Bölüm 5

İç Kontrol ve Risk Yönetimi

Murat Özcan[1]

Mehmet Günlük[2]

Özet

Bu bölüm, modern organizasyonlarda iç kontrol ve risk yönetimi sistemlerinin teorik temellerini, uygulamalarını ve dijital çağdaki dönüşümünü kapsamlı bir şekilde ele almaktadır. COSO İç Kontrol Entegre Çerçevesi ve Kurumsal Risk Yönetimi (ERM) çerçevesi temel alınarak, iç kontrolün beş bileşeni ve on yedi ilkesi detaylı olarak incelenmektedir. Çalışma, iç kontrol ve risk yönetiminin entegrasyonunu, Üç Savunma Hattı Modeli perspektifinden değerlendirerek, iç denetimin bu süreçteki stratejik rolünü vurgulamaktadır.

İç kontrol etkinliğinin değerlendirilmesi ve ölçülmesine yönelik metodolojileri, kontrol öz değerlendirmesi, kontrol testleri, sürekli izleme ve sürekli denetim yaklaşımlarını içerecek şekilde sunan bu bölümde özellikle dijital çağın getirdiği fırsatlar ve tehditler, yapay zeka ve veri analitiği uygulamaları, siber güvenlik risk yönetimi çerçeveleri ve çok katmanlı savunma stratejileri derinlemesine analiz edilmektedir. Yapay zekanın iç kontroldeki rolü, hile tespiti, süreç madenciliği ve tahmine dayalı risk skorlaması bağlamında ele alınırken, algoritma yanlılığı, açıklanabilirlik ve veri kalitesi gibi kritik riskler de tartışılmaktadır.

Bu bölümde ESG faktörlerinin risk yönetimi ve iç kontrol sistemlerine entegrasyonu, çevresel, sosyal ve yönetişim risklerinin belirlenmesi, değerlendirilmesi ve etkin bir şekilde yönetilmesi açısından kapsamlı olarak incelenmektedir. NIST Siber Güvenlik Çerçevesi, ISO 27001 ve COBIT gibi uluslararası standartların iç kontrol sistemleriyle entegrasyonu, siber dayanıklılık ve iş sürekliliği perspektifinden değerlendirilmektedir. Sonuç olarak, iç kontrol ve risk yönetimi alanındaki en son gelişmeleri,

1 Doç. Dr., Bolu Abant İzzet Baysal Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü, Muhasebe-Finansman Ana Bilim Dalı, e-posta: mozcan@ibu.edu.tr, ORCID: 0000-0001- 9106-4146

2 Doç. Dr., Muğla Sıtkı Koçman Üniversitesi, Milas Meslek Yüksekokulu, Yönetim ve Organizasyon Bölümü, İşletme Yönetimi Programı, e-posta: mehmetgunluk@mu.edu.tr, ORCID: 0000-0001-9665-7557

https://doi.org/10.58830/ozgur.pub1159.c4843

araştırma trendlerini ve gelecek perspektiflerini ortaya koyan bu çalışmada organizasyonların değişen risk ortamında sürdürülebilir başarı elde etmeleri için iç kontrol ve risk yönetimi sistemlerini nasıl güçlendirebileceklerine yönelik stratejik öneriler sunulmaktadır.

GİRİŞ

Günümüz iş dünyası, küreselleşmenin getirdiği fırsatların yanında, dijitalleşmenin yarattığı karmaşık ve sürekli değişen risk ortamını da barındırmaktadır (Mikes ve Kaplan, 2015; Power, 2016). Bu ortamda, organizasyonların sürdürülebilir bir başarı sağlaması ve paydaşlarına karşı sorumluluklarını yerine getirmesi, yalnızca finansal performansla değil, aynı zamanda kurumsal yönetişim mekanizmalarının etkinliğiyle de yakından ilişkilidir (Aguilera vd., 2015; Filatotchev ve Nakajima, 2014). İç kontrol ve risk yönetimi, bu mekanizmaların temel bileşenlerini oluşturarak, işletmelerin hedeflerine ulaşma yolunda karşılaştıkları belirsizlikleri yönetmelerine ve operasyonel verimliliklerini artırmalarına imkan sağlayan stratejik araçlar olarak öne çıkmaktadır (Arena vd., 2010; Rae vd., 2017; Spira ve Page, 2003).

Özellikle 21. yüzyılın başlarında yaşanan Enron ve WorldCom gibi büyük ölçekli finansal skandallar, iç kontrol sistemlerindeki zayıflıkların ve etik olmayan uygulamaların ağır ekonomik sonuçlar ortaya çıkarabileceğini göstermiştir. Bu skandallar, kamuoyunda ve düzenleyici otoritelerde derin bir yankı uyandırmış, sonuç olarak Amerika Birleşik Devletleri'nde Sarbanes-Oxley Yasası (SOX) gibi katı düzenlemelerin hayata geçirilmesine yol açmıştır. Bu yasal çerçeveler, yönetim kurullarının ve üst yönetimin finansal raporlama üzerindeki iç kontrollerin etkinliğine yönelik doğrudan sorumluluk üstlenmesini zorunlu kılarak, kurumsal yönetişimde yeni bir dönemin başlamasına zemin hazırlamıştır (Özer vd., 2018).

Bu düzenlemelerin merkezinde, Treadway Komisyonu Sponsor Kuruluşlar Komitesi (COSO)[1*] tarafından geliştirilen çerçeveler yer almaktadır. İlk olarak 1992 yılında yayımlanan *"İç Kontrol - Bütünleşik Çerçeve"*, iç kontrolün tanımını standartlaştırmış ve organizasyonlara etkin bir iç kontrol sistemi tasarlama, uygulama ve değerlendirme konusunda kapsamlı bir model sunmuştur. Zaman içinde iş dünyasının değişen dinamiklerine göre şekillenen bu çerçeve, 2013

1 COSO, 1985 yılında Amerika Birleşik Devletleri'nde kurumsal finansal raporlamadaki hileli uygulamaları incelemek ve önlemek amacıyla kurulan Treadway Komisyonu'nu destekleyen beş profesyonel organizasyonun oluşturduğu ortak bir girişimdir. Bu beş kurucu organizasyon; Amerikan Muhasebe Birliği (AAA), Amerikan Yeminli Mali Müşavirler Enstitüsü (AICPA), Finansal Yöneticiler Enstitüsü (FEI), Yönetim Muhasebecileri Enstitüsü (IMA) ve İç Denetçiler Enstitüsü'dür (IIA). COSO'nun temel misyonu, kurumsal yönetişim, iç kontrol, risk yönetimi ve finansal raporlama alanlarında düşünce liderliği sağlamak ve rehber çerçeveler geliştirmektir.

yılında teknoloji, kurumsal yönetişim ve risk yönetimi gibi alanlardaki yeni gelişmeleri de kapsayacak şekilde güncellenmiştir. Benzer şekilde, COSO'nun 2004 yılında yayımladığı ve 2017'de *"Strateji ve Performansla Bütünleşik Risk Yönetimi"* başlığıyla güncellediği Kurumsal Risk Yönetimi (ERM) çerçevesi, risk yönetimini sadece bir uyum faaliyeti olmaktan çıkarıp, stratejik karar alma süreçlerinin bütünleyici bir unsuru haline getirmiştir. Literatürde bu çerçevelerin gelişimi ve uygulamaları üzerine yapılan çalışmalar, iç kontrol ve risk yönetimi disiplinlerinin ne kadar dinamik ve sürekli gelişen alanlar olduğunu göstermektedir. Bu bağlamda, Qabajeh vd. (2024) tarafından yapılan bibliyometrik analiz, COSO ile ilgili denetim araştırmalarının son yirmi yılda istikrarlı bir artış gösterdiğini ve özellikle kurumsal yönetişim, iç denetim kalitesi ve teknoloji tabanlı denetim araçları gibi kavramların ön plana çıktığını ortaya koymaktadır.

İç kontrol ve risk yönetimi süreçlerinin birbirleriyle entegrasyonu, modern yönetişim anlayışının temel bir gerekliliğidir. Bu iki süreç, birbirini tamamlamakta ve güçlendirmektedir. Etkin bir iç kontrol sistemi, kurumsal risk yönetimi sürecinin başarılı bir şekilde işlemesi için gerekli olan güvenilir veriyi ve kontrol ortamını sağlarken, kurumsal risk yönetimi ise iç kontrol faaliyetlerinin odaklanması gereken risklerin belirlenmesinde yol gösterici stratejik bir görevi üstlenir. Greapca ve Lungu (2024)'nun çalışması, iç denetim ve risk yönetimi araştırmaları arasındaki kavramsal ilişkileri ortaya koyarak, bu iki alanın giderek daha fazla iç içe geçtiğini ve COSO çerçevesinin bu entegrasyonda kritik bir rol oynadığını doğrulamaktadır. Bu entegre yaklaşım, organizasyonların riskleri sadece bir tehdit olarak değil, aynı zamanda stratejik hedeflere ulaşmada birer fırsat olarak da görmelerini sağlayan proaktif bir risk kültürü oluşturulmasına zemin hazırlamaktadır. Kurumsal yönetim literatüründe de iç denetim fonksiyonunun gelişen rolü, bu entegrasyonun önemini vurgulamaktadır. Hazaea vd. (2025), iç denetimin sadece finansal kontrolleri denetleyen bir fonksiyon olması yanında, kurumsal yönetimin stratejik bir ortağı haline geldiğini; çevresel değişiklikler, iklim krizi, jeopolitik zorluklar ve teknolojik gelişmeler gibi yeni risk alanlarında da güvence sağlama sorumluluğu üstlendiğini belirtmişlerdir.

Bu bölümün temel amacı, iç kontrol ve risk yönetimi konularını, güncel literatür ve uluslararası standartlar çerçevesinde kapsamlı bir şekilde ele almaktır. Bölümde, öncelikle iç kontrol ve kurumsal risk yönetimi kavramları, COSO tarafından geliştirilen temel çerçeveler üzerinden teorik olarak açıklanacaktır. Ardından, bu iki önemli yönetişim fonksiyonunun nasıl entegre edileceği, iç denetimin bu süreçteki rolü ve üçlü savunma hattı gibi modern yönetişim modelleri detaylı bir şekilde incelenecektir. İç kontrol etkinliğinin nasıl değerlendirileceği ve ölçüleceği, metodolojik olarak açıklanacaktır. Diğer

bölümlerde, dijitalleşmenin getirdiği yeni riskler ve fırsatlar, yapay zeka ve veri analitiği gibi teknolojik yeniliklerin iç kontrole etkileri ele alınacaktır. Son olarak, sürdürülebilirlik ve ESG faktörlerinin risk yönetimi ve iç kontrol sistemlerine entegrasyonu tartışılarak, konunun günümüz iş dünyası için stratejik önemi vurgulanacaktır.

1. İç Kontrol Sistemleri: Kavramsal Çerçeve ve Teorik Temeller

İç kontrol, bir organizasyonun hedeflerine ulaşmasını sağlamak amacıyla tasarlanmış, yönetim kurulu, yöneticiler ve diğer personel tarafından yürütülen entegre bir süreçtir. Tarihsel olarak yalnızca muhasebe bilgi sistemlerinin kontrollerini doğrulamaya odaklanan bir süreç olarak görülse de günümüzdeki modern yaklaşım, iç kontrolü çok daha geniş bir bakış açısıyla ele almaktadır. Bu modern yaklaşım, iç kontrolü; *faaliyetlerin etkinliği ve verimliliği*, *finansal raporlamanın güvenilirliği* ve *ilgili yasa ve düzenlemelere uyum* olmak üzere üç temel hedef kategorisinde değerlendirir. Organizasyonun stratejik hedeflerine ulaşmasını engelleyebilecek riskleri makul bir seviyede yönetmeyi amaçlayan bu süreç, bu yönüyle reaktif bir denetim faaliyetinden ziyade, proaktif bir yönetim aracı niteliği taşır. İç kontrolün bu geniş kapsamlı yapısı, onu sadece organizasyondaki bir bölümün veya fonksiyonun sorumluluğu olmaktan çıkarıp, organizasyonun tamamına yayılan ortak bir sorumluluk haline getirir (Öztürk ve Yılmaz, 2019).

1.1. İç Kontrol Kavramı ve Tanımı

COSO'ya göre iç kontrol, "*bir kurumun yönetim kurulu, yöneticileri ve diğer personeli tarafından etkilenen; faaliyetlerin etkinliği ve verimliliği, finansal raporlamanın güvenilirliği ve ilgili yasa ve düzenlemelere uyum hedeflerine ulaşılmasına ilişkin makul güvence sağlamak üzere tasarlanmış sistematik bir süreçtir*" (COSO, 1992; 2013). COSO'nun bu tanımı ile iç kontrolün statik bir süreç veya sadece bir politika kitapçığı olmadığı, aksine organizasyonun faaliyetleriyle iç içe geçmiş, dinamik ve sürekli bir süreç olduğu; "makul güvence" ifadesi ile de iç kontrol sistemlerinin mutlak bir güvence sağlayamayacağı vurgulanmaktadır. Hiçbir iç kontrol sisteminin insan faktörü, yanlış kararlar, gizli anlaşmalar veya maliyet-fayda kısıtları gibi doğal sınırlılıklar nedeniyle riskleri tamamen ortadan kaldıramamasından dolayı bu risklerin kabul edilebilir bir düzeye indirilmesi hedeflenir (COSO, 2013).

