Journal of Business Academy
2023, 4 (2): 155-173
DOI:10.26677/TR1010.2023.1248
Dergi web sayfası: www.isakder.org

Akıllı Otomasyon Sistemlerinin Getirdiği Riskler ve İç Denetime Etkileri

Dr. Berrin KARACAER
İller Bankası A.Ş. Yatırım Değerlendirme Dairesi Başkanlığı, Ankara.
bkaracaer@ilbank.gov.tr, www.orcid.org/0000-0002-4831-8435

Özet

Akıllı otomasyon, robotik süreç otomasyonunun yapay zeka ile öğrenebilme ve karar alabilme becerileri eklenerek geliştirilmiş halidir. Çalışmanın amacı akıllı otomasyon sistemlerinin işletmelerin risk yönetimi ve iç denetim süreçlerine etkilerini incelemektir. Bu amaçla akıllı otomasyon sistemlerinin temel riskleri, yeni riskler karşısında iç denetimin karşılaştığı zorluklar ve bu zorlukların nasıl aşılabileceği konularında değerlendirmelerde bulunulmaktadır. Akıllı otomasyonun getirdiği riskler; teknolojik riskler, düzenleme ve gizlilik riskleri, etik riskler, siber riskler, kurumsal riskler ve finansal riskler olmak üzere altı temel kategori altında incelenmiştir. Akıllı otomasyon riskleri nedeniyle iç denetimin karşılaştığı temel zorluklar ise; artan yetkinlik gereklilikleri, iç denetimin akıllı otomasyonun benimsenmesindeki rolü ve konumu ile akıllı otomasyonu izleme ve denetleme yöntemleri ile ilgilidir. Son olarak iç denetimin yetkinliklerinin gelişen teknolojilere paralel olarak geliştirilmesi, esnek kaynak bulma modellerinin değerlendirilmesi, iç denetimin akıllı otomasyonu benimseme sürecine erken evrelerde dahil olması ve veri analizi yeteneklerinin geliştirilmesi tavsiye edilmektedir.

Anahtar Kelimeler: Akıllı Otomasyon Sistemleri, Yapay Zeka, İç Denetim, Risk Yönetimi.

Makale Gönderme Tarihi: 28.04.2023

Makale Kabul Tarihi: 02. 06. 2023

Önerilen Atıf:
Karacaer, B. (2023). Akıllı Otomasyon Sistemlerinin Getirdiği Riskler ve İç Denetime Etkileri, *İşletme Akademisi Dergisi,* 4 (2): 155-173.

Journal of Business Academy
2023, 4 (2): 155-173
DOI:10.26677/TR1010.2023.1248
Dergi web sayfası: www.isakder.org

The Risks of Smart Automation Systems and Their Effects on Internal Audit

Dr. Berrin KARACAER
İller Bankası A.Ş. Yatırım Değerlendirme Dairesi Başkanlığı, Ankara.
bkaracaer@ilbank.gov.tr, www.orcid.org/0000-0002-4831-8435

Abstract

Smart automation is the development of robotic process automation by adding learning and decision-making skills with artificial intelligence. The aim of the study is to examine the effects of smart automation systems on the risk management and internal audit processes of enterprises. For this purpose, evaluations are made on the main risks of smart automation systems, the challenges faced by internal audit in the face of new risks and how these difficulties can be overcome. The risks brought by smart automation; technological risks, regulatory and privacy risks, ethical risks, cyber risks, corporate risks and financial risks. The main challenges faced by internal audit due to smart automation risks are; the growing competency requirements relate to the role and position of internal audit in the adoption of smart automation, and the methods for monitoring and auditing smart automation. Finally, it is recommended to develop internal audit competencies in line with emerging technologies, evaluate flexible sourcing models, involve internal audit in the early stages of adopting smart automation, and develop data analysis capabilities.

Keywords: Intelligent Automation Systems, Artificial Intelligence, Internal Audit, Risk Management.

Received: 28. 04. 2023

Accepted: 02.06.2023

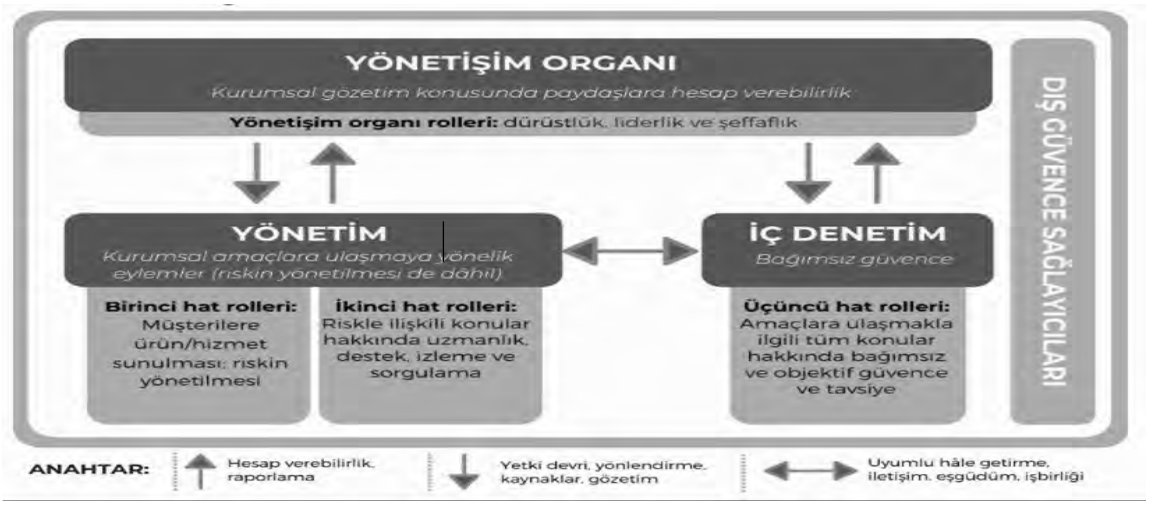
Suggested Citation:
Karacaer, B. (2023). The Risks of Smart Automation Systems and Their Effects on Internal Audit, *Journal of Business Academy*, 4 (2): 155-173.

1. GİRİŞ

Son yıllarda bilgi teknolojilerinde yaşanan önemli gelişmeler ve daha fazla verimlilik elde etmenin yollarını arayan işletmelerin bu yeni teknolojileri benimseme eğilimleri tüm sektörlerde dönüştürücü değişimlere öncülük etmiştir. Gelişmekte olan teknolojiler sunduğu fırsatların yanında önemli riskleri de beraberinde getirmektedir. İşletmeler, teknolojik yatırımların potansiyelini kullanabilmek için yeni risklerin yönetimi konusunda da yeni yaklaşımlar geliştirmek zorundadır. İşletmelerin karar alma sürecinin bir parçası olarak risk yönetiminin rolü, özellikle yeni teknolojilerin sunduğu fırsatlar ve risklerin yarattığı belirsizlik neticesinde günümüzde son derece önemli bir konu haline gelmiştir. Ayrıca, artan belirsizlik düzenleyici ortamı daha karmaşık hale getirmekte ve kurumsal risklerin dış paydaşlara rapor edilmesi gerekliliklerini artırmaktadır (Niemi, 2018: 328).

