incelendiğinde ödeme kuruluşlarının yapabileceği işlemler;

- Ödeme hesabından para yatırılması ve çekilmesi imkanını veren hizmetlerde dahil olmak üzere ödeme hesabının kullanılmasına dair işlemleri,

- Ödeme hizmeti kullanıcısının ödeme hizmeti sağlayıcısında bulunan hesabındaki fonun transferi, tek seferlik doğrudan borçlandırma işlemi, ödeme kartı veya benzeri araçla yapılan para transferini,
- Ödeme aracı ihraç veya kabulü,
- Para havalesi işlemini,
- Gönderen tarafından ödeme işleminin yapılmasına dair onayın bir haberleşme cihazı yardımıyla verilmesi ve ödeme işlemlerinin, yalnızca kullanıcılar veya hizmet sağlayıcılar arasındaki bilgi veya elektronik taşıyıcılara yapılmasını,
- Fatura ödemesi aracılığına
- Ödeme hizmet kullanıcısı tarafından bir diğer ödeme hizmet sağlayıcısında bulunan ödemeye ait hesabından ödeme emri başlatmasını
- Ödeme hizmet kullanıcısının onayı sonucunda ödeme hizmet kullanıcısının ödeme hizmet sağlayıcısı nezdinde bulunan bir veya birden fazla ödeme hesabını içeren bir araya getirilmiş bilgilerin çevirim içi sunulması hizmetine değinilmektedir.

Bu fıkralar kapsamında faaliyet izni olan faaliyette bulunan hali hazırda 27 adet ödeme kuruluşu mevcuttur. Bu kuruluşlara aşağıdaki yer alan Tablo 1.1.'de yer verilmiştir.

Tablo 1. 1. 2023 yılı Ödeme Kuruluşları Listesi

	Kuruluş Unvanı (Kodu)
1	Aypara Ödeme Kuruluşu A.Ş. (880)
2	BRQ Link Ödeme Hizmetleri A.Ş. (898)
3	Ceo Ödeme Kuruluşu A.Ş. (878)
4	Efix Ödeme Hizmetleri A.Ş. (876)
5	Elekse Elektronik Para ve Ödeme Kuruluşu A.Ş. (855)
6	Faturakom Ödeme Hizmetleri A.Ş. (858)
7	Föy Fatura Ödeme Kuruluşu A.Ş. (859)
8	Global Ödeme Hizmetleri A.Ş. (884)
9	GönderAl Ödeme Hizmetleri A.Ş. (851)
10	Klon Ödeme Kuruluşu A.Ş. (881)
11	Lidio Ödeme Hizmetleri A.Ş. (895)
12	MoneyGram Turkey Ödeme Hizmetleri A.Ş. (871)
13	Octet Express Ödeme Kuruluşu A.Ş. (874)
14	Ödeal Ödeme Kuruluşu A.Ş. (868)
15	Paragram Ödeme Kuruluşu A.Ş. (888)
16	Paratika Ödeme Hizmetleri A.Ş. (865)

	Kuruluş Unvanı (Kodu)
17	Pay Fix Elektronik Para ve Ödeme Hizmetleri A.Ş. (882)
18	Paybull Ödeme Hizmetleri ve Elektronik Para A.Ş. (892)
19	Paynet Ödeme Hizmetleri A.Ş. (866)
20	Pratik İşlem Ödeme ve Elektronik Para A.Ş. (860)
21	Ria Turkey Ödeme Kuruluşu A.Ş. (879)
22	Sender Ödeme Hizmetleri A.Ş. (875)
23	Sundus Elektronik Para ve Ödeme Kuruluşu A.Ş. (844)
24	Trend Ödeme Kuruluşu A.Ş. (862)
25	Tronapay Ödeme Hizmetleri A.Ş. (887)
26	Vezne24 Tahsilat Sistemleri ve Ödeme Hizmetleri A.Ş. (885)
27	Western Union Turkey Ödeme Hizmetleri A.Ş. (886)

Kaynak:TCMB.https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Temel+Faaliyetler/Odeme+Hizmetleri/Odeme+Kuruluslari

Bu fıkralar kapsamında faaliyet izni olan faaliyette bulunan hali hazırda 48 adet elektronik para kuruluşu mevcuttur. Bu kuruluşlara aşağıda yer alan Tablo 1.2.'de yer verilmiştir.

Tablo 1. 2. 2023 yılı Elektronik Para Kuruluşları Listesi

	Kuruluş Unvanı (Kodu)
1	A Ödeme ve Elektronik Para Hizmetleri A.Ş. (913)
2	Ahlatcı Ödeme ve Elektronik Para Hizmetleri A.Ş. (894)
3	As Ödeme Hizmetleri ve Elektronik Para A.Ş. (911)
4	Aköde Elektronik Para ve Ödeme Hizmetleri A.Ş. (836)
5	Belbim Elektronik Para ve Ödeme Hizmetleri A.Ş. (828)
6	Birleşik Ödeme Hizmetleri ve Elektronik Para A.Ş. (825)
7	BPN Ödeme ve Elektronik Para Hizmetleri A.Ş. (850)
8	Cemete Elektronik Para ve Ödeme Hizmetleri A.Ş. (826)
9	D Ödeme Elektronik Para ve Ödeme Hizmetleri A.Ş. (830)
10	Dgpara Ödeme ve Elektronik Para Kuruluşu A.Ş. (893)
11	DSM Ödeme ve Elektronik Para Hizmetleri A.Ş. (848)
12	Erpa Ödeme Hizmetleri ve Elektronik Para A.Ş. (837)
13	Fastpay Elektronik Para ve Ödeme Hizmetleri A.Ş. (891)
14	Faturamatik Elektronik Para ve Ödeme Kuruluşu A.Ş. (861)
15	Fzypay Elektronik Para ve Ödeme Hizmetleri A.Ş. (896)
16	Hızlıpara Ödeme Hizmetleri ve Elektronik Para A.Ş. (833)

	Kuruluş Unvanı (Kodu)
17	IQ Money Ödeme Hizmetleri ve Elektronik Para A.Ş. (889)
18	İninal Ödeme ve Elektronik Para Hizmetleri A.Ş. (832)
19	İstanbul Ödeme ve Elektronik Para A.Ş. (883)
20	İyzi Ödeme ve Elektronik Para Hizmetleri A.Ş. (864)
21	Lydians Elektronik Para ve Ödeme Hizmetleri A.Ş. (890)
22	Moka Ödeme ve Elektronik Para Kuruluşu A.Ş. (857)
23	Moneypay Ödeme ve Elektronik Para Hizmetleri A.Ş. (842)
24	N Kolay Ödeme ve Elektronik Para Kuruluşu A.Ş. (852)
25	Nomu Pay Ödeme ve Elektronik Para Hizmetleri A.Ş. (831)
26	Ozan Elektronik Para A.Ş. (839)
27	Paladyum Elektronik Para ve Ödeme Hizmetleri A.Ş. (834)
28	Papara Elektronik Para A.Ş. (829)
29	Papel Elektronik Para ve Ödeme Hizmetleri A.Ş. (914)
30	Parakolay Elektronik Para A.Ş. (847)
31	ParaQR Elektronik Para ve Ödeme Hizmetleri A.Ş. (897)
32	Parolapara Elektronik Para ve Ödeme Hizmetleri A.Ş. (846)
33	Payco Elektronik Para ve Ödeme Hizmetleri A.Ş. (849)

	Kuruluş Unvanı (Kodu)
34	Paypole Ödeme Hizmetleri ve Elektronik Para A.Ş. (916)
35	Paytr Ödeme ve Elektronik Para Kuruluşu A.Ş. (863)
36	Rubik Elektronik Para ve Ödeme Hizmetleri A.Ş. (899)
37	Sipay Elektronik Para ve Ödeme Hizmetleri A.Ş. (838)
38	Token Ödeme Hizmetleri ve Elektronik Para A.Ş. (840)
39	Tom Pay Elektronik Para ve Ödeme Hizmetleri A.Ş. (912)
40	TT Ödeme ve Elektronik Para Hizmetleri A.Ş. (870)
41	TTM Elektronik Para ve Ödeme Hizmetleri A.Ş. (843)
42	Turk Elektronik Para A.Ş. (827)
43	Turkcell Ödeme ve Elektronik Para Hizmetleri A.Ş. (869)
44	Turkonay Elektronik Para ve Ödeme Hizmetleri A.Ş. (915)
45	UPT Ödeme Hizmetleri ve Elektronik Para A.Ş. (853)
46	Vepara Elektronik Para ve Ödeme Hizmetleri A.Ş. (845)
47	Vizyon Elektronik Para ve Ödeme Hizmetleri A.Ş. (854)
48	Vodafone Elektronik Para ve Ödeme Hizmetleri A.Ş. (835)

Kaynak:TCMB.https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Temel+Faaliyetler/Odeme+Hizmetleri/Elektronik+Para+Kuruluslari

1.5. Ödeme Hizmetlerine İlişkin Düzenlemeler

Ödeme hizmetlerine ilişkin olarak Türkiye'de ve dünyada çeşitli düzenlemeler yer almaktadır. Türk ödeme hizmetleri mevzuatının hazırlanmasına kaynak olarak alınan PSD (Payment Services Directive) 2007 yılında yayımlanmıştır. PSD ile Avrupa bölgesinde ödemeler için kurallar ve yönergeler belirlenmiştir. 2013 yılında PSD2 oluşturulması için çalışmalara başlanmış bu kapsamda Açık bankacılık hizmetleri ve ödeme hizmetleri yönergesi kapsamının genişletilmesi amacıyla İkinci Ödeme Hizmetleri Direktifinin (PSD2) 2015 yılında yayımlanmıştır. PSD2 ile mobil ve çevirim içi ödeme hizmetlerine yönelik olarak rekabet ve güven arttırmak amacıyla yeni düzenlemeler getirilmiştir (Giambelluca ve Masi, 2016). PSD2, açık bankacılık temelinin oluşturulmasına dair olarak kullanıcı ödemelerinin bir mobil uygulama ya da ağ tarafından gerçekleştirilebileceği anlamına gelmektedir. Kullanıcı izni ya da banka API erişimi ile bu işlemler gerçekleştirilebilmekte fakat bazı sorunlarda beraberinde gelmektedir. Mansfield-Devine (2016)'ya göre müşteri verilerinin paylaşılması sebebiyle olası bir suiistimali işleminde firmaların sorumlulukları devam etmektedir.

Açık bankacılık Chan (2020)'ye göre, teknolojik kullanımla beraber müşterilerin güveni, kullanım kolaylığı ve kullanım sonucu sağlanacak fayda ile sahip oldukları varlıkları yönetmek ve finansal seçimleri iyi şekilde yapabilmeyi sağlamaktadır. Açık bankacılık son kullanıcıya fayda sağlamakla beraber finans kuruluşlarına yenilikleri ve rekabet alanlarını belirlerken verilerin gizliliği ile ilgili sıkıntıları gündeme getirmiştir. Bu sebeplerden bakıldığında sektörde düzenlemelerin yapılması ve gerekli tedbirlerin alınması önemlidir.

Fintech İstanbul 2019 raporuna göre 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun ile PSD'nin Türkiye'ye uyumlu hale getirilmesi için harekete geçilmiştir. İlgili kanunun açık bankacılığa uygun hale getirilmesi için ödeme sistemleri ve elektronik para kuruluşlarına dair yetkilendirme 2019 yılında yayımlanmıştır.

Finansal Teknoloji (Fintek) firmaları bankalara kıyasla daha az maliyetli ve daha hızlı hizmet vermeyi hedefleyen son kullanıcıya kolaylık sağlayan finansal hizmetler sunmaktadırlar. Bu sebeple kanuni düzenlemelerin olması son kullanıcıların korunması, bilgi güvenliğinin sağlanması ve para akışlarının takibi, kontrolü açısından önemlidir.

Türkiye'deki 6493 sayılı kanun Türkiye'de elektronik para kuruluşlarının faaliyetlerini düzenlerken, ödeme hizmeti sağlayıcılarının ve menkul kıymet mutabakat sistemlerinin işleyişini de içermektedir. Bunun yanı sıra ödeme sistemlerinin güvenliği, etkinliği ve rekabeti konusunda düzenleyicidir. 6493 sayılı kanunun yanında finans firmalarının uymakla yükümlü olduğu 5549 sayılı Suç Gelirlerini Aklanmasının Önlenmesi Hakkında Kanun ile bunlara bağlı olarak çıkarılan ikincil mevzuata (yönetmelik, tebliğ genelge gibi) da tabiidirler.

6493 sayılı kanun kapsamında Türkiye'deki düzenlemeler incelendiğinde

- 27.06.2013 tarihinde Resmi Gazete'de yayımlanan 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun,
- 2014 yılında Resmi Gazete'de yayımlanan Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmelik,
- 2016 yılında Resmi Gazete'de yayımlanan Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ yürürlüğe girmiştir.

01.12.2021 tarihinde Resmi Gazete'de yayımlanan;

- Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik
- Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ ile içerikte değişikliklere gidilmiştir.

6493 sayılı kanun kapsamında sistem işleticisinin faaliyet izinleri, faaliyet izin başvuruları ve iznin sona ermesi, sistem gözetimi, alınması gereken tedbirler, transfer emirleri, netleştirmeler ile sistemlerin belirlenmesi, ödeme hizmetleri ve detayları, elektronik para kuruluşları ve elektronik paranın ihracı, denetim, fonların korunması ve teminatı, belge ve kayıtların saklanması ile kişisel verilerin korunması, pay edinimleri, değişiklikleri, yaptırımlar, kovuşturma ve soruşturma usulleri belirlenmiştir.

01.12.2021 tarihinde Resmi Gazete'de yayımlanan Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ maddeler incelendiğinde kuruluşlardan beklenenlere dair bilgiler;

- *Bilgi sistemlerine yönetimine dair genel hükümler çerçevesinde* şirketin bilgi güvenliğine yönelik politika ve prosedürlerin düzenlenmesi, organizasyon şemasının belirlenmesi, bilgi teknolojileri çalışanlarının görev ve sorumluluklarının belirlenmesine dair hükümlerden
- *Bilgi sistemlerine ilişkin olarak risklerin ölçülmesi* izlenmesi ve yönetilmesine dair olarak risk yönetim politika ve prosedürlerin hazırlanması, risk matrislerinin ve çalışmalarının oluşturulmasına ve yılda bir defa risk değerlendirmesi yapılmasını içerir maddeler bulunduğu
- *Bilgi sistemleri işletimine* yönelik olarak bilgi sistemlerinin sürekliliği, dayanıklılığı, güvenilirliği, hizmet sözleşmelerinin seviyeleri, kapasitenin yönetilmesi, varlık envanteri, değişiklik yönetimi ve proje yönetimi gibi içerikleri belirleyen maddeleri içerdiği
- *Olay yönetimi ve siber olaylara ilişkin olarak* olay ve sorun yönetim prosedürlerine, siber olaylara müdahale süreci gibi içerikleri belirleyen maddeleri içerdiği
- *Bilgi güvenliği ve bilgi güvenliği yönetimine dair olarak* bilgi güvenliği politikaları ve prosedürlerine, bilgi güvenliği kayıtlarına, imha prosedürüne, birincil ve ikincil sistem ağ topolojisine, hassas müşteri verilerinin ve müşteri verilerinin özel iç ağda tutulması, bilgi teknolojileri güvenliği görevlileri ve sorumluluklarının düzenlenmesi, mobil uygulama ve cihazların çalışması ve kaybolması durumunda alınan önlemlerin varlığı gibi detayların belirlendiği maddelere
- *Veri güvenliği ve mahremiyetine ilişkin olarak* veri güvenliği ve mahremiyetine ilişkin olan politika ve prosedürlerden veri gizliliğinin sağlanmasına yönelik alınan önlemlerin varlığından yedekleme ve veri imha prosedürlerin varlığını içerir maddelere
- *Kimlik doğrulamaya ilişkin olarak* kimlik yönetim prosedürü, şifre politikası, kimlik doğrulama mekanizmasında kullanılan bileşenlerin kullanıcıya

ulaşmasına kadar olan süreçte alınan güvenlik önlemleri, güçlü kimlik doğrulama teknikleri gibi detayları içerir maddelere

- *Erişim yönetimi* kapsamında erişim yönetim prosedürlerine, rol yetki matrislerine ve gözden geçirmelerin yapılmasına, log kayıtlarına, personel işe giriş çıkışlarına ve sistem giriş çıkışlarını içerir maddelere
- *Güvenlik açıkları ve ihlallerine dair olarak* yılda asgari olarak altı defa zafiyet taraması yaptırılması, yılda azami bir defa sızma testi yaptırılması, bu testler sonucunda ortaya çıkan bulgularım takibinin yapılması, güvenlik ihlallerine dair delillerin on yıl süre için güvenli bir şekilde saklanmasına dair maddelere
- *Denetim izlerinin oluşturulmasına dair* olarak log kayıtlarının zaman damgalı olarak en az 10 sene saklanması, personel, aracı personele atanması ve kayıtları, personelin kendi denetim izlerine müdahale edememesi, denetim izlerinin yedeklenmesi ve yedeklerden geri dönülerek inceleme yapılabilmesine dair maddelere
- *Bilgi sistemleri süreklilik planına* dair olarak bilgi sistemleri ve iş sürekliliği planlarının oluşturulması, iş sürekliliği planı doğrultusunda görevli personel ve gruplar, iş etki analizlerinin yapılması, bilgi sistemleri süreklilik planını test edilmesine dair maddelere
- İkincil merkez, ikincil sistem, yedekleme merkeze dair olarak ikincil merkez için yapılan test çalışmalarını, acil durum planlarının oluşturulması, birincil merkezde kesinti olması halinde ikincil merkezde görev alacak personellerin görev ve sorumluluklarının belirlenmesine dair maddelere
- *Bilgi sistemlerine ilişkin dış hizmet alımına ilişkin olarak* dış hizmet alım prosedürü, dış hizmet alımına dair risk değerlendirme çalışmalarının yapılması, dış hizmet sağlayıcılarına tanınana erişim yetkileri, ülke içerisinde tesis edilmiş bulut bilişim hizmetleri kullanımına dair maddelere
- *Müşterilerin bilgilendirilmesi ve internet sitesine dair* olarak müşterilere sunulan hizmetlerin şartları ve risklerine ilişkin bilgilendirmeler, iki saatten uzun süreli kesintiler için müşterilerin bilgilendirilmesi, müşteri edinim sürecinde müşterilere özelleştirilmiş duyurular, uyarılar ve daha fazlası özelinde iletişim tercihlerinin belirlenmesi gibi maddelere

- *Yüksek riskli işlemlerin takibine ilişkin* olarak tasarlanmış süreç dokümanları, takip mekanizmaları, düşük değerli işlemlerde kısa süre içerisinde gerçekleştirilmesine dair yazılı kuralların varlığı, yüksek riskli işlem gerçekleştiren müşterilere dair takip mekanizmalarının varlığı, verilen hizmetlerin yasa dışı bahisler dahil olmak üzere yasa dışı işlemelerde kullanılmamasına dair maddelere yer verilmiştir. İlgili tebliğ 5 bölüm ve 34 maddeden oluşmaktadır. Yukarıda yorumlanan tebliğ maddelerinin içeriklerinde veri paylaşımı, bilgi güvenliği, bilgi güvenliği riskleri, veri güvenliği ve mahremiyeti, olay yönetimi ve siber olaylar, erişim yönetimi, güvenlik açıkları ve ihlallerine yönelik bilgi sistemleri veri paylaşım sistemleri ile ilgili hükümleri içermektedir.

Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik içerisinde yer alan maddeler incelendiğinde kuruluşların yetkilendirilmesi ve faaliyetleri, ödeme hizmeti sağlayıcılarına, ödeme hizmetlerinin sunulmasına ve elektronik para ihracının usul ve esaslarına değinilmiştir. Bu kapsamda yönetmelik maddelerinde ödeme hizmetleri, elektronik para, anonim ön ödemeli araçlar, faaliyet izni, pay edinimleri ve devri, kuruluş faaliyet esasları ve yapılmaması gereken faaliyetler, şube, temsilci ve dış hizmet alımları, yönetim kurulu görev ve yetkileri, genel müdür görev ve yetkileri, iç kontrol sistemi kurulması, risk yönetimi, öz kaynak yeterliliği, ödeme fonlarının korunması, elektronik para karşılığı fonların korunması, ücret, masraf, komisyon bilgileri gibi ödeme ve elektronik para kuruluşlarını ilgilendiren konularda tanımlara, açıklamalara, usul ve esaslara yer verilmiştir.

5549 sayılı Suç Gelirlerini Aklanmasının Önlenmesi Hakkında Kanun kapsamında finansal teknoloji firması olan Ödeme ve elektronik para kuruluşlarının tabii olduğu düzenlemelere değinecek olursak;

- Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine İlişkin Yükümlülüklere Uyum Programı Hakkında Yönetmelik
- Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik
- Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesi Kapsamında İşlemlerin Ertelenmesine Dair Yönetmelik

- Terörizmin Finansmanının Önlenmesi Hakkında Kanunun Uygulanmasına ilişkin Usul ve Esaslar Hakkında Yönetmelik
- Terörün Finansmanına Yönelik Şüpheli İşlemlerin Bildirimi Genel Tebliği

bu kuruluşlar için uyum sağlamaları gereken kanuni düzenlemelerdir.

Ödeme ve elektronik para kuruluşları 5549 sayılı Suç Gelirlerini Aklanmasının Önlenmesi Hakkında Kanun ile bunlara bağlı olarak çıkarılan ikincil mevzuata (yönetmelik, tebliğ genelge gibi) da tabii olmaları sebebiyle bunlara uymakla yükümlüdürler.

Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine İlişkin Yükümlülüklere Uyum Programı Hakkında Yönetmelik kapsamında suç gelirlerinin aklanması ve terörün finansmanının önlenmesi amacıyla yükümlülerin uyum programı oluşturması ve uyum görevlisi atamalarına ilişkin usul ve esaslar düzenlenmiştir. Bu yönetmeliğin içerdiği maddelerin bir kısmını incelediğimizde

- 2021 yılında yönetmeliğe eklenen finansal grubun mahiyeti başlığı altında finansal grubun ana kuruluşu ile diğer kuruluşları ile beraber uyum anlamında bütünlük oluşturabilmesi ve paylaşımda bulunabilmesi,
- Uyum programı oluşturması gerekli yükümlülerden bahsedilirken Sermaye piyasası aracı kurumları, bankalar, sigorta ve emeklilik şirketleri, posta ve telgraf şirketleri, elektronik para kuruluşları, ödeme kuruluşları vb.. kuruluşlara,
- Uyum programının kapsamına ilişkin maddelerde şirket politika ve prosedürlerinin oluşturulması, risk yönetimi, izleme ve kontrol faaliyetleri, eğitim faaliyetleri ve iç denetim faaliyetlerinin yürütüldüğü belirtilmekte olup MASAK tarafından her yılın mart ayı sonunda bir önceki yıla ait eğitim faaliyetlerinin, iç kontrol faaliyetlerinin raporlanmasına,
- Yönetim kurulunun yetki ve sorumluluklarının içeren maddede uyum görevlisi ve uyum görevli yardımcısının atanması, uyum görevlisi ve uyum biriminin yetkilerinin sorumluluklarını yazılı şekilde belirlemek, uyum programı kapsamında risk yönetimi izlenmesi kontrolü ve sonuçlarının değerlendirilmesi gibi uyum programı kapsamında olabilecek faaliyetlere ilişkin sorumluluklara,

- Kurum politikası ve prosedürlerine ilişkin olan maddelerde uyum programı kapsamında belirtilenler doğrultusunda kurum politika ve prosedürlerinin oluşturulması ve bunlar oluşturulurken risk değerlendirmelerinin yapılması, kimlerin nelerden sorumlu olduğu, belirli risklere göre limitler belirlenip onaylanması, raporlanmasına ilişkin detaylara,
- Risk yönetimine ilişkin olarak olası risklerin belirlenmesi, tanımlanması, derecelendirilmesi, izlenmesinin sağlanması, risk kapsamına giren konularda ulusal ve uluslararası mevzuatlara, standartlara ve tavsiyelere ilişkin olarak gerekli takiplerin yapılması ve risk izleme değerlendirme çalışmalarının belli periyodlarda Yönetim Kurulu'na raporlanmasına,
- Yüksek derecede riskli müşterilere ilişkin olarak risk derecelendirme sonucunda yüksek riskli olarak belirlenen grupların risklerinin azaltılmasına ilişik alınan tedbirlere,
- İzleme ve kontrole ilişkin olarak iş ve işlemlerin nasıl yapılacağı, örneklemlerin seçimlerinin yapılması bunlar sonucunda kimlik tespitinin yapılması, işlemlerin müşteri profili ile uygun olup olmaması, riskli ülkelerden gerçekleştirilen işlemlerin izlenmesi ve kontrolüne dair detaylara,
- Uyum görevlisi ve uyum görevli yardımcısı atanmasına ilişkin olarak uyum görevlisi ve uyum görevlisi yardımcısının atanması, izne çıkması, işten ayrılması, şartlarına yer verilmiştir.

Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik kapsamında maddelerin bir kısmını incelediğimizde;

- Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine İlişkin Yükümlülüklere Uyum Programı Hakkında Yönetmelikte yazılı olduğu gibi bu yönetmelikte de yükümlülere,
- Müşterinin tanınması esasları incelendiğinde kimlik tespiti yapmakla yükümlü olanların kimlik tespitine ilişkin olarak gerçek ve tüzel kişiler, dernek vakıflar, sendika ve konfederasyonlarda kimlik tespitinin yapılmasıyla ilgili detaylara,
- Gerçek faydalanıcının tanınması kapsamında işlemlerde nihai faydayı sağlayacak kişinin tespit edilmesi yükümlülüğüne,

- Müşteri durumunun ve işlemlerin izlenmesi yükümlülüğü maddesi kapsamında risk bazlı yaklaşımla hangi müşteri işlemlerinin riskli olabileceği ve izlenmesi gerekliliğinden daha önce bahsi geçen politika prosedürler kapsamında incelenmesine,
- Üçüncü tarafa güven maddesi kapsamında finansal kurumların aldıkları tedbirler doğrultusunda bu tedbirlere güvenerek birbirleriyle iş ilişkisi tesis etmeleri ve gerekli durumlardan istedikleri evrakları temin edebileceklerine,
- İşlem reddi ve iş ilişkisinin son erdirilmesine maddesi kapsamında çalışılmaması gereken müşterilerin belirlenmesi, daha önce müşteri olanlarda kimlik bilgilerinden şüphe duyulması halinde iş ilişkisinin son erdirilmesine ilişkin detaylara,
- Riskli ülkelerle ilişkiler maddesi kapsamında daha öncede bahsi geçen politikalarda belirlenen riskli ülkeler doğrultusunda prosedürde bu ülkeler için neler yapılacağının bahsedilmesinde gerekliliklerine,
- Basitleştirilmiş tedbirler kapsamında iş ve işlemlerde tedbir yönetmeliğinde bahsi geçen kimlik tespiti gibi detaylara girmeden basit şekilde kimlik tespit teyidi yapılabilineceği, bu işlemlerin riskleri daha az işlemler olduğu hem müşteriye hem kuruluşa kolaylık sağlaması amacıyla getirilmiş belli koşulların sağlandığı durumlarda uygulanabilir. MASAK 5 nolu tebliğ kapsamında basitleştirilmiş tedbirlerin hangi şartlarda uygulanacağına dair detaylara,
- Sıkılaştırılmış tedbirler kapsamında yüksek riskli durumlarda uygulanacak tedbirlere ilişkin detaylara,
- Şüpheli işlem bildirimleri kapsamında şüpheli işleme dair esaslara yer verilmiştir. Şüpheli işlem bildirim süresi, gizliliği ve bildirimde bulunanların korunmasına karşın yükümlülüklere,
- Bilgi ve belgelerin sağlanmasına ilişkin esaslar çerçevesinde bilgi ve belge verme yükümlülüğüne yer verilmiştir.

İKİNCİ BÖLÜM
2. İÇ KONTROL SİSTEMİ ve RİSK YÖNETİMİ

İşletmelerin şartlar ne olursa olsun hayatta kalabilmeleri ve faaliyetlerine, iş hedeflerine uygun şekilde devam edebilmeleri için risk odaklı yaklaşımı benimsemeleri gereklidir. Bu bağlamda oluşturulacak olan iç kontrol sisteminin tüm işletme faaliyetlerini kapsayıcı, faaliyetlerin etkinliğini arttırıcı ve yönetimi olası durumlar için doğru bilgilendirici ve makul düzeyde güven sağlayan bir sistem olarak oluşturulması önem taşımaktadır.

İç kontrol sistemini organizasyon içerisinde muhasebe, finans gibi birkaç alan ile sınırlandırmak yerine faaliyet gösterdiği tüm alanların incelemesi olarak ele alınmasının daha doğru olacağı bunun yanında kontrol evrenini genişletmenin de çeşitli zorlukları olacağının bilinmesi önemlidir. Bu sebeple işletmeler kontrol alanı belirlerken yasal yükümlülükleri, teknolojik gelişmeleri, operasyonel süreçleri dikkate alarak bunların olası risk etki ve olasılarını göz önünde bulundurmalı ve kontrol evreninin belirlemelidir.

Yasal düzenlemeleri bilmek ve bunlara uygun hareket etmek, şirketin faaliyetlerini sürdürebilmesi ve hedeflerine ulaşabilmesi için yönetsel kararlar almasına ve risk almayı belirlemesine büyük ölçüde yardımcı olur. Bu doğrultuda politika ve prosedürlerin oluşturulması, organizasyon şemasının oluşturulması ve görevler ayrılığı ilkelerine uygun hareket edilmesi şirketin hedeflerine ulaşmasına katkı sağlayacağı gibi kontrol noktalarında fayda sağlayacaktır.

2.1. Kontrol Tanımı, Amacı ve Türleri

Kontrolün anlamı bir şeyin aslına uygunluğunun incelenmesidir. Kontrol organizasyon şemasındaki tüm çalışanların sorumlu olduğu faaliyetler için takip edilebilecek kontrolleri içerir. Kontrol süreklilik gösteren bir faaliyet olup eş zamanlı yürütülmektedir (Uzay, 1999).

Kontroller, bir kuruluşun faaliyetlerini düzenlemeye, riskleri yönetmeye, hedeflere ulaşmaya ve kaynakları etkin bir şekilde kullanmaya hizmet eder (Korkmaz, 2007). Diğer bir deyişle kontrollerin birincil amacı, bir organizasyonun hedeflerine ulaşmasını

sağlamaktır. Kontrollerin amacı, organizasyonel plan ve politikaların etkin bir şekilde uygulanmasını, kaynakların doğru ve verimli kullanılmasını, süreçlerin etkin olmasını ve risklerin yönetilmesini sağlamaktır.

Kontrol türleri önleyici, tespit edici, düzeltici ve yönlendirici kontroller olarak sınıflandırılabilir.

Önleyici kontroller; iç kontrol sisteminin parçası olarak, olası riskleri ve hataları tespit etmeye ve bunlardan kaçınmaya yönelik kontrollerdir (Gelinas ve Sutton, 2002). Bu tanımdan yola çıkarak bu kontrol türünün olası sorunları önlemek veya etkisini azaltmak için proaktif bir yaklaşım içerdiği söylenebilir. Ayrıca kuruluşların faaliyetlerini efektif bir şekilde yönetmelerini de sağlar. Bu kontrol riski azaltmaya, hataları önlemeye ve süreçlerin düzgün çalışmasını sağlamaya yardımcı olur. Önleyici kontroller, kuruluşların varlıklarını korumaları, hedeflerine ulaşmaları, yasal ve düzenleyici gerekliliklere uymaları ve itibarlarını korumaları için yüksek etkide öneme sahiptir. Tüm bu anlatımlardan yola çıkarak önleyici kontrollere için prosedür ve politikaların hazırlanması, iş süreçlerinin tasarlanması, çalışanları bilinçlendirmek için eğitimlerin verilmesi gibi örnekler verilebilir.

Tespit edici kontroller; oluştuktan sonra istenmeyen olayları tespit etmek için kontroller içerir (Romney ve Steinbart, 2003). Tespit edici kontrollerle şirketlerin hatalarını ve sorunlarını hızlı bir şekilde belirlemesine ve zamanında müdahale etmesine fayda sağlayabilir. Bu kontrol türüne örnek olarak Risk analizlerinin incelenmesi, prosedürlerin kontrol edilmesi ile olası hata ve usulsüzlüklere yönelik tespit amacıyla inceleme yapılabilir. Müşteri şikâyetleri göz önünde bulundurularak kontrol testleri ile hata ve sorunların tespit yapılabilir.

Düzeltici kontroller; riskli bir olay meydana geldiğinde bunu düzeltmek veya bir daha olmaması adına faaliyetlerde bulunmak olarak tanımlanabilir (Romney ve Steinbart, 2003). Başka bir deyişle, düzeltici kontrol; işletmelerin hata, usulsüzlük gibi risk içeren durumları ele almasını ve tekrarının önlenmesi için harekete geçilmesi açısından önem taşımaktadır. Olay meydana geldikten sonra düzeltici eylemlerin hayata geçirilmesi için sorunun ortaya çıkış nedenin araştırılması için kök neden analizi gibi yöntemlerden faydalanılarak düzeltici kontrollere fayda sağlanabilir. Kök neden analizi soruna yol açan sebepleri bulmak ve tamamen ortadan kaldırılmasına yönelik objektif ve analitik bir yaklaşımdır (Turhan ve Ünalan, 2022).

Yönlendirici Kontroller; iş süreçlerini etkin bir şekilde yönlendirmek, uygun politika ve prosedürlerin uygulanmasını ve varlıkların efektif bir şekilde kullanılmasını sağlamak için kullanılır. Yönlendirici kontroller genel olarak beklenmeyen bir olaya verilen ilk yanıt olarak nitelendirilebilir.

Yukarıda yer verilen kontrol türlerinin açıklamaları göz önüne alındığında önleyici ve düzeltici kontrol ilişkisi incelendiğinde, önleyici kontrollerin etkin bir şekilde işlemesi halinde düzeltici kontrole daha az ihtiyaç duyulabileceği, önleyici ve tespit edici kontrollerin bir arada etkin bir şekilde çalışması halinde olası hata ve usulsüzlüklerin önlenmesi adına daha etkili bir iç kontrol yapısı oluşturabileceği, tespit edici ve düzeltici kontrol yapıları ele alındığında kök nedenlerin belirlenerek düzeltilmesi ve tekrarlarının önüne geçilmesinin sağlanacağı söylenebilir. Tüm bu kontrol türlerinin aktif ve verimli bir şekilde işlemesi iç kontrolün etkinliği ve verimliliği açısında faydalı olacaktır. Bunların yanı sıra kontrol türlerinin etkin kullanılması maliyetlerin düşürülmesine, verimliliğin artmasına, oluşabilecek hataları en aza indirmeye, işletme performansında artışa, yönetime doğru bilgi akışı sağlanmasına, uygun politika ve prosedür belirlenerek uygulanmasına ve risklerin bilinmesine katkı sağlayacaktır.

2.2. İç Kontrol Tanımı

1940'lardan sonra iç kontrol kavramsal olarak ele alınmaya başlandı. Victor Z. Brink'in 1946 tarihli bir makalesi, iç kontrol kavramından bahseder (Fülop ve Szekely, 2017). Brink'e göre, efektif bir iç kontrol sisteminin temel unsurları, güvenilir bir muhasebe sistemi, yazılı politikalar ve prosedürler, operasyonların etkinliğini analiz etmek için net bir bütçe ve iç denetimdir. (Moeller, 2005). Farklı çalışmalarda yapılan tanımlamalar da Brink'in tanımlamasıyla uyumludur.

Güredin (2000) iç kontrol kavramını "Şirket varlıklarının korunması, muhasebe bilgilerinin doğruluğunun ve güvenilirliğinin doğrulanması ve organizasyonel planlar doğrultusunda etkinliğin artırılması için alınan ve uygulanan tüm önlem ve yöntemler" olarak ifade etmektedir.

Pamukçu (2019) tarafından yapılan çalışmada "İç kontrol sisteminin temel amacı, etik ilke ve kurallara uymak, şirket varlıklarını israf etmeden etkin bir şekilde kullanmak,

muhasebe hatalarını ve hileleri önlemek ve bu sayede muhasebe bilgilerinin güvenilirliğini korumaktır" şeklinde belirtilmektedir.

The Committee of Sponsoring Organizations (COSO) Raporu'nda da İç kontrol süreci, hedeflere ulaşılması, faaliyetlerin etkinliği ve verimliliği, güvenilir finansal raporlama ve ilgili kanun ve düzenlemelere uygunluğun sağlanması olarak tanımlanmakta ve yönetim kurulu, yönetim ve kurumun diğer çalışanları tarafından yürütülmektedir şeklinde açıklanmıştır (Yılancı, 2006).

İç Denetçiler Enstitüsü'ne (The Institute of Internal Auditors - IIA) göre, iç kontroller kurumsal yönetimin ayrılmaz bir parçasıdır. Faaliyetlerin etkinliğini ve verimliliğini, bütçelerin yürütülmesini, mali raporlar dahil diğer tüm raporların güvenilirliğini ve yürürlükteki kanun ve yönetmeliklere uygunluğunu makul ölçülerde sağlayan bir sistemdir (Uzay, 1999).

Uluslararası Muhasebe Uzmanları Federasyonu'na (International Federation of Accountant- IFAC) göre iç kontrol sisteminin amacı şu şekilde özetlenebilir:

- Hataları ve hileleri saptama ve önleme,
- İşletme varlıklarının korunması.
- Finansal bilgilerin doğruluğu ve güvenilirliği,
- Muhasebe bilgilerine zamanında erişim.

Bu amaç doğrultusunda gerçekleştirilen iç kontrol süreci, iş faaliyetlerinin yönetim ilkeleri doğrultusunda düzenli ve etkin bir şekilde yürütülmesine katkı sağlar. İşletmelerde iç kontrol sistemini yetersizliği ya da eksikliği durumunda yönetimin temel fonksiyonlarında planlama, örgütleme, yürütme, koordinasyon ve denetim süreçlerinde pek çok sorunla karşılaşılabilir. Yönetimin temel işlevleri nedeniyle, karar verme sürecindeki belirsizlik de örgütsel hedefleri olumsuz etkileyebilir. Böyle bir ortamda bu durum firmaların rekabet gücünü olumsuz etkilemektedir. Kaynak israfı, zaman kaybı, idari otoritenin zayıf olması, hatalı veya eksik kararlar, yasal süreci takip etmekte güçlük, etik ve değerlerin hiçe sayılması sorunlara ve kafa karışıklığına neden olur.

Bir iç kontrol sistemi, kurumsal yönetim ve ortakları için yalnızca belirli bir güvenlik düzeyiyle iş ve mali kontrolleri garanti eder. Denetçiler için iç kontrol sistemi, "Denetim risklerinin belirlenmesi" ve "Planlanması" aşamalarında çok önemlidir (Dabbağoğlu,

2009). Şirket ile iş paydaşları arasında karşılıklı saygı ve güvene dayalı ilişkilerin kurulmasında da "İç Kontrol Sistemi" etkin rol oynamaktadır. Bir şirketin iç kontrol sistemi ile ulaşmak istediği bir hedef finansal raporlamanın doğruluğuna katkı sağlama ve kaynak verimliliğini artırmak, faaliyetlerin standartlara uygun olarak yürütülmesini sağlamaktır (Messier, 2000).

İç kontrol sistemi karmaşıktır ancak farklı gruplara hizmet eder (Shift, 1990). İç kontrol sistemi yöneticileri, paydaşları, denetçileri, çalışanları ve birçok grubu etkiler. Bu nedenle idari süreç yöneticiler için en önemli konulardan biridir. Yönetim faaliyetleri, üretim yönetimi, müşteri yönetimi ve çalışan yönetimi dahil olmak üzere geniş bir yelpazeyi kapsar. Belirlenen kontrollerin en iyi şekilde yürütülebilmesi için iç kontrol sisteminin de iç denetime entegre edilmesi gerekmektedir.

İç kontrol sistemleri ile iç denetim arasında yakın bir ilişki olduğunu gösteren araştırmalar mevcuttur. Yönetim, etkin bir iç kontrol sisteminin kurulmasından, işletilmesinden ve izlenmesinden sorumludur. Ancak, hiçbir iç kontrol mekanizması hataların meydana gelmesi ve önlenmesi konusunda mutlak kesinlik sağlayamaz. Bu nedenle iç denetçinin şirket içindeki mevcut iç kontrol sistemini bilmesi ve doğru değerlendirmesi iç kontrolün etkinliğinin sağlanmasında bir etkendir (Yılancı, 2006) ve Toroslu (2014)'e göre de "İç denetim" ve "İç kontrol" kavramları arasında yakın bir ilişki bulunmaktadır. "İç denetim" ve "iç kontrol" kavramları arasında yakın bir ilişki vardır. Kontroller iç denetim standartlarına göre belirlenir. Bu süreçte, bir iç kontrol sistemi uygun ortamı belirler. Özellikle iç denetimlerin güvenliği iç kontrol sistemine de yansımaktadır.

Etkin bir iç kontrol sisteminin varlığı, hedeflere ulaşılması ve raporlamanın güvenilirliği ile kılavuzlara ve yasal düzenlemelere uyum açısından kritik öneme sahiptir. İç kontrol sistemlerinin incelenmesi bağımsız denetimin planlaması, çalışmanın kapsamı, uygulanacak testlerin niteliğinin saptanması gibi konulara destek niteliğinde olabilir. Etkin bir iç kontrol sistemi, bağımsız denetimin kalitesine etki etmektedir. İç kontrol sisteminin bağımsız bir denetçi tarafından denetlenmesi, şirketin temel risklerinin önceden doğru bir şekilde belirlenmesi anlamına gelmekte, denetim süresini kısaltmakta ve müşteri şirket üzerindeki yükü azaltmaktadır. İç kontrol sisteminin etkinliği arttıkça denetim riski azalmaktadır. (Aksoy,2017). Bağımsız denetim, sistem güvenilirliğini incelemek, sistem etkinliğini belirlemek ve ilgili görüşleri almak için kullanılabilecek prosedürler yelpazesini belirlemek için iç kontrolleri inceler. (Kaya, 2022).

Özetle; İç kontroller makul güvence sağlar. Etkinliği ve uygunluğu değerlendirmek için iç denetim faaliyetleri gereklidir. Bu nedenle, iç denetim ve iç kontrol farklıdır. Ancak birbirini tamamlayan iki kavram olarak da görülebilirler.

İşletme hedefleri çerçevesinde iç kontrol sisteminin neden önemli ve gerekli olduğuna dair yazında farklı araştırmalar da bulunmaktadır. Örneğin, IFAC (2011)'e göre belirtilen açıklamada iç kontrol sisteminin gerekliliklerinin neler olduğu konusu ele alınmıştır. Sonuç olarak, kurumsal faaliyetlerin düzenlenmesi, zamanında ve etkin bilgi sağlanması yoluyla karar almanın teşvik edilmesi, yasal prosedürlere ve düzenlemelere uyum ve şirketlerde dolandırıcılık ve yolsuzluğun önlenmesi için gereklilikler belirlenmiştir. Genel olarak iç kontrol sisteminin organizasyon yapısının etkinliği ve devamlılığı önem taşımaktadır.

Uluslararası Yüksek Denetim Otoriteleri Örgütü (INTOSAI) ve Uluslararası Muhasebeciler Federasyonu'nun (IFAC) çabaları, iç kontrollerin doğru anlaşılması ve etkili bir şekilde uygulanması için standartlar belirlemeye çalışmıştır. Bu çalışmaların bir parçası olarak INTOSAI, 1992 yılında Kamu Sektörü İç Kontrol Standartları Kılavuzunu yayınlamış ve 2004 yılında kılavuzu revize ederek yeniden yayınlamıştır.

Bu bağlamda iç kontrol birbirleriyle bağlantılı beş unsurdan meydana gelir. İç kontrolün unsurları, kontrol ortamı, risk değerlendirme, kontrol faaliyetleri, bilgi ve iletişim ile izleme olarak kabul edilmektedir (INTOSAI GOV 9100, 2004).

- Kontrol Ortamı

  Etkili bir iç kontrol sisteminin temeli, kontrol ortamıdır. Kontrol ortamı sadece iç kontrolün kalitesini etkilemekle kalmaz, aynı zamanda iç kontrol disiplinini sağlar ve iç kontrolün temelini oluşturur. Kontrol ortamının, hangi stratejilerin ve ne tür hedeflerin belirlendiği ve kontrol faaliyetlerinin nasıl yapılandırıldığı üzerinde genel bir etkisi vardır.

- Risk Değerlendirme

  Hedefler belirleyerek ve etkin bir iç kontrol ortamı oluşturarak, kuruluşun misyon ve hedeflerine ulaşmada karşılaşılan riskleri değerlendirmek, bu risklere uygun tepkiler geliştirmek için temel oluşturur. Risk değerlendirmesi, bir organizasyonun hedeflerine ulaşmasını engelleyen önemli riskleri belirleme, analiz etme ve bunlara

uygun tepkileri belirleme sürecidir. Risk değerlendirme süreci, risk tanımlama, risk ölçümü, kuruluşun riski ele alma yeteneğinin belirlenmesi ve bir risk tepkisinin geliştirilmesi aşamalarından oluşur. Bir kuruluşun çevresel koşulları sürekli olarak değişmektedir, bu nedenle risk değerlendirmesi devam eden yinelemeli bir süreç olmalıdır. Risk değerlendirmesi, değişen koşulları, fırsatları ve riskleri belirleme ve analiz etme ve iç kontrolleri değişen riskleri yansıtacak şekilde ayarlama sürecidir.

- Kontrol Faaliyetleri

  Riski ortadan kaldırmaya yönelik birincil strateji, iç kontrol faaliyetleri aracılığıyla uygulanmaktadır. Önleyici ve/veya tespit edici kontrol tedbirleri alınabilir. İç kontrol faaliyetleri hedefi gerçekleştirmek için düzeltici önlemler alır. Kontrol faaliyetlerinin, amaca uygun olması, zaman içinde planlandığı şekilde sürekli uygulanması, uygun maliyetli, kapsamlı, uygun ve yönetim hedefleriyle doğrudan ilişkili olması önemlidir. Kontrol faaliyetlerini Delegasyon ve onay prosedürleri. Görevlerin ayrılması (delegasyon, uygulama, kayıt, inceleme). Kaynaklara ve kayıtlara erişim izinlerini kontrol etme. Onaylama, uzlaşma. İş performansı anketi. Süreçler ve izleme ile ilgili faaliyetler, süreçler ve eylemler gibi unsurlardan oluşturmaktadır.

- Bilgi ve İletişim

  Hedeflerin gerçekleştirilmesi için kurumun her kesiminden gelen bilgi önem taşımaktadır. Yönetimin iyi ve yerinde karar alma yetkinliği bilginin kalitesinden etkilenir. Bu bilgiler güncel, doğru ve erişilebilir olmalıdır. İletişim, grupların ve bireylerin sorumluluklarını etkili bir şekilde yerine getirmelerini sağlayarak beklentileri karşılamanın temelidir. Tüm çalışanlar, yönetim sorumluluklarını ciddiye almaları için üst yönetimden net bir mesaj almalıdır.

- İzleme

  Zaman içinde sistem performansının kalitesini değerlendirmek için iç kontrol sistemi izlenmelidir. İzleme yetenekleri, rutin izleme faaliyetleri, özel değerlendirmeler veya her ikisinin bir kombinasyonu şeklinde olabilir. Devam eden iç kontrol izleme, bir kuruluşun normal ve yinelenen operasyonel faaliyetlerini içerir. Bu izleme faaliyetleri, düzenli idari ve izleme faaliyetlerini ve çalışanların

görevlerini yerine getirirken aldıkları diğer önlemleri içerir. Sürekli İzleme faaliyetleri, tüm kontrol unsurlarını kapsar ve uygun, etik, ekonomik, verimli veya etkili olmadığı düşünülen iç kontrol sistemlerine karşı alınan önlemleri ifade eder.

INTOSAI, tüm önemli ve güncel iç kontrol gelişmelerini dikkate alarak INTOSAI İç Kontrol Standartları Kılavuzunu güncellemeye karar vermiş ve bu kılavuzu COSO İç Kontrol – Bütünleşik Çerçeve raporuna entegre etmiştir. COSO raporuna göre bir iç kontrol sistemi, ancak bu sistemin beş bileşenini aynı anda içeriyorsa "etkili" olarak tanımlanabilir.

COSO Modelini ihtiva eden iç kontrol standartları, bu nedenle, COSO modelini bütünleştiren iç kontrol standartları, hükümetler tarafından kuruluşlarındaki güçlü iç kontrol yapılarının örnekleri olarak ve denetçilerin iç kontrolleri değerlendirmeleri için bir araç olarak kullanılabilir. Ancak, bu yönergelerin INTOSAI Denetim Standartlarını veya diğer ilgili denetim standartlarını tamamlaması amaçlanmamıştır.

2.3. İç Kontrol Modelleri

Bir kurumun iç kontrol yapısının yeterliliğini ve etkililiğini değerlendirmek için çeşitli modeller vardır. Bu iç kontrol modellerinden en önemlileri ABD'de COSO, Kanada'da COCO ve İngiltere'de Turnbull'dur. Bu modellerin yanı sıra uluslararası geçerliliği olan ISO standartları da bulunmaktadır.

Her modelin iç kontrol yapılarına ilişkin kendi bakış açısı vardır, ancak tüm modellerin ortak amacı, iç kontrollerin etkinliğinin değerlendirilmesinde bir kılavuz görevi görmesidir. Farklı ülkelerde geliştirilen her model, geliştirildiği ülkenin özelliklerinden etkilenmekle birlikte hepsinin ortak paydası vardır ve etkin bir şekilde uygulandığında kurumsal performans artışına önemli ölçüde katkı sağlar. Bu nedenle iç kontrol kavramı giderek daha fazla önem kazanmaktadır. Bilgi teknolojilerinin çeşitlenmesi, artan risk ve kurumsallaşma, artan bilgi ihtiyacı iç kontrol sistemlerine olan ihtiyacı artırmıştır.

Bu üç modeli genel hatlarıyla kısaca karşılaştırmak mümkündür. COSO modeli diğer modellere kıyasla daha kapsamlıdır. Ayrıca içinde bulunulan dönemin gerekliliklerine göre yenilenmektedir ve uygulama için yol gösterici olmaktadır. Bu artıları nedeniyle dünya genelinde en çok kabul görmüş iç kontrol modeli olarak karşımıza

çıkmaktadır. COCO modeli ile COSO modeli büyük ölçüde örtüşmektedir. Fakat COCO modeli etkisi yerel seviyede kalmış bir model olmuştur. Turnbull modeli ise bağımsız bir yönetim kurulunun varlığına ve iç kontrol çerçevesindeki etkinliğine dayanmaktadır. COSO gibi ayrıntılı ve kapsamlı bir uygulama kılavuzu yoktur, sadece ana çerçeveler belirtilmiştir. Bu şekilde değerlendirildiğinde, etkili bir iç kontrol yapısının nasıl olması gerektiğine dair bir gösterge yoktur.

2.3.1. COSO iç kontrol modeli

1980'lerin başındaki bir muhasebe skandalı nedeniyle, Hileli Mali Raporlama Komisyonu (genellikle Treadway Komisyonu olarak bilinir), bugün hala aktif olan COSO'yu kurmuştur (Karakaya, 2016).