1.2. COSO İç Kontrol Entegre Çerçevesi

COSO İç Kontrol Entegre Çerçevesi, iç kontrol sistemlerinin tasarımı, uygulanması ve değerlendirilmesi için en yaygın kullanılan modeldir. İlk olarak 1992 yılında yayımlanan ve 2013 yılında güncellenen bu çerçeve, iç

kontrolü birbiriyle ilişkili beş bileşen ve bu bileşenleri destekleyen on yedi ilke temelinde yapılandırır. Bu bileşenler, bir organizasyonun hedeflerine ulaşmak için birlikte çalışması gereken unsurları temsil eder. Çerçevenin bu yapısal yaklaşımı, organizasyonlara iç kontrol sistemlerini daha sistematik bir şekilde analiz etme ve eksiklikleri belirleme imkanı tanır. Bibliyometrik analizler, COSO çerçevesinin akademik araştırmalarda merkezi bir rol oynadığını ve iç kontrolle ilgili çalışmaların büyük ölçüde bu model etrafında şekillendiğini göstermektedir (Öztürk ve Yılmaz, 2019; Qabajeh vd., 2024).

COSO çerçevesinin beş bileşeni şunlardır:

Kontrol Ortamı: İç kontrolün temelini oluşturan ve organizasyonun geneline yayılan dürüstlük, etik değerler ve yetkinlik standartlarını belirleyen kontrol ortamı, yönetim kurulunun ve üst yönetimin liderliği, felsefesi ve operasyon tarzı, organizasyon yapısı, yetki ve sorumlulukların dağıtımı gibi unsurları içerir. Güçlü bir kontrol ortamı, diğer iç kontrol bileşenlerinin etkinliği için bir ön koşuldur.

Risk Değerlendirmesi: Bu bileşen, organizasyonun hedeflerine ulaşmasını engelleyebilecek iç ve dış risklerin belirlenmesi ve analiz edilmesini içerir. Risk değerlendirme süreci, yönetimin bu risklerin olasılığını ve potansiyel etkilerini anlamasını ve bunlara nasıl yanıt verileceğine karar vermesini sağlar. COSO'nun ERM çerçevesi, bu bileşeni daha da detaylandırarak stratejik bir bakış açısı kazandırmıştır.

Kontrol Faaliyetleri: Risklerin azaltılması için yönetim tarafından verilen talimatların yerine getirilmesini sağlayan politika ve prosedürlerden oluşan kontrol faaliyetleri, manuel süreçler ve bilgi teknolojisi destekli süreçler için tasarlanmış önleyici ve tespit edici kontrolleri içererek, organizasyonun hedeflerine ulaşmasına yönelik risklerin etkili bir şekilde yönetilmesini sağlamaktadır. Onaylar, yetkilendirmeler, doğrulamalar, mutabakatlar, performans gözden geçirmeleri ve görevler ayrılığı gibi çok çeşitli faaliyetleri kapsayan kontrol faaliyetleri, organizasyonun tüm seviyelerinde ve tüm fonksiyonlarında uygulanır (Chalmers vd., 2019; COSO, 2013).

Bilgi ve İletişim: Etkin bir iç kontrol sistemi için, ilgili, kaliteli ve zamanında bilginin kurum içinde ve dışında belirlenmesi, elde edilmesi ve iletilmesi gerekir. Bilgi, personelin kontrol sorumluluklarını yerine getirmesini sağlamak için gerekli olup, yönetimin iç kontrolün tüm bileşenlerinin işleyişini desteklemek amacıyla hem iç hem de dış kaynaklardan elde ettiği veya ürettiği ilgili ve kaliteli bilgiyi kullanmasını içermektedir. İletişim ise, iç kontrol hedefleri, süreçleri ve sorumlulukları hakkında net mesajların yukarıdan aşağıya, aşağıdan yukarıya ve organizasyon geneline yayılmasını ifade eder (COSO, 2013; Chalmers vd., 2019; Chan vd., 2021).

İzleme Faaliyetleri: İzleme, iç kontrol sisteminin zaman içinde performansının ve kalitesinin değerlendirilmesi sürecidir. İç kontrollerin etkinliğini sürdürmek üzere devam eden ve/veya ayrı değerlendirmeler yoluyla periyodik olarak yapılan izleme faaliyetleri, iç kontrol sisteminin beklendiği gibi çalışıp çalışmadığını ve değişen koşullara uyum sağlayıp sağlamadığını belirler (COSO, 2013; Chalmers vd., 2019; Chan vd., 2021).

COSO İç Kontrol Entegre Çerçevesinin iç kontrol ile ilişkili beş bileşeni ve bu bileşenleri destekleyen on yedi ilke Tablo 1'de görülmektedir.

Tablo 1: COSO Çerçevesi: 5 Bileşen ve 17 İlke

Bileşen	İlke No	İlke
1. Kontrol Ortamı	**1**	Dürüstlük ve etik değerlere bağlılık
	2	Yönetim kurulu bağımsızlığı ve denetimi
	3	Yönetim yapısı, yetki ve sorumluluklar
	4	Yetkinlik için bağlılık
	5	İç kontrol sorumluluklarını yerine getirme konusunda hesap verebilirlik
2. Risk Değerlendirmesi	**6**	İç kontrolü değerlendirmede uygun hedefler belirleme
	7	Riskleri belirleme ve analiz etme
	8	Hile potansiyelini değerlendirme
	9	İç kontrol sistemini önemli ölçüde etkileyebilecek değişiklikleri belirleme ve değerlendirme
3. Kontrol Faaliyetleri	**10**	Riskleri makul bir seviyeye indirmeye katkıda bulunan kontrol faaliyetlerini seçme ve geliştirme
	11	Teknoloji üzerinde genel kontrol faaliyetlerini seçme ve geliştirme
	12	Politikalar ve prosedürler aracılığıyla kontrol faaliyetlerini uygulama
4. Bilgi ve İletişim	**13**	İlgili ve kaliteli bilgiyi elde etme, üretme ve kullanma
	14	İç kontrol hedeflerinin yerine getirilmesini desteklemek için dahili olarak bilgi iletişimi
	15	İç kontrol hedeflerinin yerine getirilmesini desteklemek için dış taraflarla bilgi iletişimi
5. İzleme Faaliyetleri	**16**	İç kontrolün bileşenlerinin mevcut olup olmadığını ve işleyip işlemediğini belirlemek için sürekli ve/veya ayrı değerlendirmeler gerçekleştirme
	17	İç kontrol eksikliklerini zamanında değerlendirme ve üst yönetime bildirme

Kaynak: COSO (2013). Internal Control — Integrated Framework. Durham, NC.

1.3. İç Kontrol Türleri ve Sınıflandırması

Organizasyonların risklere karşı çok boyutlu bir savunma mekanizması oluşturmasına yardımcı olan iç kontrol, risk yönetiminin temel bir bileşeni olarak organizasyonların hedeflerine ulaşmalarında makul güvence sağlar (Chalmers vd., 2019; COSO, 2013). İç kontrol sistemleri amaçlarına ve uygulanma zamanlarına göre aşağıdaki gibi sınıflandırılabilir:

Önleyici Kontroller: Hata ve hilelerin meydana gelmeden engellenmesi için tasarlanan önleyici kontroller görevler ayrılığı, yetkilendirme ve onay mekanizmaları, erişim kontrolleri ve güvenlik duvarları gibi uygulamalardan oluşmaktadır. Sorunların ortaya çıkmasını önceden önlemek, meydana geldikten sonra bunları tespit edip düzeltmeye çalışmaktan çok daha düşük maliyetli bir yaklaşım olduğundan önleyici kontroller genellikle maliyet etkinliği yüksek olan kontrol türü olarak kabul edilirler (COSO, 2013; Chalmers vd., 2019).

Tespit Edici Kontroller: Önleyici kontrollerin engelleyemediği hata ve hileleri ortaya çıkarmak için tasarlanan tespit edici kontroller banka mutabakatları, envanter sayımları, denetim kayıtlarının gözden geçirilmesi ve performans raporları gibi uygulamalardan oluşur. Bu kontroller, bir sorunun ne zaman ve nerede meydana geldiğini belirlemeye yardımcı olur ve önleyici kontrollerin etkin şekilde çalışıp çalışmadığına dair kanıt sağlar (COSO, 2013; Länsiluoto vd., 2016; Chalmers vd., 2019).

Düzeltici Kontroller: Tespit edilen hata ve hilelerin nedenlerini ortadan kaldırmak ve olumsuz etkilerini düzeltmek için kullanılan düzeltici kontroller veri yedeklerinden geri yükleme, disiplin prosedürleri ve süreç iyileştirme planlarından oluşur. Bu kontroller, benzer sorunların gelecekte tekrarlanmasını önlemeyi amaçlar (COSO, 2013).

Yönlendirici Kontroller: Belirli bir hedefe veya sonuca ulaşılmasını teşvik etmek ve yönlendirmek için tasarlanan yönlendirici kontroller eğitim programları, politika ve prosedür el kitapları ve teşvik sistemleri gibi uygulamalar ile personelin istenen şekilde davranmasını sağlamaya yönelik yönlendirici kontrollerden oluşur (COSO, 2013).

Etkin bir iç kontrol sistemi, yukarıda yer alan farklı iç kontrol türlerini, organizasyonun risk yapısına ve hedeflerine uygun bir şekilde bir araya getirerek dengeli bir yapı oluşturur. Araştırmalar, kontrol faaliyetlerinin etkin bir şekilde tasarlanması ve uygulanmasının organizasyonel etkinlik üzerinde önemli bir etkiye sahip olduğunu göstermektedir (Feng vd., 2015; Länsiluoto vd., 2016; Chang vd., 2019).

2. Kurumsal Risk Yönetimi: COSO ERM Çerçevesi ve Uygulamaları

İç kontrol sistemlerinin etkinliği, büyük ölçüde organizasyonun riskleri anlama ve yönetme kapasitesine bağlıdır. Bu çerçevede, Kurumsal Risk Yönetimi (ERM), riskleri izole ve parçalı bir bakış açısıyla değerlendirmek yerine, organizasyonun bütününü içeren, stratejik amaçlarla uyumlu ve portföy odaklı bütünsel bir yönetim yaklaşımıdır. ERM, risk yönetimini sadece potansiyel kayıpları önlemeye yönelik bir savunma mekanizması olarak görmez; aynı zamanda riskleri, stratejik avantajlar sağlamak ve değer yaratmak için birer fırsat olarak da değerlendirir. Bu proaktif ve stratejik bakış açısı, ERM'yi geleneksel risk yönetimi yaklaşımlarından ayırarak onu kurumsal yönetişimin vazgeçilmez bir unsuru haline getirir. Organizasyonlar, yüksek belirsizlik içeren bir ortamda faaliyetlerini yürütürken, ERM onlara bu belirsizlikleri yönetme, dayanıklılıklarını artırma ve stratejik hedeflerine ulaşabilme yeteneği kazandırır (COSO, 2024a).

2.1. Risk Kavramı ve Risk Yönetiminin Temelleri

Bir olayın meydana gelme olasılığı ile bu olayın hedefler üzerindeki etkisinin bir bileşkesi olan risk (Aven, 2016), ERM çerçevesinde "*hedeflere ulaşmayı etkileyebilecek olayların belirsizliği*" olarak tanımlanır. Bu tanım, riskin sadece kaçınılması gereken bir tehlike olmadığını, aynı zamanda yönetilmesi gereken bir belirsizlik olduğunu vurgular. Risk yönetiminin temelinde *risk iştahı* ve *risk toleransı* olmak üzere iki önemli kavram bulunmaktadır (COSO, 2017). Risk iştahı, bir organizasyonun hedeflerine ulaşmak için stratejik olarak kabul etmeye istekli olduğu toplam risk miktarını ve türünü ifade eder. Üst yönetim tarafından belirlenen bu stratejik seviye, kurumun risk kültürünü ve genel yaklaşımını şekillendirir. Risk toleransı ise, belirli bir risk veya risk kategorisi için kabul edilebilir sapma düzeyini belirten daha operasyonel bir kavramdır (Gontarek ve Bender, 2019).

Riskler, *stratejik riskler* (pazar riski, teknolojik değişim riski, yanlış strateji seçimi, birleşme ve satın alma riskleri, yatırım kararı riskleri), *operasyonel riskler* (süreç hataları, insan kaynakları riskleri, tedarik zinciri riskleri, teknoloji ve sistem arızaları), *raporlama riskleri* (hatalı finansal tablolar, veri güvenilirliği problemleri, iç kontrol eksiklikleri, şeffaflık eksikliği) ve *uyumluluk riskleri* (yasa ve düzenlemelere uyulmamasından kaynaklanan riskler) olmak üzere dört ana başlık altında sınıflandırılır (COSO, 2024a)

2.2. COSO Kurumsal Risk Yönetimi (ERM) Çerçevesi

COSO tarafından ilk olarak 2004 yılında yayımlanan ve 2017 yılında *"Strateji ve Performansla Bütünleşik Kurumsal Risk Yönetimi"* adıyla güncellenen ERM çerçevesi, bu alandaki en etkili ve yaygın kabul gören modeldir. 2017 yılında yapılan güncelleme, ERM'yi kurumun strateji belirleme sürecinden performans yönetimine kadar tüm yaşam döngüsüyle daha sıkı bir şekilde bütünleştirmiştir. Bu yeni çerçeve, riskin kurum kültürü, strateji ve hedeflerle olan dinamik ilişkisine odaklanır. Model, organizasyonların risk yönetimi süreçlerini strateji belirleme ve performans yönetimi ile entegre etmelerini sağlayan birbiriyle ilişkili beş bileşen ve bu bileşenleri destekleyen yirmi ilke üzerine kuruludur (COSO, 2017). Bu yapı, ERM'nin sadece bir prosedürler listesi olmadığını, aynı zamanda kurumun yönetişim ve kültürünün bir parçası olduğunu gösterir. COSO çerçeveleri iç denetim ve risk yönetimi fonksiyonları arasında bir entegrasyon mekanizması olarak işlev görmekte ve bu iki fonksiyonun bütünleşmesini desteklemektedir (Greapca ve Lungu, 2024). COSO ERM çerçevesinin beş bileşeni şunlardır:

Yönetişim ve Kültür: Çerçevenin temel taşını oluşturarak, kurumun risk yönetimi felsefesini, etik değerlerini ve risk kültürünü şekillendiren yönetişim ve kültür, yönetim kurulunun gözetim sorumluluklarını, organizasyonel yapıyı ve risk yönetimi konusundaki kurumsal tonu belirleyerek, ERM'nin etkinliği için gerekli olan kültürel altyapıyı oluşturur (Farrell ve Gallagher, 2015). ERM'nin başarısı için kritik bir öneme sahip olan güçlü bir risk kültürü (Hazaea vd., 2025), çalışanların risk bilinciyle hareket etmelerini ve karar alma süreçlerinde risk perspektifini içselleştirmelerini sağlar (Power, 2009). Yönetişim, ERM için tonu belirler ve kurumun denetim sorumluluklarını şekillendirirken kültür ise etik değerler, istenen davranışlar ve risk anlayışıyla ilgilidir.