Risk yönetiminin amacı, işletmelerin hedeflerine ulaşmasına yardımcı olmak için faaliyetlerini etkileyebilecek riskleri belirlemek, izlemek ve yönetmektir (Niemi, 2018: 322). Risk yönetiminin amacı sadece sınırlar koymak değil, aynı zamanda risk iştahı açısından makul fırsatların değerlendirmesini sağlayarak kuruluşun hedeflerine ulaşmasına katkıda bulunmaktır. Kurumsal risk yönetimi, risk yönetiminin organizasyonel düzeyde gerçekleştirilmesi ve strateji planlamasında dikkate alınması açısından geleneksel risk yönetiminden farklıdır. Kurumsal risk yönetiminde temel amaç, kurumu etkileyebilecek potansiyel olayları belirleyerek, bunları belirlenen risk iştahı dahilinde yönetmek ve organizasyonun stratejik hedeflerine ulaşmaktır. (Fraser ve Simkins, 2010: 1)

Uluslararası İç Denetçiler Enstitüsü (The Institute of Internal Auditors-IIA)'nün geliştirdiği "Üçlü Savunma Hattı" modeli risk yönetimi süreçlerinde yaygın olarak kullanılmaktadır. Model, büyüklükleri ve karmaşıklıkları ne olursa olsun tüm işletmelere uygun olacak şekilde tasarlanmıştır ve risk yönetiminin rollerini ve görevlerini netleştirmektedir. Modele göre, işletmelerde etkin risk yönetimini sağlamak için üç hat gereklidir. İlk savunma hattı, yönetim kontrolleri ve iç kontrol önlemleridir. İkinci hat, yönetim tarafından oluşturulan çeşitli risk kontrol ve uyum gözetim fonksiyonlarından oluşmaktadır. Bağımsız güvence, yani iç denetim ise üçüncü savunma hattıdır. Her hattın kuruluşun yönetişim çerçevesinde ayrı bir rolü bulunmaktadır (IIA, 2013a: 2).



Kaynak: KPMG, Dijitalleşme Yolunda Türkiye Raporu,2021.

Şekil 1. Üçlü Hat Modeli

Kurumların riskleri değiştikçe bir güvence fonksiyonu olarak iç denetimin de değişerek güncellenmesi kaçınılmazdır. Yeni tür riskler, işletmeleri yalnızca riskleri farklı şekilde yönetmeye değil, aynı zamanda organizasyonel değişiklikler yapmaya da zorlamaktadır.

İç denetimin misyonu; risk yönetimi, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirerek ve iyileştirerek, kuruluşun gelişimini ve hedeflere ulaşmasını desteklemek için objektif bir değerlendirme, güvence ve danışmanlık sağlamaktır (www.iia.org.uk). İç denetimin birincil işlevi, kuruluş ve faaliyetleri hakkında bağımsız ve nesnel görüşler sağlayarak ve bunların iyileştirilmesi için önerilerde bulunarak kuruluşun en yüksek yönetim organını (Yönetim Kurulu) ve üst yönetimi desteklemektir. Dolayısıyla iç denetim, yönetim kurulu, üst düzey yönetim ve denetçilerle birlikte kurumsal yönetişim sisteminin bir parçasıdır (Niemi, 2018: 13).

İç Denetimin gelişimi, denetimin yalnızca destekleyici bir işlevi olduğu zamandan bu yana devam etmektedir. Bu gelişim süreci içerisinde muhasebe mesleğini ve iç denetimi de etkisi altına alan Sarbanes-Oxley Yasası (veya SOX Yasası) büyük bir dönüm noktası olmuştur. SOX Yasası'nın ardından, COSO[1] çerçevesi, bilişim teknolojileri (BT) denetimi ve veri analizi gibi gelişmeler, iç denetim fonksiyonunun ilerlemesine katkı sağlamıştır. Ancak günümüzde dünyada dördüncü endüstriyel devrim yaşanmaktadır ve işletmeler yeni ve sürekli gelişen risklerle yüzleşmek durumundadır. Yeni stratejiler, uygulamalar ve teknolojiler karşısında iç denetim, güncel kalmak ve işletmelerde değer yaratmak için yeni vizyon ve yöntemler benimsemelidir (Hatherell, 2018: 1).

İç denetim fonksiyonunun geliştirilmesine yönelik araştırma ihtiyacı, IIA ve COSO gibi organizasyonların yanında başta dört büyük şirket (KPMG, Deloitte, E&Y ve PWC) olmak üzere dış denetim hizmeti veren şirketler tarafından da fark edilmiştir. Bu çerçevede COSO ve Deloitte 2015 yılında Siber Çağda COSO (COSO in the Cyber AGE) adında ortak bir rapor yayınlamışlardır. Rapor ile gelişen teknolojilerin getirdiği siber risklerin değerlendirilme süreçleri doğrultusunda COSO modelinin nasıl güncelleneceği ifade edilmektedir (COSO, 2015: 1-2).

KPMG'nin 2016-2017 yıllarında 250 organizasyon üzerinde gerçekleştirdiği araştırmasında gelişen teknoloji risklerinin değerlendirilmesi ve hafifletilmesi kapsamında esneklik, etkinlik ve etkililik hususlarının yanında kaynak kısıtlılığı, BT iç denetçilerinin karşısına çıkan engeller olarak tespit edilmiştir. Araştırmada BT iç denetçileri tarafından odaklanıldığı tespit edilen operasyonel risklerin; nitelikli personel gereksinimi, bütçe değişiklikleri , risk değerlendirmede yeterlilik ihtiyacı, veri analitiğinden faydalanma ve entegre güvence yaklaşımı gibi konular olduğu ortaya konulmaktadır (KPMG, 2017: 12). ABD'de bilgi teknolojileri üzerine bir araştırma ve danışma kuruluşu olan Gartner'ın 2019 yılındaki araştırması denetçilerin gelecek yıl odaklanmaya hazırlandıkları riskleri belirlemeyi ve analiz etmeyi amaçlamaktadır. Araştırma ile altı çizilen on iki risk arasında siber güvenlik, verilerin gizliliği, dijitalleşmenin neden olduğu iş değişiklikleri ve otomasyonun stratejik iş gücü planlaması üzerindeki etkisi yer almaktadır (Christofferson vd., 2018: 18).

Avrupa İç Denetim Enstitüleri Konfederasyonu (European Confederation of Institutes of Internal Auditing-ECIIA) da yıllık olarak Avrupa'da faaliyet gösteren kuruluşların denetim yöneticileri

[1] COSO, "Hileli Mali Raporlama Üzerine Ulusal Komisyon"a destek olarak 1985 yılında gönüllü kuruluşlar tarafından oluşturulmuştur. Amacı kurumsal yönetim araçlarıyla finansal raporlamanın kalitesini artırmaktır. COSO, "İç Denetçiler Enstitüsü" tarafından yayımlanan 'İç Kontrole İlişkin İşletme Raporunun Hazırlanmasında İç Denetçilerin Rolü' adlı raporda açıklandığı şekilde, denetim sürecine entegre edilmiş bir iç kontrol modelidir. Model uyarınca iç kontrol sisteminin temel hedefi; organizasyonun etkin şekilde çalışmasını, finansal raporlarının güvenilirliğini ve yasal çerçeveye uyumunu sağlamaktır. COSO modeli şu beş unsura dayanmaktadır: "kontrol ortamı, risk değerlendirme, kontrol faaliyetleri, bilgi ve iletişim ile izleme".

tarafından belirlenen temel iş risklerini araştırmaktadır. Risk in Focus 2020 adlı araştırma, şirketlerin yeni teknolojilerin neden olduğu risklere odaklandığını ortaya koymaktadır. Araştırmada, iç denetim yöneticilerine kuruluşları için en önemli buldukları riskin ne olduğu sorulmuş ve %21 ile en yüksek risk unsuru siber ve veri güvenliği riskleri olurken, bunu %18 ile dijitalleşme, yıkıcı teknolojiler ve diğer yenilikler izlemiştir (ECIIA, 2019: 8).