COSO'nun orijinal tasarımında iç kontroller bir piramit şeklinde temsil edilmiş ve beş ana unsurdan oluşmuştur. İç kontrol bileşenleri işletme içerisinde tatmin edici bir iç kontrol yapısı sürdürülmesine olanak sağlar. Bunlar "Kontrol Ortamı", "Risklerin Değerlendirilmesi", "Kontrol Faaliyetleri", "Bilgi Paylaşımı ve İletişim" ve "İzleme" olmak üzere beş adettir (Moeller, 2014).

Yenilenmiş COSO iç kontrol yapısı üç boyutlu bir küp olarak temsil edilir. Bu boyutlar "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 üç boyutlu organizasyon yapısı, şirketin genel organizasyon yapısını, alt bölümlerini, varsa yan kuruluşlarını ve ayrıntılı fonksiyonlarını içerir. Her iş fonksiyonu için oluşturulan kontrollerin tüm organizasyon için oluşturulan kontrollerle tutarlı olması gerektiğinin vurgulanması önemlidir.

Kontrol Ortamı

> Kontrol ortamı, iç kontrol yapısını, yönetişim ilkelerini, şirketin organizasyon yapısını, yetki ve sorumluluk dağılımında izlenen prosedürleri, yönetimin ve çalışanlarının personel politikalarına ilişkin davranış ve tutumlarını içerir
>
> COSO modelinde kontrol ortamını oluşturan prensipler şu şekilde özetlenebilir (Moeller, 2011):

- Dürüstlük ve etik değerlere bağlılık
- Organizasyon yapısının, yetki ve sorumlulukların tanımlanması
- Yetkinlikleri olan çalışanları elde tutabilmek için insan kaynakları politikaları
- Kurum içi tüm çalışanlarıniç kontrolle ilgili sorumluluklarının bilincinde olması
- Yönetim kurulunun bağımsız gözetim fonksiyonunu yerine getirmesi

- Risklerin Değerlendirilmesi

  Risk yönetimi, kuruluşların amaç ve hedefleri doğrultusunda belirledikleri hedeflere ulaşmalarına yardımcı olan bir araçtır. Risk tanımlama ve değerlendirme, şirketin amaç ve hedeflerine ulaşmasını engelleyebilecek iç ve dış risklerin sistematik analizlerle değerlendirilmesi ve alınacak önlemlerin tanımlanmasıdır. (Maliye Bakanlığı, 2014).

  COSO modelinde risklerin değerlendirme ilkeleri şu şekilde özetlenebilir;

  - Kurumun hedeflerinin net olarak belirlenmiş olması,
  - Hedeflere etki edebilecek olası risklerin belirlenmesi,
  - Hileye yol açabilecek olası risklerin irdelenmesi,
  - Önemli değişimlerin belirlenmesi ve değerlendirilmesi.

- Kontrol Faaliyetleri

  Kontrol faaliyetleri, öngörülebilir risklerin etkilerini veya olasılığını azaltmayı amaçlayan, böylece şirketin amaç ve hedeflerine ulaşma olasılığını artıran faaliyetlerdir. Yönetim aksiyonlarının belirlenmesi, risk değerlendirmesinin tamamlanmasına bağlıdır. COSO modelinde kontrol faaliyetleriyle ilgili prensipler şu şekilde özetlenebilir;

  - Kontrol faaliyetlerinin tanımlanması ve uygulanmasına yönelik çalışmalar,
  - Genel bilgi sistemleri yönetimine dair kontrolleri tanımlanması ve uygulanması,
  - Kurum tarafından belirlenmiş prosedürler ve politikalar yoluyla kontrollerin desteklenmesi

Bilgi paylaşımı ve İletişim

İç kontrol yapısının önemli noktalarından olan bilgi ve iletişim, bir diğer dört unsur arasındaki ilişkiyi bilgi paylaşımı ve iletişim yoluyla sağlanmasına katkı verir. İşletme kurumsal hedef ve amaçlara ulaşma yolunda bilgi akışının düzenlenmesi iç kontrolün etkinliği ve uygulama kabiliyetinin artmasında önemli role sahiptir.

COSO modelinde bu prensiple ilgili olarak;

- Yüksek kaliteli verilerin toplanmasını, işlenmesini, aktarılmasını ve kullanılmasının sağlanması,
- Kuruluş içinde iç kontrol bilgilerinin paylaşılması,
- Kuruluş içinde paylaşılan bilgilerin dış paydaşlara iletilmesini sağlamak

- İzleme

İzleme, işletmenin faaliyetlerinin misyonunun, iş hedefleri ile uyumlu olup olmadığı, risk yönetimi politikası çerçevesinde gerekli kontrollerin sağlanıp sağlanmadığı, öngörülen kontrollerin uygulanıp uygulanmadığı, iletişimin açık ve yeterli olup olmadığı değerlendirilmektedir. (Maliye Bakanlığı, 2014)

COSO modeli izleme prensipleri incelendiğinde;

- Sürekliliği olan ve bir defaya mahsus inceleme faaliyetlerinin belirlenmesi ve uygulanması,
- İç kontrol eksikliklerinin değerlendirilmesi ve açıklanması

2.3.2. COCO iç kontrol modeli

COCO İç Kontrol Modeli, iç kontrol yapılarını değerlendirmek için Kanada Mali Müşavirler Odası tarafından geliştirilmiştir. COSO modeline göre daha anlaşılır ve pratik bir modeldir. Ancak etkisi yerel seviyede kalmıştır. COCO modelinde iç kontrol kavramı yerine kontrol kavramı kullanılmıştır.

COCO, kontrolü, örgütsel hedeflere ulaşmak için çalışanları destekleyen ve birbirine bağlayan kaynaklar, sistemler, süreçler, kurum kültürü, organizasyon yapısı ve görevler gibi herhangi bir organizasyonel unsur olarak tanımlar. (Root, 1998).

COSO ve COCO modelleri tamamlayıcı roller oynar. İki farklı modelin, COSO ve COCO'nun ortaya çıkması, aralarında önemli olmasa da metodolojik farklılıklar olduğunu gösterir. En temel fark, COCO modelinde işletme bünyesinde inşa edilen iç kontrol yapısının yapısal kontrol prosedürlerinden çok davranışsal değerlere dayalı olmasıdır. (CICA- The Certified Internal Controls Auditor, 1995).

COCO modeline göre iç kontrol, bir örgütün amaçlarına ulaşmasına yardımcı olan kaynaklar, sistemler, süreçler, kültür, örgütsel yapı ve görevler gibi bileşenlerden oluşur. COCO modeli, kontrol kılavuzları adı verilen dört ana grupta 20 alt ilkeye sahiptir. Dört ana bileşen "amaçlar", "sorumluluk", "yetkinlik", "izleme ve öğrenme" olarak belirtilmektedir (Özbek, 2012).

2.3.3. Turnbull modeli

Turnbull modeli beş ana bölümden oluşmaktadır. Bunlar "giriş", "etkin bir iç kontrol yapısını işletmek", "iç kontrollerin etkinliğini değerlendirmek", "iç kontrolle ilgili yönetim kurulu açıklamaları" ve "ilaveler" şeklinde sıralanmaktadır.

Turnbull modelinde etkin bir iç kontrol yapısının unsurları sıralanması aşağıdaki maddelerde yer almaktadır(The Financial Reporting Council, 2015):

- İç kontrol yapısı, bir işletmenin hedeflerine ulaşması için yönetmesi gereken risklerin belirlenmesinde önemli bir rol oynar.
- Bir şirketin varlıklarının korunmasını, iç ve dış raporlamanın güvenilirliğini, verimli ve etkin operasyonların devamını ve yasa ve yönetmeliklere uyumu teşvik eder.
- Düzenli muhasebe kayıtları ve etkili mali yönetim, iç kontrolün önemli parçalarıdır. Şirketinizin gereksiz riskler almadığı ve finansal raporlamanızın güvenilirliğini sağlar

- Bir şirketin ortamı, hedefleri ve iş süreçleri değiştikçe karşı karşıya olduğu riskler de değişir. İç kontrol yapısının etkinliği, sürekli değişen risklerin tanımlanmasına ve yönetilmesine imkan verecek nitelikte olmalıdır.

2.4. BT Kontrol Modelleri

2.4.1. COBIT

COBIT, açılımı ile Control Objectives for Information and Related Technology olarak adlandırılmaktadır. Sawyer's İç Denetçiler Rehberinde, Yöneticilerin, teknik detaylar, kontroller ve iş risklerini ilgilendiren konularda birbirleriyle bağlantı kurmasını sağlayan bir çerçeve çiziyor olmasında bahsedilmekle birlikte çerçevesinin detaylarına değinilmiştir. BT yönetiminin etkinliğini sağlayabilmek adına BT için olası faaliyetleri ve bunların risklerini kavrayabilmek için planlama, inşa etme, işletme ve izleme alanlarını sıralamıştır. Bu kapsamda;

Planlama ve Organizasyon; Çözüm ve hizmet sağlama için yönlendirme sağlanması

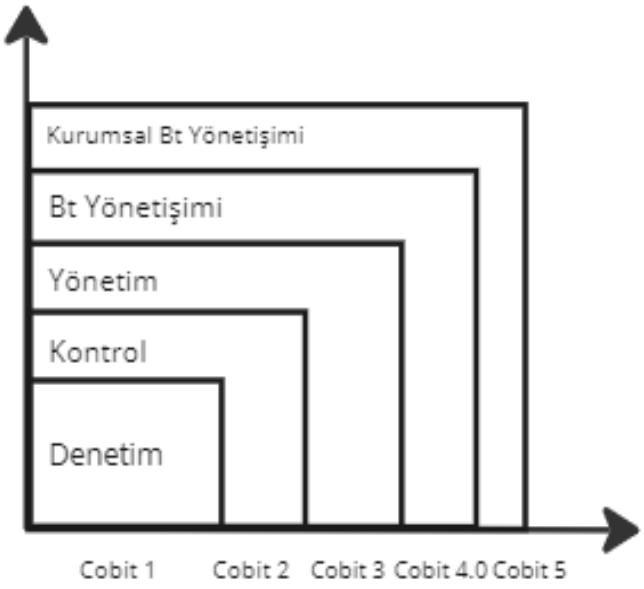
Tedarik ve Uygulama; Çözüm sağlayıp hizmet haline dönüştürülmesi

Teslimat ve Destek; Çözümlerin kabul edilerek son kullanıcılar için kullanılabilir hale getirmek

İzleme ve değerlendirme ise sağlanan yönlendirmelerin takip edilmesi süreçlerini kapsamaktadır.

COBIT BT alanında kontroller geliştirilmesi için açık ve net politikaların geliştirilmesini ve uygulanmasını sağlayarak, işletmelerin BT değerlerini arttırmaya yardımcı olurken uyumluluğu sağlamaktadır.

COBIT 1996 yılında ortaya çıkmış olmakla beraber gelişen teknoloji ile değişime uğramıştır. COBIT ortaya çıkış amacı, denetçilere profesyonel bir şekilde yol göstermek ve klavuzluk etmektir. Günümüzde BT yönetişimi de kapsamına alarak bütünsel bir şekil almıştır (Frelinger,2012).



Şekil 2. 1. COBIT Gelişim Aşamaları

Kaynak: Bob Frelinger(CGEIT), "Introducing COBIT 5"

COBIT 5'in çerçevesi temelde iç kontrol ve yönetişimin ve benzeri alanların kapsayan 5 maddeden oluşmaktadır Şekil 2.1. incelendiğinde; COBIT 1'de kapsam temel olarak denetimle sınırlıyken COBIT 2'de Kontrol kavramı geliştirildi. COBIT 3 ile beraber Yönetim kapsama dahil edildi. 2005 te yayımlanan COBIT 4 ile BT yönetişim ele alınırken COBIT 5'te Kurumsal BT yaklaşımı öne çıktı.

. COBIT 5 ilkeleri kapsamında BT' nin kurumsal yönetişimini, BT' den istenen katkıların alınmasına yönelik fayda sağlamayı hedeflemektedir (Tapia,2015).

5 temel prensip;

- Paydaş ihtiyaçlarının karşılanması,
- İşletmeyi kapsayıcı olması,
- Tek bir bütünleşik çerçeve oluşturulması,
- Bütünleşik bir yaklaşım sergilemek,
- Yönetişim ve yönetimin birbirinden ayrılması,

Yukarıda bahsedilen prensiplerden yola çıkarak COBIT'in sadece BT konusu olmaktan çıktığı tüm paydaş ve işletmeyi ilgilendiren bir çerçeve haline geldiğini

söyleyebiliriz. COBIT 5, diğer bölümlerde bahsedilecek Val IT ve Risk IT çerçevelerini bir araya getiren bir yaklaşım sergilemektedir. Bunlarla beraber ITIL ve ISO 27001 gibi standartlarla da temas halindedir.

2.4.2. Val IT

Val IT, BT kullanımına yoğun bir şekilde maruz kalan iş yatırımlarının yönetimine yönelik olan bir çerçeve sunar. Val IT varsayımları, BT yoğun ticari yatırımlardan oluşan dengeli bir portföyün maliyetlerini, risklerini ve etkilerini ele alır. Ayrıca kuruluşların değer yönetimi en iyi uygulamaları konusundaki deneyimlerini paylaşmalarını sağlamak için kıyaslama yetenekleri sağlar (TİDE, 2016). Val IT bilgi teknolojileri yatırımlarına değer yaratmak, iş süreçlerinin kalitesini yükseltmek ve risklerin detaylı şekilde ele alınmasına katkı sağlamaktadır.

2.4.3. Risk IT

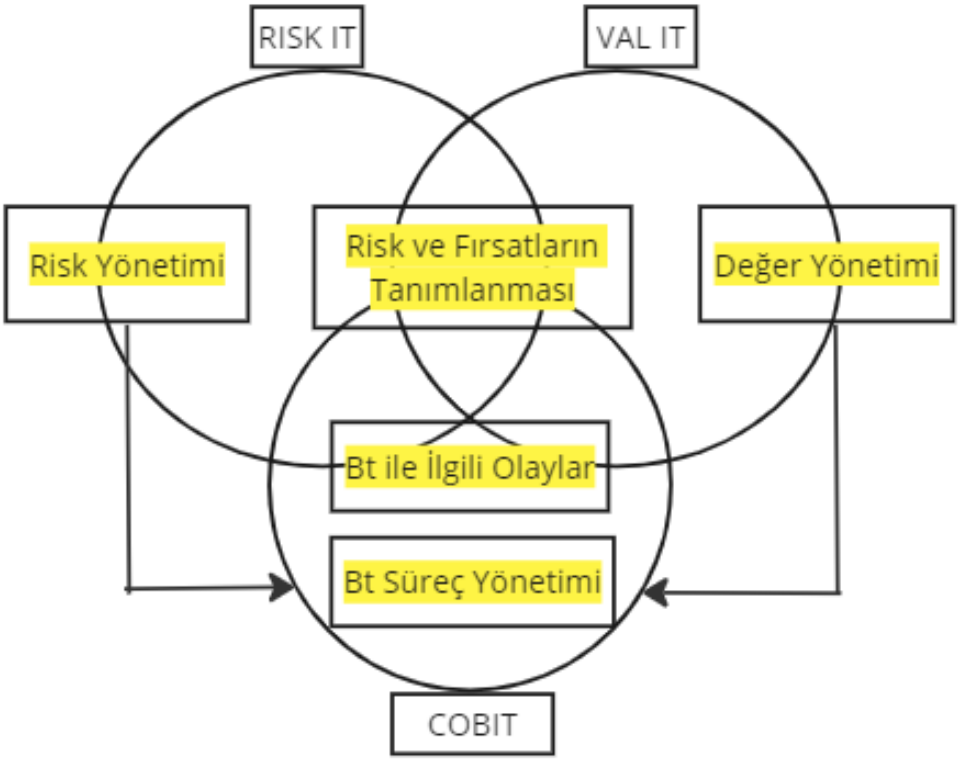
Risk IT bilgi teknolojileri alanında olası risklerin ele alınmasında ve etkin yönetilmesinde katkı sağlamaktadır. ISACA tarafında yayınlanan Risk IT Framework incelendiğinde Risk IT metodoljisi;

İşletme genelinde mevcut ve olası risklerin belirlenmesi

Olumsuz olaylara rağmen iş süreçlerinin devamlılığı için çalışmaların yapılması

BT ile ilgili risklerin azaltılması için uyum ve iç kontrol sistemlerinden faydalanılması şeklinde tanımlanmıştır. İşletmelerde riskler daha çok piyasa riski, operasyonel riskler olarak ele alınmakta BT kullanımıyla ilgili riskler gözden kaçırılmaktadır. BT riskleri iş kolları tarafında uzmanlara havale edilerek yönetilmeye çalışılmaktadır (TİDE, 2016).

Şekil 2.2.'de Risk IT, Val IT ve COBIT arasındaki ilişkiye yer verilmiştir.



Şekil 2. 2. Risk IT, Val IT ve COBIT Arasındaki İlişkiler

2.4.4. ISO 27001 Bilgi Güvenliği Yönetim Sistemi

Bilgi güvenliği, bilginin bütünlüğünden ödün vermeden, bilginin iletilmesi ve saklanması sırasında elektronik ortamdaki verileri yetkisiz erişime karşı koruyan güvenli bir bilgi işlem platformunun inşasıdır. (Canbek ve Sağıroğlu, 2006).

Bilgi güvenliği, iş sürekliliği, acil durumlarda kaybın minimize edilebilmesi için kaynakların gizliliği, ulaşılabilirliği ve bütünlüğünün korunmasını amaçlar (Çetinkaya, 2008).

ISO 27001'in bir sertifikasyon süreci olması durumunu dikkate alırsak işletmelerin bilgi güvenliği konusundaki yetkinleri hakkında bilgi verirken müşteri ve üçüncü taraflar için güvenilirlik sağlar. İşletmelere yasal düzenlemelere uyumluluk kapsamında destek

sağlar. İşletmelere sürekli iyileştirme yapmalarına teşvik sağlarken denetime hazırlıklı olmaları konusunda da yarar sağlayabilir.

Bir bilgi güvenliği standardı olarak ISO 27001 standardı, bilgi güvenliği yönetimini daha etkin hale getirmeyi amaçlar. Bu standardın amacı, bir bilgi güvenliği yönetim sisteminin kurulması, işlenmesi, izlenmesi, gerekli kontrollerin yapılması, iyileştirilmesi ve sürdürülmesi olarak tanımlanmaktadır. Bilgi güvenliği yönetim sistemi, bilginin erişebilirliği, gizliliği ve tamlığı sağlamak amacıyla sistemler ve kurallarla oluşturulmuş, planlanmış, yönetim tarafından kabul edilmiş uluslararası güvenlik standartlarına dayalı faaliyetlerdir (Ersoy,2012).

Gizlilik; Hassas bilgilerin erişimlerinin yetkisiz kişilerin eline geçmesinin engellenmesi, tamlık; bilginin bir kısmı ya da tamamının bütünlüğünün korunması, erişebilirlik ise bilgi veya bilgi sistemlerinin sürekli ulaşılabilir durumda olması halidir (Marttin ve Pehlivan, 2010).

Bilgi Güvenliği Yönetim Sisteminin işletmeler için katkısı büyüktür. Bunlardan bazıları;

- İşletmelere bilgi güvenliği politikaları oluşturmalarında ve yönetmelerinde
- Bilgiye yönelik varlıkların korunmasında
- Risklerin ve tehditlerin yönetilerek iş sürekliliği sağlanmasında
- Kurum itibarının arttırılmasında
- Olası bilgi güvenliği ihlal olaylarının etkin şekilde yönetilip zararları minimuma çekmeye katkı sağlayabilir.

2.4.5. ITIL (Information Technologies Infrastructure Library)

ITIL, Bilgi Teknolojileri Alt Yapı Kütüphanesi anlamına gelmekte olup COBIT ve ISO/IEC 27001 standartları gibi sadece bilgi güvenliği vermenin yanı sıra BT süreçleri ve operasyonların tam ve kesintisiz bir performansa sahip olmasın ve bunların kalitesi için belirli standartlar oluşturulmasına odaklanmaktadır (ClydeBank Technology, 2017). Başka bir deyişle, işletmelerin bilgi teknolojileri hizmetlerini tasarlama, yönetme ve sürekli iyileştirmeleri konusunda rehberlik sağlamaktadır.

ITIL bilgi teknolojileri hizmet yönetimi kapsamında hizmet kalitelerini iyileştirmek, süreçleri kolaylaştırmak ve müşteri memnuniyetlerine katkıda bulunduğu için kabul gören bir bilgi teknolojileri standardıdır.

ITILi COBIT, Risk IT ve ISO/IEC 27001 standardını ele aldığımızda etkin işleyen bir sistem oluşturmak için COBIT'in çerçevesinden faydalanılarak ITIL'ı hizmet kaliteleri konusuna uyarlayarak ISO/IEC 27001 standardını Bilgi güvenliği konusunda faaliyetlere ekleyerek ve Risk IT ile riskler göz önünde bulundurularak çalışma yapılması işletmeler için ideal bir yapı kurulmasına katkı sağlayabilecektir.

2.4.6. NIST SP 800-37

ABD'de Ulusal Standartlar ve Teknoloji Enstitüsü (The National Institute of Standarts and Technology, NIST) NIST SP 800-37 adıyla risk yönetim çerçevesi geliştirmiştir. Bu çerçevede bilişim güvenliği ve risk yönetim faaliyetleri üzerine birbirleriyle entegre süreç tasarlanmıştır. Bu süreç adımları;

Sınıflandırma; Bilgilerin sınıflandırılması, saklanması ve analizinin sistem taraflı iletilmesi

Seçim; Bilgi teknolojileri güvenliği için kontrol noktaları seçilip gerekli hallerde risk değerlendirmesi yaparak içinde bulunulan koşullara uyarlama

Uygulamaya almak; Güvenlik kontrollerini uygulamaya almak ve sistemlere yerleşmesi için tanımlamalar yapmak

Değerlendirmek; etkin olabilecek değerlendirme süreçlerinin kullanarak kontrolleri doğru bir şekilde uygulamaya almak, çalışmalarını ve sistem gerekliliklerine uygunluklarını kontrol ederek, çıktılarını değerlendirmek

Onaylamak; Bilgi teknolojileri kaynaklı işletmeye olası etkisi olabilecek risklerein belirlenmesi ve bu risklerin kabul edilebilir seviyelerde olduğunun onaylanması

İzleme; Kontrol etkinliğinin, tüm süreçlere ilişkin değişikliklerin dokümantasyonunun yapılması ve sonuçlara gören güvenlik etki analizlerinin yapılması, raporlanması, bilgi sistemi güvenlik kontrollerinin sürekli olarak izlenmesi şeklindedir.

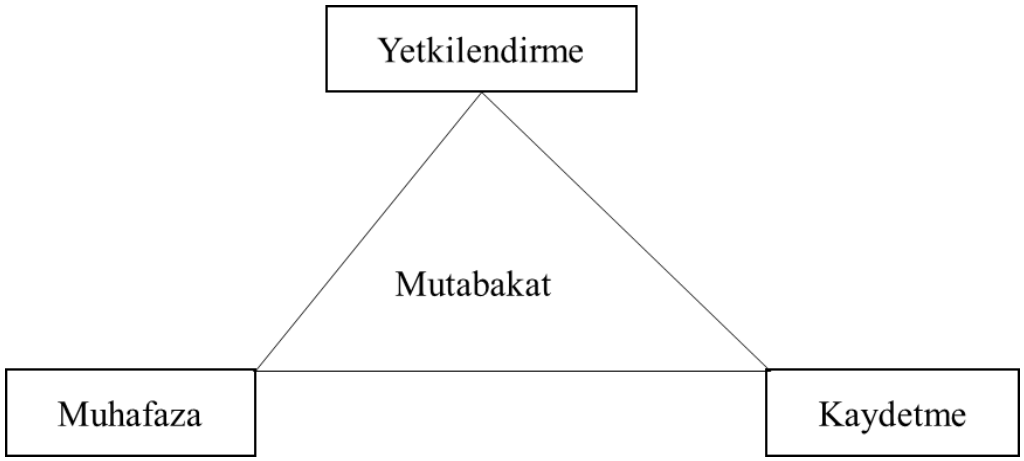
2.5. Görevler Ayrılığı İlkesi

Görevler ayrılığı ilkesi, bir kuruluş içinde farklı rol ve sorumlulukların tanımlanması ve bu rollerin farklı kişilere dağıtılması anlamına gelir. Kamu iç kontrol standartları tebliği çerçevesinde yer alan tanımı organizasyon içerisinde yer alan tüm seviye çalışanlara hata, eksiklik, usulsüzlük ve yolsuzluk risklerini minimize etmek için mali işlemlerin onaylanması, alınması, kaydedilmesi ve kontrolü sorumluluğunun paylaştırılmasıdır.

Organizasyon içerisinde iş süreçlerine ilişkin tüm adımların tek bir kişiye verilmesi hata, hile, yolsuzluk gibi riskleri arttırabilir. İşin kapsamı, niteliği göz önüne alınarak faaliyetlere ilişkin sorumlulukların birden fazla kişi arasında dağıtılması gereklidir (Bozkurt, 2000).