Strateji ve Hedef Belirleme: Stratejik planlama sürecine entegre edilen ERM'nin bu bileşeni kurumun misyon ve vizyonu doğrultusunda stratejik alternatiflerin değerlendirilmesi, risk iştahının tanımlanması ve iş hedeflerinin belirlenmesi süreçlerini kapsar. Bu süreçte, potansiyel stratejilerin risk profilleri analiz edilerek, kurumun risk kapasitesi ve risk toleransı ile uyumlu stratejik seçimler yapılır (Kaplan ve Mikes, 2016). Risk iştahının açık bir şekilde tanımlanması, kurum genelinde tutarlı risk kararlarının alınmasını mümkün kılar (Gontarek, 2016).

Performans: ERM uygulamalarının temelini oluşturan bu bileşen kurumun, iş hedeflerine ulaşmasını etkileyebilecek risklerin tanımlanması, değerlendirilmesi, önceliklendirilmesi ve bunlara yönelik yanıtların geliştirilmesi süreçlerini içerir. Bu bileşen kapsamında, kurumun hedeflerine ulaşmasını etkileyebilecek riskler sistematik olarak analiz edilir, risk portföyü perspektifinden değerlendirilir ve

uygun risk yanıt stratejileri belirlenir (Mikes ve Kaplan, 2015). Kurumun tüm varlıklarını, birimlerini ve fonksiyonlarını kapsayan bir portföy görünümüyle ele alan bu süreç, risklerin birbirleriyle olan etkileşimlerinin ve kümülatif etkilerinin değerlendirilmesini sağlar (McShane vd., 2011).

Gözden Geçirme ve Revizyon: Bu bileşen ERM süreçlerinin ve risk yönetimi performansının sürekli olarak izlenmesi, değerlendirilmesi ve iyileştirilmesi faaliyetlerini kapsar; hem bireysel risk yanıtlarının etkinliğini hem de ERM sisteminin bütünsel performansını değerlendirerek değişen iç ve dış koşullara uyumunu sağlar (Beasley vd., 2015). Risk raporlarının analizi ve ERM uygulamalarının etkinliğinin değerlendirilmesi kurumsal risk yönetimi yetkinliklerinin geliştirilmesi için sistematik olarak kullanılır (Hayne ve Free, 2014).

Bilgi, İletişim ve Raporlama: Sürekli olarak bilgi toplama ve paylaşma sürecine dayanan bu bileşen risk bilgisinin organizasyon genelinde etkin bir şekilde tespit edilmesi, işlenmesi ve paylaşılması süreçlerini yönetir. Hem iç hem de dış kaynaklardan gelen verileri kullanarak riskler hakkında bilgi üreten ve bu bilgiyi kilit paydaşlara raporlayan bu bileşen hem iç hem de dış paydaşlarla risk iletişimini, teknoloji altyapısının kullanımını ve risk raporlama mekanizmalarını içerir (Meidell ve Kaarbøe, 2017). Zamanında, doğru ve ilgili risk bilgisinin uygun seviyelere iletilmesi, bilinçli karar alma süreçlerini destekler ve kurumsal şeffaflığı artırır (Soin veCollier, 2013).

Bu beş bileşen, birbirleriyle dinamik bir etkileşim içinde çalışarak, organizasyonların belirsizlikleri yönetmelerini, fırsatları değerlendirmelerini ve sürdürülebilir değer yaratmalarını sağlayan bütünsel bir risk yönetimi ortamı oluşturur (Fraser ve Simkins, 2016). COSO ERM çerçevesinin bu yapısı, risk yönetiminin izole bir fonksiyon olmaktan çıkarak, stratejik planlama ve performans yönetimi süreçlerinin ayrılmaz bir parçası haline gelmesini temin eder (Bromiley vd., 2015).

Tablo 2: COSO Kurumsal Risk Yönetimi (ERM) Çerçevesi 2017

2.3. Risk Yönetimi Süreci

Risk yönetimi, belirli adımlardan oluşan sistematik ve döngüsel bir süreçtir. Bu süreç, organizasyonların riskleri tutarlı ve kontrollü bir şekilde yönetmelerini sağlar. Etkin bir risk yönetimi sürecinin temel aşamaları Şekil 1'de görülmektedir.

Şekil 1. Risk Yönetimi Sürecinin Döngüsel Yapısı

Kaynak: Goswami (2024) çalışmasından uyarlanmıştır.

1) *Risklerin Belirlenmesi:* Kurumun hedeflerini etkileyebilecek potansiyel iç ve dış olayların veya belirsizliklerin tanımlandığı bu aşamada beyin fırtınası, SWOT analizi, süreç haritalama ve uzman görüşleri gibi çeşitli teknikler kullanılır.
2) *Risk Analizi ve Değerlendirmesi:* Belirlenen risklerin gerçekleşme olasılıklarının ve etkilerinin analiz edildiği bu aşama risklerin önem derecesini ve önceliğini belirlemeye yardımcı olur. Değerlendirme sonucunda riskler, genellikle bir risk haritası üzerinde görselleştirilir.
3) *Risk Yanıtı:* Kurumun risk iştahı ve risk toleransı doğrultusunda, risklerin potansiyel etkilerini yönetmek için tasarlanan risk yanıtı stratejileri, tanımlanan ve değerlendirilen risklere karşı kurumun geliştirebileceği stratejileri ifade eder. Dört temel risk yanıt stratejisi bulunmaktadır. Bunlar:
    a) Riskten Kaçınma: Bu strateji belirli bir riski tetikleyebilecek faaliyetlerden tamamen uzak durulmasını veya bu faaliyetlerin

sonlandırılmasını içerir. Bu strateji riskin potansiyel etkisi kurumun risk toleransını aştığında veya risk-getiri dengesi olumsuz olduğunda tercih edilir.

b) Riski Azaltma: Bu strateji, riskin gerçekleşme olasılığını veya potansiyel etkisini düşürmek için kontrol mekanizmalarının uygulanmasını içerir. Bu strateji, riskin oluşmasını engelleyen önleyici kontroller ve risk gerçekleştiğinde erken uyarı sağlayan tespit edici kontroller aracılığıyla gerçekleştirilir.

c) Riski Paylaşma veya Transfer Etme: Bu strateji, riskin finansal etkilerinin sigorta poliçeleri, reasürans anlaşmaları, hedging işlemleri ve outsourcing uygulamaları yoluyla üçüncü taraflara aktarılması yaklaşımıdır.

d) Riski Kabul Etme: Bu strateji, mevcut risk seviyesinin kurum için kabul edilebilir olduğu ve ek kontrol maliyetlerinin potansiyel faydaları aşacağı durumlarda benimsenir.

4) Risk İzleme ve Raporlama: Uygulanan risk yanıt stratejilerinin etkinliğinin ve risk profilindeki değişikliklerin sürekli olarak izlendiği aşamadır. Risk izleme, tanımlanmış risklerin ve uygulanan kontrol mekanizmalarının etkinliğinin sürekli olarak gözlemlenmesi, risk profilindeki değişimlerin tespit edilmesi ve yeni risklerin belirlenmesi süreçlerini kapsar. Bu süreç, anahtar risk göstergelerinin (KRI) takibi, kontrol testlerinin yapılması ve risk olaylarının kaydedilmesi gibi sistematik faaliyetler aracılığıyla gerçekleştirilir. Risk raporlama ise, toplanan risk verilerinin analiz edilerek, ilgili paydaşlara zamanında, doğru ve anlaşılır formatta sunulmasını sağlayan önemli bir iletişim mekanizmasıdır. Etkili raporlama, kurumdaki tüm farklı kademelerin ihtiyaçlarına uygun detaylı risk raporlarını içererek, kurumsal karar alma süreçlerini destekler ve risk kültürünün güçlenmesine katkıda bulunur. Risk göstergeleri ve periyodik raporlar, yönetimin riskler hakkında güncel bilgi sahibi olmasını ve gerekli durumlarda müdahale etmesini sağlar.

Etkili risk yönetimi, bu dört stratejinin en uygun bileşiminin oluşturulmasını zorunlu kılar. COSO Kurumsal Risk Yönetimi Çerçevesi, risk yanıt stratejilerinin kurum genelinde bir bütün olarak ele alınmasını ve portföy yaklaşımıyla değerlendirilmesini önemle vurgulamaktadır (Baxter vd., 2013; COSO, 2017). Literatür, kurumların her bir risk için en uygun yanıt stratejisini belirlerken, maliyet-fayda analizini, kurumsal hedefleri ve kaynak kısıtlarını dikkate alması gerektiğini göstermektedir (Lundqvist, 2015; Malik vd., 2020). Araştırmalar, risk yönetimi stratejilerinin etkinliğinin sürekli izlenmesinin ve

değişen koşullara göre revize edilmesinin kurumsal performans üzerinde olumlu etkiye sahip olduğunu ortaya koymaktadır (Callahan ve Soileau, 2017; Cohen vd., 2017). Risk yönetimi sürecinin dinamik yapısı, kurumların risk yanıtlarını düzenli olarak gözden geçirmelerini ve iç ve dış çevredeki değişikliklere uyum sağlamalarını gerektirmektedir (Beasley vd., 2015; Florio ve Leoni, 2017). Özellikle, risk komitelerinin etkin gözetim rolü, seçilen stratejilerin kurumsal hedeflerle uyumlu kalmasını sağlamada kritik öneme sahiptir (Malik vd., 2020).

2.4. Risk Değerlendirme Metodolojileri

Risk değerlendirme metodolojileri, kurumların karşı karşıya oldukları belirsizlikleri sistematik olarak tanımlamak, analiz etmek ve önceliklendirmek için kullanılmaktadır. Literatürde, bu metodolojiler genel olarak *nitel*, *nicel* ve *senaryo* bazlı olmak üzere üç temel başlık altında sınıflandırılmaktadır (Aven, 2016; Hopkin, 2018). Her bir metodoloji, farklı kurumsal çerçevede ve risk türlerinde kendine özgü avantajlar sunarak, kurumların risk profillerini daha etkin bir şekilde yönetmelerine olanak tanımaktadır.

Nitel Risk Değerlendirme: Risklerin olasılık ve etki düzeylerini tanımlayıcı ölçekler kullanarak kategorize eden metodolojileri kapsar (Cox, 2008). Bu metodolojide riskler genellikle "düşük", *"orta"*, *"yüksek"* veya *"çok yüksek"* gibi kategorik sınıflandırmalar kullanılarak değerlendirilir ve risk matrisleri aracılığıyla görselleştirilir (Duijm, 2015). Nitel metodolojilerin en önemli avantajı, uzman görüşlerinin ve deneyimlerin sistematik bir şekilde risk değerlendirme sürecine dahil edilebilmesi ve sayısal veri eksikliğinde dahi uygulanabilir olmasıdır (Renn, 2008). Ancak, bu metodolojinin sübjektif olması ve farklı değerlendiriciler arasında tutarlılık sağlama zorluğu en önemli sınırlılıklarını oluşturmaktadır (Ball ve Watt, 2013).

Nicel Risk Değerlendirme: Risklerin olasılık ve etkilerini Monte Carlo simülasyonu, karar ağaçları, Value at Risk (VaR) modelleri, Bayesian ağları ve duyarlılık analizi gibi istatistiksel ve matematiksel teknikler kullanarak sayısal ve genellikle parasal değerlerle ifade eden bu metodoloji, daha objektif ve karşılaştırılabilir sonuçlar sunar (Bedford ve Cooke, 2001; Vose, 2008). Daha fazla veri, zaman ve uzmanlık gerektiren bu metodoloji, risk pozisyonunun parasal değer olarak ifade edilmesini, farklı risk senaryolarının karşılaştırılmasını ve en uygun risk yanıt stratejilerinin belirlenmesini kolaylaştırmaktadır (McNeil vd., 2015). Bu metodolojilerin etkinliği, güvenilir veri kaynaklarının varlığına ve kullanılan modellerin varsayımlarının geçerliliğine bağlıdır (Embrechts vd., 2013).

Senaryo Analizi ve Stres Testleri: Büyük bir ekonomik kriz veya doğal afet gibi potansiyel gelecek senaryolarının kurum üzerindeki etkilerini

değerlendirmek için kullanılan bu metodolojiler (Rebonato, 2010), özellikle düşük olasılıklı ancak yüksek etkili risklerin anlaşılmasına yardımcı olarak kurumun dayanıklılığını test eder (Taleb, 2007). Senaryo analizi, alternatif gelecek senaryolarının yapılandırılmış bir şekilde geliştirilmesini ve bunların potansiyel etkilerinin değerlendirilmesini içerirken (Wright ve Cairns, 2011), stres testleri özellikle finansal kurumlar özelinde anormal piyasa koşullarının simülasyonuna odaklanmaktadır (Drehmann, 2008).