Tüm sektörlerdeki işletmeleri dönüştüren teknolojilerden biri de akıllı otomasyon sistemleridir. Robotik süreç otomasyonu (RPA) ile birleştirilen yapay zeka yeteneklerine akıllı otomasyon denmektedir. Akıllı otomasyon, tüm iş akışlarının otomasyonunu sağladığı için işletmeler üzerinde büyük bir etkiye sahip olabilmektedir. Akıllı otomasyon ile insan algısı gerektiren tahminler ve kararlar otomatikleştirilebilmekte ve bu sistemler finans sektöründen hukuk, eğitim vb. sektörlere kadar birçok alanda kullanılabilmektedir. Akıllı otomasyon sistemlerinin iş süreçlerinde sağladığı fayda açıktır ancak aynı zamanda yeni risk türlerini de beraberinde getirmektedir.

İşletmeler, akıllı otomasyon risklerini yönetmenin yeni yollarını ararken, , üçüncü savunma hattı olarak iç denetimin de geliştirilmesi gerekmektedir. Özellikle akıllı otomasyon sistemlerinin karar alma sürecindeki opak yapıları, sistemin anlaşılmasını zorlaştırmaktadır. Bu araştırmanın amacı, akıllı otomasyon sistemlerinin işletmeler için getirdiği temel riskleri, bu risklerin iç denetim için ne tür zorluklar oluşturduğunu ve iç denetimin yeni teknolojilere ayak uydurmak ve güncel kalabilmek için ne tür önlemler alabileceğini araştırmaktır.

2. LİTERATÜR

Akıllı otomasyonun kullanımının tüm sektörlerde artış göstermesi, bu konudaki ulusal ve uluslararası çalışmaların sayısında da artış yaratmıştır. Denetim alanında yapılan çalışmalar akıllı otomasyon sistemlerinin denetim faaliyetlerindeki kullanımı konusuna yoğunlaşmaktadır. Literatürde akıllı otomasyon sistemlerine risk perspektifinden yaklaşan az sayıda çalışma bulunmaktadır. Önceki literatürden tanımlanan akıllı algoritmaların riskleri çoğunlukla algoritma opaklığı, yanlış algoritma tasarımı veya uygulaması ve algoritmalara artan güven ile ilgilidir.

Osoba ve Wesler (2017) kitap çalışmalarında özellikle algoritmalar ve algoritmalara duyulan tam güven ile ilgili riskleri belirlemişlerdir. Lehto (2017) ve Băjenescu (2018) da yayınlarında algoritma risklerini tartışmaktadır. Petrasic vd. (2017) çalışmalarında finans endüstrisindeki algoritmalar ve yanlılık riski üzerinde durmuşlardır.

Çoğu çalışma, büyük miktarda veri ve veri işlemede insan müdahalesinin olmaması gibi yapay zekanın özellikleriyle de ilgilenmiştir. Gizli verilerin kişisel veya diğer yollarla kullanılması, kuruluşlar için daha fazla ve sürekli artan düzenleyici gereklilikler anlamına da gelmektedir. Bu veriler ve gizlilikle ilgili riskler, Lehto (2017), Lehto ve Nettaanmäki (2015) tarafından tartışılmıştır. Jedrzejka (2019), robotik süreç otomasyonunun muhasebe uygulamalarında kullanımı; Ting-Po vd. (2002), akıllı otomasyon teknolojileri ve performansı; Kokina ve Davenport (2017) yapay zeka ve kontrol üzerine çalışmalar yapmıştır. Zhang (2019) ise akıllı otomasyon sistemlerinin denetimin etkinliğini ve verimliliğini artıracağını ortaya koymuştur.

Türkiye'de Erdoğan (2019) yapay zeka ve kontrol; Kurnaz ve Kestane (2020) ise yapay zekanın iç denetim üzerindeki etkisi konusunda çalışmalar yapmıştır. Karyağdı (2022) nitel araştırma yöntemlerini kullanarak güncel teknolojilerin denetim sürecine etkisi üzerine yaptığı çalışması ile denetimin niteliği ve süresi üzerinde olumlu, istihdam konusunda ise olumsuz etkilerinin olabileceği sonucuna varmıştır.

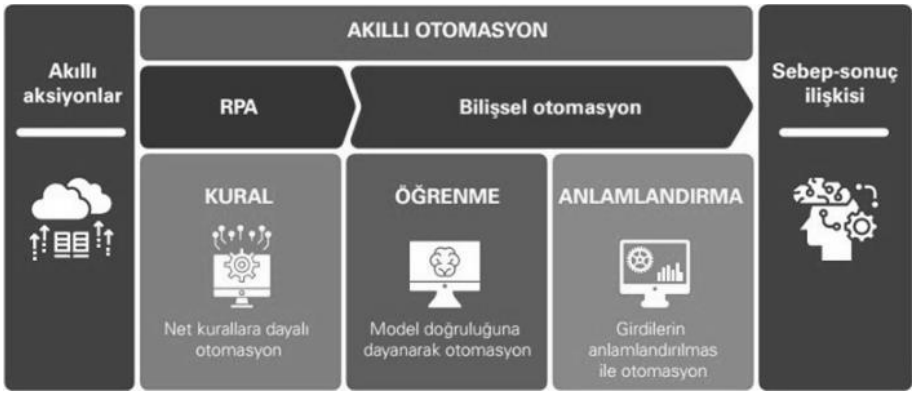
Akıllı otomasyon sistemlerine risk perspektifinden bakan çalışmalar daha çok siber riskler ve siber risklerin yönetimi konusunda yoğunlaşmaktadır. Kurt ve Uysal (2015) çalışmalarıyla COSO

modeli çerçevesinde siber risklerin yönetilmesine ilişkin geliştirilecek iç kontrol sistemi üzerinde durmuşlardır. Öztürk (2018) ise çalışmasında önerilen denetim modeli çerçevesinde siber tehditleri tartışmıştır. Selimoğlu ve Saldı (2019) da siber risklerin yönetiminde iç denetimin rolü üzerine çalışmışlardır.

3. AKILLI OTOMASYON SİSTEMLERİ

Gelişen teknolojilerin işletmeler üzerindeki etkisi yüzyıllardır kaçınılmaz olmuştur. İlk örneklerden biri olarak sanayi devrimi ile üretim sistemleri kısmen otomatikleştirilmiş ve böylece üretim kapasitesinde önemli bir artış sağlanmıştır. İkinci aşamada elektronik iş sistemlerinin yaygınlaşması ile işletmeler takibi zaman alan iş süreçlerini elektronik ortama taşıyarak verim ve hız avantajı sağlamışlardır. İnternet teknolojisinin gelişimiyle ise işletmeler bilginin hızlı iletilmesini ve iletişimin yaygınlaşmasını iş süreçlerine yansıtmışlardır. Günümüzde teknolojinin işletmeler üzerindeki etkisinin en güncel örneğinin akıllı otomasyon sistemleri olduğu söylenebilir.

Akıllı otomasyon, RPA süreçlerinin yapay zeka teknolojileri kullanılarak geçmiş verilerden öğrenebilme ve karar alabilme becerileri eklenmiş şekilde geliştirilmiş halidir. RPA, kesme, yapıştırma ve birleştirme gibi kurallara dayalı, tekrarlayan görevleri taklit edebilen bir yazılım programıdır ve basit BT görevlerini harici yazılımla otomatikleştirmek için kullanılmaktadır (Christofferson vd, 2018: 25). Bilişsel beceriler gerektiren uçtan uca süreçleri otomatikleştirmek için yapay zeka yeteneklerinin RPA'ya entegre edilmesi gerekmektedir. Basitçe yapay zeka, makinelerin tahminlerde bulunma, verilerden öğrenme, resim ve seslerden anlam bulma gibi insan zekası gerektiren görevleri yerine getirebilmesi anlamına gelmektedir (Watson vd., 2019: 13). RPA'ya entegre edilen bilişsel teknolojilerin bu kombinasyonuna akıllı otomasyon denmektedir.



Kaynak: KPMG, Dijitalleşme Yolunda Türkiye Raporu,2021.