Görevler ayrılığı ilkesi iç kontrol sisteminin etkinliğinin ve güvenilirliğinin sağlanması için önemli bir kriterdir. Bir organizasyonda kişilerin rol ve sorumluluklarının belirlenmiş olmasıyla süreçlerin kontrollerinin tarafsız şekilde incelemesi gerçekleştirilerek çıkar çatışmalarından kaçınılabilir. Görevlerin ayrılmış ve belirlenmiş olması iş süreçlerinin daha verimli bir şekilde yürütülmesine olanak sağlayacaktır. Görevlerin ayrılması şeffaflık ve hesap verilebilirlik anlamında fayda sağlayacağı için yapılacak incelemeleri daha da kolaylaştıracaktır. İç ve dış paydaşlar açısında güven oluşturacağı gibi itibarı arttırıcı da etkisi olacağı söylenebilir. Tüm bunların yanı sıra yetki ve sorumlulukların ayrılmış olası kişiler arası iletişim kopukluğu ve yanlış anlaşılmalara sebep olabileceği ve iş süreçlerinde bilgi akışında problemlere neden olabileceği de düşünülebilir. Bu anlamda görev ve sorumluluklar belirlenirken iş akışlarının oluşturulması süreçlerin daha etkin ilerlemesine katkı sağlayabilir. Görev ve sorumlulukların ayrılmasıyla beraber ek personellere ve kaynaklara duyulan ihtiyaç artabilir. Bu durum katlanılması gereken maliyetlerin artmasına yol açabilecektir. Tüm bu yorumlar ışığında bir organizasyon içerisinde gerçekleştirilecek kontrollere bu detaylar ışığında yaklaşmak iç kontrol sistem etkinliğini sağlayabilecektir.

Görevler ayrılığı prensibi faaliyetlere ilişkin olarak Şekil 2.3.'de gösterilen muhafaza, yetkilendirme ve kaydetme fonksiyonlarının tek bir kişide toplanmasını önlemeyi de amaçlamaktadır (Louwers ve diğerleri, 2005).



Şekil 2. 3. Görevler Ayrılığı

Kaynak: Louwers,T.J. Ramsay R.J., Sinason, D.H., Strawser, J.R. Auditing&Assurance Services International Edition.

Görevlerin tek bir kişide toplanmaması gerekliliğine dair olarak; muhasebe süreçleri kapsamında düşündüğümüzde işlemlerin kaydedilmesinin ve onaylanmasının başka kişilere verilmesi kaydeden kişinin bilgilerin doğruluğu sağlarken, kayıtları onaylayan kişi bunların doğruluğunu kontrol eder ve onaylanmasını sağlar. İnsan kaynakları özelinde görevler ayrılığını tartışmak gerekirse işe alım yapan kişinin uygun personel seçimini yapması, alım onayını veren kişinin de sürecin doğru, adil ve prosedürlere uygun işlerliğini kontrol etmesin iş süreçlerinin ve iç kontrol süreçlerinin etkinliği ve güvenilirliği açısında önemi büyük olacaktır.

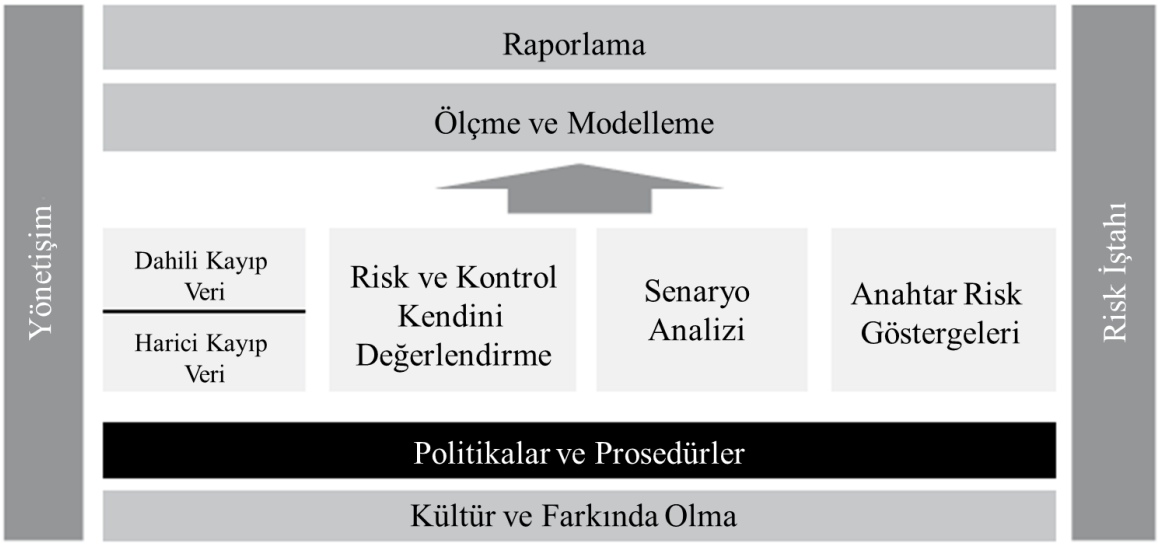
2.6. Politika ve Prosedürlerin Oluşturulması

Politika ve prosedürlerin oluşturulması 2013 yılında yayımlanan COSO İç Kontrol - Bütünleşik çerçeveye göre işletmelerin amaçlarına ulaşmasına destekleyici olunması için gereken yetkinliğe ilişkin beklentileri yansıtmasıdır. Prosedürler; dokümanlar, akış diyagramları, kontrol matrisleri gibi formatlarda olabilirler.

Politika ve prosedürler bir işletme için faaliyetlerinin standart hale gelmesini iş süreçlerinde uygulanacak adımların belirlenmesiyle tutarlı ve verimli işleyen bir sistem kurulmasını sağlar. Bunun yanı sıra işletmeler politika ve prosedürlerle beraber risklerin tanımlanıp yönetilmesine dair stratejiler belirler. İş sürekliliği politikası, acil durum politikası, iş süreçlerini içeren prosedürlerin oluşturulmasıyla beraber faaliyetlerin

standartlaştırılması sağlanırken iç kontrol açısından olası risklerin belirlenip değerlendirilerek kontrollerin güvenilir şekilde yürütülmesine olanak sağlar.

Girling (2022) politikalar ve prosedürlerin etkili bir risk yönetimi çerçevesinin sunulması için olmazsa olmaz bir bileşen olduğunu belirtmektedir ve kurguladıkları modelin diğer bileşenleri ile olan ilişkisini Şekil 2.4.'deki gibi göstermiştir.



Şekil 2. 4. Politikalar ve Prosedürler

Buna göre, politika ve prosedürlerin oluşturulması işletmelerin gereksinimlerini karşılamak için kural ve düzenlemeleri yorumlaması ve yazılı hale getirilmesidir. Özellikler son yıllarda finansal kuruluşların açıkça ifade edilmiş ve tutarlı bir şekilde yazılmış politika ve prosedürlere sahip olduğunu belirtmiştir. Özellikle FINTEK firmalarında üçüncü taraflarla yapılan sözleşmelere kapsamında bu belgelerin talep edilmesi politika ve prosedürlerin hazırlanması hususunu daha önemli kılmıştır. İyi bir şekilde çerçevesi belirlenmiş politika ve prosedürler performans ölçülmesinde objektif hedeflere sahip olunması gerekliliğini de ortaya çıkarmaktadır.

2.7. Risk

İç kontrol sisteminin tasarımında riskin farklı tanımlarının göz önünde bulundurulması ve benimsenen tanım üzerinden, yapılan işe ve bağlama özgü risk iştahının belirlenip buna göre riskin nasıl yönetileceğine karar verilmesi çok önemlidir. Bu nedenle bu bölümde risk tanımı, risk iştahı ve risk yönetimi başlıklarının detaylarına değinilecektir.

2.8. Risk Tanımı

Literatürün farklı risk tanımları bulunmaktadır. Sözlük anlamıyla risk, zarar, kayıp ve tehlikeli durumlara sebep olabilecek olayların ortaya çıkma olasılığıdır (Büyük Larausse, 1986). Uluslararası İç Denetçiler Enstitüsü (IIA)'ne göre risk "hedeflere ulaşılmasına etki edecek bir olayın meydana gelme olasılığı" şeklinde tanımlanmıştır. Başka bir tanıma göre risk, gelecekte ortaya çıkabilecek ve hedeflere ulaşılmasını engelleyebilecek tehditler veya hedeflere ulaşılmasını kolaylaştırabilecek fırsatlar olarak ifade edilmektedir. (Akçay, 2011). The Institute of Risk Management (IRM) riski, bir olayın olma olasılığı ve onun sonuçlarının kombinasyonu olarak tanımlamaktadır.

Her ne kadar riskin sözlük anlamı sonuçlar üzerinde olumsuz etki yaratabilecek olası olayları kapsasa da iç kontrol yazını kapsamında ele alındığında olumsuzluk vurgusunun olmadığı ve varılmak istenen hedeflere etki edebilecek olası tüm olayları kapsadığı görülmektedir. Daha geniş kapsamıyla riskin ele alındığı bu tanım olası bir olayın hedeflere olumlu yansımalarının da ele alınmasına alan yaratmakta ve risk olgusuna karşı farklı bir perspektif geliştirmeye yardımcı olmaktadır. Bu tez kapsamında da risk hedeflenen sonuçlara ulaşmada, sonuçlara etki edebilecek tüm olası olaylar şeklinde ele alınmaktadır.

Bu kapsamda risk tanımı doğrultusunda olası risklerin belirlenmesinde şirketlerin karar almada akılcı davranmaları, riskleri bilerek risk iştahlarını belirlemeleri risk yönetim etkinliğini arttıracağı söylenebilir.

2.9. Risk İştahı

Bir kuruluş, strateji ve hedefleri doğrultusunda üstlenmek istediği riskleri belirlemeli ve bu risklere karşı önlem alma ihtiyacını belirlemeden önce üstlenmek istediği risklerin boyutlarını belirlemelidir. Bunun için risk iştahının belirlenmesi, doğru bir şekilde analiz edilmesi ve aksiyon planının hazırlanması önem taşımaktadır.

Risk iştahı, bir organizasyonda kısa dönemde fırsat ve tehditleri içeren risklerin aktivitelerinin üstlenilmesi olarak tanımlanmaktadır. Risk iştahı risk yönetiminin uygulanmasında hayati derecede önem içermektedir. Bununla beraber tanımlanması ve

uygulanması zor bir süreçtir. Risk iştahı kavramının zorluklarından biri de risk iştahı için doğrudan bir risk belirlemekle beraber kuruluşların belli bir operasyonel sürece devam etmesi, bir projeye başlaması veya stratejiyi kabul etmesidir. Risk yönetim standartlarının çoğu risklerin kendi bağlamı içerisinde yönetilmesini söyler. Bir organizasyonda risk iştahı, strateji bağlamında, taktikler, operasyonlar ve uyum aktivitelerini içermelidir (Hopkin ve Thompson, 2022). Risk iştahı ile ilgili kararlar tek başına değil tüm iş birimlerini kapsayacak şekilde alınmalıdır. Bu doğrultuda bakıldığında riskler yönetilmesi zor süreçler olsa dahi tüm birimleri kapsayacak şekilde iş akışına etki etmeden risk iştahı bağlamı dikkate alınarak uygulanabilecek süreçlerdir.

Risk Appetite Guidance note HMG (2021)'e göre risk iştahı, bir kuruluşun faaliyet göstermeyi amaçladığı risk düzeyi Kurul veya yönetim tarafından kabul edilebilir risk olarak tanımlanmıştır.

Risk iştahına farklı bir açıdan yaklaşıldığında yönetim kurulunun almaya istekli olduğu risklerin kurumsal kaynaklarının toplam değeri olarak tanımlandığı görülmektedir (Bozkurt, 2010). Çoğu organizasyon risklerin gerçekte değerinin ne olduğunu ya da alınabilecek risk kapasitelerinin ne olduğunu saptayamayabilir. Risk kapasitesi tam olarak anlaşılmalı ve maksimum fayda ve en uygun seviyede risk belirlenmesi sağlanmalıdır. Maksimum fayda ve uygun seviyede riskler belirlenirken risk yönetiminde kullanılan riskten kaçınma, riski transfer etme gibi ilerleyen sayfalarda bahsi geçen risk yönetimi teknikleri risk iştahının yönetilmesine katkı sağlayacaktır.

Risk iştahı, riskten kaçınmanın tersi olarak ifade edilirken, risk iştahının artması riskten kaçınmanın azalması anlamına gelmektedir (Misina, 2006).

İşletmeler için risk iştahının belirlenmesi ve farklı seviyelerde uygulanması muhakeme gerektirir. Risk iştahını dikkate almak yönetim kurulu düzeyinde stratejik bir faktördür. Riskler farklı seviyelerde çalışan yöneticiler açısından risk iştahı politikalarına uyulması anlamında kısıtlayıcı olarak görülmesi muhtemeldir. Bireysel düzeyde risk iştahının dikkate alınması davranışı düzenleyici olması açısından da önemli olacaktır (Hopkin ve Thompson,2022).

Risk iştahının doğrudan gözlemlenebilir bir değer olmaması çeşitli modeller ortaya konularak sayısal verilere dönüştürülmesine sebep olmaktadır. Bunların sayısal verilere

dönüştürülebilmesi amacıyla çeşitli endeksler oluşturularak rasyonel olmayan davranışların açıklanması için yarar sağlanmaktadır (Çifçi ve Reis, 2020).

COSO'ya göre risk iştahı altı temel maddeyi içerir (Tysiac, 2020). Bu maddeler;

- Riskin ayrı bir çerçeve olmaması; Sadece bir faaliyet olmamaklar beraber örgütsel eylem ve iletişimin ayrılmayan bir parçasıdır.
- Risk iştahı ve toleransının aynı olmaması; Farklı fikirler olarak yer almaktadır.
- Risk iştahı, finansal hizmetler endüstrisinden daha fazlasını kapsar; Tüm örgüt performansının etkin yönetimi ve anlaşılması için önemlidir.
- Risk iştahı karar vermenin odağındadır; Kararların gerekliliğini belirlemede önemlidir.
- Risk iştahı bir ölçümden fazlasıdır; Geleceğe yönelik bir uygulamada gelecekteki eylem için strateji belirlenmesini sağlar
- Risk iştahı şeffaflığı arttırır; İşletmelerin katlanabileceği risklerin yanı sıra amaçlanan riskler için şeffaflık yaratır.

2.10. Risk Yönetim Süreci

Risk yönetimi, insanlık tarihi kadar eskiye dayanan bireylerin aile ve sahip olduğu varlıklara tehdit oluşturabilecek tehlikelerin değerlendirilmesi için çeşitli argümanlar geliştirmesini sağlayan çok yeni olmayan bir süreçtir. Modern risk yönetimi, eskiden gelen uygulamalar yeni bir perspektiften bakılmasını sağlamaktadır (Greene, 1997).

Akademik anlamda iş hayatına katkı sağlanması amacıyla risk yönetiminin gelişmesini sağlayacak modeller, yaklaşımlar ortaya atılmıştır (Dima ve Orzea, 2012). Risk yönetim çalışmasının ilki kabul edilebilecek çalışma 1963 yılında Mehr ve Hedges tarafından yayımlanmıştır. Çalışmada risk yönetim amacı organizasyonda üretim etkinliğinin üst seviyeye çıkarılması olduğu, risklerin basit bir şekilde sigortalanması yerine detaylı şekilde yönetilmesi gerekliliği savunulmuştur. 1970lerde Bretton Woods anlaşmasının süresinin dolmasıyla kur dalgalanmaları, petrol fiyatları ile faiz oranı artışları şirketler için finansal risklere yol açmış bu riskleri yönetmek için yeni yöntemler geliştirilmiştir (D'Arcy ve Brogan, 2001). 1980lerde riskler kredi riski, kayıp riski, piyasa risklerini içerirken 1990'larda şirketlerin maruz kaldıkları risklerin çoğalmasıyla beraber risk yönetimine ağırlık verilmeye başlanmıştır. 2000'lerde riskler tüm şirketlerde yaygın

olarak kullanılmaya başlanmıştır (Arslan, 2008). Risk kapsamının genişlemesi sonucunda kurumsal risk yönetimi kavramı ortaya atılmış ve şirket hedeflerine ulaşmak için makul güvence sağlayan, şirket risk iştahını kapsayacak şekilde yönetilmesine imkân sağlayan şirketi etkileyebilecek potansiyel olayları tanımlayan yönetim kurulu ve diğer çalışanlardan etkilenen bir süreç olarak geliştirilmiştir (COSO, 2004).

Yönetim, hedeflere ulaşmada karşılaşacakları sorunlarla baş edebilmek için bu sorunları bulmak, çözüm yollarına karar vermek zorunda kalmaktadır. Bu kararların akılcı kararlar olması gerektiği ve karar almanın geleceğe dair olması sebebiyle riskleri içerdiği ortadadır. Bu nedenle akılcı kararlar verilmelidir (Demir ve Gümüşoğlu,1988) . Karar verme sorunları çözmek ve fırsatları ortaya çıkarma sürecini içermektedir (Daft, 1991).

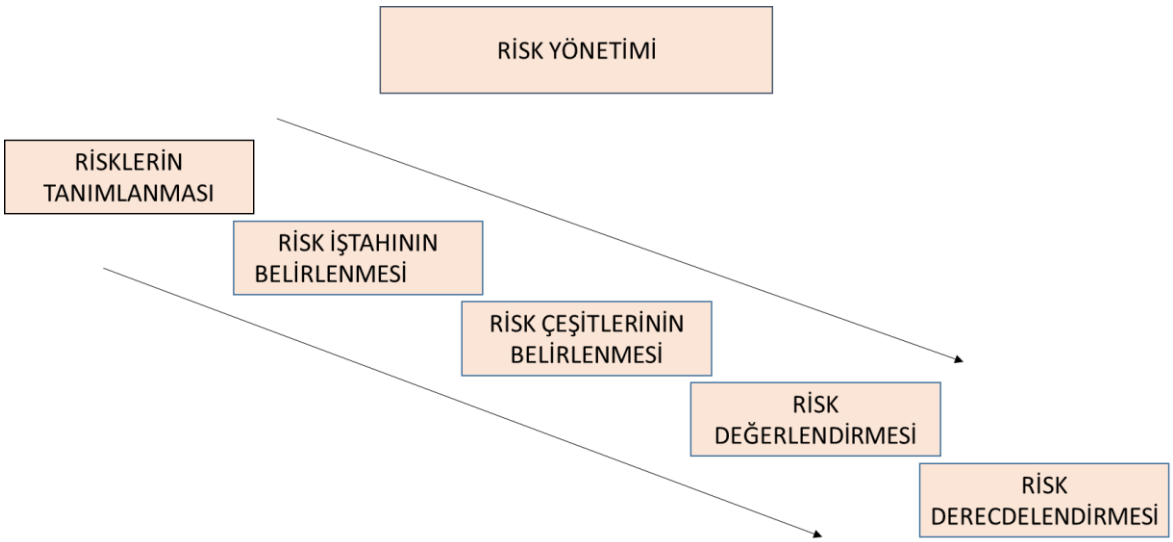
Şirketin hedeflerine ulaşabilmesi ve doğru kararlar alabilmesi için şirketin maruz kaldığı ve kalabileceği riskleri tespit etmek, değerlendirmek, analiz etmek ve son aşamalarda bu riskleri yönetmek zorundadır (Ionescu, 2007). Hem şirket içerisinde hem de departmanlar seviyesinde açık, anlaşılır ve tutarlı hedeflerin oluşturulması, risklerin tanımlanıp değerlendirilmesi için ön şarttır (Dinapoli, 2016). Riskler bir organizasyon içerisinde hedeflere ulaşmayı ve bu hedeflerin gerçekleştirilmesini olumsuz şekilde etkileyen tehditlerdir. Bu kavram çerçevesinde risk değişken bir tehdittir ve bu tehdit bir olay ile bağlantılı olarak gerçekleşir, olayın meydana gelmesi ise organizasyon hedeflerine ulaşılmasına engel olmaktadır (Griffiths, 2005). Bir olay sonucu olası ihtimalleri riskleri doğururken, bu oluşabilecek risklerin etkisini belirlemek ve bunlarla faaliyetlerin yürütülmesi konularından kararlar almak gereklidir.

Bir şirketin hedeflerine ulaşabilmesi ve doğru kararlar alabilmesi için içinde bulunduğu ve maruz kalabileceği risklerin tanımlanması, değerlendirilmesi, analiz edilmesi ve nihayetinde yönetilmesi gerekmektedir. Risk belirleme işletmelerde risk profilinin oluşturulması için önemlidir. Riskin ilk aşaması, şirketin ilk defa karşılaştığı riskler ile gelecekte ortaya çıkabilecek risklerin tespit edilmesidir. Riskin ikinci aşaması, işletme ile ilgili mevcut risklerin ortadan kalkması veya değişmesi veya çeşitli risklerin ortaya çıkmasıdır. (Treasury, 2004).

Risk yönetiminin doğru bir şekilde sürdürülmesi risk odaklı yaklaşım belirlenerek yapılacak olan kontrollerin daha verimli olmasını sağlayacaktır. İç denetçiler sadece kontrol faaliyetlerini denetlememekte, bunun yanı sıra riskleri tanımlayarak, işletmenin

risklerini sürekli izlemeyle, risk yönetim sürecini destekler (Lindow & Race, 2002). İç denetçiler için iç kontrolün standart bir hale getirilmesi amacıyla kontrol modelleri oluşturulmakta ve bu modellerden biri olan COSO İç Kontrol Modeli, işletme hedeflerine ulaşmak için yürütülen faaliyetlerin düzenli olarak kontrolünün yapılması, yöntem ve teknik geliştirilmesi, risklerin belirlenmesi şeklinde risklerin analizini, sınıflandırılmasını içeren bir modeldir. Başka bir yönetim modelini temsil eden ISO 31000:2018 standardı kapsamında şirketler, risk yönetimi süreçlerini genel yönetişim, strateji ve planlama, yönetim ve raporlama süreçleri ile organizasyonel politika ve değerlerle bütünleştiren sistemler geliştirmektedir. Bu standart her türlü riskin yönetilmesine yönelik şeffaf, güvenilir bir kapsamda ilke ve yönergeleri sağlamaktadır (Rubino, 2018). Risk yönetme süreçlerini geliştirmek ve kontrol faaliyetlerinin yürütülmesi, strateji ve planların gerçekleştirilmesi amacıyla çeşitli standartlar geliştirilerek bunlara katkıda bulunulmaktadır.

Risk yönetimi Şekil 2.5.'de yer gösterildiği haliyle değerlendirilip aşamalandırılabilir.



Şekil 2. 5. Risk Yönetim Süreci Modeli

Risk gelecekteki olası kayıplar olarak ele alındığında şirket için yapılacak planlamada SWOT analizi kullanılarak belirsizliklerin ve risk kaynaklarının belirlenmesi için faydalı olacaktır. Bu analizin organizasyonların zayıf yönlerinin saptanması ve olası tehlikelerin belirlemesine katkısı olabilecektir (Emhan, 2006) .

2.11. Risk çeşitleri

Finansal kuruluşlar da dahil olmak üzere tüm kurum ve kuruluşlar faaliyetlerini sürdürürken risklerle karşı karşıya kalmaktadır. Bu risklerin olumsuz etkileri ve bunları önlemek için önlemler alınmalıdır. Riskler sonucunda kuruluşların faaliyetlerinin geçici veya sürekli olarak durması söz konusu olabilir. Ayrıca bu risklerin çeşitli fırsatları doğurabileceği ve bu fırsatların sonuçlarının da iyi bir şekilde tespit edilmesi için risk çeşitlerinin belirlenip bunlarının sonuçlarının ne olacağının iyi bir şekilde analiz edilmesi önem taşımaktadır.

İşletmelerin karşılaştığı risklerin için farklı sınıflandırmalarla karşılaşılmaktadır. Şirketlerin maruz kaldığı finansal riskler, sistematik riskler ve sistematik olmayan riskler olarak iki gruba ayrılabilir.

Sistematik risk; ekonomik, politik ve sosyal çevre değişimleri doğrultusunda ortaya çıkan, korunması mümkün olan ama tamamen ortadan kaldırılamayan risktir (Mandacı, 2003). Sistematik riskler piyasayı ve piyasada işlem gören tüm finansal varlıkları etkiler. Şirketlerin riskli durumları tetikleyecek değişkenleri belirleyerek önlemler almaları gerekmektedir. Sistematik risklerin etkisini en aza indirgeyebilmek için şirketlerin akılcı stratejiler geliştirmesi gereklidir.

Sistematik olmayan riskler ise, işletmeyle veya toplu olarak işletmenin faaliyet alanlarıyla ilişkili olan endüstri riski, yönetim riski gibi risklerdir. Bu risklerin çoğu sektörel uzmanlaşma dışında, genel ekonomik bilgi ve piyasa deneyimine sahip tüm ekonomik birimlerde eş zamanlı olarak yöneticiler tarafından sistematik bir şekilde yönetilen risklerdir (Sayım ve Aydın, 2011).

Piyasaların hareketli olması, küreselleşme, işlem şekillerinin gelişmesi, bilgi teknolojilerinin gelişmesi beraberinde yeni risk çeşitlerinin ortaya çıkmasına sebep oldu. Sistematik ve sistematik olmayan risklere ilaveten işletmelerin karşı karşıya kalabileceği piyasa riski, operasyonel riskler, stratejik riskler, uygunluk ve yasal riskler, bilgi teknolojileri riskleri gibi çok çeşitli riskler şeklinde yeni sınıflandırmalara ihtiyaç duyuldu (Sakarya ve Kara, 2012). Bu risk çeşitlerine ilişkin olarak;

Piyasa riski; İşletmenin aldığı finansal pozisyonlar neticesinde oluşabilecek döviz kuru dalgalanmaları, faiz riski, likidite riski gibi riskleri içerir. Farklı bir deyişle içinde

bulunulan koşullar değiştiğinde finansal varlıkların, mali araçların pozisyon değerinin azalması riski olarak tanımlanabilmektedir (Alkin, 2001). Piyasa fiyatı dalgalanmaları veya fiyatlardaki karşı yönlü hareketlerden dolayı bir işletmenin karşı karşıya kalabileceği riskler olarak nitelendirilebilir. Piyasa riskinin unsurları; faiz riski, döviz kuru riski, likidite riski, piyasa oranlarına ilişkin risklerdir (Yüksel ve diğerleri, 2002).