Günümüzde birçok kurum, risk değerlendirme süreçlerinde büyüklüklerine, sektörlerine, risk kültürlerine ve mevcut veri kalitesine bağlı olarak nitel ve nicel metodolojileri içeren bütünleşik yaklaşımları benimsemektedir (Lam, 2014). Bu bütünleşik yaklaşımlar, nitel değerlendirmelerin esnekliğini nicel analizlerin kesinliğiyle birleştirerek, daha kapsamlı bir risk profili sağlamaktadır (Power, 2007; Mikes, 2011). Etkin risk yönetimi için kurumların büyüklüklerine, risk profillerine ve kaynak kapasitelerine uygun risk değerlendirme metodolojilerini seçmeleri ve uygulamaları kritik öneme sahiptir. Risk değerlendirme metodolojilerinin seçimi ve uygulanması, kurumsal risk kültürünün gelişimi ve risk yönetimi olgunluk seviyesinin artırılması açısından da belirleyici bir rol oynamaktadır (Fraser ve Simkins, 2016).

3. İç Kontrol ve Risk Yönetiminin Entegrasyonu

Kurumsal yönetişimin etkinliği, kurumun tüm fonksiyonlarının birbiriyle uyumlu ve entegre bir şekilde çalışabilme kapasitesine bağlıdır. Bu çerçevede, iç kontrol ve kurumsal risk yönetimini birbirinden ayrı olarak ele almak, verimliliği esas alan günümüzün yönetişim anlayışıyla bağdaşmayan bir yaklaşımdır. Bu iki fonksiyon, yapıları gereği birbirini tamamlayan ve aralarında ilişki bulunan süreçlerdir (Bento vd., 2018).

Etkin bir entegrasyon, risklerin daha bütüncül bir bakış açısıyla anlaşılmasını, kaynakların en önemli risk alanlarına odaklanmasını ve bunun sonucunda kurumun stratejik hedeflerine ulaşma olasılığının artırılmasını sağlar. Bu entegrasyon, kurumun sadece risklere karşı savunma mekanizmalarını güçlendirmekle kalmaz, aynı zamanda risk ve kontrol bilincini kurum kültürünün ayrılmaz bir parçası haline getirerek daha dayanıklı ve proaktif bir yapı oluşturur.

İç kontrol, COSO çerçevesine göre, tüm kontrol ortamını kapsadığı ve iç kontrolün önemli bir yönünün risk değerlendirmesi olduğu için, risk yönetimi ile yakından bağlantılıdır (Jones, 2008). Risk yönetiminin, kurumsal hedeflerin oluşturulmasında, iş süreçlerinde ve genel olarak tüm kurumsal faaliyetlerde entegre edilmesi gerekmektedir (Arena vd., 2017; Power, 2009).

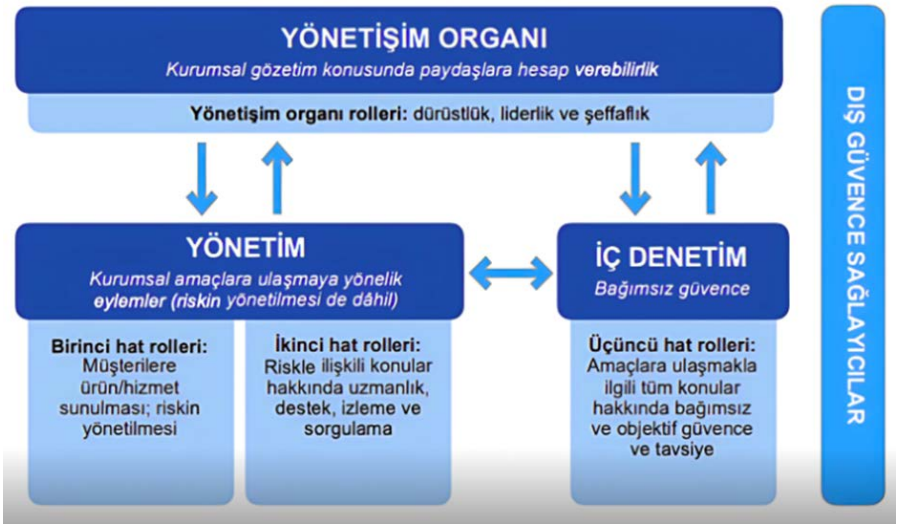
Kurumsal risk yönetimi uygulamalarının etkinliği, ERM kültürü ve bilgi sistemleri desteği bağlamında değerlendirilmelidir. ERM ve firma performansı arasındaki ilişki, ERM ile çevresel belirsizlik, sektör rekabeti, firma büyüklüğü, firma karmaşıklığı ve yönetim kurulu gözetimi gibi faktörler arasındaki uygun eşleşmeye bağlıdır (Gordon vd., 2009). Kurumların bu entegrasyonu başarılı bir şekilde gerçekleştirebilmeleri için hem iç kontrol mekanizmalarının hem de risk yönetimi süreçlerinin stratejik planlama ve karar alma süreçlerine gömülü olması gerekmektedir (COSO, 2017).

3.1. İç Kontrol ve Risk Yönetimi İlişkisi

Kurumsal risk yönetimi (ERM), kurumun hedeflerini etkileyebilecek potansiyel risklerin belirlenmesi, değerlendirilmesi ve bunlara verilecek yanıtların stratejik düzeyde kararlaştırılmasına odaklanır (Gordon vd., 2009; COSO, 2017). İç kontrol ise, ERM sürecinde belirlenen bu riskleri azaltmak için tasarlanan ve uygulanan politika, prosedür ve faaliyetlerdir (Beasley vd., 2005; COSO, 2013). Dolayısıyla, ERM, iç kontrol sistemi için stratejik bir hareket tarzı belirlerken, iç kontrol sistemi de ERM stratejilerinin operasyonel düzeyde uygulanmasını sağlayan mekanizmaları oluşturur (Baxter vd., 2013). Bu sinerjik ilişki, risklerin sadece uyum sağlanması gereken bir yükümlülük olarak değil (Chi vd., 2024), aynı zamanda etkin bir şekilde yönetildiğinde rekabet avantajı yaratabilecek bir unsur olarak görülmesini teşvik eder (Hoyt ve Liebenberg, 2011; Malik vd., 2020).

3.2. Üç Savunma Hattı Modeli

İç kontrol ve risk yönetiminin entegrasyonunu yapılandırmak için en yaygın kabul gören modellerden biri, Uluslararası İç Denetçiler Enstitüsü (IIA) tarafından geliştirilen *"Üç Savunma Hattı"* modelidir. Bu model, risk yönetimi ve kontrol ile ilgili görev ve sorumlulukları, kavram karmaşıklığını önlemek ve koordinasyonu sağlamak amacıyla üç gruba ayırır. 2020 yılında IIA tarafından güncellenerek *"Üç Hat Modeli"* olarak yeniden kavramsallaştırılan, değer yaratma ve koruma üzerine daha fazla odaklanarak yönetişimin önemini vurgulayan bu model Şekil 2'de görülmektedir.



Şekil 2: Üçlü Savunma Hattı Modeli

Kaynak: İç Denetim Enstitüsü (IIA) (2020)

Birinci Hat: Operasyonel Yönetim. Müşterilere ürün veya hizmet sunan operasyonel birimlerin yöneticileri ve çalışanlarından oluşan bu hat, günlük operasyonlar sırasındaki riskleri belirlemek, değerlendirmek ve yönetmek için gerekli kontrol faaliyetlerinin uygulanmasından, süreçlerin ve kontrollerin tasarımından ve etkin bir şekilde işletilmesinden birinci derecede sorumludur.

İkinci Hat: Risk Yönetimi ve Uyum Fonksiyonları. Birinci hattın risk yönetimi faaliyetlerini destekleyen ve denetleyen uzman fonksiyonlardan oluşan ikinci hatta, kurumsal risk yönetimi, uyum, kalite, bilgi güvenliği ve finansal kontrol gibi birimler yer alır. İkinci hat, risk yönetimi çerçevelerini, politikalarını ve araçlarını geliştirir; birinci hatta uzmanlık ve danışmanlık sağlar ve risk yönetimi uygulamalarının tutarlılığını ve etkinliğini izler.

Üçüncü Hat: İç Denetim. Üçüncü hat olan iç denetim, yönetim kuruluna ve üst yönetime, yönetişim, risk yönetimi ve iç kontrol süreçlerinin etkinliği hakkında bağımsız ve objektif bir güvence sağlar. Birinci ve ikinci hatlardan bağımsız olan iç denetim, doğrudan denetim komitesine veya yönetim kuruluna raporlama yapar. Bu bağımsızlık, iç denetimin değerlendirmelerinde tarafsız olmasını ve kurumun genel risk ve kontrol çerçevesi hakkında güvenilir bir görüş sunmasını sağlar. İç denetimin ayrıca kurum genelinde kontrol kültürünün tasarımında ve işleyişinde etkili olduğuna dair düzenleyicilere ve dış denetçilere güvence sağlama görevi de bulunmaktadır. Risk tabanlı iç denetim

yaklaşımı, denetim kaynaklarının en önemli risk alanlarına odaklanmasını temin eder (Almgrashi ve Mujalli, 2024).

3.3. İç Denetimin Risk Yönetimindeki Rolü

Modern iç denetim anlayışı, iç denetim fonksiyonun rolünü geleneksel finansal denetimin dışına çıkararak kurumsal yönetişimin ve risk yönetiminin stratejik bir ortağı haline getirmiştir. Literatürde, iç denetim araştırmalarının son yıllarda denetim komitesi etkinliği, iç denetim kalitesi ve risk değerlendirmesi gibi konulara giderek daha fazla odaklanılması (Chi vd., 2024) iç denetimin risk yönetimindeki rolünün ne kadar önemli hale geldiğinin bir kanıtıdır. ERM sürecinin tüm aşamalarında önemli bir rol oynayan iç denetim, *risk belirleme aşamasında*, kurumun gözden kaçırdığı potansiyel riskleri ortaya çıkarabilir; *risk değerlendirme aşamasında*, yönetimin risk analizlerinin makul olup olmadığını değerlendirir; *risk yanıtı aşamasında* ise uygulanan kontrol faaliyetlerinin riskleri istenen seviyeye indirip indirmediğini test eder. İç denetim, ERM çerçevesinin kendisinin etkinliğini değerlendirerek yönetim kuruluna güvence verir. Bu ise iç denetimin sistemin bütününü denetlediği anlamına gelir.

4. İç Kontrol Etkinliğinin Değerlendirilmesi ve Ölçümü

Bir iç kontrol sisteminin mevcut olması, kurumun stratejik ve operasyonel hedeflerine ulaşmasında tek başına yeterli değildir. Tasarlanan kontrollerin amaçlandığı gibi çalışıp çalışmadığı ve hedeflere ulaşmada makul güvence sağlayıp sağlamadığının göstergesi olan iç kontrol etkinliği, düzenli olarak değerlendirilmesi gereken önemli bir unsurdur. İç kontrol etkinliğinin değerlendirilmesi, yönetime ve yönetim kuruluna sistemin işleyişi hakkında önemli bilgiler sunar, zayıflıkların zamanında tespit edilip giderilmesine olanak tanır ve sürekli iyileştirme kültürünü destekler. Bu süreç, iç kontrolü statik bir yapı olmaktan çıkarıp (Länsiluoto vd., 2016), kurumu değişen iç ve dış koşullara uyum sağlayan, dinamik bir mekanizma haline getirir. Etkinlik değerlendirmesi, aynı zamanda, Sarbanes-Oxley (SOX) gibi düzenlemeler kapsamında üst yönetimin yasal sorumluluklarını yerine getirmesinin de temel bir gereğidir.

4.1. İç Kontrol Etkinliği

COSO çerçevesine göre, bir iç kontrol sisteminin etkin olarak kabul edilebilmesi için iki temel koşulun sağlanması gerekmektedir: Bu koşulların birincisi, iç kontrolün beş bileşeninin ve ilgili on yedi ilkenin tamamının mevcut olması ve uygulanmasıdır. İkincisi ise, bu beş bileşenin hedeflere ulaşılmasına yönelik olarak bütünleşik bir şekilde birlikte çalışmasıdır. Bir sistemin etkinliği,

kurumun operasyonel, raporlama ve uyum hedeflerine ulaşması konusunda yönetime mutlak değil, *"makul bir güvence"* sağlar.

4.2. Değerlendirme Metodolojileri

İç kontrol etkinliğini değerlendirmek için genellikle birbirini tamamlayıcı nitelikte olan, kurumun büyüklüğüne, karmaşıklığına ve risk profiline göre uyarlanan çeşitli metodolojiler kullanılmaktadır. Bu metodolojiler aşağıda yer almaktadır.

Kontrol Öz Değerlendirmesi: Bir birim veya fonksiyondaki yönetici ve çalışanların, kendi iş süreçlerindeki riskleri ve bu riskleri yöneten kontrollerin etkinliğini yapılandırılmış bir şekilde bizzat değerlendirdiği bir metodolojidir. Bu yaklaşım, kontrol sorumluluğunu ve bilincini kurumun geneline yayması, risklerin ve kontrol zayıflıklarının operasyonun içinde tespit edilmesini sağlaması gibi önemli avantajlar sunar (Öztürk ve Yılmaz, 2019).

Kontrol Testleri ve Denetim Prosedürleri: Genellikle iç denetçiler veya bağımsız denetçiler tarafından yürütülen bu metodoloji, belirli kontrol faaliyetlerinin tasarımının uygunluğunu/etkinliğini ve uygulamasının tutarlılığını/etkinliğini test etmeyi kapsar. Gözlem, soruşturma, belgelerin ve kayıtların incelenmesi ile yeniden hesaplama gibi denetim teknikleri kullanılarak, kontrolün gerçekten beklendiği gibi çalışıp çalışmadığına dair kanıt toplanır. Yönetimin kendi kontrol sistemine ilişkin öz değerlendirmesinin doğasında bulunan subjektifliği, bağımsız ve objektif güvence sağlayarak dengeleyen kontrol testleri, operasyonel süreçler ve uyumluluk üzerindeki iç kontrollerin etkinliğini değerlendirmede önemli bir rol oynamakta ve iç denetim özelliklerinin kalitesi bu testlerin güvenilirliğini doğrudan etkilemektedir (Chalmers vd., 2019; Chang vd., 2019; Lu vd., 2011).