Şekil 2. Akıllı Otomasyon Sistemi

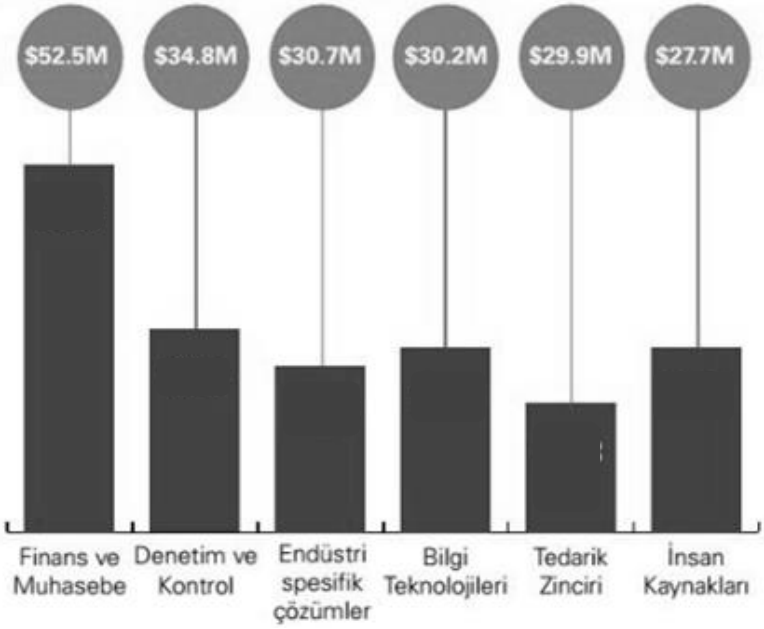
Akıllı otomasyon sistemleri ile tüm iş süreçlerini otomatikleştirmek neredeyse mümkün hale gelmiştir; çünkü yapay zeka, insan değerlendirmesi gerektiren görevleri de gerçekleştirebilmektedir. RPA, üretkenliği artırma, maliyeti düşürme ve müşteri deneyimini iyileştirme gibi birçok fayda sağlarken bilişsel yetenekleri RPA'ya entegre etmek bu faydaları daha da ileriye götürmektedir.

Deloitte'un akıllı otomasyon anketi, kuruluşların akıllı otomasyon uygulamasından bekledikleri ilk üç faydanın verimlilik artışı, maliyet azaltma ve müşteri deneyimini geliştirme olduğunu ortaya koymaktadır (Watson vd, 2019: 18). Akıllı sistemler doğru bir şekilde uygulandığında işlem hızını artırmakta, insan hatalarını azaltmakta, işçilik maliyetlerini düşürmekte ve aynı

zamanda müşteri hizmetleri deneyimini geliştirmektedir. Akıllı otomasyonun sekiz temel avantajı; doğruluk, hız, hizmet sürekliliği, daha yüksek işlem verimliliği, kullanım kolaylığı, iş gücü çevikliği, ölçeklenebilir altyapı ve stratejik odaklanma şeklinde özetlenmektedir (Patel, 2018: 33).

Büyük miktarda veriyi dikkate alan ve kısıtlı zamanda etkili kararlar almak isteyen işletmeler algoritmalara giderek daha fazla güvenmektedir. Akıllı otomasyon sistemleri, ekonominin hemen her sektöründe iş yapma biçimlerini değiştirmeye başlamıştır (Laurent vd., 2015: 2). KPMG'nin uluslararası 90 işletme üzerinde yaptığı bir araştırmaya göre işletmelerin %94'ü yapay zeka kullanımını rekabet açısından son derece önemli bulurken; %60'dan fazlası akıllı otomasyon sistemlerini aktif olarak kullanmaktadır (KPMG, 2021: 16). Ayrıca araştırma işletmelerin %52'sinin akıllı otomasyon teknolojisine 10 milyon dolardan fazla yatırım yaptığını, akıllı otomasyonu devreye sokan yöneticilerin %30'unun akıllı otomasyonu aynı zamanda hizmetlerini geliştirmek için bir fırsat olarak gördüğünü ortaya koymaktadır (KPMG, 2021: 16). Bu durum işletmelerin akıllı otomasyonun faydalarını kavradıklarını göstermektedir.

Hemen hemen tüm sektörlerde kullanılmaya başlanmakla birlikte, akıllı otomasyon sistemlerine yönelik en büyük yatırım harcamaları finans ve muhasebe sektöründe yapılmaktadır. Denetim ve kontrol alanında da özellikle son yıllarda akıllı otomasyon teknolojilerinden önemli derecede faydalanılmaktadır.



Kaynak: KPMG, Dijitalleşme Yolunda Türkiye Raporu,2021.

Şekil 3. Akıllı Otomasyon Harcamalarının Sektörel Dağılımı

4. AKILLI OTOMASYON SİSTEMLERİNİN GETİRDİĞİ RİSKLER

İşletmeler, akıllı otomasyon sistemlerinden fayda sağlarken aynı zamanda yeni zorluklar ve risklerle de karşı karşıya kalmaktadır. Genel olarak yeni teknolojilerin tamamı, işletmelerin risk yönetimi, iç denetim planlaması ve yürütülmesi faaliyetlerini yeniden gözden geçirmesini zorunlu kılmaktadır. Bu bölümde akıllı otomasyon teknolojilerinin işletmelere getirdiği yeni riskler üzerinde durulacaktır. Literatürden ve önceki araştırmalardan yola çıkılarak bu riskler şu kategoriler altında incelenecektir: teknolojik riskler, düzenleme ve gizlilik ile ilgili riskler, etik riskler, siber riskler, kurumsal riskler ve finansal riskler.

4.1. Teknolojik Riskler

Yapay zeka sistemlerinin karar verme ilkeleri genellikle işletmeler için opak yapıdadır. Başka bir deyişle sonuçlar için açıklama üretilmez yani karar süreci şeffaf değildir. Bu durum işletmeler için uygunsuz kararların izlenmesini zorlaştırabilmektedir. Dolayısıyla yanlı veriler, uygun olmayan modelleme teknikleri ve yanlış algoritmalar gibi güvenlik açıklarının fark edilmesi zaman alabilmektedir. Bu zaman zarfında yapay zeka sistemleri, işletme operasyonları üzerinde büyük etkisi olabilecek taraflı sonuçlar üretebilmektedir.

Akıllı robotlar öğretilen algoritmalara göre çalışmaktadır Algoritmalar, insan düşünme ve karar verme sürecini modeller. Algoritma tasarımındaki zorluk, farklı durumları ve koşulları yöneten, mantıklı ve analitik karar verebilen tasarımları sağlamaktır. Algoritmalar karar verebilmeli ancak sınırlı çözüm seçeneklerine göre çalışmalıdır (Lehto, 2017: 9). Agoritmaların şeffaflığı gelişmekte olan bir araştırma alanı olmakla birlikte, işletmelerin ölçekleri büyüdükçe depolanan veri miktarının da büyümesi ve karar verme süreci için kullanılan veri analitiğinin karmaşıklaşması şeffaflık gereksinimleri de artırmaktadır. Algoritmik şeffaflık birkaç nedenden dolayı önemlidir. İlk olarak, karar verme sürecinin mantığı net değilse, algoritmik kararlardaki hataları belirlemek de zor olmaktadır. Karar verme sürecindeki şeffaflık, uygun olmayan karar modellerinin belirlenmesi durumunda işletmeleri uygun düzeltici önlemleri almaya teşvik etmektedir. İkincisi, şeffaflık, algoritma tarafından kullanılan girdi verilerindeki hataları belirlemeye yardımcı olmaktadır. Son olarak, hatalar veya olumsuz kararlar şeffaflıkla fark edilirse zaman kaybetmeden önlenebilmektedir. Karar verme mantığı düzeltilebilir veya girdi verilerindeki özellikler amaca uygun olacak şekilde değiştirilebilir (Datta vd., 2016: 1).