Operasyonel Riskler; İşletme faaliyetlerinden kaynaklanan itibar kaybı ve maddi kayıplara yol açabilecek risklerdir. Çalışan kaynaklı hatalar, suiistimaller, etkin olmayan kontrol süreçleri ve teknolojik alt yapı ve sistemlerin varlığı sonucunda işletme faaliyetlerinin zarara uğraması riskidir. Operasyonel risk yönetimi pazar ve kredi riskinin içermeyen tüm riskler olarak nitelendirilirken Basel II düzenlemesiyle daha somut bir tanımlama getirildi (Girling, 2022). Bu tanımlamaya göre;

- Yetersiz veya başarısız iç süreçler insanlar, sistemler veya harici olaylardan kaynaklanan kayıp riski.
- Strateji ve itibar riski dışında kalan yasal risklerdir.

Operasyonel risklere ilişkin analizlerin yapılabilmesi için riski yaratan olay, olayın ortaya çıkış şekli ve karşılaşılabilecek kayıplara dair bilginin olması gereklidir. Operasyonel risklerin analizinin doğru şekilde yapılması ve değerlendirilmesi kuruluşu gereksiz operasyonel yükten koruyacaktır ve risklerden kaçınma fırsatı yaratacaktır.

Stratejik Riskler; İşletme hedeflerine ulaşmasını engelleyebilecek nitelikteki riskleri içermektedir. Bu riskler hisse değer kaybı, şirket başarısızlığı gibi yönetmesi güç risklerdir (Allan ve Davis, 2006). Stratejik riskler, şirket hedefleri doğrultusunda planlamanın kötü yürütülmesi, ekonomik ortam ve yasal düzenlemeler gibi değişikliklere uyum sağlanamamasında kaynaklanabilir. İşletmelerin yeni rakiplerinin teknoloji kullanımları, iş modelleri, yasal değişimler stratejik riskler üzerinde etkilidir. Üst yönetim ve Kurul'un stratejik olabilecek riskleri tanımlaması, izlemesi ve altında yatan nedenleri sürekli olarak gözden geçirmesi gereklidir (Frigo ve Anderson, 2011).

Kredi Riski; Sözleşme taraflarının yükümlülüklerini sözleşmeye uygun şekilde yerine getirmemesi riskidir. Karşı taraf riski olarak da nitelendirilmektedir (Principles for the Management of Credit Risk, 2000).

Uyum Riski; Finans kuruluşlarının ve bankaların tabii olduğu yasa ve düzenlemelere uyumluluğu zorunludur. Bu uyumun olmaması durumunda maruz kalınabilecek yaptırımlara uyum riskini oluşturur. Diğer bir deyişle uyum riski paydaşların beklentilerinin karşılanmasına odaklanır ve kuruluşa tahmil edilen çevresel kısıtlamalarla ilişkilidir (Ramakrishna, 2015).

Kuruluşlar mevcut yasalar ve düzenlemelerden oluşan bilgi havuzuna dayanan çerçevenin ötesinde, sayısız makam ve düzenleyici tarafından ortaya konan yasa ve düzenlemelerin üzerinden proaktif şekilde ilerleyecek bir mekanizma geliştirmelidir. Buna ek olarak bu mekanizmanın geliştirilmesinde sadece bilgi yeterli değildir. Bu bilgilerin yorumlanması ve anlamı değişebilir (Ramakrishna, 2015).

Uyum riskinin kuruluşların tabii olduğu yasa ve düzenlemelerde yer alan yaptırımlardan dolayı yüklü miktarda ceza alma, operasyonel kısıtlamalarla karşılaşma ve iş sürekliliği kapsamında kesintiye uğrama gibi sonuçları bulunmaktadır. Uyum risk analizlerinin doğru bir şekilde yapılması önemlidir. İlgili yasa ve düzenlemelere uyulmamasının çıktısı olarak itibar riski, finansal, operasyonel ve teknoloji riskleri maruz kalınabilecektir.

Bilgi Teknolojileri Riski; Bilgi teknolojileri riskleri ISACA tarafından yayımlanan The Risk IT Framework'e göre kuruluş hedeflerini etkileme potansiyeli yüksek, bilgi teknolojileri ile ilgili olayları ifade etmektedir. IIA tarafından geliştirilen GAIT metodolojisi de riskleri iş hedeflerine etkilerine göre değerlendirip sonuca ulaştırılması gerekliliğidir. Bilgi teknolojileri kapsamında belirlenen riskler sonucunda yazılım, donanım, veri güvenliği, uygulama kontrolü, idari kontrol gibi kontroller yapılabilir. Bilgi teknolojileri risklerinde yıl içinde meydana gelme olasılıkları, tehdidin değeri, potansiyel kayıplar, beklenen yıllık kayıplar önem taşımaktadır (Laudon ve diğerleri, 2022).

2.12. Risk Değerlendirme

Risk değerlendirmesi, şirketin hedeflerine ulaşmasını engelleyen ana risklerin belirlenmesine ve analiz edilmesine yardımcı olur (Moeller, 2014). Riskin ölçülebilmesi ve yönetilebilmesi için riske dair verilerin olması gereklidir. Bu verilerin risk değerlendirmenin bir parçası olması için de risk tanıma ve ölçmenin yapılması gereklidir.

Riskler işletmeyi tüm faaliyetleri kapsamında etkileyebileceği gibi belli projeleri ya da faaliyet alanlarında da etkileyebilir (Türedi ve Koban, 2016). Bu süreçte maruz kalınabilecek *riskin gerçekleşme olasılığının* belirlenmesi ve gerçekleştiğinde *etkisinin* neler olabileceğinin tespit edilmesi önemlidir. Yazında riskin gerçekleşme olasılığını *frekans* olarak ve etkisine de *büyüklük* olarak ele alan çalışmalar mevcuttur (Girling, 2022). Ancak bu tez kapsamında bu kavramlar olasılık ve etki olarak ele alınacaktır çünkü frekans kavramı kesinlikle olan olaylara atfen de kullanılabilen bir ölçü birimidir (Hopkin ve Thompson, 2022).

Risk değerlendirmenin bir şirketin faaliyetleri süresince yapılması ve süreklilik içermesi gerekir çünkü belirli bir zamanda yapılan risk değerlendirmesi, yapılan analizler ve atılan adımlar risk yapısını değiştirmektedir. Bu nedenle yazında farklı risk seviyelerinden bahsedilmektedir ve bu risk seviyelerini üç seviyede ele almak mümkündür (Hopkin ve Thompson, 2022). Bunların ilki riskin gerçekleşme ihtimalini ve etkisini değiştirebilecek herhangi bir faaliyet gerçekleştirilmediği durumları kapsayan *doğal risk* seviyesidir. İkincisi ise ilk kontrol ölçümlerinin yapılmasının hemen akabinde oluşan *mevcut (artık) risk* seviyesidir. Sonuncusu ise kontrol ölçümlerinin yapılması durumunda hedeflenen veya arzu edilen risk seviyesini kapsayan *hedef risk* seviyesidir.

Risk değerlendirmesinin sağlıklı yapılabilmesi için şirketin iç kontrol faaliyetlerinin risk odaklı olması ve şirket hedeflerinin açık ve anlaşılır olması gerekir. Hedefleri belirledikten sonra, iç ve dış riskleri tanımlamalı ve analiz etmeli, risk toleransını belirlemeli ve risklere nasıl tepki vereceğine karar verilmelidir. (Saltık, 2007). Bu çerçevede yapılması gereken ilk iş riskin etki ve olasılığını belirten ve bunu görsel olarak ortaya koyan risk matrisinin oluşturulmasıdır.

2.12.1. Risk Matrisi

Risk matrisi çok kullanılan bir yöntem olmakla birlikte ABD tarafında askeri bir standart olarak sistem güvenliğinin sağlanması için geliştirilmiştir (Aker ve Özçelik, 2020). Mevcut tehditlerin gerçekleşme olasılıkları ve bunların gerçekleşmesi halinde ortaya çıkabilecek kayıpların belirlenmesi ve katlanılabilecek risklerin ortaya konması bakımından risk matrisi kullanımı önemlidir. Bu aşamada süreç sahipleri ile görüşmeler, sistem kontrolleri, yasal incelemeler gibi yöntemler kullanılarak risk belirlenir. Yazında

risk matrisi oluşturulurken kullanılabilecek yaklaşımlara "risk değerlendirme yaklaşımları" bölümünde detaylı bir şekilde değinilecektir.

Riskin gerçekleşme olasılığını ve hedeflere etkisini değerlendirmeye yarayan risk matrisleri farklı formatlarda gösterilebilir. Aşağıda yer verilen Şekil 2.6.'daki risk matrisinde eksenlerden biri risklerin ortaya çıkma olasılığı diğer tarafı ise risklerin ortaya çıkmasıyla beraber oluşabilecek kayıpların büyüklüğü hakkında bilgi verir. Risk olasılığının en yüksek düzeyden en düşük düzeye kadar derecelendirilmesiyle bir çıktı elde edilir ve riskler değerlendirilir (Hopkin ve Thompson, 2022).

Şekil 2. 6. Risk Etki ve Olasılık

2.12.2. Risk Değerlendirme Yaklaşımları

Risk değerlendirmesinin nasıl gerçekleştirileceğini planlarken kullanılabilecek birçok yaklaşım vardır. Yazında kullanılacak olan yaklaşımlar '*yukarıdan-aşağıya'* ve *'aşağıdan-yukarıya'* olarak nitelendirilen türleri olacaktır (Grundke, 2008). Bu yaklaşımda risk değerlendirmesine katılacak çalışan veya paydaşların doğru bir şekilde belirlenmesi gerekir.

- *'Yukarıdan- aşağıya'* yaklaşımında sürece liderlik eden üst yönetim tarafından aşağıya doğru bilgi akışı sağlanır.
- *'Aşağıdan- yukarıya'* yaklaşımında üst yönetim dışında kalan çalışanların katılımı ile bilgi akışı sağlanır.

Yukarıda yer verilen iki maddede belirtilen yaklaşımların avantaj ve dezavantajları bulunmaktadır. Örneğin; Üst Yönetimde bulunan bir kişinin yaklaşımı daha çok dışsal

riskleri dikkate alarak daha genel bir çerçeve çizebilecek durumda olacakken diğer kadrolarda çalışan kişiler dışsal riskler konusuna daha az odaklanabilecektir. Bir bilgi teknolojileri yöneticisi işlerin hızlı ilerleyebilmesi için çeşitli uygulama veya sistemleri almanın faydalı olacağını düşünüp yasal riskleri üzerinde herhangi bir risk belirlemeyebilir. Aynı konu için yasal düzenlemelere hakim olan bir Uyum ekibi yöneticisi bu durumun risklerini belirleyip bir analiz ortaya koyabilir. Oluşturulacak risk değerlendirme gruplarında bu tip bir farklı bakış açıları olası risklerin ortaya çıkarılması durumunu üst seviyelere taşıyacaktır. Bu yaklaşımlardan birinin ya da her ikisi birden seçilerek risk değerlendirme yaklaşım grupları kurularak olası riskler belirlenebilir. Aşağıda yer alan Tablo 2.1. ve Tablo 2.2.' de yaklaşımlarda olabilecek avantaj ve dezavantajlara yer verilmiştir.

Tablo 2. 1. Yukarında-Aşağıya Yaklaşımın Avantaj ve Dezavantajları

Yukarıdan- Aşağıya Yaklaşımı	
Avantajları	Dezavantajları
İşletmenin etkilebileceği risklere daha tepeden bir bakış açısıyla yaklaşım sağlanabilir	İşletmenin risklerinin dışsal risk odaklı olarak yönetilmeye çalışılmasına yol açabilir
Önemli ve stratejik riskler hızlı bir şekilde belirlenip yönetilebilir hale getirilebilir.	İçsel operasyonel işlere ve bağımlılıklara karşı sınırlı bir farkındalıkla hareket edilebilir.
Üst yönetimin riskler hakkında bilgi sahibi olması ve kabul etmesine etki eder	Risklerin yönetilmesinin sadece üst yönetim nezdinde olacağı fikri ortaya çıkabilir
Üst yönetimin katılımı olduğu için tüm organizasyonda stratejiler kabul edilebilir	Operasyonlardan doğan yeni riskler tam anlamıyla tanımlanamayabilir

Tablo 2. 2. Aşağıdan-Yukarıya Yaklaşımın Avantaj ve Dezavantajları

Aşağıdan-Yukarıya Yaklaşımı	
Avantajları	Dezavantajları
İşletmede her seviyede gerçekleşmesi sağlanır	Dışsal veya stratejik risklere daha az odaklanılabilir
Mevcut risklerin etkileri grafik gibi gösterimler dışında da görünür hale gelerek bilgi sahibi olunur	Zaman alıcı ve uzun süreli geliştirilmeye açık olduğu için motivasyon düşürücü etkisi olabilir
Yapılan operasyonel işin riskleri hakkında üst yönetime kıyasla daha çok bilgi sahibidirler	Operasyonel işler daha iyi bilindiği için bunların üzeri örtülmeye veya raporlanmamaya çalışılabilir

Kaynak: Grundke, P. (2008). Top-Down Versus Bottom-Up Approaches in Risk Management.

Risk değerlendirmesi yapılırken kullanılabilecek bu tip yaklaşımlarda üst yönetim ile beraber tüm seviye çalışanların katılımlarının olması risklerin belirlenmesini sağlamanın yanı sıra risk algısının artmasına ve tüm organizasyon içerisinde bir kültür haline gelmesine katkı sağlayabilecektir. Bununla beraber süreklilik gerektiren bir süreç olması çalışanların motivasyonunu kırabileceği gibi yeni risklere karşı körlük yaratabilecektir. Süreçlerin doğru ve sürekli bir şekilde yürütülmesi riskleri bilmek ve yönetebilmek adına önem taşımaktadır.

2.12.3. Risk Değerlendirme Teknikleri

Literatürde çok çeşitli risk değerlendirme teknikleri yer almakla beraber ISO/IEC 31010:2019: Risk Yönetimi –Risk Değerlendirme Teknikleri incelendiğinde risk değerlendirme grupları oluşturulduktan sonra bilgileri toplamak için tekniklerin seçilmesine karar verilmelidir. Bu tekniklerden başlıcaları (Hopkin ve Thompson, 2022);

- Soru listesi ve kontrol listesi hazırlanması,
- Atölye çalışmaları düzenlenmesi,
- Akış şemaları veya bağımlılık analizlerinin hazırlanması şeklinde olabilir.

Soru listesi ve kontrol listesi hazırlanması; Önemli olabilecek bilgileri toplamak için soru listesi ve kontrol listelerinin hazırlanması sistematik olmak açısından faydalı olacaktır.

Atölye çalışmaları düzenlenmesi; Hedefler, etkileri ve süreçlerin paylaşılıp tartışılması açısından düzenlenecek atölyeler fayda sağlayacaktır.

Akış şemaları veya bağımlılık analizlerinin hazırlanması; Kritik bileşenlerin tanımları yapılarak süreçlerin ve operasyonların analizinin doğru şekilde yapılmasına olanak sağlayacaktır.

Risk değerlendirme tekniklerinin doğru seçilmesi risk değerlendirme gruplarına zaman, performans ve takip konusunda sistematik bir akış sunabilecektir. İşletme içerisinde sektör, büyüklük, çalışan sayısı gibi veriler dikkate alınarak gruplar kurulması ve bunlar için doğru tekniklerin belirlenmesi etkin bir risk yönetimi için etkili olacaktır.

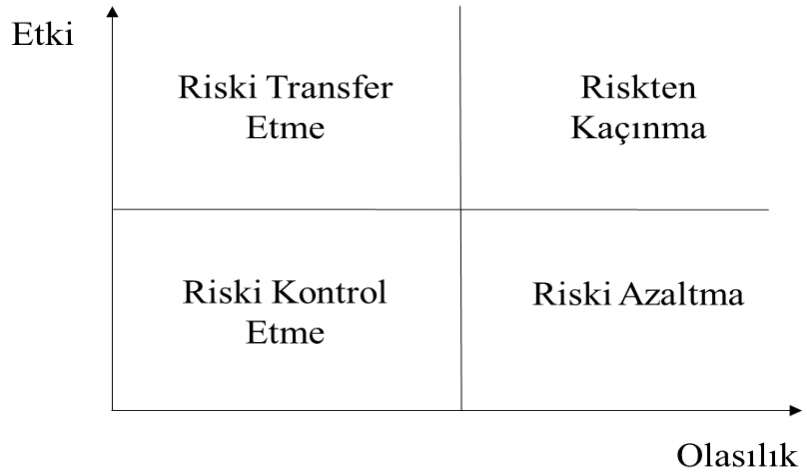
2.13. Risk Değerlendirme Sonrası Riske Cevap Verme Teknikler

İşletmenin amaçlarına ulaşmasında fırsat ve tehditleri belirlemek ve değerlendirmek, bunlar için alınacak önlemleri saptamak ve raporlamak için planlı, süreklilik gerektiren bir süreç kurgulanmalıdır. Bu süreçte risk iştahı belirlenerek risk değerlendirmelerinin doğru şekilde yapılmasıyla risk yönetimi gerçekleştirilebilir.

Risklerin önlenmesi veya azaltılması için çeşitli yöntemler kullanılmaktadır. Riskten kaçınma, riski kontrol altında tutma, riski transfer etme, riski azaltma olarak sınıflandırılabilir (Vaughan-Vaughan, 1995).

İşletmeler karşılaşabilecekleri risklerde riskten kaçınma ile politik istikrarsızlık bölgelerinde örneğin döviz kuru değişimi ile maddi kayba uğrama ihtimali yüksek ülkelerde faaliyet göstermeme ya da devam etmeme kararı alarak, riski transfer etme ile maddi zarara uğrama ihtimalini düşünerek sigorta yaptırılarak, risk azaltma yöntemi ile iç kontrol sistemini kurarak, riski kontrol altına almaya çalışarak riskleri yönetebilirler.

Aşağıda yer alan Şekil 2.7.'de Risk Etki ve Olasılığı gösterilen matris dikkate alınarak ' Düşük Etki, Yüksek Olasılık' olan bölgede riski transfer etme yöntemi, 'Yüksek Etki, Yüksek Olasılık' olan bölgede riskten kaçınma yöntemi, 'Düşük Etki, Düşük Olasılık' olan bölgede riski kontrol etme yöntemi, 'Yüksek Etki, Düşük Olasılık' olan bölgede ise riski azaltma yöntemi kullanılabilir



.

Şekil 2. 7. Risk Etki ve Olasılığına Cevap Verilmesi

ÜÇÜNCÜ BÖLÜM
3. MODEL ÖNERİSİ VE TARTIŞMA

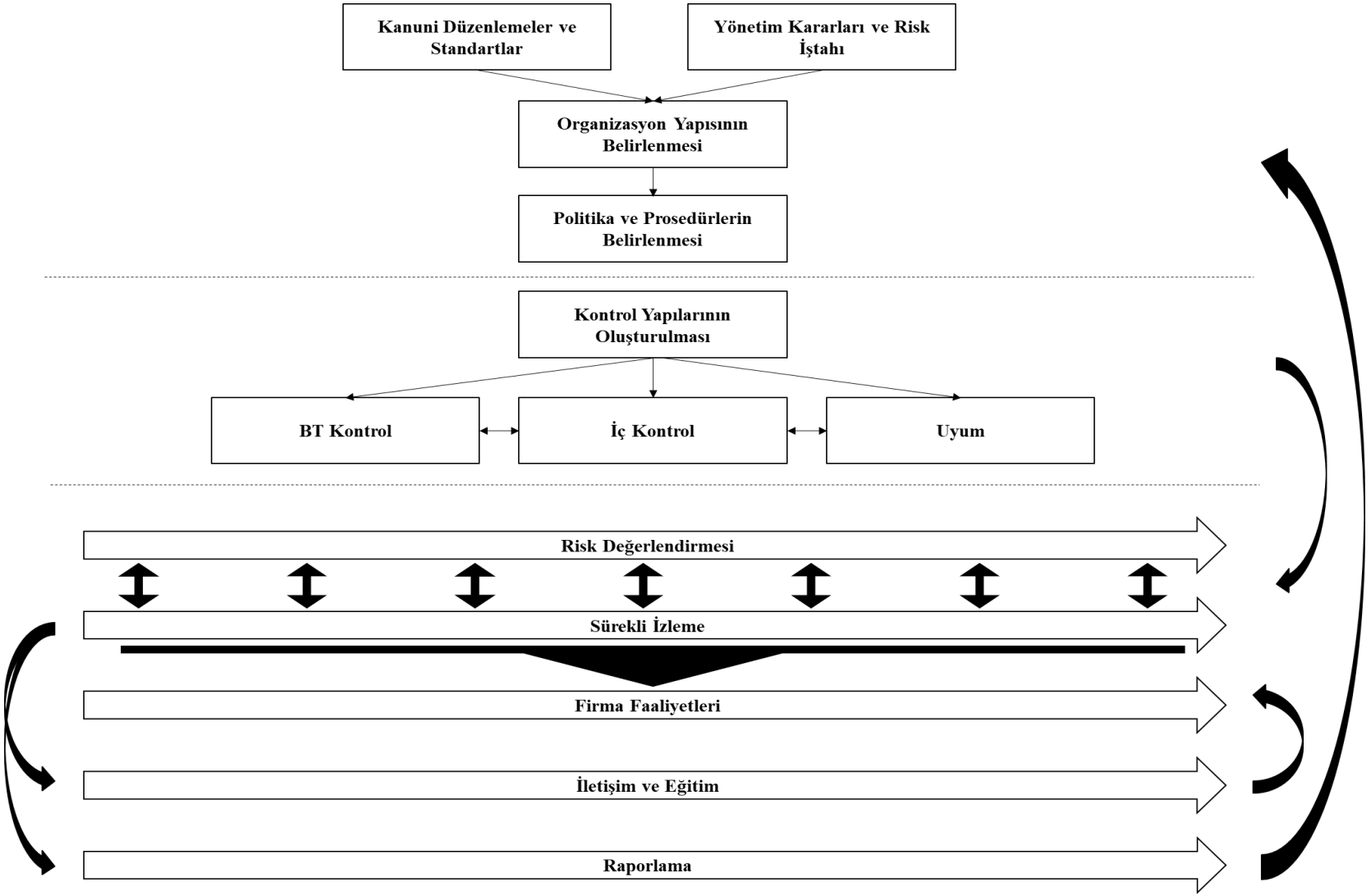
Finans endüstrisinde faaliyet gösteren ve teknoloji araçlarını da kullanarak müşterilerine hizmet sunan Fintek firmalarında etkin bir iç kontrol sisteminin kurulması elzemdir (Tepegöz, 2022). Bu Fintek firmaları arasında önemli bir yer tutan ödeme kuruluşları için de iç kontrol sisteminin kurulması gerekmektedir. Etkinliği yüksek bir iç kontrol sistemi; kullanılan teknolojilerin verimli kullanılması, uluslararası standart ve mevzuatlara uyumun sağlanarak kurumsal meşruiyetin sağlanması, hatalı uygulamaların ve kötüye kullanımların sıfıra yakın seviyelere indirilmesi ve dolayısıyla ödeme kuruluşlarının yaşamsal faaliyetlerini sürdürmesini sağlamaktadır. Buradan hareketle bu tez kapsamında ödeme kuruluşlarında kullanılacak etkin bir iç kontrol modeli geliştirilmiştir (Şekil 3.1.).

3.1. Kanun Düzenleme ve Standartlar

Fintek firmaları içerisinde yer alan Ödeme Hizmetleri ve Elektronik Para İhracı ve Ödeme Hizmeti sağlayıcıları ilgili kanunda (6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Kanunu) yer verildiği üzere A.Ş. olarak kurulması gereken şirketler olup bu şirket nev'i dolayısıyla birden fazla yasa ve bunlara bağlı olarak çıkarılan ikincil mevzuatın (Vergi Kanunu, Türk Ticaret Kanunu, Kişisel Verilerin Korunması Kanunu vb.) düzenlemelerine tabidir. Bu açıdan değerlendirildiğinde düzenlemelere uyum riski finans sektöründe yer alan diğer şirketlerde olduğu gibi daha büyük öneme haizdir.

Bu tez kapsamında değerlendirmede bu şirketlerin tabi olduğu yasal düzenlemelerden başlıcaları olan 6493 sayılı kanun ve 5549 sayılı Suç Gelirlerini Aklanmasının Önlenmesi Hakkında Kanun ile bunlara bağlı olarak çıkarılan ikincil mevzuata (yönetmelik, tebliğ genelge gibi) yer verilecektir. Bu iki kanun yanı sıra değinilecek olan ikincil mevzuatlar;

- Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik



Şekil 3. 1. İç Kontrol Sistem Model Önerisi

- Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ
- Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesi Kapsamında İşlemlerin Ertelenmesine Dair Yönetmelik
- Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine İlişkin Yükümlülüklere Uyum Programı Hakkında Yönetmelik
- Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik
- Terörizmin Finansmanının Önlenmesi Hakkında Kanunun Uygulanmasına ilişkin Usul ve Esaslar Hakkında Yönetmelik
- Terörün Finansmanına Yönelik Şüpheli İşlemlerin Bildirimi Genel Tebliği

27.06.2013 tarihinde Resmi Gazete'de yayımlanan 6493 sayılı kanun çerçevesinde ödeme hizmetlerine, ödeme kuruluşlarına ve elektronik para kuruluşlarına ilişkin usul ve esaslar belirlenmiştir. Bu kanun içeriği incelendiğinde 25.12.2007 tarihinde Avrupa Birliği içerisinde geçerli olan Payment Services Directive (PSD) ile uyum sağlamak amacıyla yürürlüğe girdiği ve ülke mevzuatımızda menkul kıymet mutabakat sistemi ve ödeme hizmet sağlayıcısı gibi terimlerin ilk defa tanımlandığı görülmüştür (Erdem, 2021).