Sürekli İzleme ve Sürekli Denetim: Sürekli denetim, iç veya dış denetçilerin bir kurumun bilgi teknolojileri sistemleri, süreçleri, işlemleri ve kontrolleri üzerinde teknoloji tabanlı otomatik sistemler kullanarak sürekli veya sık aralıklarla denetim kanıtlarını toplama metodolojisidir. Sürekli izleme ise yönetimin sorumluluğunda olan ve iç kontrollerin etkin bir şekilde çalışıp çalışmadığını sürekli olarak değerlendiren bir yönetim süreci olarak tanımlanmakta ve Üç Savunma Hattı Modeli'nde birinci veya ikinci savunma hattı tarafından yürütülmektedir (Vasarhelyi vd., 2012). Her iki yaklaşım da bilgi teknolojilerini ve veri analitiğini temel alan otomatik sistemler kullanarak geleneksel periyodik değerlendirmelerin ötesine geçmekte, gerçek zamanlı sürekli değerlendirme imkânı sunmaktadır (Acar vd., 2021). Sürekli denetim, üçüncü savunma hattı olan iç denetim fonksiyonunun risk ve kontrol değerlendirmelerini devam eden bir temelde yapmasını sağlarken, sürekli izleme yönetimin kontrol etkinliğine

ilişkin sürekli görünürlük elde etmesine olanak tanımaktadır (Nigrini ve Johnson, 2008). Bu iki yaklaşımın entegrasyonu, organizasyonlara sürekli güvence sağlamakta ve kontrol başarısızlıklarının geleneksel yaklaşımlara göre çok daha zamanında tespit edilmesini mümkün kılmaktadır (Alles vd., 2018). Sürekli denetim ve sürekli izlemenin birlikte kullanımı, kurumsal yönetişimin etkinliğini artırmakta, risklerin proaktif yönetimini desteklemekte ve düzenleyici gerekliliklere uyum süreçlerinin verimliliğini önemli ölçüde geliştirmektedir (Hardy ve Laslett, 2015).

4.3. İç Kontrol Zayıflıkları ve Eksiklikleri

Değerlendirme süreci sonucunda iç kontrol sistemlerinde tespit edilen aksaklıklar, denetim standartları ve düzenleyici otoriteler tarafından belirlenen kriterlere ve önem derecelerine göre sınıflandırılmaktadır. Bu sınıflandırma sistemi hem denetçilerin hem de yönetimin iç kontrol sistemlerinin etkinliğini değerlendirmelerinde ve belirlenen eksikliklerin finansal raporlama kalitesi üzerindeki potansiyel etkisini anlamalarında kritik bir rol oynamaktadır (Berglund ve Sterin, 2021).

ABD Menkul Kıymetler ve Borsa Komisyonu (SEC), Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurulu (PCAOB) ve ilgili denetim standartları, iç kontrol eksikliklerini üç temel kategoride tanımlamaktadır. Bunlar:

Kontrol Eksikliği: Bir kontrolün tasarımındaki veya işleyişindeki bir eksiklik nedeniyle, yönetim veya çalışanların görevlerini yerine getirirken finansal tablolardaki bir yanlışlığın zamanında önlenememesi veya tespit edilememesi durumudur (Doyle vd., 2007a)

Önemli Eksiklik: Finansal raporlamaya ilişkin iç kontroldeki bir eksiklik veya eksiklikler kombinasyonu olup, kurumun yıllık veya ara dönem finansal tablolarında önemli bir yanlışlığın zamanında önlenmesini veya tespit edilmesini olumsuz etkileyen ve denetim komitesine raporlanan birden fazla kontrol eksikliğidir (Ashbaugh-Skaife vd., 2007).

Önemli Zayıflık: Finansal tablolarda maddi bir yanlışlığın zamanında önlenememesi veya tespit edilememesi konusunda makul bir olasılığın bulunduğu bir önemli eksiklik veya eksiklikler bileşimidir. Önemli zayıflıkların kamuoyuna açıklanması gerekmektedir. Hile tespiti üzerine yapılan çalışmalar, etkin kontrollerin hile riskini azaltmadaki rolünü ve kontrol zayıflıklarının hileye zemin hazırlayabildiğini göstermektedir (Doyle vd., 2007b; Tümmler ve Quick, 2025).

4.4. İyileştirme ve Düzeltici Faaliyetler

İç kontrol zayıflıklarının giderilmesine yönelik adımlara aşağıda yer verilmiştir.

Kök Neden Analizi: Kök neden, bir uygunsuzluğa neden olan ve süreç iyileştirme yoluyla kalıcı olarak ortadan kaldırılması gereken bir faktör olarak tanımlanmaktadır (ASQ). Kök neden analizi ise tespit edilen bir kontrol zayıflığının sadece belirtilerini değil, altında yatan yetersiz eğitim, kaynak eksikliği, hatalı süreç tasarımı gibi temel nedenleri anlamak için yapılan analizdir. Bu analiz sonucunda kök nedenin ortadan kaldırılması, sorunun tekrarlanmasını önler (Pangastuti, 2023).

Düzeltici Eylem Planı Geliştirme: Her bir kontrol zayıflığı için, yapılacak faaliyetleri, sorumlu kişileri ve tamamlanma tarihlerini içeren somut bir eylem planı oluşturulur. Bu tür eylemler genellikle denetlenen şirket tarafından üzerinde anlaşılan bir zaman dilimi içinde kararlaştırılır ve üstlenilir. Düzeltici eylem planlarının etkinliği, kontrol zayıflığın türüne, şirketin kaynak mevcudiyetine ve kurumsal yönetişim kalitesine bağlı olarak değişmektedir (Bedard vd., 2012; Johnstone vd., 2011).

Uygulama ve İzleme: Eylem planları hayata geçirilir ve ilerleme, yönetim ve/veya iç denetim tarafından düzenli olarak izlenir. Bu izleme, düzeltici faaliyetlerin zamanında ve etkin bir şekilde tamamlanmasını sağlar İç denetimler ve değerlendirmeler yoluyla yürütülen bu süreç, iç kontrollerin etkili kalmasını ve değişen koşullara uyum sağlayabilmesini garanti eder (Ashbaugh-Skaife vd., 2008; Johnstone vd., 2011; Bakarich ve Baranek, 2020).

Doğrulama: Düzeltici faaliyetlerin tamamlanmasının ardından, kontrol zayıflığının ortadan kaldırıldığını ve yeni kontrolün etkin çalıştığını doğrulamak için takip testleri yapılır. Bu testler kapsamında özel iç denetim çalışmaları, katmanlı süreç denetimlerinin güncellenmesi veya sistem değişikliklerinin etkinliğini gösteren verilerin izlenmesi gerçekleştirilebilir (Bakarich ve Baranek, 2020; Johnstone vd., 2011). İyileştirme ve düzeltici faaliyetlere yönelik adımlar Tablo 3'te gösterilmiştir.

Tablo 3: İyileştirme ve Düzeltici Faaliyet Adımları

Adım	Açıklama	Sorumlu Departman/Kişi
1. Kök Neden Analizi	Kontrol zayıflığının altında yatan temel nedenlerin (eğitim, kaynak, süreç vb.) belirlenmesi.	İç Denetim / Kalite Yönetimi
2. Eylem Planı Geliştirme	Kök nedeni ortadan kaldıracak faaliyetlerin, sorumluların ve takvimin netleştirilmesi.	İlgili Birim Yöneticisi
3. Uygulama ve İzleme	Geliştirilen eylem planının hayata geçirilmesi ve ilerlemenin düzenli olarak takip edilmesi.	İlgili Birim / Proje Ekibi
4. Doğrulama	Faaliyet tamamlandıktan sonra, sorunun giderildiğini ve kontrolün etkin çalıştığını test etme.	İç Denetim / Yönetim

Kaynak: ASQ (American Society for Quality). Plan-Do-Check-Act (PDCA) Cycle.

5. Dijital Çağda İç Kontrol ve Risk Yönetimi

İçinde bulunduğumuz dijital çağ, Endüstri 4.0, nesnelerin interneti (IoT), bulut bilişim ve büyük veri gibi teknolojik gelişmeler iş süreçlerinde köklü değişimlere yol açmıştır (Maqsood vd., 2024). Bu gelişmeler, kurumlar için yüksek verimlilik artışları ve yeni iş modelleri oluşturma fırsatları sunarken, aynı zamanda geleneksel iç kontrol ve risk yönetimi yaklaşımlarını da zorlayan yeni ve karmaşık riskler ortaya çıkarmaktadır (Daway vd., 2025). Verinin hacim, hız ve çeşitlilik açısından üstel olarak artması, iş süreçlerinin giderek daha fazla otomatikleşmesi ve sistemlerin birbirine daha entegre hale gelmesi, iç kontrol ortamını daha dinamik ve karmaşık bir yapıya dönüştürmüştür (Cheng vd., 2024). Dijital çağda, periyodik ve insan odaklı kontrollere dayalı geleneksel yaklaşımlar yetersiz kalmakta, teknoloji destekli, proaktif ve sürekli izlemeye dayalı mekanizmalara olan ihtiyaç artmaktadır (Alles vd., 2018; Vasarhelyi vd., 2004). Dolayısıyla, dijital çağda iç kontrol ve risk yönetimi, sadece mevcut kontrollerde teknolojiyi kullanmak değil, aynı zamanda teknolojinin kendisinin yarattığı riskleri yönetmek ve teknolojiyi bir kontrol aracı olarak stratejik bir şekilde kullanmayı gerektirmektir (Horvey ve Moloi, 2024; COSO, 2017).

5.1. Dijital Dönüşümün İç Kontrole Etkisi

Dijital dönüşümün, iç kontrol sistemleri üzerinde çift yönlü bir etkisi bulunmaktadır (Maqsood vd., 2024; Cheng vd., 2024). Bir yandan, otomasyon ve Robotik Süreç Otomasyonu (RPA) gibi teknolojiler, insan odaklı ve tekrarlayan kontrol faaliyetlerini otomatikleştirerek insan hatası riskini azaltır, kontrol verimliliğini artırır ve çalışanların daha katma değerli analitik görevlere

odaklanmasını sağlar (Eulerich vd., 2024; Kogan vd., 2024). Diğer yandan, dijitalleşme yeni kontrol noktaları ve risk alanları yaratır (COSO, 2024b). Bulut bilişime geçiş, veri güvenliği ve gizliliği konusunda yeni sorumluluklar getirirken (COSO, 2021; Cloud Security Alliance, 2024), IoT cihazlarının yaygınlaşması ve RPA kullanımı, siber saldırı yüzeyini genişleterek yeni güvenlik zafiyetleri ve operasyonel riskler oluşturur (Fagan vd., 2020; National Institute of Standards and Technology [NIST], 2019). Bu nedenle, dijital dönüşüm sürecinde iç kontrol fonksiyonu, sadece mevcut süreçleri değil, aynı zamanda dönüşümün kendisini de bir risk değerlendirmesine tabi tutmalı ve yeni teknolojik altyapıya uygun kontrol mekanizmalarını proaktif olarak tasarlamalıdır (Horvey ve Moloi, 2024; Tiron-Tudor vd., 2024).

5.2. Yapay Zeka ve Veri Analitiği

5.2.1. Yapay Zeka ve Veri Analitiğinin İç Kontroldeki Rolü

Yapay zeka (AI) ve veri analitiği, iç kontrol ve denetim alanında köklü değişimlere yol açmıştır. Geleneksel denetim metodolojisi örnekleme tekniğine dayalı olarak işlemlerin yalnızca bir kısmını test ettiğinden, evrenin tamamına ilişkin çıkarımlarda örnekleme riski içermektedir. Veri analitiği ise, denetçilerin ve kontrol sorumlularının işlemlerin tamamını analiz etmesine olanak tanıyarak anormallikleri ve potansiyel hile göstergelerini yüksek bir doğrulukla tespit etmelerini sağlar. Yapay zeka (AI) ve veri analitiği gibi teknoloji tabanlı denetim araçları, denetim etkinliğini ve verimliliğini artırmada önemli bir bileşen olarak ortaya çıkmaktadır (Qabajeh vd., 2024). Yapay zekanın iç kontroldeki özel uygulamaları şunlardır:

Hile Tespiti ve Anomali Analizi: Makine öğrenmesi algoritmaları, geçmiş hileli işlem verilerinden öğrenerek gelecekteki şüpheli işlemleri gerçek zamanlı olarak tahmin edebilir ve işaretleyebilir (Bao vd., 2020; Perols vd., 2017). Bu sistemler, denetçilerin gözden kaçırabileceği hile göstergeleri ve şemaları ile bunlar arasındaki ilişkileri (örneğin, tedarikçi ödemeleri, satın alma siparişleri ve çalışan ilişkileri arasındaki olağandışı bağlantıları) otomatik olarak belirleyebilir. Bu sistemlerin gerçek zamanlı izleme kapasitesi, denetçilerin potansiyel hile olaylarına zamanında müdahale etmesini ve denetim kaynaklarını daha yüksek riskli işlemlere odaklamasını sağlamaktadır (Han vd., 2023).

Süreç Madenciliği: Süreç madenciliği, bir iş sürecinin işleyişini sistem loglarından hareketle görselleştirebilir ve görev ayrılığı ihlalleri gibi tasarlanan süreç akışından sapmaları otomatik olarak tespit edebilir. Süreç madenciliği, iç kontrol etkinliğinin değerlendirilmesinde, özellikle gerçek veriler kullanıldığında, güçlü bir araç olarak kabul edilmekte; kontrol ihlallerinin

sadece tespit edilmesini değil aynı zamanda kök nedenlerinin anlaşılmasını da kolaylaştırmaktadır (Ceia vd., 2024).