"Algoritmaların yanlış davranması" riskini daha ciddi hale getiren şey, algoritmalara karşı eleştirel olmayan güvenin artmasıdır. Otomasyon, insan yanlılığı olasılığını azaltsa bile, tutarlılıkları tarafsızlıkla eşdeğer değildir (Osoba vd, 2017: 2). Bu nedenle, akıllı sistemlere aşırı güvenin ek risk alınmasına yol açabileceği ve hatta sistem riskini artırabileceği unutulmamalıdır (Jaksic & Marinc 2019, 11). Algoritmaların doğruluğuna sorgusuz güvenmek, özellikle tüm süreçleri otomatikleştirmek için kullanılan akıllı otomasyonda büyük bir soruna yol açabilmektedir. Herhangi bir insan müdahalesi olmadan, tüm iş süreçleri geri dönülemez sonuçlara yol açacak kadar uzun süre yanlış çalışabilir. Bu noktada hesap verebilirlik konusu da tartışmalıdır. Algoritmik kararlara güvenen tarafın mı yoksa algoritmayı tasarlayan tarafın mı hesap verebilir olduğunu belirlemek de işletmeler açısından önemlidir (Datta vd., 2016: 3).

Teknolojik riskin temelinde insan olduğunu kabul etmek gerekmektedir. Tüm yazılımlar insanlar tarafından geliştirildiğinden, geliştirilen yazılımlar da her zaman tarafsız olamamaktadır. Bu durum, yazılımların çalışması gerektiği gibi çalışmamasına veya yazılımların siber saldırılara yol açabilecek güvenlik açıklarına sahip olmasına neden olmaktadır. Yazılım riskleri, kendi kendini yöneten yapıları ve işledikleri büyük miktarda veri nedeniyle özellikle yapay zeka yazılımlarında çok büyük etkilere sebep olabilmektedir (Lehto, 2017: 8).

Özellikle küçük ölçekli işletmeler donanım yetersizliği ve maliyet baskıları nedeniyle akıllı otomasyon için destek geliştirme becerilerine sahip olmadığından, dışarıdan temin yoluyla üçüncü taraf satıcılara olan talep artmaktadır (Watson vd., 2019: 2). Üçüncü taraf satıcıların artan kullanımı, kesinti riskleri gibi geleneksel üçüncü taraf risklerini de artırmaktadır. Bunun yanında dışarıdan temin edilen akıllı otomasyon, yeni risk türleri de oluşturmaktadır. Algoritma tasarımına ve temel alınan verilere ilişkin şeffaflık, harici satıcılar kullanıldığında daha da sınırlı olmaktadır (Albinson vd., 2019: 7).

Son olarak; akıllı otomasyon sistemlerini izleme teknolojsinin gelişimi, akıllı otomasyon sistemlerinin gelişimi kadar hızlı değildir. Ayrıca izleme tekniklerinin işletmeler tarafından benimsenmesinin gecikmesi de risk oluşturmaktadır (Albinson vd., 2019: 6). Dolayısıyla akıllı

otomasyonun teknolojik risklerini yönetmek için akıllı otomasyon kararlarında iç denetim yoluyla şeffaflık aramak son derece önemlidir (Albinson vd., 2019: 6).

4.2. Düzenleme ve Gizlilik İle İlgili Riskler

Yasal düzenlemeler teknolojik gelişmelere gecikmeli olarak tepki verdiğinden bu durum bir takım risklere yol açmaktadır. Özellikle büyük hacimli veri kullanan sistemler için gizlilik ile ilgili düzenlemelerin hayata geçirilmiş olması son derece önemlidir.

Teknolojinin evrimi hiç olmadığı kadar hızlı olduğundan ve işletmeler yeni sistemleri çok daha rekabetçi bir ortamda hızla uygulamaya zorlandığından, bir süre düzenleyici çerçeve yokluğuyla mücadele edilmektedir. İşletmelerin bu süre boyunca gelecekteki düzenleyici ortam hakkında bilgi sahibi olmadan dijital stratejiler oluşturması gerekmektedir. Düzenlemelerdeki bu gecikme, işletmeler için yasal çerçeveyle uyumlu olmama ile uyumluluk gerekliliklerini karşılamak için büyük çaba sarf etme veya dijital öncelikli bir strateji yürütme ile mevcut ve gelecek tüm düzenlemelere uyma arasında bir seçim yapma riski yaratmaktadır. Rakiplerin dijital stratejileri uygulayabilecekleri ve bu nedenle önemli rekabet avantajlarına sahip olabilecekleri düşünüldüğünde, gelecek düzenlemeleri bekleme stratejisi de riskli bir seçim olabilmektedir (Christofferson vd., 2018: 17).

Akıllı otomasyon sistemlerinde kullanılan kişisel bilgiler ve tüketici gizliliği birçok ülkede yasal düzenlemelerle korunmaktadır. Türkiye'de bu husus Kişisel Verilerin Korunması Kanunu ile düzenlenmiştir. Kanun genel olarak kişisel bilgilerin kullanımına ilişkin pek çok düzenlemenin yanı sıra özel olarak otomatik bilgi işlemeye ilişkin düzenlemeleri de içermektedir. Kanun ile veri işleme yapan gerçek ve tüzel kişilerin sorumlulukları düzenlenerek, kişisel veri gizliliğinin sağlanması amaçlanmaktadır. Kanun kapsamında veri sorumlusu; kişisel verilerin işlenmesinin amaçlarını ve araçlarını belirleyerek, veri kayıt sisteminin oluşturulması ile yönetilmesinden sorumlu olan kişi şeklinde tanımlanmaktadır. Ayrıca veri sorumlusu, organizasyon içinde kişisel verilerin korunmasına ilişkin düzenlemelere uyumu sağlamak amacıyla denetimler yapmakla görevlendirilmiştir.

İşletmelerin akıllı otomasyonun arkasındaki mantığın doğru olduğundan, hata risklerinin en aza indirildiğinden, verilerin güvence altına alındığından ve otomasyonun herhangi bir şekilde ayrımcı olabilecek sonuçlar sağlamadığından emin olması zorunludur. Bu zorunluluk işletmeler için dış ve iç denetimde birçok gerekliliği de beraberinde getirmektedir.

4.3. Etik Riskler

Yapay zeka sistemleriyle ilgili önemli konulardan biri de etiktir. Genellikle insan davranışını belirleyen ahlaki ilkeler, algoritmaların davranışını da belirlemektedir. Buradaki zorluk, insanların etik konularda her zaman hemfikir olmaması ve bazen topluma göre neyin kabul edilebilir olduğunu belirlemenin zor olabilmesidir (Kananen ve Puolitaival, 2019: 220).

Yapay zekanın geliştirilmesinde amacın insan düşüncesine mümkün olduğunca yaklaşmak olduğunu savunanlar olduğu gibi ideal rasyonaliteyi yansıtmak olduğunu savunanlar da bulunmaktadır (Ollila 2019, 29). Yapay zekanın amacı konusundaki bu fikir ayrılığı, etikliği konusunda da fikir birliğinin sağlanmasını zorlaştırmaktadır. Yapay zekanın davranışını bu yorumlar belirlediğinden, sonuçlara nasıl vardığından ve sonuçların doğruluğundan emin olmak zor olabilmektedir. Algoritmanın kararlarında etik kuralları dikkate aldığından ve etik kurallarla tahminler yaptığından emin olmak zor olabileceğinden, algoritmanın bu konudaki opaklığı akıllı otomasyonun kullanımında risk yaratmaktadır (Kananen ve Puolitaival, 2019: 221).