6493 sayılı Kanunun yayımlanmasında sonra Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmelik ve Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ yürürlüğe girmiştir. 01.12.2021 tarihinde Resmi Gazete'de yayımlanan Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik ve Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ ile içerikte değişikliklere gidilmiştir.

6493 sayılı Kanun incelendiğinde faaliyet izni çerçevesinin, iptalinin ve sona ermesi durumlarının belirlendiği görülmektedir. Bu kapsamda örneklendirecek olursak faaliyet izin iptali gerekçelerine dair iznin alınmasında itibaren yetki kullanımına 1 yıl içerisinde başlanmaması, faaliyet izni çerçevesinde gerçeğe aykırı beyan ve belgelerinin verildiğinin tespiti edilmesi ve iznin iptaline yönelik olarak maddeler sıralanmıştır.

Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ bilgi sistemleri yönetimine ve bağımsız denetim firmaları tarafında denetlenmesine yönelik olarak ödeme hizmetleri alanında veri paylaşımı servislerine ilişkin usul ve esasları belirlemektedir. Kuruluş bu tebliğ çerçevesinde örnek teşkil edecek şekilde, ulusal ve uluslararası sertifikalara sahip gerçek veya tüzel kişiler tarafından olası iç ve dış tehdit senaryolarına göre yılda en az bir kez düzenli olarak sızma testleri yapmak zorundadır. Bunun yanı sıra aynı tebliğ kapsamında kuruluş yılda asgari bir defa olmak şartıyla bilgi sistemlerine ilişkin olarak kapsamlı risk değerlendirmesini yapıp her yıl Ocak ayı sonuna kadar Bankaya sunmakla yükümlüdür. Bilgi sistemlerinin yönetimine ilişkin olarak ilgili tebliğ maddeleri göz önünde bulundurularak risklerin belirlenmesi ve kuruluşun bu maddelerle uyumlu hale getirilmesi önem taşımaktadır.

Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ maddeleri dikkate alınarak oluşturulabilecek kontrol noktalarını içeren listeye Tablo 3.1'de yer verilmiştir.

Tablo 3. 1. Tebliğ Maddeleri Kapsamında Olası Kontrol Noktaları

Tebliğ Madde No	Tebliğ Kapsamında Olası Kontrol Noktaları	Kontrol Türü
4.3	*Bilgi Güvenliği Politikası *Temiz Masa Politikası Yönetim Kurulu Onayları	Önleyici
4.4	Organizasyon Şeması	Önleyici
4.5	BT Görev Sorumlulukları ve Onayları	Önleyici
4.5-19.7	Risk ve uyum ekibinin görev sorumluluk dokümanı	Önleyici
5.1 5.4	*Risk Yönetim Politika ve Prosedürü *Risk Değerlendirme Prosedürü *Risk Yönetim ve Uyum Bölümü Müdür ve Uzman Görev Tanımları *Risk Matrislerini İncelemesi	Önleyici
6.1	Dış Hizmet Alım Sözleşmeleri ve Şartlarının İncelenmesi (SLA süreleri vs.)	Tespit Edici
6.1	BTnin kurum içinde verdiği hizmet süreleri	Tespit Edici
6.3	Kapasite Yönetimine İlişkin Kanıtlar	Tespit Edici
6.4	BT varlık envanteri ve envanter kayıtlarının doğruluğunun incelenmesi	Tespit Edici
6.4	*Konfigürasyon Bilgileri *Konfigürasyon log kayıtları	Tespit Edici
6.6	Kapsam uygulamaları değişikliği canlı ortama taşıyan kullanıcıların listesi	Önleyici
7.1	*Olay ve Sorun Yönetim Prosedürü (Talep Sorun Şikayet Değerlendirme *Müşteri Şikayet Raporu	Tespit Edici
7.2	Olay yaşandıysa etkilenen müşterilere yapılan bilgilendirmeler	Yönlendirici
7.5	Siber Olaylara Müdahale sürecinin yönetilmesine dair dokümanların incelemesi	Tespit Edici

Tebliğ Madde No	Tebliğ Kapsamında Olası Kontrol Noktaları	Kontrol Türü
7.6	Siber olaylara müdahale planı, test çalışması	Yönlendirici
8.5	Bilgi güvenliği olayları ve kayıtlarının tutulması	Tespit Edici
8.6	Bilgi varlıklarının sınıflandırılması ve Yönetim Kurulu onayı (Veri Prosedürü)	Tespit Edici
8.6	Varlık sınıflandırma prosedürünün tüm personele iletilmesi ve personellerin yükümlülüklerinin olduğuna dair bilgilendirmeler	Önleyici
8.6	İmha Prosedürü	Önleyici
8.8-10-11	İşe giriş çıkışı yapılan personellerin listesi ve giriş çıkış kayıtlarının incelemesi	Tespit Edici
8.9	Sistem Odası Ziyaretleri Tutanaklar	Tespit Edici
8.10	Birinci ve ikincil sistem ağ topolojisi	Önleyici
8.11	İç ağ segmentasyonu ve kritik ağ segmentlerine ilişkin bağlantılar, tespiti yapılan kritik ağların tespiti ve değerlendirilmesi	Önleyici
8.14	Ağ güvenlik yönetimine ilişkin prosedür	Önleyici
8.15	İç ağdan dış ağa trafik nasıl kontrol ediliyor/ Dış ağa gerçekleşen olağandışı uzun süreli oturumlar	Tespit Edici
8.18	BG eğitimlerinin atanması ve tamamlayanların listesi	Tespit Edici
8.22	Elektronik kanallar aracılığıyla sunulan hizmetlere ilişkin yazılım ve mobil uygulamaların bilgi güvenliğini tehlikeye atacak nitelikte olmaması için alınan tedbirler	Önleyici
8.23	Elektronik kanallardan sunulan hizmetlere ilişkin yazılım ve mobil uygulamaların bilgi güvenliğini tehlikeye atmaması için alınan tedbirler	Önleyici

Tebliğ Madde No	Tebliğ Kapsamında Olası Kontrol Noktaları	Kontrol Türü
8.26	Veri tabanı, uygulama seviyesi, ve işletim sistemi seviyesinde hazırlanmış görevler ayrılığı matrisi (SOD)	Önleyici
8.31	Giden posta için posta sunucusunda gönderen kimlik doğrulama teknolojisi	Tespit Edici
8.32	Harici cihazlara ve taşınabilir medyalara sahip olan personel listesi ve iş gereksinimleri	Önleyici
9.1	Veri güvenliği ve mahremiyeti sağlanmasına ilişkin prosedür ve dokümanlar (veri envanteri/sınıflandırması çalışmaları)	Önleyici
9.2	Veri gizliliğinin sağlanması dair alınan önlemler	Önleyici
9.3	Şirket bünyesinde müşterilere yönelik hassas verilerin ve müşteri bilgileri ile rekabete duyarlı verilerin şifreli olarak tutulduğuna dair ekran görüntüsü	Tespit Edici
9.5	*İmha edilen herhangi bir doküman cihaz vs var mı? Varsa nedir dokümanları *Yedekleme ve imha prosedürü *Verilerin saklanma süresi	Tespit Edici
10	*AD giriş çıkış log kayıtları *Domain/admin grupları kullanıcı listesi	Tespit Edici
10.1	Kimlik Yönetim Prosedürü	Önleyici
10.2	Kimlik doğrulama tekniklerine ilişkin yapılan risk değerlendirmesi incelemesi	Önleyici
10.4	*Şifre Politikası *Tek kullanımlık şifre konfigürasyon ayarı ve kod parçacığı	Önleyici
10.5	Kimlik doğrulama mekanizması bileşenlerinin üretiminden kullanıcıya ulaştırılmasına kadar olan süreçte kullanılan güvenlik önlemleri/ AD şifre parametreleri	Tespit Edici
10.6	Kimlik doğrulama için kullanılan verilerin(müşterinin bildiği unsur ve SMS OTPyi cep telefonu üzerinden alacak ise cep telefonu bilgisinin) veri tabanında şifreli saklandığına yönelik kanıt dokümanlar	Tespit Edici

Tebliğ Madde No	Tebliğ Kapsamında Olası Kontrol Noktaları	Kontrol Türü
10.19	Bilgi sistemleri kullanımında oturum güvenliği sağlayacak alınan tedbirler ve kimlik doğrulama sisteminin başından sonuna kadar doğru olmasını sağlayacak önlemler	Önleyici
10.21	Numara taşıma nedeniyle SIM kartını veya operatörünü değiştiren müşterilerin listesi	Önleyici
10.31	Kuruluş tarafından müşterinin aranması durumunda, numaranın başka bir numaraya yönlendirilmesi durumunda çağrının sonlandırılması	Tespit Edici
11.1	Erişim Yönetimine ilişkin prosedürler	Önleyici
11.2	Rol yetki matrislerinin incelemesi ve BT çalışanlarının yetkilerinini ilgili yıl içinde gözden geçirilmesini yapılma durumu	Tespit Edici
11.3	Görevler ayrılığı prensibinin uygulanamadığı durumlarda alınacak önlemleri içerir dokümanlar	Düzeltici
11.5	Uzun süre aktivite göstermeyen kullanıcıları tespit etmeye yönelik tanımlanmış kurallar, alertler ve var ise alınan aksiyonlar	Tespit Edici
11.6	Ayrıcalıklı yetki tanımlama süreci	Önleyici
11.7	Acil durum yetkilendirme log kayıtları	Önleyici
12	Test sunucuna, geliştirme sunucuna ve prod ortama erişebilen kullanıcı listesi	Tespit Edici
12.2	Yıl içerisinde meydana gelen güvenlik ihlalleri ve alınan aksiyonlar	Tespit Edici
12.3	Sızma test sonuçları	Düzeltici
12.5	Sızma test sonuçlarının takibi, durumu ve tedbirler	Tespit Edici
12.5	Zafiyet taraması sonucunda tespit edilen açıklıkların giderildiğine ilişkin kanıtlar(bununla ilgili örneklem seçilecektir)	Tespit Edici

Tebliğ Madde No	Tebliğ Kapsamında Olası Kontrol Noktaları	Kontrol Türü
12.7	Güvenlik ihlallerinin en az 10 sene boyunca saklanabildiğine ilişkin kanıtlar	Tespit Edici
13	Firewall tanımlı kuralları	Önleyici
13.4	Personelin kendi faaliyetlerine ilişkin denetim izlerine müdahalesinin engellendiğine ilişkin kanıt	Tespit Edici
13.5	Diğer kuruluşlar nezdinde yapılan sorgulamalara ilişkin log kayıtları	Tespit Edici
13.6	Denetim izlerinin yedeklendiği ortam üzerinden yapılan geri dönüş çalışmaları	Önleyici
13.7	Denetim izi kayıt sisteminin durması halinde tanımlanmış kural	Önleyici
13.8	Denetim izi kayıt sistem durması durumunda log üreten sistem üzerinde herhangi bir işlem yapılamayacağına dair tanımlanmış kuralların incelemesi	Önleyici
14.1	Bilgi sistemleri süreklilik planı ve iş süreklilik planı incelemesi	Önleyici
14.3	İş etki analizlerinin yapılması ve bunların incelenmesi	Düzeltici
14.4	İkincil merkezden birincil merkeze geri dönüşe yönelik prosedürel dokümanlar	Önleyici
14.5	Bilgi sistemleri süreklilik planı test çalışması, raporu, katılımcılar Test faaliyetlerinin yapıldığına dair kanıtlar	Tespit Edici
15.1	İkincil merkez için yapılmış test çalışmaları ve sonuçları içerir rapor	Tespit Edici
15.2	Acil ve beklenmedik durum planı incelemesi	Önleyici
15.3	Birincil merkezde kesinti olması durumunda ikincil merkezde görev alacak personelin görev ve sorumluluk dokümanı	Önleyici
16.2	Dış hizmet alımına yönelik yapılmış risk ve değerlendirme çalışmaslarını içerir dokümanlar	Önleyici

Tebliğ Madde No	Tebliğ Kapsamında Olası Kontrol Noktaları	Kontrol Türü
16.3	Dış hizmet alınan firma listesi ve sözleşmeleri	Tespit Edici
16.5	Dış hizmet sağlayıcılarına verilen erişim hakları için yapılan risk değerlendirme çalışması	Önleyici
16.7	Alınan bulut bilişim hizmetleri	Önleyici
16.10	Reklam hizmeti almak için arama motorları, sosyal medya platformları vb. Sağlayıcıların listesi ve sağlayıcılarla yapılan anlaşmalar	Önleyici
17.3	Müşterilere ödeme hizmetinde 2 saatten ve daha uzun süreli bir kesinti oldu ise yapılan bilgilendirmeler	Tespit Edici
18.1	Kullanılan elektronik sertifikalar	Önleyici
19.1	Yüksek riskli işlemlerin takibi için oluşturulmuş dokümanlar Takip mekanizmaları	Önleyici
19.2	Yüksek riskli işlemlerin takibi için yazılmış kurallar listesi(senaryolar beklenmektedir)	Önleyici
19.4	Düşük değerli olan ödeme işlemlerinin kısa süre içerisinde tekrarlanması durumunda yazılmış kural ve bunun takibi	Önleyici
19.5	Yüksek riskli işlem gerçekleştiren müşterilere uygulanan ek takip mekanizmaları	Önleyici
19.6	Sağlanan hizmetlerin yasa dışı kumar da dahil olmak üzere yasa dışı işlemler için kullanılıp kullanılmadığını belirlemek için sosyal medya ve çevrimiçi platformların araştırılması	Önleyici
20.4	5549 Kanun kapsamında alınması gereken önlemler ile dolandırıcılık, sahtekarlık yöntemleri hakkında Temsilcilere verilen eğitimler	Tespit Edici

6493 sayılı Kanunun yayımlanmasında sonra Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmelik açısında örnekler yer verecek olursak kuruluş ödeme hizmetlerini elektronik ve fiziki kanallar üzerinden temsilci aracılığıyla yönetilmesine dair olan madde 18'de temsilcilerin sağlaması gereken şartlar, temsilci sayısı artışı ile beraber özkaynak artışı yapması gerekliliğine dair bilgiler ve temsilcilerden kaynaklı kuruluş yükümlülüklerini içeren bent ve fıkralar yer almaktadır. İlgili yönetmelik kapsamında tez içinde verilebilecek örnekleri çoğaltmak mümkündür.

5549 sayılı Kanun kapsamında suç gelirlerini aklanması ve önlenmesine yönelik usul ve esaslar belirlenmiştir. Bu usul ve esaslar kapsamında yükümlülüklerden bazıları;

- Müşteri Tanınması (Kimlik tespit yükümlülüğü)
- Şüpheli İşlem Bildirimlerinin Yapılması
- Uyum Görevlisinin Ataması
- Bilgi, Belge Verme Yükümlülüğü
- Muhafaza ve İbraz Yükümlülüğü
- Devamlı Bilgi Verme
- Elektronik Tebligat

Suç gelirlerinin aklanması bağlamında kara para aklamanın anlamı dikkate alındığında, yasa dışı yollarla elde edilen kazançların meşru olduğunu gizleyerek veya meşru gibi görünerek ekonomik sisteme sızmasını ifade eder (MASAK,2015). Aklama suçunda bahsedebilmek için bir suç işlenmiş olması, suç sonucu ekonomik değer elde edilmesi ve ekonomik değere yasal görünüm kazandırmak amacıyla bir fiilin işlenmesi gereklidir (MASAK,2016).

5549 sayılı kanun yükümlülükleri kapsamında yükümlülerin yapması gerekenlere birkaç örnekle detaylandıracak olursak 3.maddede müşterinin tanınmasına ilişkin esaslar göz önünde bulundurulduğunda kendileri nezdinde veya aracı oldukları işlemler için işlem yapılmadan önce işlem yapan ve işlem yapılanların kimliklerini tespit etme ve tedbirleri almakla yükümlüdür.4.madde kapsamında şüpheli işlem bildirimlerine dair denetim ile görevli elemanlar ile yargı sırasında mahkemeler dışında işlem tarafları da dahil olmak üzere hiç kimseye açıklamama yükümlülükleri mevcuttur.

Tedbirler Yönetmeliğinin 3. Fıkrası h bendinde gerçek faydalanıcı; bir işlemin tamamlanmasını sağlayan, onlar adına işlem yürüten veya tüzel kişiliği olmayan bir kuruluşu nihai olarak kontrol eden veya etkileyen kişi veya kişiler olarak tanımlanır. Bu kapsamda ödeme kuruluşlarının aracılığıyla gerçekleştirilen işlemlerde gerçek faydalanıcının belirlenip belirlenmesine yönelik tedbirlerin alınması bu işlemler sonucunda gerçek faydalanıcının gizlenmesi durumlarından şüphelenilmesi hallerinde ise gerekli bildirimlerin yapılması gerekmektedir. Ödeme hizmetleri ve elektronik para hizmetleri kapsamında tabii olunan kanun ve ikincil mevzuatlar ele alındığından örnekleri çoğaltmak mümkündür. Kanuni düzenlemeler dikkate alınarak yönetim tarafında risk iştahının oluşturulması, bu riskler sonucunda oluşturulacak politika ve prosedürlerin içeriğinin oluşturulması ve organizasyonel süreçlerin oluşturulması etkin kontrol mekanizmalarının oluşturulmasında katkısı olacaktır. Kanun yükümlülükler dışında ISO 27001 Bilgi Güvenliği yönetim standardı, ISO 31000 Risk Yönetim Sistemi Standardı, ISO 22301 Toplumsal Güvenlik ve İş Sürekliliği Yönetim Sistemi standardı gibi standartlar göz önünde bulundurularak sistemlerin oluşturulması kuruluşun ulusal ve uluslararası anlamda prestijli olması, çalışanlara ve üçüncü taraflara güven vermesi açısında katkı sağlayacaktır. Bunun yanında bu standartlara ulaşabilmek için kuruluşun sağlaması gerek temel şartlara uyumluluk anlamında süreçlerde iyileştirmeler yapılacağı ve işleyişin daha standart hale gelmesinden kaynaklı olarak çalışanlar ve kontroller açısından daha etkin işleyen bir yapının kurulmuş olacağı söylenebilir.

3.2. Yönetim Kararları ve Risk İştahının Belirlenmesi

Karar almak ve vermek kişiler, işletmeler ve örgütlerin hayatlarını sürdürebilmek için ve faaliyetlerine devam edebilmek için önemli unsurlar içerisinde yer almaktadır. İşletmelerde yönetim sürecinin temeli olarak belirtilebilecek karar mekanizması yarar sağlamak ve süreçlerin etkinliği açısında önem arz etmektedir (Torunlar, 2018). Dessler (2004)'e göre karar verme, hedeflere ulaşmak için seçenekleri belirleme, geliştirme ve analiz etme ve en iyisin seçme olarak tanımlamaktadır. Bu doğrultuda bakıldığında karar verme için herhangi bir eylem gerçekleşmeden seçenekleri gözden geçirmek ve bunlar üzerinde risk, fayda maliyet gibi işletme için fayda sağlayacak analizleri yaparak karar alma sürecine başlanması olarak nitelendirilebilir. Karar vericilerin yönetici olduğunu dikkate alırsak kararların niteliği, etkisi ve sonuçlarının değişebileceğinin karar alma

süreçleri incelendiğinde bilginin kullanılarak analiz teknikleri ile ilerlemenin süreci iyi analiz etmenin önemli olduğu görülmektedir (Kıral, 2015).

Torunlar'a göre yönetimin doğru ve etkin işleyen kararlar alabilmesi için karar vereceği alanın bilgi ve belgelerle desteklenmesi yönetim karar süreçleri açısında önemli bir yöntemdir. Bu desteklenme yöntemi karar vermeyi olumlu açıdan etkilediği ve zaman bakımında kaybı önlediği ve bilgi/belge ile alınan kararları güçlendirdiğini belirtmiştir. Kuruluşlar anlamında yönetim kararlarının kanuni düzenlemeler, standartlar ve politika prosedürler kapsamında bilgi ve belgeye dayalı olarak alınması, olası risklerin bu kararlar alınırken dikkate alınması kuruluşların süreçlerinin iyileştirilmesine ve etkinliğin sağlanmasına katkı sağlayabilecektir. Bununla beraber yönetim kararları sonucunda belirlenecek olan risk iştahı dikkate alınarak kontrol yapılarının şekillenmesinde katkı sağlanacaktır. Şirketler hedefleri doğrultusunda kabul edecekleri ve kaçınabilecekleri riskleri belirlemeli ve bu risklere ne şekilde cevap verebileceklerini doğru bir şekilde analiz edebilmeleri gereklidir. Risk iştahının doğru şekilde belirlenmesi fırsat ve tehditleri içeren aktivitelerin de tanımlanmasını ortaya çıkarırken yönetime kararlarında yol gösterici olacaktır. Tüm bu kararların etkin bir şekilde alınması politika, prosedürlerin, organizasyon şemasının şekillenmesinde etkisi olacaktır. Bununla beraber etkin bir kontrol yapısının oluşturulmasına katkı sağlayacaktır.

3.3. Organizasyon Yapısının Belirlenmesi

Organizasyon yapısı, işletme hedeflerine ulaşılması için hangi işlerin kimler tarafında yapılacağını bunların hangi bölümlerde bir araya geleceğini ve bölümlerin hiyerarşi içerisindeki yerini belirleyen bir çerçeve çizmektedir (Akkoç ve Erdoğan, 2011). Kuruluş içerisinde üst yönetimden başlayarak kimin kime bağlı olarak çalışacağının ve görev tanımlarının belirlenmesi hedeflere ulaşılmasında etkin ve verimli bir yol izlemek için önemlidir. Bir işletme içerisinde belirlenen stratejilerin uygulanmasında yetki ve görevlerin bölümlendirilmesi, yetki ve görevler arasında koordinasyonun sağlanması ile kararların alınması organizasyon yapısının belirlenmesi ile sağlanır (Parthasarthy ve Sethi, 1992).

Etkin işleyen kontrol yapısının oluşturulmasında organizasyon yapısının belirlenmesi ve görevler ayrılığı ilkesine bağlı kalınarak bunların oluşturulmasının katkısı büyük

olacaktır. Pazarlama, İnsan Kaynakları, Satış, Operasyon gibi bölümlerin iş tanımlarının belirlenmesi, rol yetkilerinin ve onay yetkilerinin doğru bir şekilde tanımlanması ve bağlı olarak çalışılacak kişilerin netleştirilmesi bölümler arasında iletişimin doğru kurulmasına etki edecektir. Bununla beraber rol yetkilerinin ve onay yetkilerinin doğru belirlenmesi görev tanımlarının çerçevesinin çizilmesinde etkili olacaktır.

Birimler arasında görevler dağılımına ödeme kuruluşları açısından örnek verecek olursak Temsilci edinim sürecine ilişkin olarak satış birimi tarafında temsilci kazanımı kapsamında görüşmeler yapılarak gerekli dokümanların temininin sağlanması sonrasında temsilci kabulüne ilişkin gerekli incelemelerin gerçekleştirilmesi amacıyla uyum ekibi görüşüne sunulması ve uygun görülmesi halinde üst yönetimin onayına sunulması aşamaları tamamlanır. Bu aşamalardan sonra temsilciye tanımlanacak komisyon oranları, ekran tanımlamaları gibi operasyonel işler operasyon birimi tarafından gerçekleştirildikten sonra bu işlemlerin onaylarını verecek personelin onayına gönderilmesi ve gerekli kontroller sonucunda yetki dahilinde tamamlanması gereklidir. Tüm bu iş süreçleri dikkate alındığında görev tanımlarında ilgili personellerin iş süreçlerinin belirtilmesi, iş akış şemalarının oluşturulması iş süreçlerinin etkin ve verimli işlemesini yanı sıra birimler arası iletişimin sağlıklı olmasında etkili olacaktır. Tüm bu süreçlerin doğru şekilde tanımlanıp belirlenmesi kontrol yapılarının daha etkin işlemesine ve kontrol noktalarının doğru bir şekilde belirlenmesine katkı sağlayacaktır.

3.4. Politika ve Prosedürlerin Oluşturulması

Politika ve prosedürlerin belirlenmesi işletmelerin nihai hedeflerine ulaşmasında sahip olması gereken yetkinliklerin belirlenmesinde faaliyetlerinin standart hale gelmesinde ve iş süreçlerinde uygulanacak adımların belirlenmesinde etkili olacaktır. İş süreçlerinin yasal yükümlülükler dikkate alınarak politika ve prosedürlerde belirtilmesi tutarlı, verimli ve etkin işleyen kontrol yapılarının oluşturulmasına katkı sağlayacaktır. Bununla beraber işletmelerin politika ve prosedürlerle riskleri tanımlaması ve bunların yönetimine dair stratejiler belirlemesi kontrol mekanizmalarına fayda sağlayacaktır.