Tahmine Dayalı Risk Puanlaması: Yapay zeka modelleri, geçmiş performans, piyasa koşulları, davranış biçimleri gibi çok sayıda değişkeni analiz ederek belirli işlemlerin veya hesapların risk puanlarını dinamik olarak hesaplayabilir. Tahmine Dayalı Risk Puanlaması, denetçilerin yüksek riskli denetim alanlarına odaklanmalarını ve kaynakların da etkin kullanılmasını sağlar (Kahyaoglu ve Aksoy, 2021).

Doğal Dil İşleme (NLP): NLP teknolojileri, sözleşmeler, e-postalar, toplantı notları gibi yapılandırılmamış metinleri analiz ederek potansiyel uyumsuzlukları, yükümlülükleri veya risk göstergelerini otomatik olarak belirleyebilir. Böylelikle NLP teknolojileri, insan odaklı belge incelemesinin gerektirdiği zamandan tasarruf sağlayarak daha kapsamlı inceleme yapılmasını sağlar.

5.2.2. Yapay Zeka ile İlişkili Riskler ve Yönetişim Zorlukları

Yapay zekanın iç denetim ve risk değerlendirmesinde sunduğu kolaylıkların yanı sıra, beraberinde getirdiği etik ve güvenlik gibi önemli riskler ile yönetişim zorlukları da bulunmaktadır (Kahyaoglu ve Aksoy, 2021). Bu riskler ve yönetişim zorlukları şunlardır:

Algoritma Yanlılığı: Yapay zeka ve büyük veri entegrasyonunun iç kontrol sistemlerine dahil edilmesinde, adalet ve tarafsızlık ilkelerinin korunmasının kritik önemi bulunmaktadır. Yapay zeka modelleri, eğitildikleri verilerdeki önyargıları öğrenebilir ve bunları kararlarına yansıtabilir. Örneğin, geçmiş denetim verilerinde belirli demografik gruplara veya bölümlere karşı bir önyargı varsa, model bu önyargıyı sürdürebilir ve gerçek dışı risk puanlaması yapabilir. Bu durum, sadece etik bir sorun değil, aynı zamanda yasal uyumluluk riskleri de oluşturur (Al Sinani ve Al Awaimri, 2025).

Açıklanabilirlik ve Şeffaflık Sorunu: Derin öğrenme gibi karmaşık yapay zeka modellerinde algoritmik karar süreçlerinin anlaşılması güçlükler yaratmaktadır. Bir modelin tahmin performansı arttıkça genellikle açıklanabilirliği azalmakta ve model "kara kutu" gibi anlaşılması güç bir yapıya dönüşmektedir (Zhang vd., 2022; Lipton, 2018). Bu açıklanabilirlik eksikliği, muhasebe ve denetimde yapay zeka benimsenmesinin önündeki temel zorluklardan biridir (AICPA, 2020; CPAB, 2021). Mevcut denetim dokümantasyonu ve kanıt standartları, denetçilerin yapay zeka modelinin iç işleyişini açıklayamaz ve belgeleyemezlerse, model çıktılarına güvenme konusunda sınırlamalar getirmektedir (Zhang vd., 2022). Buna bağlı olarak, düzenleyiciler ve denetim otoriteleri giderek artan bir şekilde "*Açıklanabilir Yapay Zeka*" talep etmektedir (Zhang vd., 2022; ACCA, 2020).

Veri Kalitesi ve Bütünlüğü: Yapay zeka modellerinin etkinliği, eğitildikleri ve çalıştıkları verilerin kalitesine doğrudan bağlıdır. Eksik, hatalı veya manipüle edilmiş veriler, modelin yanlış sonuçlar üretmesine yol açar. Dolayısıyla, veri yönetişimi ve veri kalitesi kontrolleri, yapay zeka tabanlı sistemlerin temelini oluşturur (Al Sinani ve Al Awaimri, 2025). *Büyük Veri Analitiği* çağında, veri miktarından daha önemli bir faktör haline gelen veri kalitesi (Appelbaum vd., 2017) rasyonel karar verme süreçlerinin temelini oluşturmaktadır (Knauer vd., 2020).

Siber Güvenlik Tehditleri: Yapay zeka sistemleri, siber güvenlik açısından önemli güvenlik açıklarına sahiptir. Siber saldırganlar, modelin eğitim aşamasında eğitim veri setine kötü amaçlı örnekler sızdırarak modelin öğrenme sürecini manipüle eden veri zehirleme saldırıları gerçekleştirebilmekte (Cinà vd., 2024; Goldblum vd., 2023) veya tahmin aşamasında modelin karar mekanizmalarındaki güvenlik açıklarını hedef alan kötü amaçlı örnekler aracılığıyla sistemin hatalı sınıflandırmalar yapmasına neden olabilmektedir (Zhang vd., 2022). Bu siber saldırılar, yapay zeka tabanlı muhasebe ve denetim sistemlerinde olumsuz sonuçlara yol açabilmektedir; örneğin, makine öğrenmesi tabanlı hile tespit sistemleri kötü amaçlı örneklerle kolaylıkla yanıltılabilmekte ve hileli işlemler tespit edilemeyebilmektedir (Munoko vd., 2020). Siber saldırılar sonucunda muhasebe bilgi sistemlerinde meydana gelen veri ihlalleri hem finansal kayıplara hem de şirketlerin piyasa değerlerinde düşüşe yol açabilmektedir (Demek ve Kaplan, 2023).

Yönetişim ve Hesap Verebilirlik: Yapay zeka sistemlerinin kurumlarda giderek daha fazla karar verme süreçlerine entegre edilmesiyle birlikte, hesap verebilirlik ve sorumluluk atfının nasıl yapılacağı konuları önemli bir yönetişim sorunu haline gelmiştir. Geleneksel kurumsal yapılarda çalışanların hesap verilebilirlikleri net bir şekilde tanımlanmışken, yapay zeka tabanlı karar verme süreçlerinde bu tanımlama belirsizleşmekte ve karmaşık hale gelmektedir. Yapay zeka modelinin hatalı risk değerlendirmesi sonucunda finansal kayıplar ortaya çıktığında sorumluluk atfının nasıl yapılacağı, algoritma geliştiricilerin mi, veri sağlayıcıların mı, yoksa sistemi kullanan yöneticilerin mi sorumlu tutulacağı gibi sorular, etik karar verme süreçlerinin tüm bileşenlerini etkilemektedir (Lehner vd., 2022).

5.3. Siber Güvenlik ve Dijital Riskler

Kurumların dijital varlıklarının ve verilerinin artmasıyla birlikte, siber güvenlik riskleri, kurumsal risk yönetimi açısından önemli hale gelmiştir. Siber saldırılar, sadece finansal kayıplara değil, aynı zamanda faaliyetlerin durmasına, kurum itibarının zedelenmesine, müşteri güveninin azalmasına ve

yasal yaptırımlara da yol açabilir (Lee, 2021). Stratejik bir yönetişim sorunu haline gelen siber risklerin yer aldığı siber tehdit ortamı sürekli olarak değişim göstermektedir (Kure vd., 2022; Lee, 2021). Günümüz siber tehdit ortamı, geleneksel kötü amaçlı yazılımların ötesinde, fidye yazılımları, gelişmiş kalıcı tehditler (APT), sosyal mühendislik, tedarik zinciri ve IoT tabanlı saldırılar gibi özellikli tehdit türlerini içermektedir. Bu durum, siber risk yönetiminin bilgi teknolojileri departmanının operasyonel sorumluluğundan çıkarak, kurumsal düzeyde stratejik bir yönetişim konusu haline gelmesini gerektirmiştir (Moeti vd., 2025).

Etkin bir siber güvenlik risk yönetimi, yapılandırılmış ve standartlaştırılmış çerçevelerin kullanılmasını gerektirir. Veri güvenliğinin korunması için entegre bir siber güvenlik risk yönetimi çerçevesi (i-CSRM) geliştirilerek, risk belirleme, değerlendirme ve azaltma süreçlerinin sistematik bir şekilde ele alınması gerekmektedir (Kure vd., 2022). En yaygın kullanılan çerçeveler şunlardır:

NIST Siber Güvenlik Çerçevesi (CSF): Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından geliştirilen bu çerçeve, *tanımlama*, *koruma*, *tespit etme*, *yanıt* ve *iyileştirme* olmak üzere beş temel fonksiyon olarak yapılandırılmıştır. Bu çerçeve, tüm sektörleri kapsayan, her büyüklükteki kurumlar tarafından kullanılabilir (NIST, 2025).

ISO/IEC 27001: Uluslararası Standardizasyon Örgütü (ISO) tarafından yayımlanan bu standartlar, Bilgi Güvenliği Yönetim Sistemi (BGYS) yaklaşımı ile organizasyonların siber güvenlik kontrollerini sistematik bir şekilde tasarlamasını, uygulamasını ve sürekli iyileştirmesini sağlamaktadır. Bu sertifikasyon, bir organizasyonun bilgi güvenliği yönetiminde uluslararası standartlara uyduğunu gösterir (ISO/IEC 27001, 2022).

Bilgi ve İlgili Teknolojiler için Kontrol Amaçları (COBIT): Bilgi Sistemleri Denetim ve Kontrol Derneği (Information Systems Audit and Control Association-ISACA) tarafından geliştirilen bilgi teknolojileri yönetişimi için kapsamlı bir çerçeve olan COBIT, siber güvenlik kontrollerini, daha geniş bilgi teknolojileri yönetişimi ve iş hedefleriyle bütünleştirerek, bilgi teknolojilerinin iş değeri yaratmasını sağlar.

***Otomatik Soruşturma ve Yanıt (AIR)*:** Siber riskleri finansal terimlerle ölçmeye ve ifade etmeye yarayan kantitatif bir risk analizi metodolojisidir. Riskleri para cinsinden değerlendirerek karar vericilere somut bilgiler sunar.

Operasyonel Kritik Tehdit, Varlık ve Güvenlik Açığı Değerlendirmesi (OCTAVE): Kurum içi bilgi güvenliği risklerini belirlemek, yönetmek ve değerlendirmek için kullanılan bir risk değerlendirme metodolojisidir. Bu

metodoloji, bir kurumun operasyonel risk toleranslarını tanımlayarak nitel risk değerlendirme kriterleri geliştirmesine yardımcı olur.

6. SONUÇ

Modern kurumsal yönetişim anlayışı, iç kontrol sistemleri ile kurumsal risk yönetimi arasındaki entegrasyonu, kurumların sürdürülebilir başarı elde etmelerinin temel koşulu olarak konumlandırmaktadır. Bu çalışma, iç kontrolün COSO İç Kontrol Entegre Çerçevesi temelinde ele alınan beş bileşeni ile kurumsal risk yönetiminin COSO Kurumsal Risk Yönetimi (ERM) Çerçevesindeki beş bileşeninin, birbirlerinden bağımsız yönetişim fonksiyonları olmalarının ötesinde, karşılıklı etkileşim içinde işleyen ve birbirlerini güçlendiren dinamik süreçler olduğunu ortaya koymuştur. İç kontrol sistemleri, risk yönetimi süreçlerinin operasyonel düzeyde uygulanmasını sağlayan mekanizmaları oluştururken, kurumsal risk yönetimi ise iç kontrol faaliyetlerinin odaklanması gereken risk alanlarını stratejik düzeyde belirlemektedir. Bu sinerjik ilişki, kurumların riskleri yalnızca bir tehdit değil, aynı zamanda etkin yönetildiğinde rekabet avantajı yaratabilecek fırsatlar olarak görmelerini sağlayan proaktif bir risk kültürünün gelişimine zemin hazırlamaktadır. Dolayısıyla, iç kontrol ve risk yönetimi entegrasyonu, kurumsal yönetişimin etkinliğini artıran, kaynakların en önemli risk alanlarına odaklanmasını sağlayan ve kurumsal dayanıklılığı güçlendiren stratejik bir zorunluluk olarak değerlendirilmelidir.

Üç Savunma Hattı Modeli açısından değerlendirildiğinde, iç kontrol ve risk yönetiminin entegrasyonunda roller ve sorumlulukların açık ve anlaşılır bir şekilde tanımlanmasının önemi daha da belirginleşmektedir. Birinci savunma hattını oluşturan operasyonel yönetimin günlük riskleri belirlemesi ve yönetmesi, ikinci savunma hattındaki risk yönetimi ve uyum fonksiyonlarının çerçeveler geliştirmesi ve gözetim sağlaması, üçüncü savunma hattı olan iç denetimin ise bağımsız güvence sunması şeklindeki katmanlı yapı, iç kontrol ve risk yönetiminin birbirini tamamlayan yapısını ortaya koymaktadır. Özellikle iç denetimin, ERM sürecinin tüm aşamalarında oynadığı rol, bu entegrasyonun başarısı için önem taşımaktadır. İç denetim, yalnızca mevcut kontrollerin etkinliğini değerlendirmekle kalmayarak, risk belirleme süreçlerinde gözden kaçan riskleri ortaya çıkarma, risk değerlendirmelerinin kabul edilebilirliğini test etme ve ERM çerçevesinin kendisinin etkinliğini bağımsız olarak gözden geçirme sorumluluğu taşımaktadır. Bu çok yönlü rol, iç denetimi geleneksel bir uyumluluk fonksiyonundan kurumsal yönetişimin stratejik ortağına dönüştürmekte ve risk tabanlı denetim yaklaşımının benimsenmesini zorunlu kılmaktadır. Sonuç olarak, iç kontrol ve risk yönetiminin etkin entegrasyonu, bu üç savunma hattının koordineli bir şekilde çalışmasını ve aralarındaki bilgi akışının kesintisiz olmasını gerektirmektedir.