Yeni yapay zeka yetenekleri geliştikçe, işletmeler bu teknolojileri kullanmaya etik etkilerini de dikkate alarak karar vermelidir. Uluslararası danışmanlık ve araştırma şirketi olan Gartner'ın

2019 yılında gerçekleştirdiği "Denetimin Sıcak Noktaları Anketi"ne göre işletmelerin %59'u dijitalleşmeyle ilgili etik zorluklarla karşılaştığını bildirmektedir (Christofferson vd., 2018: 19). Algoritmik kararların karmaşıklığı ve şeffaflığının olmaması önemli zorluklar yaratmaktadır. Tıp ve hukuk gibi alanlarda veri analitiği ve yapay zeka kullanımları genişledikçe, etik risklerin sonuçlarının da şiddetlenerek artacağı düşünülmektedir (Christofferson vd., 2018: 21).

Dijital gelişmelerin etik etkilerinin yeterince yönetilmemesi kritik sonuçlar yaratabilmektedir. Akıllı otomasyonun etik riskinin iki yönü bulunmaktadır. İlki, akıllı otomasyonun etik açıdan taraflı davranması nedeniyle ayrımcılığa yol açan yapay zeka uygulamaları ile ilgili risklerdir. Amazon'un iş başvurularını taramak için kullandığı yapay zeka sisteminin kadınlara yönelik ayrımcı olduğunun ortaya çıkması bu duruma örnektir. İkinci olarak; itibar riski ve müşteri memnuniyetsizliği nedeniyle önemli iş fırsatlarından yararlanılamaması da işletmeler için önemli sonuçlar doğurmaktadır. Tüketicilerin %85'i, kişisel verilerinin korunduğuna güvenmediği takdirde o işletme ile ilişkilerini keseceğini belirtmektedir (PwC, 2017: 3). Aynı zamanda önyargılı, ayrımcı ve opak yapıdaki yapay zeka sistemleri işletmeler için önemli yasal riskler de doğurmaktadır.

4.4. Siber Riskler

Siber riskler bilgi teknolojilerinin gelişmesiyle oluşan siber ortamdan kaynaklı risklerdir. Siber ortam, dünyaya ve uzaya yayılmış olan bilişim sistemleri ile bu sistemler arasında bağ kuran ağlardan oluşmaktadır (Türkiye Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı: 2).

Şirketler dijitalleşirken ve ileri teknolojileri daha fazla benimserken, aynı zamanda yeni zayıf bağlantılar oluşmaktadır. Her yıl 111 milyar yeni yazılım kodu üretildiği ve 2016'da 6,4 milyar olan bağlı cihaz sayısının 2022'de 20,4 milyar olduğu tahmin edilmektedir (Christofferson vd, 2018: 11). Akıllı teknolojilere artan güven, güvenlik sorunlarının fark edilmesini de yavaşlatmaktadır (Christofferson vd., 2018: 11). Yapay zeka sistemleri çok büyük miktarda veriyi işleyebildiğinden, kişisel verileri veya bir şirket hakkındaki gizli bilgileri çalmak isteyen bilgisayar korsanlarının yapay zeka sistemlerini hedef alma olasılığı giderek artmaktadır (Kananen and Puolitaival, 2019: 225). Siber güvenlik, insan faaliyetleri, organizasyonel süreçler ve bilgi teknolojisi üzerine kuruludur ve akıllı otomasyonun benimsenmesi, uygulanması ve kullanılmasının önemli bir parçasıdır. Siber güvenlik çözümleri mümkün olan en iyi şekilde yürütülmezse, işletmenin bilgi teknolojisi altyapısı ve verileri üzerinde ciddi sonuçlara neden olabilmektedir (Lehto, 2017: 12). Siber güvenlik, yalnızca olası tehditleri önlemekle ilgili olmamalı, aynı zamanda rekabetçi bir değer yaratıcısı olmalıdır. Verileri güvende tutma ve siber ihlallere hızla yanıt verme yeteneği, paydaşlarla güven oluşturmak için önemli bir fırsattır (ECIIA, 2019: 16).

Uyum sürecinin başından itibaren olası siber tehditlerin belirlenmesi, akıllı otomasyonun veya genel olarak yeni teknolojilerin kullanılması için bir ön koşuldur. Ancak siber tehditlerin tespit edilmesi ve değerlendirilmesi, uyum aşamasıyla sınırlı kalmamalıdır. Güvenli yazılım tasarımı, sistem yaşam döngüsü boyunca devam etmelidir. Ayrıca, doğru uygulanan güvenlik çözümleri, örneğin etik riskler gibi ilgili diğer risklerin yönetilmesine de yardımcı olabilmektedir.

ECIIA'nın "Risk in Focus 2020"adlı risk araştırmasına göre Avrupa çapında 528 iç denetim yöneticisinden %78'inin siber güvenlik ve veri güvenliğini işletmelerinin karşı karşıya olduğu en önemli beş riskten biri olarak gördüğünü ve %21'inin en yüksek risk unsuru olarak seçtiğini ortaya koymuştur. Ayrıca iç denetim yöneticilerinin %68'i siber güvenlik ve veri güvenliğinin, işletmelerde iç denetimin zamanının çoğunu harcadığı ilk beş riskten biri olduğunu ifade etmiştir (ECIIA, 2019: 11).

Yeterli kontrol ortamının güvencesi ve sağlayıcısı olarak iç denetimin siber güvenlik üzerinde önemli etkisi olmaktadır. COSO tarafından siber risklerin yönetimi dikkate alınarak "Siber Çağda COSO (COSO in the Cyber Age)" isminde bir rapor hazırlanmıştır (COSO, 2015). Rapor ile siber risklerin değerlendirilmesi için, güncellenen bir bakış açısıyla iç kontrol bileşenlerine vurgu yapılmakta ve siber risklerin yönetimi için rehberlik sağlanmaktadır. Ayrıca COSO dışındaki standartlar ve çerçeveler de işletmelerin siber risklerinin yönetilmesine yardımcı olmaktadır.

4.5. Kurumsal Riskler

Günümüzün belirsiz ve karmaşık ortamı nedeniyle, risk bilincine sahip kurum kültürüne her zamankinden daha fazla ihtiyaç duyulmaktadır. Güvenlik tehditleri ile risk yönetimi arasındaki koordinasyon eksikliği, yıkıcı teknolojilerin neden olduğu risklere karşı verimli sonuçlar alınamamasına yol açabilmektedir. Koordinasyon ve planlama sorunları, kuruluşların yaklaşık yarısının risk iştahı veya tolerans beyanlarına ve %77'sinin resmi bir siber güvenlik müdahale planına sahip olmaması nedeniyle şiddetlenmektedir (Christofferson vd., 2018: 20). Kuruluş çapında geliştirilmiş bir risk kültürünün olmaması; kuruluşların risklere yanıt verecek uygun stratejileri belirleme ve mevcut risk ortamında faaliyetlerini sürdürebilme yeteneklerini azaltmaktadır (Christofferson vd., 2018: 21). ECIIA'nın "Risk in Focus 2020" anketine göre, iç denetim yöneticilerinin %58'i dijitalleşme, yıkıcı teknoloji ve diğer yeniliklerin işletmeler için ilk beş risk arasında olduğunu, ancak aynı zamanda yalnızca %30'u en çok denetlenen ilk beş riskli alan içerisinde olduğunu belirtmektedir (ECIIA, 2019: 18).