Girling'e göre politika ve prosedürler oluşturulurken işletme ihtiyaçları doğrultusunda kural ve düzenlemelere ilişkin yorumlamaların yapılması ve yazılı hale getirilmesi önem teşkil etmektedir. Ödeme hizmeti ve elektronik para ihracı ile ödeme

hizmeti sağlayıcılarını ilgilendiren kanuni düzenlemeler dikkate alındığında şirketin insan kaynakları politikasının, risk yönetimi politikasının, bilgi teknolojileri ve iç kontrol faaliyetlerine ilişkin politikalarının ve stratejilerinin yönetim kurulu tarafından belirlenmesi gerekmektedir. Bilgi teknolojileri kapsamında süreçlerin etkin ve iş sürekliliği açısından uyumlu şekilde devam edebilmesi adına "Temiz Ekran Temiz Masa Politikası", "Bilgi Güvenliği Politikası", "İş ve BT Sürekliliği Prosedürleri", "Varlık Sınıflandırma Prosedürü", "Acil Durum Planı Prosedürü", "Yedekleme ve İmha Prosedürü", "İşe Alım ve İşten Ayrılma Prosedürü", "Avans Prosedürü", "Risk Yönetim Politikası" gibi iç işleyişi detaylandıran işletmenin etkin ve verimli olması açısından önem teşkil edecek politika ve prosedürlerin belirlenmesi gerekmektedir. Bu politika ve prosedürler detaylandırılacak olursa;

- "Temiz Ekran Temiz Masa Politikası" kapsamında işletme çalışma alanlarında kullanımda olan bilgisayarlarda bulunan bilginin gizliliğinin, bütünlüğünün ve erişebilirliğin bozulmasına engel olabilecek durumların önüne geçebilmek adına kuralların yazılı olduğu tüm çalışanları kapsayacak prosedürlerin oluşturulması
- "Bilgi Güvenliği Politikası" kapsamında Bilgilerin işlenmesi, iletilmesi, depolanması ve yedeklenmesine yönelik olarak verilerin gizlilik, bütünlük ve erişebilirliğini sağlayacak önlemlerin alınmasına dair kural ve kontrollerin belirlenmesi,
- "İş ve BT Sürekliliği Prosedürleri" kapsamında deprem, yangın, sel, teknik hatalar, elektrik kesintisi gibi olası riskler göz önüne alınarak tehlike oluşturabilecek durumlarda yaşanabilecek aksaklıkların belirlenmesi ve bu aksaklıklara karşı alınabilecek önlemler ve süreklilik kapsamında iş etki analizlerinin yapılması ve ulaşılabilecek kişilerin belirlenmesinin yazılı hale getirilmesi,
- "Varlık Sınıflandırma Prosedürü" kapsamında Şirketin sahip olduğu elektronik dokümanların, veri tabanlarının ve belgelerin içeren varlıkların belli standartlar çerçevesinde tanımlanması ve uygun şekilde sınıflandırılmasını, değerlerinin belirlenerek etkilerinin belirlenmesi saklama ortamlarına ilişkin sürelerin, ortamların ve erişimlerin detaylandırıldığı bir prosedürün yazılı hale getirilmesi

- “Acil Durum Planı Prosedürü” kapsamında yangın, deprem, terör saldırısı, salgın hastalıklar gibi acil durumlar için plan hazırlanması ve bu gibi durumlarda alınacak aksiyonların tahliye, acil servis çağırılması, iletişim, ulaşım sağlanamaması halinde neler yapılacağı bilgisinin sağlanması ilkyardım ekibi, ulaştırma ve iletişim ekibi gibi kurulması gerekli ekiplerin oluşturulması ilgili personellerin belirlenmesi ve tüm çalışanların haberdar edilmesinin sağlanması için yazılı bir prosedür hazırlanması
- “Yedekleme ve İmha Prosedürü” kapsamında herhangi bir arıza veya kasıtlı şekilde oluşabilecek veri kaybı, tahribatı ve hizmet kesintilerinin önlenmesine yönelik olarak yedeklemelerin nasıl yapılacağı ve ihtiyaç doğrultusunda geri dönüşlerin gerçekleştirilmesi, imha sürelerin yasal yükümlülükler dikkate alınarak belirlenmesi ve yazılı hale getirilmesi
- “İşe Alım ve İşten Ayrılma Prosedürü” İş kanunu Hükümlerinin içeren işe alım ve işten ayrılma sürecini içeren mülakat, oryantasyon, deneme süreci, ihbar süresi gibi süreçleri içeren detayların yer aldığı personeli bilgilendirici kuralların yazılı hale getirilmesi
- “Avans Prosedürü” kapsamında avans kullanım şekillerini, miktarını, ödenme sürecini gösteren personeli bilgilendirici ve yasal yükümlülüklerle uyumlu kuralların yazılı hale getirilmesi
- “Risk Yönetim Politikası” kapsamında şirketin risk algısının tanımının yapılması, risk çeşitlerinin belirlenmesi, risk sorumlularının ve görevlerinin belirlenmesi ve konuyla ilgili yasal yükümlülükler kapsamında yazılı hale getirilmesi bakımında önemli olacaktır.

Yukarıda örneklerine yer verilen politika ve prosedürlerin ihtiyaçlar doğrultusunda birimler bazında çoğaltılabilmesi mümkündür. Bunların yasal yükümlülükler ve risklerinde ele alınarak hazırlanmasının, personelin süreçler hakkında bilinçlenmesinde, süreçlerin etkin ve verimli kullanılmasında etkili olacaktır.

Başka bir şekilde değerlendirecek olur politika ve prosedürler, çalışanların neler yapması gerekliliğini ve sorumluluklarını netleştirirken işletmenin beklenti ve hedefleri doğrultusunda standartların oluşmasını sağlar. Prosedürler doğrultusunda farklı birimlerdeki kişilerin çalışmaları kolaylaşırken iletişim daha etkili hale gelecektir. Bunların sürekli gözden geçirmelerle değişen koşullara, yasal yükümlülüklere uygun hale

getirilmesi rekabetçi ortamda şirket lehine hareket edilmesine sebep olabilecekken politika ve prosedürlerle iş süreçlerinde standartlaşma sağlanması kontrol yapılarında oluşturulacak süreçlerin ve risklerin belirlenmesinde etkili olacaktır.

3.5. Kontrol Yapılarının Oluşturulması

Kontroller, işletme faaliyetlerini düzenlemek, riskleri yönetmek, hedeflere ulaşmak ve kaynakları etkin bir şekilde kullanmak için önemli bir işleve sahiptir (Korkmaz, 2007). Kontroller, işletme içerisinde plan ve politikaların etkin bir şekilde uygulanmasını, kaynakların doğru ve verimli kullanılmasını, süreçlerin etkin işlemesi ve risklerin yönetilmesini sağlamayı amaçlamaktır. Kontrol ve risk değerlendirme birbirileriyle sıkı ilişki içerisindedirler. Kontroller işletmelerin belirlenmiş hedeflere ulaşması, işletme faaliyetlerinin verimli ve etkin olması için makul güvence sağlamaktadır. Risk değerlendirmede ise işletme hedeflerine ulaşılmasını engelleyebilecek risklerin belirlenmesi, analizi ve yönetilmesi önem taşımaktadır. İki süreç içerisinde de hedeflere ulaşılması için işletme menfaatleri ve işletme faaliyetlerinin sürdürülebilirliği önem taşımaktadır.

Ödeme kuruluşlarının tabii olduğu yasal düzenlemeler göz önüne alındığında *"6493 sayılı Kanunun yayımlanmasında sonra Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmelik"* 26. Maddede etkin ve yeterli bir iç kontrol sistemi kurulması zorunlu tutulmuştur.*"* *Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ"* kapsamında Yönetmelik 26.maddesine değinerek bilgi sistemleri yönetimine ilişkin olarak gerekli deneyim ve bilgi birikimine sahip bilgi teknolojileri kontrol faaliyetinin yürütülmesine yönelik personel istihdam edilmesi yükümlülüğü getirilmiştir. İlgili kanuni düzenlemeler dikkate alındığında Ödeme kuruluşları açısından bilgi teknolojileri kontrol sistemi ve iş süreçlerine yönelik kontrolleri gerçekleştirecek iç kontrol sistemi kurulması yükümlülükler arasındadır. Bunların yanı sıra MASAK kapsamında yapılması gereken kontroller ele alındığında "*Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine İlişkin Yükümlülüklere Uyum Programı Hakkında Yönetmelik*" 1.maddesinde suç gelirlerinin aklanmasının ve terörün finansmanının önlenmesi amacıyla yükümlülerin uyum programı oluşturmaları ve uyum görevlisi atamaları gereklidir. Bahsi geçen kanuni düzenlemelere

bakıldığında Ödeme kuruluşları içerisinde kontrol yapılarının oluşturulması yükümlülükler içerisindedir. Bu kontrol yapıları Bilgi Teknolojileri, İç Kontrol ve Uyum olarak üç bölüme ayırabiliriz. Bu yapılar kanuni düzenlemelerin olmadığını var saydığımız bir noktada da işletmelerin verimli ve etkin işleyişine yönelik yönetime bilgi akışı sağlayacağı ve makul güven vereceği için sürdürülebilirlik açısından önem arz etmektedirler.

Bilgi Teknolojileri Kontrollerine Yönelik olarak yasal düzenlemelerde kontrol noktalarına örnek verecek olursak ödeme kuruluşları bilgi sistemleri tebliğ kapsamında kuruluş yılda en bir defa düzenli olarak sızma testi yaptırmak zorundadır ifadesi yer almaktadır. Bunun yasal bir yükümlülük olmasını göz önüne alırsak sızma testlerinin yılda bir kez yapılması bunların sonuçlarının ve kapatılma durumlarını takip edilmesi önem taşımaktadır. Bu test sonucunda ortaya çıkan bulgular risk iştahı doğrultusunda önem derecelerine göre risk matrislerine eklenerek değerlendirmeleri ve takipleri yapılabilir. Kanunu düzenlemeler dışında ödeme kuruluşlarının belirli sistemleri kullanarak işlemleri gerçekleştiriyor olması personel işe giriş çıkışlarında sistem erişim kontrollerinin yapılması önem taşımaktadır. Personellerin sistem erişimlerinin resmi işe giriş ve çıkış tarihleri dikkate alınarak kontrollerini yapılması gerekliliğini ortaya çıkarmıştır. Bununla beraber log kayıtlarının kontrolü, bilgi teknolojilerine yönelik politika ve prosedürlerin güncel olması kontrolleri, birincil ve ikincil merkezlerin çalışabilir olması durumları, veri mahremiyeti gibi çoğaltılabilecek örneklerle kontrol noktalarının ve risklerin belirlenmesi bilgi teknolojileri kontrol faaliyetlerine verilebilecek örnekler arasındadır.

Ödeme kuruluşlarının teknoloji ile iç içe olmasını göz önüne alırsak bilgi teknolojileri tüm alanlarla temas halindedir. Uyum ve İç kontrol süreçlerini bilgi teknolojilerinden soyutlamak bu sebeple imkansız bir hal almaktadır. İç kontrol her ne kadar bilgi teknolojileri ile iç içe olduğu düşünülse bile tez kapsamında daha çok firma faaliyetlerini etkileyen operasyonel, finansal, insan kaynakları gibi birimler dikkate alınarak oluşturulan kontrol faaliyetleri olarak düşünülebilir. Bu kontrol faaliyetine birkaç örnek verecek olursak ödeme kuruluşunun hizmetlerini temsilci aracılığıyla yürütebilmesi adına ilgili yönetmelikte temsilci adaylarından alınması zorunlu belgeler yer almaktadır. Bu süreçte alınması gereken belgelerin tam ve doğruluğunun kontrolünün yapılması yükümlülüklere uyumlu olmak açısından önemlidir. İnsan kaynakları açısında ele alacak olur iş kanunu kapsamında yıllık izin kullanımlarının kontrollerini yapılması, muhasebe açısında ele alınacak olursak vergi hukuku kapsamında ödenen vergilerin kontrolü, çok

sayıda müşteri ve personel olması sebebiyle kişisel verilerin korunması kanunun ele alınarak yapılabilecek kontroller şeklinde kanuni yükümlülükler kapsamında kontrolleri çoğaltabiliriz. Tüm bu kontroller risk değerlendirmesi sonucunda ortaya çıkan risklerin ölçümlerini etkileyebilir aynı zamanda kontrol sonucu ortaya çıkan bulgular risk değerlendirmesine konu olabilir.

Uyum açısından yapılacak kontroller dikkate alındığında *"Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik"* kapsamında yükümlüler nezdinde veya bunlar aracılığıyla yapılan ve yapılmaya kalkışılan işleme konu malvarlığının; yasa olmayan şekilde elde edilmiş olmasında dair veya amacı dışında kullanıldığında bu kapsamda terör eylemi, terör örgütü, terörist ya da terörü finanse edenler tarafından kullanılması veya bunlarla bağlantılı olduğuna dair bilgi, şüphe ya da şüpheyi gerektirecek husus olması halinde şüpheli işlem bildirimi yapılması gerekir. Şüpheli işlem şüphenin oluşma tarihinden en geç on iş günü içinde Başkanlığa bildirilmek zorundadır. Bu doğrultuda kontrol noktası oluşturulduğunda şüpheli işlem bildirimlerinin on iş günü içinde yapıldığının kontrol edilmesi gereklidir. Süresi içerisinde yapılmayan şüpheli işlem bildirimleri için para cezası yaptırımı uygulanmaktadır.

3.6. Risk Değerlendirmesi

Risk değerlendirmesi şirket hedeflerine ulaşılmasını engelleyebilecek risklerin belirlenmesi ve değerlendirilmesi konusunda önem taşımaktadır. Risk değerlendirmenin bir parçası olarak risk tanıma ve ölçmenin yapılması gereklidir. İşletme içerisinde risk değerlendirme süreklilik taşımalıdır. Risklerin etki ve olasılıkları belirlenmelidir. Belirli zamanlarda yapılan risk analizleri kanuni düzenlemeler, teknolojik gelişmeler, operasyonel süreçler, stratejik kararlarla gibi etkenlerle beraber değişiklik gösterebilir. Ödeme kuruluşlarının Fintek firması olması sebebiyle dinamik bir yapıda olması riskleri sürekli gözden geçirmeyi gerektirmektedir. Risk odaklı yaklaşım tarzı benimsenerek oluşturulacak kontrol yapıları için risk süreçlerinin doğru değerlendirilmesi büyük önem taşımaktadır. İşletme içerisinde tüm birimlerle koordinasyon sağlanması ile "*aşağıda-yukarıya*" ve *"yukarıdan aşağıya"* yaklaşımı benimsenerek risk matrislerinin oluşturulması, sürekli olarak bunların değerlendirilmesi işletme faaliyetlerinin sürdürülmesine ve alınacak kararların akılcı olmasına etki edecektir. Ayrıca riskler dikkate alınarak yapılacak

kontrollerle risk seviyelerinin değişebileceği ve risk olarak sayılmayan alanlarda oluşabilecek farkındalıklarla risklerin önlenebileceği söylenebilir.

Risklerin doğru analiz edilebilmesi için şirket politika, prosedürlerin sürekli gözden geçirmelerinin yapılması, personellerin yetki, sorumluluklarının doğru bir şekilde dağıtılmış olması ve şirket içi eğitimlerle personellere farkındalıkların yaratılması önemli olacaktır.

Kontrol yapıları içerisinde risk değerlendirme sürecine tabi olmamış bulgularla karşılaşılması muhtemeldir. Bu bulguların değerlendirilip risk matrisine eklenmesi ve derecelerinin belirlenmesi yapılacak kontrollerin seyrini etkileyebilecektir. Aynı şekilde risk değerlendirmesine alınmış riskli görülen bir durum için kontrol yapıları içerisinde herhangi bir bulguya rastlanmayabilir ve risk matrisinin ilgili bulgusunun risk düzeyinin değişimine etki edebilir.

Fintek firmaları yapılarında bulunan her bir bölüm için farklı bir risk iştahı belirlemeli ve mevcut riskler ile olası riskleri her bir bölüm için ayrı ayrı değerlendirmelidir. Örneğin; İç sistemler bölümü için kanuni düzenlemeler gereği risk iştahı minimum seviyede tutulması gerekirken Operasyonel bölümlerde risk iştahı katlanılabilecek bir maddi değer üzerinden belirlenebilir.

Risk matrisi oluşturulması bu risklerin etki ve olasılıklarının ölçülebilirliğini gösterirken süreçlerin dizaynı risk matrisi kapsamında oluşturulmalı, risk matrisine konu olabilecek her olası risk ve bu riske karşı alınabilecek aksiyonlar mutlaka politika ve prosedürlere işlenmelidir. Oluşturulmuş olan risk matrisi Fintek firmalarının tüm çalışanları tarafından incelenmeli ve tüm çalışanlar karşılarına çıkabilecek olası riskler için farkındalık sahibi olmalıdır.

Risk değerlendirmesi ve yönetimi tüm firma içerisinde süreklilik göstermeli, risk matrisinde yer almayan olası riskler karşısında ilgili bölümler tarafsız bir şekilde ivedilikle bilgilendirilmelidir. Böylece risk yönetimi firma içerisinde tüm tabana yayılmış bir biçimde dinamik olarak değerlendirilip yönetilebilir.

3.7. Sürekli İzleme

İzleme, iç kontrol yapısının ve sistemin karşı karşıya kaldığı risklere ve değişimlere uygun yapıya ulaşmasında etkili olmaktadır. Kontrol yapısının etkin olup olmadığını belirlemek amacıyla sürekli izleme yapılmasıdır. Bu sürekli izlemeler kontrol yapılarının güncel durumunu anlamak, risk taşıyan alanlarda etkinliği kavrayabilmek adına önemlidir. Sürekli izleme iç kontrol verimliliğini arttırmaya yönelik fırsatları belirlerken kuruluşun hedeflerine ulaşmasını arttırabileceği alanları da tanımlayabilir (TİDE,2016).

Risk olarak değerlendirilen alanların kontrol yapılarına yansımış olması kontrol yapılarının etkinliğinin ölçülmesine katkı sağlayabilir. Bunların etkin olduğu düşünülen kontrol yapılarında görülmemesi ise risk değerlendirmesinin tekrar gözden geçirilmesine etki edebilir.

Sürekli izlemenin altında yatan temel ilkeler aşağıda yer alan şekilde belirtilebilir (Kurnaz ve Çetinoğlu, 2010).

- Belirlenen her kontrol noktasında güvenlik durumu ve kontrol hedeflerinin oluşturulması,
- Herhangi bir hatalı işlemin varlığını belirlenmesine yönelik testlerin oluşturulması,
- Gerçekleşen işlemlere dair testlerin belirlenip uygulanması,
- Hatasız işlem ve kayıtların belirlenmesi,
- Kontrol etkinliği olmayan alanların belirlenmesidir.

Sürekli izleme verimli ve efektif işleyen bir iç kontrol sistemi oluşturulmasında ve sürekliliğinin sağlanmasında elzem durumdadır. Yukarıda değinilen maddeler izlemenin verimli yapılma durumunun şirket içerisinde uygulanması faydalı olacaktır.

Bu maddeler ele alındığında yapılan kontrollerde kullanılan yöntemlerin test edilmesi etkili olacaktır. Bunun yanı sıra kontrol alanına dahil edilmeyen alanların incelenip bu alanların risklerinin gözden geçirilmeli ve bir kontrol eksikliği olup olmadığı belirlenmelidir. Ayrıca hatasız işlem ve kayıtlar göz önüne alınarak bunlarında testleri gerçekleştirilerek güvenilirliği ölçülmelidir.

Sürekli izlemeyle beraber kontrol yapılarının etkinliğini ölçebilecek iç denetim mekanizmasının da kurulması etkili olacaktır.

Sürekli izlemelerde kontrol ve risk değerlendirmeleri sistem üzerinde etkin hale getirilerek kontrol noktalarının sistemsel hale getirilmesi sağlanabilir. Böylece zamanı ve personel gücünü verimli kullanarak sistem üzerinden yapılabilecek kontroller otomasyon haline getirilebilir. Böylelikle insan hatalarının önüne geçilmesi sağlanırken daha kaliteli verilere ulaşılabilir.

Sürekli izleme sonucunda çıkan veriler dahilinde risk değerlendirmeleri ve kontrol yapıları gözden geçirilebilir. Bu gözden geçirme sonucunda firma faaliyetleri ele alınarak yeniden değerlendirme yapılabilir. Değerlendirmeler sonucunda şirket politika ve prosedürleri incelenebilir ve risk değerlendirmeleri kapsamında bunlarda gözden geçirmeler yapılabilir. Bunun yanı sıra personel ile yapılacak mülakatlarla firma faaliyetleri, risk algıları, şirket için hedeflere uyumlu davranmaları ve kontrol sonucu ortaya çıkan eksiklikler, bulgular hakkında bilinçlendirme sağlamak amacıyla eğitim, seminer gibi erkinlikler düzenlenebilir.

3.8. Firma Faaliyetleri

Şirketler faaliyetleri ve kuruluş yapıları itibariyle fazla sayıda yasa ve bunlara bağlı olan ikincil mevzuatın (Vergi Kanunu, Türk Ticaret Kanunu, Kişisel Verilerin Korunması Kanunu vb.) düzenlemelerine tabidir. Bu kanun ve düzenlemeler şirket faaliyetlerine göre Vergi Kanunu, Kişisel Verilerin Korunması Kanunu, İş Hukuku, Bankacılık kanunu, Sermaye Piyasası Kanunu, Ödeme Kuruluşları ve Elektronik Para kuruluşlarını ilgilendiren kanun, Suç Gelirlerini Aklanmasının Önlenmesi Hakkında Kanun ve bunlara bağlı olarak çıkarılan ikincil mevzuatlara (yönetmelik, tebliğ genelge gibi) uymakla yükümlüdürler.

Kanun maddeleri ve ikincil düzenlemeler ele alındığında ödeme ve elektronik para kuruluşlarının faaliyet izinleri kapsamında ne işlerle iştigal edebileceğinin firma içerisinde bilinmesi ve bunlara göre politika ve prosedürlerin oluşturulup sistemin kurulması önem taşımaktadır.

Tüm bu süreçlerden sonra organizasyon yapısının ve iş süreçlerinin kanun, ikincil düzenleme, politika ve prosedürler ele alınarak şirket hedefleri doğrultusunda

oluşturulması bu bağlamda risk iştahı belirlenerek risk değerlendirmelerinin yapılması gereklidir. Oluşturulacak kontrol yapılarında (BT kontrolü, iç kontrol ve uyum kontrol) risk iştahı dikkate alınarak oluşturulan risk değerlendirme sonuçlarının kontrol noktalarına eklenmesi etkin bir kontrol sistemi açısında faydalı olacaktır.

3.9. İletişim ve Eğitim

Kontrol sistemlerinde doğru, eksik olmayan, güvenilir iletişimin sağlanması faaliyetlerin kontrolünde çok büyük önem taşımaktadır. İşletmelerin hedeflerine ulaşmada ve kontrol yapılarının etkinliğini sağlamada bilgiye ihtiyaç duymaktadır. Yönetime doğru bilgi akışının sağlanması doğru iletişimin kurulmasıyla etkili olmakta ve firmanın yaşam döngüsünü etkileyebilecek kararların alınmasında hayati derecede önem taşımaktadır. Ayrıca BT kontrol, İç kontrol ve Uyum kontrol ilk etapta ilgili birimlerle doğru iletişim kurarak bilgi akışını sağlaması kontrol sonucu ortaya bulguların kalitesini etkileyebileceği gibi bu bulguların birimlerle paylaşılması sırasında çalışanların hata ve eksikliklere verecekleri tepki ve gelişime etki edebilecektir.

Şirket personelleri kanuni düzenlemelerde zorunlu olarak alınması gereken eğitimler ve incelemeler sonucunda ortaya çıkan bulgular doğrultusunda bilinçlendirme amaçlı eğitimler atanması sağlanmalıdır. Bu eğitimlerle personellerin kişisel gelişimine katkı sağlanabileceği gibi şirket faaliyetleri, amaçları, sektör ve şirket riskleri hakkında bilinçlendirme ve farkındalık yaratılmalıdır.

Şirket personellerine verilen eğitimlerin kapsayıcı ve dinamik olması önem arz etmektedir. Eğitim içeriğinde mevcut ve olası riskler hakkında birden fazla örnek yer alması risk farkındalığını oluşturulması hususunda daha etkili olacaktır.

3.10. Raporlama

Raporlama işletmelerin şeffaflık ve hesap verilebilirliğine etki eden, yönetsel kararların alınmasına fayda sağlayan bir mekanizmadır. IIA (The Institute of Internal Auditors) Uluslararası Mesleki Uygulama Çerçevesi (UMUÇ)'a göre raporlamaların doğru, objektif, açık, özlü, yapıcı, tam olmak ve zamanında sunulması zorunludur. Bu

sebeple kaliteli bir raporlama için bu 7 maddeye dikkate alınmalıdır. Bu maddeler kapsamında;

Doğruluk; Raporlamanın doğru ve eksiksiz olması için kontrol süresince toplanan kanıtlarla güçlendirilecek anlaşılır ve net bir anlatım kullanmak önemlidir. Raporlama çarpıtma ve hatalardan uzak doğru bir şekilde yapılmalıdır.

Objektiflik; Mesleği yerine getirirken tarafsız bir tavır sergilemeyi ifade etmektedir. Bağımsız ve tarafsız davranışlar sergilemek ve ifadelerde bulunmak gereklidir.

Açık; Raporlamanın kolay anlaşılır olması ve işletme içerisinde kullanılan dile uygun olmalıdır. Gereksiz teknik tabiler ve ağdalı bir dil kullanımında kaçınılmalıdır. Açık raporlamada sonuçlar ve verilen tavsiyeleri destekleyecek önem teşkil eden bulgulara yer verildiğinde raporun açıklığı da artar.

Özlü olması; Görev ile ilgili olmayan ayrıntılardan uzak, laf kalabalığı içermeyen, gerekli ve önemli bilgilerin paylaşılmasının sağlanması

Yapıcı; Raporlamanın işletme veya görev bazında pozitif yönde değişime sebep olacak çözümlerin tespiti için iş birliğine dayanan süreçlere katkı sağlayan iletişimlerdir. İşletmeye hedeflerine ulaşmasını sağlayan süreçlerdir.

Tam (Eksiksiz); Raporlamanın tam ve eksiksiz olarak yapılması raporlamanın yapıldığı tarafında aynı sonuca ulaşmasına olanak sağlayacaktır. Raporlama yapacak kişinin tüm bilgileri dikkate alarak doğru bir şekilde değerlendirmesi yarar sağlayacaktır.