Dijital çağın getirdiği dönüşüm, iç kontrol ve risk yönetimi alanında hem yeni fırsatlar hem de beraberinde yeni tehditler sunmaktadır. Yapay zeka, büyük veri analitiği, robotik süreç otomasyonu ve sürekli denetim teknolojilerinin iç kontrol sistemlerine entegrasyonu, kontrol etkinliğini ve verimliliğini önemli ölçüde artırırken, hile tespiti, anomali analizi, süreç madenciliği ve tahmine dayalı risk puanlaması gibi alanlarda denetçilere analitik yetenekler kazandırmaktadır. Bununla birlikte, bu teknolojik gelişmeler, algoritma yanlılığı, açıklanabilirlik sorunu, veri kalitesi riskleri ve siber güvenlik tehditleri gibi yeni risk alanlarını da beraberinde getirmektedir. Özellikle, siber güvenlik risklerinin stratejik bir yönetişim sorunu haline gelmesi, NIST Siber Güvenlik Çerçevesi, ISO 27001 ve COBIT gibi uluslararası standartların iç kontrol sistemleriyle entegrasyonunu zorunlu kılmaktadır. Bu çerçevede, kurumlar için kritik başarı faktörü, teknolojik yenilikleri bir kontrol aracı olarak stratejik biçimde kullanırken, aynı zamanda bu teknolojilerin kendilerinin yarattığı riskleri etkin şekilde yönetebilme kapasitesine sahip olmalarıdır. Dijital dönüşüm sürecinde, iç kontrol fonksiyonunun sadece mevcut süreçleri değil, dönüşümün kendisini de kapsamlı bir risk değerlendirmesine tabi tutması ve yeni teknolojik altyapıya uygun kontrol mekanizmalarını proaktif olarak tasarlaması gerekmektedir.

Sonuç olarak, iç kontrol ve risk yönetimi sistemlerinin entegrasyonu, kurumların günümüzün karmaşık ve dinamik risk ortamlarında sürdürülebilir başarı elde etmelerinin temel şartıdır. COSO çerçeveleri etrafında şekillenen bu entegrasyon, yalnızca düzenleyici gereklilikleri karşılamak için değil, aynı zamanda stratejik hedeflere ulaşmayı kolaylaştırmak, operasyonel verimliliği artırmak ve paydaş güvenini güçlendirmek için kritik öneme sahiptir. İç kontrol sistemlerinin risk yönetimi süreçleriyle bütünleştirilmesi, kurumlara riskleri bütünsel bir bakış açısından değerlendirme, kaynakları en önemli risk alanlarına tahsis etme ve değişen iç ve dış koşullara hızla uyum sağlama yeteneği kazandırmaktadır. Üç Savunma Hattı Modelinin sunduğu yapılandırılmış yaklaşım, bu entegrasyonun operasyonel düzeyde nasıl gerçekleştirileceğine dair net bir yol haritası sunarken, iç denetimin stratejik ortaklık rolü, sistemin sürekli iyileştirilmesi ve güvence sağlanması açısından vazgeçilmez bir unsur olmaktadır. Dijital çağın sunduğu teknolojik imkanların etkin kullanımı ve beraberinde getirdiği risklerin proaktif yönetimi, iç kontrol ve risk yönetimi entegrasyonunun başarısını belirleyen temel faktörlerdir. Bu çalışmanın ortaya koyduğu kavramsal çerçeve ve entegrasyon modeli hem akademisyenler hem de uygulayıcılar için iç kontrol ve risk yönetimi sistemlerinin tasarımında, uygulanmasında ve değerlendirilmesinde yol gösterici bir referans kaynağı olarak kullanılabilir.

Kaynakça

Acar, D., Gal, G., Öztürk, M. S., & Usul, H. (2021). A case study in the implementation of a continuous monitoring system. *Journal of Emerging Technologies in Accounting*, *18*(1), 17-25. https://doi.org/10.2308/JETA-17-04-29-9

ACCA. (2020). *Explainable AI: Driving business value through greater understanding*. Association of Chartered Certified Accountants.

Aguilera, R. V., Desender, K., Bednar, M. K., & Lee, J. H. (2015). Connecting the dots: Bringing external corporate governance into the corporate governance puzzle. *Academy of Management Annals, 9*(1), 483-573. https://doi.org/10.1080/19416520.2015.1024503

AICPA. (2020). *Guide to audit data analytics*. American Institute of Certified Public Accountants.

Al Sinani, S. M. K., & Al Awaimri, J. J. D., (2025). Leveraging artificial intelligence and big data for enhanced internal control and business risk mitigation. In: Khairy, S., Hayder, G., Al Shukaili, A., Al Abri, S., Soosaimanickam, A., Raja Kasim, R.S. (eds) Exploring Trends, Innovations, and Digitalization of Entrepreneurship. MENAREC 2024 (pp. 584-595). Sustainable Economy and Ecotechnology. Springer, Cham. https://doi.org/10.1007/978-3-031-92942-7_39

Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2018). Putting continuous auditing theory into practice: Lessons from two pilot implementations. In: David Y. Chan, D. Y., Chiu, V., Vasarhelyi, M. A. (eds) Continuous Auditing: Theory and Application, (pp. 247-270). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78743-413-420181011

Almgrashi, A. & Mujalli, A. (2024). The influence of sustainable risk management on the implementation of risk-based internal auditing. *Sustainability*, 8455. https://doi.org/10.3390/su16198455

American Society for Quality (ASQ). Root Cause Analysis definitions and methodologies.

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big Data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory, 36*(4), 1-27. https://doi.org/10.2308/ajpt-51684

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society, 35*(7), 659-675. https://doi.org/10.1016/j.aos.2010.07.003

Arena, M., Arnaboldi, M., & Azzone, G. (2017). Management accounting and risk management. *Management Accounting Research*, *37*, 1-11. https://doi.org/10.1016/j.mar.2016.12.001

Ashbaugh-Skaife, H., Collins, D. W., & Kinney, W. R. Jr. (2007). The discovery and reporting of internal control deficiencies prior to SOX-mandated au-

dits. *Journal of Accounting and Economics*, *44*(1-2), 166-192. https://doi.org/10.1016/j.jacceco.2006.10.001

Ashbaugh-Skaife, H., Collins, D. W., Kinney, W. R., Jr., & LaFond, R. (2008). The effect of SOX internal control deficiencies and their remediation on accrual quality. *The Accounting Review, 83*(1), 217-250. https://doi.org/10.2308/accr.2008.83.1.217

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research, 253*(1), 1-13. https://doi.org/10.1016/j.ejor.2015.12.023

Bakarich, K., & Baranek, D. (2020). Repeat offenders: Examining cases of multiple years of internal control weaknesses. *Managerial Auditing Journal, 35*(4), 499-520. https://doi.org/10.1108/MAJ-05-2019-2302

Ball, D. J., & Watt, J. (2013). Further thoughts on the utility of risk matrices. *Risk Analysis*, *33*(11), 2068-2078. https://doi.org/10.1111/risa.12057

Bao, Y., Ke, B., Li, B., Yu, Y. J., & Zhang, J. (2020). Detecting accounting fraud in publicly traded U.S. firms using a machine learning approach. *Journal of Accounting Research*, *58*(1), 199-235. https://doi.org/10.1111/1475-679X.12292

Baxter, R., Bedard, J. C., Hoitash, R., & Yezegel, A. (2013). Enterprise risk management program quality: Determinants, value relevance, and the financial crisis. *Contemporary Accounting Research, 30*(4), 1264-1295. https://doi.org/10.1111/j.1911-3846.2012.01194.x

Beasley, M. S., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, *24*(6), 521-531. https://doi.org/10.1016/j.jaccpubpol.2005.10.001

Beasley, M., Branson, B., & Pagach, D. (2015). An analysis of the maturity and strategic impact of investments in ERM. *Journal of Accounting and Public Policy*, *34*(3), 219-243. https://doi.org/10.1016/j.jaccpubpol.2015.01.001

Bedard, J., Hoitash, R., Hoitash, U., & Westermann, K. (2012). Material weakness remediation and earnings quality: A detailed examination by type of control deficiency. *Auditing: A Journal of Practice & Theory, 31*(1), 57-78. https://doi.org/10.2308/ajpt-10190

Bedford, T., & Cooke, R. (2001). *Probabilistic risk analysis: Foundations and methods*. Cambridge University Press.

Bento, R. F., Mertins, L., & White, L. F. (2018). Risk management and internal control: A study of management accounting practice. In M. A. Malina (Ed.), *Advances in Management Accounting, 30*, 1-25. Emerald Publishing Limited. https://doi.org/10.1108/S1474-787120180000030002

Berglund, N. R., & Sterin, M. (2021). Internal controls and operational performance of nonprofit organizations. *Journal of Governmental & Nonprofit Accounting*, *10*(1), 134-156. https://doi.org/10.2308/JOGNA-19-001

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning, 48*(4), 265-276. https://doi.org/10.1016/j.lrp.2014.07.005

Callahan, C., & Soileau, J. (2017). Does enterprise risk management enhance operating performance? *Advances in Accounting*, 37, 122-139. https://doi.org/10.1016/j.adiac.2017.01.001

Canadian Public Accountability Board [CPAB]. (2021). *Audit quality insights report*. Ottawa: CPAB.

Ceia, M. F., Marques, R. P., Inácio, H. (2024). Bridging artificial intelligence and internal controls: Insights from the literature. In: Azevedo, G., Vieira, E., Marques, R., Almeida, L. (eds) *The Challenges of Era 5.0 in Accounting and Finance Innovation. ICAFI 2024. Information Systems Engineering and Management*, 28, 401-419. Springer, Cham. https://doi.org/10.1007/978-3-031-77531-4_24

Chalmers, K., Hay, D., & Khlif, H. (2019). Internal control in accounting research: A review. *Journal of Accounting Literature, 42*(1), 80-103. https://doi.org/10.1016/j.acclit.2018.03.002

Chan, K. C., Chen, Y., & Liu, B. (2021). The linear and non-linear effects of internal control and its five components on corporate innovation: Evidence from Chinese firms using the COSO framework. *European Accounting Review*, *30*(4), 733-765. https://doi.org/10.1080/09638180.2020.1776626

Chang, Y. T., Chen, H., Cheng, R. K., & Chi, W. (2019). The impact of internal audit attributes on the effectiveness of internal control over operations and compliance. *Journal of Contemporary Accounting & Economics*, *15*(1), 1-19. https://doi.org/10.1016/j.jcae.2018.11.002

Cheng, W., Li, C., & Zhao, T. (2024). The stages of enterprise digital transformation and its impact on internal control: Evidence from China. *International Review of Financial Analysis, 92*, 103079 (1-15). https://doi.org/10.1016/j.irfa.2024.103079

Chi, Z., Shah, S. M., Wai, L. Y., & Ngalim, S. M. (2024). Mapping out internal audit research: A bibliometric analysis. *Journal of Modern Accounting and Auditing*, *20*(4), 145-170. http://psasir.upm.edu.my/id/eprint/116922/

Cinà, A. E., Grosse, K., Demontis, A., Biggio, B., Roli, F., & Pelillo, M. (2024). Machine learning security against data poisoning: Are we there yet? *Computer, 57*(3), 26-34. https://doi.org/10.1109/MC.2023.3299572

Cloud Security Alliance. (2024). Security guidance for critical areas of focus in cloud computing (Version 5). Cloud Security Alliance. https://cloudsecurityalliance.org/research/guidance

Cohen, J., Krishnamoorthy, G., & Wright, A. (2017). Enterprise risk management and the financial reporting process: The experiences of audit committee members, CFOs, and external auditors. *Contemporary Accounting Research*, *34*(2), 1178-1209. https://doi.org/10.1111/1911-3846.12294

COSO. (1992). *Internal Control—Integrated Framework*. New York, NY.

COSO. (2004). *Enterprise risk management – Integrated framework*. American Institute of Certified Public Accountants.

COSO. (2013). *Internal Control—Integrated Framework*. Jersey City, NJ.

COSO. (2017). *Enterprise Risk Management Framework*. *Enterprise Risk Management—Integrating with Strategy and Performance*.

COSO. (2021). *Enterprise risk management for cloud computing*. Durham, NC: COSO.

COSO. (2024a). *Compliance Risk Management: Applying the COSO ERM Framework*.

COSO. (2024b). *Achieving effective internal control over robotic process automation*. Durham, NC: COSO.

Cox, L. A. (2008). What's wrong with risk matrices? *Risk Analysis, 28*(2), 497-512.

Daway, A. M., Daway, W. M., Zghair, K. A., & Flayyih, H. H. (2025). The impact of digital transformation of accounting information system in enhancing the effectiveness of internal control. *Journal of Lifestyle and SDGs Review, 5*(3), 1-14. https://doi.org/10.47172/2965-730X.SDGsReview.v5.n03.pe05572

Demek, K. C., & Kaplan, S. E. (2023). Cybersecurity breaches and investors' interest in the firm as an investment. *International Journal of Accounting Information Systems, 49*, 100616. https://doi.org/10.1016/j.accinf.2023.100616

Doyle, J. T., Ge, W., & McVay, S. (2007a). Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics*, *44*(1-2), 193-223. https://doi.org/10.1016/j.jacceco.2006.10.003

Doyle, J. T., Ge, W., & McVay, S. (2007b). Accruals quality and internal control over financial reporting. *The Accounting Review*, *82*(5), 1141-1170. https://doi.org/10.2308/accr.2007.82.5.1141

Drehmann, M. (2008). Stress tests: Objectives, challenges and modelling choices. *Riksbank Economic Review, 2*, 60-92.

Duijm, N. J. (2015). Recommendations on the use and design of risk matrices. *Safety Science*, 76, 21-31. https://doi.org/10.1016/j.ssci.2015.02.014

Embrechts, P., Klüppelberg, C., & Mikosch, T. (2013). *Modelling extremal events: For insurance and finance*. Springer.