İşletmeler açısından otomasyon değişikliğe ve yeniliğe en açık alan olarak görülmesine rağmen birçok işletme bunun kuruluşlarının yetenek ihtiyaçlarını nasıl etkileyeceğini anlamakta zorlanmaktadır. Dijital bir iş dönüşümü beklenirken, otomasyonun istihdam ihtiyacını artırıp artırmayacağı, istihdam şekillerinde değişiklik yaratıp yaratmayacağı veya mevcut işçilerin durumunun ne olacağı gibi konular belirsizlik alanlarıdır. Bu belirsiz alanlar işletmelerin sektörüne ve şirket türüne göre şekillenmektedir. 2020 yılında yapay zekanın 2,3 milyon yeni iş yarattığı ve 1,8 milyon işi ortadan kaldırdığı tahmin edilmektedir (KPMG, 2021: 8). Gelecekteki dijital iş dönüşümlerini desteklemek için ihtiyaç duyulacak iş gücü ve yeterlilikleri konusundaki belirsizlik, işletmelerin hedeflerine ulaşmak için ihtiyaç duydukları işgücüne ve yeterliliklere sahip olmalarını da zorlaştırmaktadır (Christofferson vd., 2018: 29).

Gelişmekte olan teknolojilerin kullanılması, hedeflere ulaşmak ve artan karmaşık güvenlik tehditlerine karşı korunmak için yeni yeterlilikler gerektirmektedir (Christofferson vd., 2018: 29). Gartner'ın "Denetimin Sıcak Noktaları Anketi"ne göre yönetim ve stratejik beceri eksikliğine ek olarak, günümüzde işletmelerin karşı karşıya olduğu en büyük sorunlardan biri de teknik beceri eksikliğidir (Christofferson vd., 2018: 29). Yapay zeka ve veri analitiği ile ilgili pozisyonların doldurulması zordur ve bu zorluk teknolojinin benimsenmesinde gecikmelere ve devam eden projelerde aksamalara neden olmaktadır. Diğer bir endişe de, işletmelerin güvenlik tehditlerine ayak uydurabilme yeteneğidir. BT siber güvenlik uzmanlarının %52'si, çalışan becerilerinin eksikliğini göz önüne alarak işletmelerin güvenlik tehditlerinin üstesinden gelme becerilerinden şüphe duymaktadır (Christofferson vd., 2018: 36). İşletmelerin sahip olduğu beceriler ile teknolojinin hızı arasındaki boşluk, işletmeleri öncelikle akıllı otomasyon planlamasını başlatamama, akıllı otomasyonu uygulayamama, halihazırda başlamış projeleri yürütememe ve kendilerini güvenlik tehditlerinden koruyamama riskleriyle karşı karşıya kalmaya zorlamaktadır.

İşletmeler açısından zorluk yalnızca yetenekli personel bulmakla sınırlı değildir. Aynı zamanda personeli eğitmek ve iş gücünü teknolojik uyuma entegre etmek de son derece zordur. Kurum kültürünün inşası her türlü dijital dönüşümde önemli bir faktördür ve yalnızca kuruluşun kendi işgücünü değil, aynı zamanda satıcı tarafları da ilgilendirmektedir (Albinson vd., 2019: 20).

İşletmelerin kurumsal olarak yeni teknolojilere karşı kültürel direnç göstermesi, işletmelerin teknolojinin benimsenmesinden beklenen faydayı almalarını engelleyecektir. Öte yandan, akıllı otomasyona güvenin şüpheci bir güven olduğu işletmenin kurumsal kültür bilincine yerleştirilmelidir.

4.6. Akıllı Otomasyonun Benimsenmesi ve Finansal Riskler

Akıllı otomasyonun benimsenmesinin başarılı olup olmadığı ve risklerin gerçekleşmesinin önlenip önlenemeyeceği, akıllı otomasyonu kullanmanın amaçlarının neler olduğuna ve hedeflerin akıllı otomasyon stratejisiyle uyumluluğuna bağlıdır. Akıllı otomasyonun büyük potansiyel faydaları olmasına rağmen, akıllı teknolojilerin uygulanması sadece robotik süreç otomasyonunun uygulanmasından daha karmaşıktır. Bu nedenle, akıllı otomasyonu benimsemede başarılı olmak için, akıllı teknolojilerin RPA'ya uygulanması ile süreçlerin manuel olarak gerçekleştirilmesi arasındaki dengeyi bulmak önemlidir. Bu denge, riskleri ve gereksiz karmaşıklığı en aza indirirken yatırım getirisini en üst düzeye çıkarmanın önemli bir parçasıdır (Joseph, 2018: 9). Bununla birlikte, akıllı otomasyonu uygularken yalnızca maliyetin düşürülmesi düşünülmemelidir. Tutarlılık, kalite ve doğruluk gibi diğer avantajlar göz ardı edilerek yalnızca maliyetleri düşürmeye odaklanıldığında akıllı otomasyonun tam potansiyelini gerçekleştirmek zor olabilmektedir (Albinson vd., 2019: 9).

Akıllı otomasyon hedeflerinin işletmenin stratejisiyle uyumluluğunun başarısız olması, işletmelerdeki akıllı otomasyon yetenekleri ve vizyonunun eksikliğiyle ilgilidir. Bütüncül değişim yönetimi yaklaşımını benimsemek, akıllı otomasyonun tüm avantajlarını gerçekleştirmenin ön koşullarından biridir (Albinson vd., 2019: 8). Ayrıca, otomatik süreç için tüm kontrol ortamı yeniden tanımlanmalı ve eski kontrol noktaları güncellenmelidir. Yeni kontrollerin tasarlanması ve eskilerinin analitik veya diğer teknolojiler aracılığıyla dijitalleştirilmesi gerekmektedir. Risk yönetimi ve kontrol tasarımı, halihazırda hedef belirleme ve planlama aşamalarının bir parçası olmalıdır (Albinson vd., 2019: 8).

Akıllı otomasyon sistemleri ile ilgili bahsedilen tüm riskler, işletmeyi farklı şekillerde etkileyebileceğinden finansal sonuçlara yol açabilmektedir. Örneğin, itibar kaybı, yasal yaptırımlar, yüksek işe alım maliyetleri ve arızalı BT altyapısı. Tüm bu faktörler akıllı otomasyon sistemlerine yapılan yatırımın getirisini etkilemektedir. Akıllı otomasyonu planlarken tüm bu riskleri hesaba katmak, akıllı otomasyonu benimsemenin finansal riskini yönetmenin ilk adımıdır.

Akıllı otomasyonun benimsenmesinin sağlanamaması işletmelerde çok büyük finansal sonuçlar ortaya çıkarabilmektedir. Bu durumda akıllı otomasyon yatırımının getirisi negatiftir ve yatırım sermayesi boşa harcanmış demektir. Özellikle uygulamada çok ağır sonuçlar doğurabilecek bu tür riskler, akıllı otomasyon hedefinin belirlenmesinin ve benimsenmesinin planlamasında dikkatli bir şekilde değerlendirilmelidir. Örneğin, değişen mevzuat veya büyük ölçekli siber saldırı otomasyonun benimsenmesini durdurabilir veya ileriye taşıyabilir. Bu nedenle risk yönetimi ve iç denetim fonksiyonları otomasyonun planlama aşamasının en başından itibaren bir parçası olmalıdır.

5. AKILLI OTOMASYON RİSKLERİNİN İÇ DENETİME ETKİLERİ

Akıllı otomasyon sistemleriyle ilgili bir önceki bölümde bahsedilen riskler iç denetim süreci için birtakım zorluklar yaratmakta, dolayısıyla iç denetim faaliyetlerinin bu zorluklara uygun şekilde önlemler alması zorunlu olmaktadır. Akıllı otomasyon risklerinin iç denetime etkisi artan yeterlilik gereksinimleri, iç denetimin organizasyon yapısı içerisindeki konumu ve akıllı otomasyonun benimsenmesine katılımı, kaynak sağlama modellerinin çeşitliliği ve veri analitiğinin artan kullanımı olmak üzere dört başlık altında incelenecektir.