Zamanında Sunulan; Raporlamalar planlama süresinde belirlenen son bildirim tarihine kadar yapılmalıdır.

Nihai raporlarda hata veya eksikliklerin olduğunun fark edilmesi halinde bunların önem derecesine göre aksiyon alınması gerekmektedir. Alınacak aksiyonların belirlenmesinde hata veya eksikliklerin sonucu değiştirip değiştirmeyeceği, bulgu ve sonuçlar için farklı bir çıkarımda bulunup bulunamayacağı, verilen tavsiyeleri değiştirip değiştirmeyeceği bu hususta önem taşımaktadır.

Raporlamanın yukarıda bahsi geçen kriterler göz önüne alınarak hazırlanması raporlamanın yapılacağı tarafa doğru bilginin aktarılması açısında fayda sağlayacağı gibi

raporlama sonucun varılacak kanaatlerle yönetim alacağı kararları etkileyebilecektir. Aynı zamanda kurum içerisinde kontrol faaliyetlerine duyulan güvenin sağlanması açısında doğru, güvenilir tarafsız raporlama yapılması büyük önem taşımaktadır.

SONUÇ

Yapılan bu tez ile önemi her geçen gün artan Ödeme ve Elektronik Para Kuruluşlarına yönelik etkili bir iç kontrol yapısının nasıl olması gerektiği ile ilgili bir model geliştirilmiştir. Böylece Ödeme ve Elektronik Para Kuruluşları özelinde dikkate alınması gereken tüm iç kontrol bileşenleri arasındaki ilişkiler gösterilerek ilgili yazına önemli bir katkı sağlanmış ve uygulayıcılara kılavuzluk edebilecek bir genel çerçeve sunulmuştur.

Bu modelde kontrol yapılarının kurulması aşamalarına yer verilmiştir. Bu aşamalar şirketin tabi olduğu kanuni düzenlemeler ve standartlar dikkate alınarak yönetim kararlarının ve risk iştahının belirlenmesi bunlar sonucunda politika ve prosedürler oluşturularak organizasyon yapısının oluşturulmasıdır. Tüm bu aşamaların titizlikle hazırlanarak tüm iş birimlerinin uyacakları kuralların çerçevesinin belirtilmiş olması ve tüm iş birimlerince bunların sahiplenilerek iş akışlarına entegre edilmesi verimli ve efektif bir sistem için hayati önem taşımaktadır.

Bu aşamalardan sonra kontrol yapılarını içeren BT Kontrol, İç Kontrol ve Uyum birimlerini kurulması ve sorumluluklarının belirlenmesi önem taşımaktadır. Daha önceki aşamada belirlenmiş olan risk iştahı seviyesi ve kanuni düzenlemeler, standartlar, şirket politika ve prosedürleri dikkate alınarak risk değerlendirmeleri yapılmalıdır. Bu değerlendirmeler kontrol yapılarının kontrol noktalarında değerlendirilerek süreçlere eklenmesi ve kontrol sonucu ortaya çıkan riskler risk değerlendirmesine katkı sağlayarak birbirini besleyen risk odaklı kontroller oluşturulmalıdır. Bununla beraber sürekli izlemeler yapılarak kontrol yapılarının etkinliğinin ölçülmesi gerekmektedir. Tüm bu aşamalar firma faaliyetlerinden etkilenmekte kontrol sonucu bulgularla firma faaliyetleri gözden geçirilmektedir.

Son aşamada şirket içi iletişim ve eğitimle süreçlerin iyileştirilmesi sağlanmalıdır. Kontrol yapılarının raporlamaları ile yönetime süreçlerin işleyişi hakkında güvenilir ve doğru bilgi akışı sağlanarak şirket hedeflerine ulaşılmasına ve karar almaya katkı sağlanacaktır. Bu modelin kapsamı ödeme ve elektronik para kuruluşlarına bütüncül şekilde yaklaşarak tüm iş süreçlerinin oluşturulması ve kontrol yapılarının oluşturulması ve sürekli geliştirilmesine yönelik rehber olabilecek niteliktedir. Bu tez sonucunda geliştirilen model ile literatüre sektör bazında katkıda bulunulacaktır.

Bu çalışma kapsamında geliştirilen iç kontrol modeli finans kuruluşlarının özel bir çeşidi olan Ödeme ve Elektronik Para Kuruluşlarını kapsamaktadır. Dolayısıyla finans sektöründeki diğer dikey alanlarda faaliyet gösteren kuruluşlara veya üretim, sağlık ve bunun gibi farklı sektörlerdeki organizasyonlara uygulanabilirliği veya uyarlanabilirliği yapılacak farklı akademik çalışmalarla incelenmelidir. Ayrıca yapılan çalışma kavramsal boyutta bir model önerisini içermektedir. Modelde gösterilen etkileşimler ve bu etkileşimlerin detayları gelecekte yapılacak görgül çalışmalarla desteklenebilir veya daha iyi anlaşılmasını sağlayacak yeni kavramların geliştirilmesiyle zenginleştirilebilir.

KAYNAKLAR

Akçay, G. (2011). Kurumsal Risk Yönetiminde İç Denetimin Rolü ve Kamu İdarelerinde Yaşanan Gelişmeler. *Denetişim*, 25-46.

Akçay, M., Adar, N,. Seke. E, ve Canbek, S. (2007). Kümeli Hesaplama Modelinin Değişik Parametrelerle İncelenmesi. *TMMOB Türkiye I. Enerji Sempozyumu*, Eskişehir.

Aker, A., Özçelik, T.Ö. (2020). Metal Sektöründe 5x5 Matris ve Fine-Kinney Yöntemi ile Risk Değerlendirmesi, *Karaelmas İş Sağlığı ve Güvenliği Dergisi, 4*(1), 65-75.

Aksoy,T. (2017). Bağımsız Denetim Şirketleri için Ulusal ve Uluslararası Düzenlemelerle Uyumlu Çok Yönlü Bir İç Kontrol Anket Önerisi*, ISMMMO Yayın Organı*, 169-171.

Akkoç, İ., ve Erdoğan, B.Z. (2011). Organizasyon Yapısı ve Liderliğin İş Performansına Etkisi, *Çağ Üniversitesi Sosyal Bilimler Dergisi, 8*(1).79-108.

Aktan, E. (2018). Büyük veri: uygulama alanları, analitiği ve güvenlik boyutu. *Bilgi Yönetimi Dergisi, 1*(1), 3-7.

Alkin, E., Savaş, T., Akman, V. (2001). *Bankalarda Risk Yönetimine Girişi* (1). İstanbul: Çetin Matbaacılık.

Allan, N., ve Davis, J. (2006). Strategic Risks Thinking About Them Differently. *ICE Proceedings Civil Engineering*, *159*(6), 10-14.

Arner, D. W., Barberis, J. N., ve Buckley, R. P. (2015). The Evolution of Fintech: A New Post-Crisis Paradigm?. *University of New South Wales Law Research Series*, 1-44.

Arner, D. W., Barberis, J., Buckley, P.R. (2016). Fintech, RegTech, and Reconceptualization of Financial Regulation, *Northwestern Journal of International Law and Business, 37(*3). 371.

Arslan, I. (2008). Kurumsal Risk Yönetimi. Maliye Bakanlığı Strateji Geliştirme Başkanlığı Yayınlanmamış Uzmanlık Tezi.

Büyük Larausse Sözlük ve Ansiklopedi (1986), Milliyet Yayınları, İstanbul.

Bob Frelinger(CGEIT). "Introducing COBIT 5", 2012.

Bozkurt, N. (2000). Muhasebe Denetimi. (3. Baskı). İstanbul: Alfa Yayınları.

Bozkurt, C. (2010). Risk, Kurumsal Risk Yönetimi ve İç Denetim. *Denetişim,(4)*,17-30.

Bughin,J., Chui, M. ve Manyika, J. (2010). "Clouds, Big Data, And Smart Assets: Ten Tech-Enabled Business Trends To Watch," *Mckinsey Quarterly, 56*(1):75-86.

Canbek, G., Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme.*Politeknik Dergisi, 9*(3), 165-174.

Charniak, E. ve McDermot, D. (1985). *Introduction to Artifical Intellingence*. Boston: Addison-Wesley Company.

Chan, R. S. O. (2020). Open Banking: does it open up a new way of banking? A case of financial technology adoption from a consumer's perspective. University of Adelaide, Avusturalya.

Cica (1995), Guidance on Control, Criteria of Control Board, The Canadian Institute of Chartered Accountants.

ClydeBank Technology. (2017). ITIL for beginners: the complete beginner's guide to ITIL(2nd ed).

"COBIT 5 Principles and Enablers Applied to Strategic Planning". ISACA. Erişim 18 Aralık 2019. http://www.isaca.org/COBIT/focus/Pages/cobit-5-principles-and-enablers-applied-to-strategic-planning.aspx.

COSO Enterprise Risk Management Integrated Framework (2004): www.coso.org.

Çetinkaya, M. (2008). Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması. *Akademik Bilişim*, 511-516.

Çelik, S. (2017). Büyük Veri Teknolojilerinin İşletmeler için Önemi. *Sosyal Bilimler Dergisi, 3*(6) ,873-883.

Çifçi, G. ve Reis, Ş.G. (2020). Risk İştahı ile Piyasa Likiditesi Arasındaki Nedensellik İlişkisi. *Ekonomi, Politika ve Finans Araştırmaları Dergisi, 5*(2),389-403.

Dabbağoğlu, K. (2009). İç Kontrol Sistemi, *Journal of Qafqaz University*, 26,109-115.

Dal, D. ve Aydın,T. (2013). Hesaplamanın Farklı Formları Ve Hesaplamada Paradigma Kaymaları. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi,* 70-75.

D'Arcy, S. P. ve Brogan, J. C. (2001). Enterprise risk management. *Journal of Risk Management of Korea*, *12*(1), 207-228.

Daft, R. L. (1991), Management, Sec. Edit., Dryden, Press, USA.

Demir, M. H. ve Gümüşoğlu, Ş. (1988). *Yönetsel Karar Verme*. İzmir: Mess

Demir, M., Ülker, Y., Arslan, Ö. (2018), İç Kontrol, İç Denetim ve Bağımsız Denetim İlişkisi, *Van Yüzüncü Yıl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 82-104.

Dessler, G. (2004). Management. New Jersey: Pearson Education Ltd

Dinapoli, T. (2016), Standards for Internal Control in New York State Government, https://www.osc.state.ny.us/files/state-agencies/guidance/pdf/agencies-ictf-docs-int-control-stds.pdf

Dima A. M. ve Orzea, I. (2012). Risk Management in Banking. Academy Publish.

Emhan, A. (2006). *"Risk Yönetiminden Ne Anlıyoruz? Birliğimizdeki Uygulama Durumu Nedir?"* .7 nci Ana Jet Komutanlığı Üs Uçuş ve Yer Emniyeti Semineri, Malatya.

Erdem, D. (2021). *6493 Sayılı Kanun Kapsamında Ödeme Hizmeti Sözleşmesi*. Bilkent Üniversitesi, Ankara.

Ersoy, E. V.(2012). *ISO/IEC 27001 Bilgi Güvenliği Standardı*. Ankara; ODTÜ Yayıncılık.

Federal Reserve Bank. (2014). Assessment of Compliance with the Core Principles for Systemically Important Payment Systems (s. 7). Erişim Linki: https://www.federalreserve.gov/paymentsystems/files/fedfunds_coreprinciples.pdf

Firican, G. (2017). The 10 Vs of Big Data. https://tdwi.org/articles/2017/02/08/10-vs-of-big-data.aspx

Frigo, M. L., ve Anderson, R. J. (2011). *Strategic risk management: A foundation for ımproving enterprise risk management and governance*. The Journal of Corporate Accounting & Finance, 22(2), 81-88.

Fülop, M.T. ve Szekely, S.V. (2017). The Evolution of Internal Auditing Function in The Context of Corporate Transparency. *Audit Financiar*, *3*(147),440-450.

Gelinas, U. J., Sütton S. G. (2002). Accounting Information Systems, Fifth Edition.

Girling, P. (2022). *Operational Risk Management* (2. Baskı). New Jersey: John Wiley & Sons.

Güredin, E. (2000). Denetim. İstanbul: Beta.

Greene, M., (1997). Risk and Insurance. England.

Grundke, P. (2008). Top-Down Versus Bottom-Up Approaches in Risk Management.

Giambelluca, G., ve Masi, P. (2016). The Regulatory Machine: An Institutional Approach to Innovative Payments in Europe. *In Bitcoin and Mobile Payments*, 3-25.

Griffiths, P. (2005).Risk-Based Auditing. (1.baskı). England: Gower Publishing Limited.

Haddad, C., ve Hornuf, L. (2016). The emergence of the global fintech market: economic and technological determinants. *CESifo Center for Economic Studies & Ifo Institute, 7*(6131), 7.

He, D., Leckow, R., Haksar, V., Mancini- Griffoli, T., Jenkinson, N., Kashime, M., Khiaonarng, T., Rochon, C., Tourpe, H.(2017). Fintech and Financial Services: Initial Considerations. International Monetary Found.

Hopkin, P. ve Thompson, C. (2022). Fundamentals of Risk Management (6.baskı). Londra: Kogan Page Limited.

Huang, F., ve Vasarhelyi, M.A. (2019) Applying robotic process automation (RPA) in auditing: A framework. International Journal of Accounting Information Systems, 35. doi:10.1016/j.accinf.2019.100433

IFAC (2011). Annual Report. https://www.ifac.org/publications/2011-ifac-annual-report.

Ionescu, L. (2007), "Internal Control, Human Resource Management and Risk Assessment". *Economics, Management and Financial Markets, 2* (2), 129-136.

INTOSAI GOV 9100 (2004), Guidelines for International Control Standarts for the Public Sector.

IPFC Online Web Agency. (2018,). The incridible growth of fintech [infographic]. IPFC Online Web Agency: http://ipfconline.fr/blog/2018/02/27/the-incredible-growth-of-fintech-infographic/

Karakaya, G. (2016). Çalışan Hileleri ve İç Kontrol İlişkisi, *Vergi Sorunları Dergisi*, 330.

Kaya, F. (2022). Türkiye'de Bağımsız Dış Denetim, Bağımsız Dış Denetimin Sorunları ve Çözüm Önerileri . Türkiye'de Bağımsız Dış Denetim, Bağımsız Dış Denetimin Sorunları ve Çözüm Önerileri, 16.

Kaya, P. (2022). UBS Skandalı. Ş. Babuşçu ve A. Hazar (Ed.), *Finansal Skandallar* (101-113). Ankara: Akademi Araştırma Planlama Danışmanlık Eğitim Yayıncılık Ltd. Şti.

Khan, M. A., Uddin, M. F. ve Gupta, N. (2014). Seven V's of Big Data understanding Big Data to extract value. Conference of the American Society for Engineering Education, IEEE, DOI: 10.1109/ASEEZone1.2014.6820689

Kıral, E. (2015). Yönetimde Karar ve Etik Karar Verme Sorunsalı. *Adnan Menderes Üniversitesi Eğitim Fakültesi Eğitim Bilimleri Dergisi, 6* (2), 73-89.

Korkmaz, U. (2007). "Kamuda İç Denetim ".*Bütçe Dünyası Dergisi, 2*(25), Bahar, 4- 15.

Korga, S., Aslanoğlu, S. (2020), İç Kontrol Sisteminin Unsurları ile Risk Yönetimi Arasındaki İlişkini İncelenmesi: Bankacılık Sektöründe Bir Uygulama, *Muhasebe ve Denetime Bakış*, 95-116.

KPMG Türkiye. (2018). Robotik süreç otomasyonu. 09 08, 2020 tarihinde https://assets.kpmg/content/dam/kpmg/tr/pdf/2018/11/robotik-surec-otomasyonu.pdf adresinden alındı

Kurnaz, N. ve Çetinoğlu, T. (2010), "İç Denetim Güncel Yaklaşımlar", Umut Tepe Yayınları.

Laudon, K.C., Laudon, J.P.(2022). Management Information Systems. (17.baskı). Pearson,

Lewis, T. (2014). A Brief History of Artificial Intelligence. LiveScience Retrieved.

Lindow, P. E. ve Race, J. D. (2002), ''Beyond Traditional Audit Techniques'', *Journal of Accountancy*, 28-29.

Louwers,T.J. Ramsay R.J., Sinason, D.H., Strawser, J.R. (2005). Auditing&Assurance Services International Edition.A.B.D. ; Mc Graw Hill

Maliye Bakanlığı Bütçe ve Mali Kontrol Genel Müdürlüğü.(2014), Kamu İç Kontrol Rehberi.

Mandacı, P. E. (2003). Türk Bankacılık Sektörünün Taşıdığı Riskler ve Finansal Krizi Aşmada Kullanılan Risk Ölçüm Teknikleri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, (1),*67-84.

Mars, M. M., Bronstein, L.J. (2017). "The Promise of the Organizational Ecosystem Metaphor: An Argument for Biological Rigor", Journal of Management Inguiry

Marttin V., Pehlivan İ. (2010). ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir inceleme. *Mühendislik Bilimleri ve Tasarım Dergisi, 1*(1) ,50.

Messier, W. F. (2000). Auditing and Assurance Services A Systematic Approach (2th ed.). New York: McGraw-Hill.

Misina, M. (2006). Benchmark Index of Risk Appetite. *Bank of Canada Working Paper,* 16.

Mansfield-Devine, S. (2016). Open Banking: Opportunity And Danger. Computer Fraud & Security, 8-13.

Moeller,R.R. (2005) . Brink's Modern Internal Auditing. New Jersey: John&Wiley Sons Ltd.

Moeller,R.R. (2011). COSO Enterprise Risk Management (Second Edition). New York: John Wiley & Sons Inc.

Moeller,R.R. (2014). Executive's Guide to COSO Internal Controls-Understanding and Implementing the New Framework. New York: John Wiley & Sons Inc.

Nabiyev, V. V. (2012). Yapay Zekâ: İnsan-Bilgisayar Etkileşimi. Baski Yeri: Seçkin Yayıncılık.

National Institute of Standards and Technology . (2018). Risk Management Framework for Information System and Organizations (2) National Institute of Standards and Technology Special Publication.

Ohlhorst, F. (2013). Big Data Analytics : Turning Big Data into Big Money. New Jersey: Wiley Publicity

Özbek. Ç. (2012). İç Denetim, Kurumsal Yönetim, Risk Yönetimi, İç Kontrol. İstanbul: Türkiye İç Denetim Enstitüsü Yayınları.

Öztürk. K, Şahin. M.E. (2018). Yapay Sinir Ağları ve Yapay Zeka'ya Genel Bir Bakış. Takvim-i Vekayı.

Pavaloiu A. (2016), The Impact of Artificial Intelligence on Global Trends. *Journal of Multidisciplinary Developments, 1* (1), 21-37.

Pamukçu, A. (2019). Küçük ve Orta Büyüklükteki İşletmelerde İç Kontrol ve İç Denetim. Ankara: Ekin Yayınevi.

Parthasarthy, R. ve Sethı, S. P. (1992). The Impact Of Flexible Automation On Business Strategy And Organizational Structure. *Academy of Management Review, 17*(1), 86-111.

Peltoniemi, M (2006). "Preliminary theoretical framework for the study of business ecosystems". *Emergence: Complexity and Organization, 8*(1), 1-10.

Popov, E. V., (1990). Yapay Zekâ. Uzman Sitemler ve Doğal Dil İşleme. Moskova: Radio i Svyaz, 461.

Principles for the Management of Credit Risk (2000). Basel Committee on Banking Supervision. https://www.bis.org/publ/bcbs75.htm

Ramakrishna, S. (2015). Enterprise Compliance Risk Management (1.baskı). Singapur: John Wiley & Sons

Risk IT Framework . https://www.isaca.org/about-us/newsroom/press-releases/2020/isacas-risk-it-framework-offers-a-structured-methodology

RiskAppetiteGuidanceNote.(2021).https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1012891/20210805__Risk_Appetite_Guidance_Note_v2.0.pdf

Root,S.T. (1998). Beyond COSO: Internal Control to Enhance Corporate Governance. New York: John Wiley&Sons Inc.

Romney, M. B., Steinbart, P. J. (2003), Accounting Information Systems (9.baskı), Prentice Hall.

Rubino, M. (2018). A Comparison of the main ERM Frameworks: How limitations and weaknesses can be overcome ımplementing IT governance. *International Journal of Business and Management, 13*(12), 203-214.

Sakarya, Ş. ve Kara, S. (2012), Kurumsal Risk Yönetimi Çerçevesinde Risk Odaklı İç Denetim ve İMKB Uygulaması. *Ankara SMMO Muhasebe ve Vergi Uygulamaları Dergisi*, 69-95.

Saltık, N. (2007). İç Kontrol Standartları. T.C. Maliye Bakanlığı ve Mali Kontrol Genel Müdürlüğü İç Kontrol Merkezi Uyumlaştırma Dairesi, (Erişim) https://kontrol.bumko.gov.tr/Eklenti/6855,saltik-nihal-ic-kontrol-stanadrtlari arastirma-raporu.pdf?0.

Satyanarayana, L. V. (2015). A Survey on challenges and advantages in big data. *IJCST, 6*(2), 115–119.

Sawyer's İç Denetçiler için Rehber. İstanbul: Türkiye İç Denetim Enstitüsü Yayınları.

Sayım, F. ve Aydın, V. (2011). Hizmet Sektörü Özellikleri ve Sistematik Olmayan Risklerin Sektör Menkul Kıymetleri İle Etkileşimine Dair Teorik Bir Çalışma. *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, (29), 245- 262.

Scherer, M. U. (2016). Regulating artificial intelligence systems: risks, challenges, competencies and strategies. *Harvard Journal of Law & Technology*, 354

Shueffele, P. (2016). Tamming the beast: a scientific definition of fintech. *Journal of Innovation Management*, 32

Shift,M. (1990). What İs İnternal Control? Who Owns It?.*Management Acounting*.

Sultan,N.,(2011). "Reaching For The "Cloud: How Smes Can Manage," *International Journal Of Information Management*, 272-278.

Tapia, D.M. (2015). Cobit 5 Principles and Enablers Applied to Strategic Planning.ISACA.

T.C. Maliye Bakanlığı Mali Suçları Araştırma Kurulu Başkanlığı 2015 Yılı Faaliyet Raporu, s.4, Erişim: http://www.masak.gov.tr/userfiles/file/2015_Faaliyet_Raporu.pdf, Erişim Tarihi: 24.09.2016

T.C. Maliye Bakanlığı Mali Suçları Araştırma Kurulu Başkanlığı.(Aklama Suçu, Erişim: http://www.masak.gov.tr/tr/content/aklama-sucu/57)

T.C.MerkezBankası.(2023).https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Temel+Faaliyetler/Odeme+Sistemleri/

Tepegöz, Ş.M. (2022).Finansal Teknoloji Uygulamaları, Bankaların Risk Yönetimi ve İç Kontrol Yapısı Üzerindeki Etkisi ve Sonuçları, *Beykoz Akademi Dergisi, 10*(1),158-168.

The Financial Reporting Council (2015), Internal Control: Revised Guidance for Directors on the Combined Code.

Toroslu, M.V. (2014). İç Kontrol ve İç Denetim. İstanbul: Vedat Kitapçılık.

Torunlar, M. (2018). Yönetim Eyleminin Bir Parçası Olarak Karar Verme Süreçlerinde Belge/Bilgi Yönetiminin Önemi ve Katkıları, Bilgi Yönetim Dergisi.

Treasury, H. M. (2004). The Orange Book Management of Risk- Principles and Concepts. HM Treasury

Turhan B., Ünalan, D. (2022). Hasta Düşmelerinin Sıklığının Kök Neden Analizi ile İncelenmesi: Kayseri Şehir Hastanesi Örneği. Türkiye Sağlık Enstitüleri Başkanlığı Dergisi.

Türedi, H. ve Koban, A.O. (2016). Coso İç Kontrol Modelinde Risk Değerlendirme Faaliyetleri, Marmara Üniversitesi Öneri Dergisi.

Türkiye İç Denetim Enstitüsü. (2016). *COSO İç Kontrol-Bütünleşik Çerçeve*. İstanbul. Türkiye İç Denetim Enstitüsü Yayınları.

Tysiac,K. (2020). COSO provides new guidance on risk appetite. Journal of Accountancy: https://www.journalofaccountancy.com/news/2020/may/new-coso-guidance-risk-appetite.html.

UiPath (2019). "The Ultimate RSO Glossary: Robotic Process Automation Definitions to Know", https://www.uipath.com/automation/ai-and-rpa.

Uluslararası Mesleki Uygulama Çerçevesi (2019). İstanbul. Türkiye İç Denetim Enstitüsü.

Uzay, Ş. (1999). İşletmelerde İç Kontrol Sistemini İncelemenin Bağımsız Dış Denetim Karar Sürecindeki Yeri ve Türkiye'deki Denetim Firmalarına Yönelik Bir Araştırma. Ankara: Sermaye Piyasası Kurulu.

Vaughan, E. Ve Vaughan, T., (1995). Essential of Insurance: A Risk Management Perspective, New York.

Witman, P.D. (2018). “What gets measured, gets managed” the wells fargo account opening scandal. Journal of Information System Education, 29 (3), 131-138.

Wulan, V. R. (2017). Financial technology (fintech) a new transaction in future. Journal of Electrical Engineering and Computer Sciences, 179.

Yüksel, A.S., Yüksel, A., Yüksel, Ü. (2002). *Banka Yönetimi El Kitabı*, Alfa Basım, İstanbul.

Yılancı, M. (2006). İç Denetim: Türkiye’nin 500 Büyük Sanayi İşletmesi Üzerine Bir Araştırma (2.baskı). Eskişehir: Nobel Yayın Dağıtım.