Eulerich, M., Waddoups, N., Wagener, M., & Wood, D. A. (2024). Development of a framework of key internal control and governance principles for robotic process automation (RPA). *Journal of Information Systems, 38*(2), 29-49. https://doi.org/10.2308/ISYS-2023-067

Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). Foundational cybersecurity activities for IoT device manufacturers (NISTIR 8259). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8259

Farrell, M., & Gallagher, R. (2015). The valuation implications of enterprise risk management maturity. *Journal of Risk and Insurance, 82*(3), 625-657.

Feng, M., Li, C., McVay, S. E., & Skaife, H. (2015). Does ineffective internal control over financial reporting affect a firm's operations? Evidence from firms' inventory management. *The Accounting Review, 90*(2), 529-557. https://doi.org/10.2308/accr-50909

Filatotchev, I., & Nakajima, C. (2014). Corporate governance, responsible managerial behavior, and corporate social responsibility: Organizational efficiency versus organizational legitimacy? *Academy of Management Perspectives, 28*(3), 289-306.

Florio, C., & Leoni, G. (2017). Enterprise risk management and firm performance: The Italian case. *The British Accounting Review*, *49*(1), 56-74. https://doi.org/10.1016/j.bar.2016.08.003

Fraser, J. R., & Simkins, B. J. (2016). The challenges of and solutions for implementing enterprise risk management. *Business Horizons*, *59*(6), 689-698. https://doi.org/10.1016/j.bushor.2016.06.007

Goldblum, M., Tsipras, D., Xie, C., Chen, X., Schwarzschild, A., Song, D., Mądry,A., Li, B., & Goldstein, T. (2023). Dataset security for machine learning: Data poisoning, backdoor attacks, and defenses. In IEEE Transactions on Pattern Analysis and Machine Intelligence, 45(2), pp. 1563-1580. https://doi.org/10.1109/TPAMI.2022.3162397

Gontarek, W. (2016). Risk governance of financial institutions: The growing importance of risk appetite and culture. *Journal of Risk Management in Financial Institutions*, 9(2), 120-129. https://doi.org/10.69554/VAMF6201

Gontarek, W., & Bender, R. (2019). Examining risk governance practices in global financial institutions: the adoption of risk appetite statements. *Journal of Banking Regulation, 20*, 74–85. https://doi.org/10.1057/s41261-018-0067-2

Gordon, L. A., Loeb, M. P., & Tseng, C.-Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Ac-*

counting and Public Policy, 28(4), 301-327. https://doi.org/10.1016/j.jaccpubpol.2009.06.006

Goswami, V. (2024). The effectiveness of risk management in project success. *Harrisburg University Digital Commons*. https://digitalcommons.harrisburgu.edu/cgi/viewcontent.cgi?article=1053&context=dandt

Greapca, N. M., & Lungu, C. I. (2024). The connectivity of internal audit and risk management research. *Journal of Accounting and Management Information Systems*, *23*(2), 339-364. http://dx.doi.org/10.24818/jamis.2024.02003

Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial intelligence: A literature review. *International Journal of Accounting Information Systems*, 48, 100598. https://doi.org/10.1016/j.accinf.2022.100598

Hardy, C. A., & Laslett, G. (2015). Continuous auditing and monitoring in practice: Lessons from Metcash's Business Assurance Group. *Journal of Information Systems*, *29*(2), 183-194. https://doi.org/10.2308/isys-50969

Hayne, C., & Free, C. (2014). Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management. *Accounting, Organizations and Society, 39*(5), 309-330. https://doi.org/10.1016/j.aos.2014.05.002

Hazaea, S. A., Zhu, J., Al-Matari, E. M., Senan, N. A. M., Khatib, S. F. A., & Ullah, S. (2025). Mapping the literature trends of internal auditing in the United States: A systematic review and directions for future research. *SAGE Open, January-March,* 1–20. https://doi.org/10.1177/21582440251318071

Hopkin, P. (2018). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management* (5th ed.). Kogan Page.

Horvey, S. S., & Moloi, T. (2024). Digital transformation in enterprise risk management. In T. Moloi (Ed.), Digital transformation in South Africa. Professional Practice in Governance and Public Organizations . (pp. 21-44). Springer, Cham. https://doi.org/10.1007/978-3-031-52403-5_2

Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management. *Journal of Risk and Insurance*, 78(4), 795-822. https://doi.org/10.1111/j.1539-6975.2011.01413.x

IIA. (2020). Üçlü Savunma Hattı ile ilgili güncelleme. https://na.theiia.org/translations/PublicDocuments/Three-Lines-Model-Updated-Turkish.pdf

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*.

Johnstone, K., Li, C., & Rupley, K. H. (2011). Changes in corporate governance associated with the revelation of internal control material weaknes-

ses and their subsequent remediation. *Contemporary Accounting Research, 28*(1), 331-383. https://doi.org/10.1111/j.1911-3846.2010.01037.x

Jones, M. J. (2008). Internal control, accountability and corporate governance: Medieval and modern Britain compared. *Accounting, Auditing & Accountability Journal*, 21(7), 1052-1075. https://doi.org/10.1108/09513570810907474

Kahyaoglu, S.B., & Aksoy, T. (2021). Artificial intelligence in internal audit and risk assessment. In: Hacioglu, U., Aksoy, T. (eds) *Financial Ecosystem and Strategy in the Digital Era. Contributions to Finance and Accounting*. (pp. 179-192), Springer, Cham. https://doi.org/10.1007/978-3-030-72624-9_8

Kaplan, R. S., & Mikes, A. (2016). Risk management—the revealing hand. *Journal of Applied Corporate Finance, 28*(1), 8-18.

Knauer, T., Nikiforow, N., & Wagener, S. (2020). Determinants of information system quality and data quality in management accounting. *Journal of Management Control*, *31*(1-2), 97-121. https://doi.org/10.1007/s00187-020-00296-y

Kogan, G., Kokina, J., Stampone, A., & Boyle, D. M. (2024). RPA in accounting risk and internal control: Insights from RPA program managers. *Accounting Horizons, 38*(4), 137-148. https://doi.org/10.2308/HORIZONS-2022-191

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, *34*, 15241-15271. https://doi.org/10.1007/s00521-022-06959-2

Lam, J. (2014). *Enterprise risk management: From incentives to controls* (2nd ed.). John Wiley & Sons.

Länsiluoto, A., Jokipii, A., & Eklund, T. (2016). Internal control effectiveness–a clustering approach. *Managerial Auditing Journal*, *31*(1), 5-34. https://doi.org/10.1108/MAJ-08-2013-0910

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671. https://doi.org/10.1016/j.bushor.2021.02.022

Lehner, O. M., Ittonen, K., Silvola, H., Ström, E., & Wührleitner, A. (2022). Artificial intelligence based decision-making in accounting and auditing: Ethical challenges and normative thinking. *Accounting, Auditing & Accountability Journal, (35)*9, 109–135. https://doi.org/10.1108/AAAJ-09-2020-4934

Lipton, Z. C. (2018). The mythos of model interpretability: In machine learning, the concept of interpretability is both important and slippery. *Queue, 16*(3), 31-57. https://doi.org/10.1145/3236386.3241340

Lu, H., Richardson, G., & Salterio, S. (2011). Direct and indirect effects of internal control weaknesses on accrual quality: Evidence from a unique Canadian regulatory setting. *Contemporary Accounting Research, 28*(2), 675-707. https://doi.org/10.1111/j.1911-3846.2010.01058.x

Lundqvist, S. A. (2015). Why firms implement risk governance - Stepping beyond traditional risk management to enterprise risk management. *Journal of Accounting and Public Policy*, 34(5), 441-466. https://doi.org/10.1016/j.jaccpubpol.2015.05.002

Malik, M. F., Zaman, M., & Buckby, S. (2020). Enterprise risk management and firm performance: Role of the risk committee. *Journal of Contemporary Accounting & Economics*, *16*(1), 100178. https://doi.org/10.1016/j.jcae.2019.100178

Maqsood, U. S., Wang, S., & Zahid, R. M. A. (2024). Digital age imperatives and firm internal control quality: Evidence from CEOs personal trait and type of state-owned enterprises. *Managerial Auditing Journal, 39*(6), 700-727. https://doi.org/10.1108/MAJ-10-2023-4071

McNeil, A. J., Frey, R., & Embrechts, P. (2015). *Quantitative risk management: Concepts, techniques and tools* (Revised ed.). Princeton University Press.

McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does enterprise risk management increase firm value? *Journal of Accounting, Auditing & Finance*, 26(4), 641-658. https://doi.org/10.1177/0148558X11409160

Meidell, A., & Kaarbøe, K. (2017). How the enterprise risk management function influences decision-making in the organization: A field study of a large, global oil and gas company. *The British Accounting Review, 49*(1), 39-55. https://doi.org/10.1016/j.bar.2016.10.005

Mikes, A. (2011). From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society*, *36* (4-5), 226-245. https://doi.org/10.1016/j.aos.2011.03.002

Mikes, A., & Kaplan, R. S. (2015). When one size doesn't fit all: Evolving directions in the research and practice of enterprise risk management. *Journal of Applied Corporate Finance*, *27*(1), 37-40. https://doi.org/10.1016/j.aos.2011.03.002

Moeti, W., Moyo, S., & Moropana, T. (2025). Compliance and internal controls: Standards and practices in cyber security governance. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5581811

Munoko, I., Brown-Liburd, H. L., & Vasarhelyi, M. (2020). The ethical implications of using artificial intelligence in auditing. *Journal of Business Ethics*, *167*, 209-234. https://doi.org/10.1007/s10551-019-04407-1

National Institute of Standards and Technology [NIST]. (2019). Considerations for managing Internet of Things (IoT) cybersecurity and priva-

cy risks (NISTIR 8228). U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8228

National Institute of Standards and Technology. (2025). *NIST risk management framework (RMF)*. U.S. Department of Commerce. https://csrc.nist.gov/projects/risk-management

Nigrini, M. J., & Johnson, A. J. (2008). Using key performance indicators and risk measures in continuous monitoring. *Journal of Emerging Technologies in Accounting*, *5*(1), 65-80. https://doi.org/10.2308/jeta.2008.5.1.65

Özer, G., Günlük, M., & Okutan, K. (2018). İç ve bağımsız denetçiler arasındaki ilişkilerin, üst yönetim desteğinin ve iç denetimin bağımsızlığının iç denetimin etkinliği üzerindeki etkileri. *Muhasebe Bilim Dünyası Dergisi, 20* (Özel Sayı), 590-613.

Öztürk, S., & Yılmaz, C. (2019). Bibliometric analysis of internal control, internal auditing and control self-assessment. In M. H. Bilgin, H. Danis, E. Demir, & U. Can (Eds.), *Finance and Accounting I* (pp. 13-30). Springer.

Pangastuti, L. A. (2023). The role of internal auditing in upholding corporate governance standards. *Advances in Managerial Auditing Research*, *1*(3), 114-124. https://doi.org/10.60079/amar.v1i3.214

Perols, J. L., Bowen, R. M., Zimmermann, C., & Samba, B. (2017). Finding needles in a haystack: Using data analytics to improve fraud prediction. *The Accounting Review*, *92*(2), 221-245. https://doi.org/10.2308/accr-51562

Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford University Press.

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society, 34*(6-7), 849-855. https://doi.org/10.1016/j.aos.2009.06.001

Power, M. (2016). Riskwork: Essays on the organizational life of risk management. Oxford University Press.

Qabajeh, M., Qubbaja, A., Jebreel, M., AlQudah, M. Z., & Alkhatib, F. S. F. (2024). Trends and patterns in COSO-related auditing research: A bibliometric study. *EDPACS*, *69*(10), 30-53. https://doi.org/10.1080/07366981.2024.2371537

Rae, K., Sands, J., & Subramaniam, N. (2017). Associations among the five components within COSO internal control-integrated framework as the underpinning of quality corporate governance. *Australasian Accounting, Business and Finance Journal, 11*(1), 28-54. https://doi.org/10.14453/aabfj.v11i1.4

Rebonato, R. (2010). *Coherent stress testing: A Bayesian approach to the analysis of financial stress*. John Wiley & Sons.

Renn, O. (2008). *Risk governance: Coping with uncertainty in a complex world*. Earthscan.

Soin, K., & Collier, P. (2013). Risk and risk management in management accounting and control. *Management Accounting Research*, *24*(2), 82-87. https://doi.org/10.1016/j.mar.2013.04.003

Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal, 16*(4), 640-661. https://doi.org/10.1108/09513570310492335

Taleb, N. N. (2007). *The black swan: The impact of the highly improbable*. Random House.

Tiron-Tudor, A., Deliu, D., Farcane, N., & Dontu, A. (2024). Perspectives on how robotic process automation is transforming accounting and auditing services. *Accounting Perspectives, 23*(1), 7-38. https://doi.org/10.1111/1911-3838.12351

Tümmler, M., & Quick, R. (2025). How to detect fraud in an audit: A systematic review of experimental literature. *Management Review Quarterly,* https://doi.org/10.1007/s11301-024-00480-7

Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2004). Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting, 1*(1), 1-21. https://doi.org/10.2308/jeta.2004.1.1.1

Vasarhelyi, M. A., Romero, S., & Kuenkaikaew, S. (2012). Adopting continuous auditing/continuous monitoring in internal audit. *ISACA Journal*, *3*, 1-5.

Vose, D. (2008). *Risk analysis: A quantitative guide* (3rd ed.). John Wiley & Sons.

Wright, G., & Cairns, G. (2011). *Scenario thinking: Practical approaches to the future*. Palgrave Macmillan.

Zhang, C. (A.), Cho, S., & Vasarhelyi, M. (2022). Explainable artificial intelligence (XAI) in auditing. *International Journal of Accounting Information Systems, 46*, 100572. https://doi.org/10.1016/j.accinf.2022.100572