5.1. Artan Yeterlilik Gereksinimleri

İç denetçilerin yeterlilik seviyesi ve yeterliliklerini devamlı güncelleme ihtiyacı, akıllı otomasyon sistemlerinin getirdiği tüm risk kategorileri için ortak bir zorunluluktur. Özellikle algoritmaların şeffaf olmamasının denetim açısından yarattığı zorluk, iç denetçilerin yüksek düzeyde spesifik teknik becerilere sahip olmasını gerektirmektedir.

Akıllı sistemlerin opaklığı otomasyonla çalışan yönetim ve çalışanlar için olduğu kadar iç denetçiler için de büyük zorluklar oluşturmaktadır. Taraflı sonuçların tespit edilmesi şeffaflığın yeterli olmaması nedeniyle iç denetim için zor olmaktadır. Yapay zekanın karar verme sürecinin soyutluğu sürecin, hangi verilerin kullanıldığının ve sonucu etkileyebilecek bir hususun göz ardı edilip edilmediğinin anlaşılmasını zorlaştırmaktadır. İç denetim önemli bir hususun atlanıp atlanmadığını veya otomasyonun yanlış sonuçlar üretip üretmediğini fark edebilmek için otomasyonun bilgileri nasıl işlediğini anlayabilecek yeterliliğe sahip olmalıdır.

Akıllı otomasyonun iç denetim için gerektirdiği yeni beceriler arasında düzenlemeler konusunda yeterli ve güncel kalabilme zorunluluğu da bulunmaktadır. Akıllı otomasyon söz konusu olduğunda, iç denetçiler, profil oluşturma ve kişisel verileri kullanmanın tüm gerekliliklerini bilmelidir. Ayrıca iç denetçiler yasal düzenlemeler dışındaki etik hususları da dikkate almak zorundadır. İç denetim, etik ilkelerin tanımlandığını ve işletmenin bunları izlediğini garanti edebilmelidir. Ancak neyin etik olup olmadığı konusunda sınır koymak zordur. Bu nedenle, iç denetimin güncel kalabilmesi için etik konulara ayak uydurması gerekmektedir.

İç denetim, kullanılan teknolojinin güvence altına alınmasında önemli bir rol oynamaktadır. Bununla birlikte, iç denetim birincil sorumluluğa sahip değildir, ancak risk bazlı plana göre kontrollerin yeterli olduğunu ve uyum gerekliliklerinin yerine getirildiğini garanti etmektedir. Gerekli kontroller, bilgi otomasyonunun ne kadar hassas işlediğine ve bilgilerin düzenleme kapsamında olup olmadığına bağlıdır. Akıllı otomasyonun girdi verilerinden sonuçlara kadar sağlıklı çalışmasını sağlamak için analitik araçların kullanılmasının gerekmesi nedeniyle, iç denetimin önündeki zorluk yine denetçilerin siber güvenlik ve araçlarla ilgili yetenekleridir.

IIA Küresel İç Denetim Yetkinlik Çerçevesi gereğince iç denetçiler, etkili bir iç denetim için gerekli olan mesleki gelişimlerini sürekli olarak devam ettirmeli ve güncel yetkinliklerini sürdürmelidir (IIA, 2013b: 7). İç denetim fonksiyonu görevlilerinin profesyonel gelişim şansına ve etkin iç denetim için gerekli yetkinliklere sahip olduğundan emin olmak için iç denetim birimi yönetimine önemli sorumluluk düşmektedir. Denetim ekibi gerekli yetkinliklere sahip değilse, denetim riski artacaktır. Denetim riskleri, hem iç denetimin geçersiz veya yetersiz sonuçlara varması hem de işletmeye hatalı veya yetersiz tavsiyelerde bulunması olasılığını içermektedir. Bu nedenle oldukça spesifik bilgi gerektirdiği için özellikle akıllı otomasyon konusunda iç denetimin asgari bilgi ve yetkinliğe sahip olması gerekmektedir. Ayrıca diğer taraftan iç denetim planlamasının, iç denetimin yetkinlik sınırlamalarına dayandırılması da işletme açısından olumsuz sonuçlanacaktır. İç denetim planlaması risk bazlı olmalı ve yalnızca iç denetimin denetleme yetkisine sahip olduğu şeylerle sınırlı kalmamalıdır. Bu nedenle iç denetim, iç denetim planlamasında risk temelli yaklaşımı sağlamak için gerekli yetkinlikleri kazanmalıdır. İç denetimin denetim konusuyla ilgili yeterli anlayışa ve teknik becerilere sahip olması gerekmektedir. Temel olarak, işletmenin iş süreçleriyle ilgili hiçbir şey denetim konusu olarak sınır dışı bırakılmamalıdır. İç denetimin kapsamı, denetleme yeterliliğine sahip olunan konularla sınırlı tutulursa, riskleri nedeniyle denetlenmesi gereken alanlar denetim planından çıkarılmış olacaktır ve denetim eksikliği sorunu daha büyük riskler yaratacaktır.

5.2. İç Denetimin Konumu ve Akıllı Otomasyonun Benimsenmesine Katılımı

Yeni teknolojilerin benimsenmesi sürecinde iç denetçilerin yetkinlikleri gibi iç denetimin işletmenin organizasyon yapısı içindeki konumu da önemli konulardan biridir. İç denetimin konumu ve akıllı otomasyon benimseme sürecindeki rolü avantaj ya da dezavantaj yaratabilir. Akıllı otomasyon veya başka herhangi bir yeni teknoloji benimsenirken iç denetimin erkenden, henüz tasarım aşamasında dahil edilmesi ve aynı zamanda iç denetimin bağımsızlığının sağlanması gerekmektedir. İç denetim yalnızca süreç tamamlandığında güvence işlevi olarak görülüyorsa ve teknolojilerin benimsenmesinin erken aşamalarında sürece dahil edilmemişse, sonrasında akıllı otomasyonla ilgili kapsamlı denetim sonuçlarına ulaşmak da zor olmaktadır.

İç denetimin teknolojilerin benimsenme sürecine erken katılımı, akıllı otomasyonu benimsemede başarılı olmayı ve otomasyonun gerektiği gibi uygulandığından ve çalıştığından emin olabilmeyi sağlayacak, iç denetime akıllı otomasyon konusunda daha fazla anlayış kazandıracaktır. İç denetim, yeni teknolojilerin tasarlanması noktasında iç denetimin bakış açısından, iç denetimin bağımsızlığını riske atmayacak şekilde en baştan tavsiyelerde bulunmalıdır. İç denetimin rolünün sadece tasarımı denetlemek olmayıp aynı zamanda uygulamayı da denetlemek olabilmesi için, yeni teknolojilerle kendi anlayışıyla erkenden ilgilenmesi gerekmektedir.

İç denetimin proaktif olarak tasarım ve uygulama aşamalarının bir parçası olması; aynı zamanda tavsiyelerini uygulamadan önce verebilmesi için sürece erken katılımı gerekmektedir. Uygulama zaten yapılmışsa ve iç denetimin rolü, uygulamanın doğru bir şekilde, gerektiği gibi çalışmasını sağlamaksa, iç denetimin tavsiye edebileceği düzeltmeleri yapmak için çok geç olabilir. İç denetim akıllı otomasyonu ne kadar erken benimserse o kadar iyi olacaktır.

Kurumsal risk yönetiminde temel amaç, doğru risk iştahını belirlemeyi de içerecek şekilde, işletmenin stratejik hedeflerine ulaşmaktır (Fraser ve Simkins, 2010: 1). Bu nedenle akıllı otomasyonla ilgili hedeflerin ve risk iştahının baştan belirlenmesi ve net olması gerekmektedir. Hedefler ve risk iştahı net bir şekilde anlaşılmadan, riskleri etkili bir şekilde belirlemek, değerlendirmek, izlemek ve yönetmek zordur. Ayrıca, otomasyonda yeterli kontrollerin bulunmaması organizasyonun güvenlik, uyumluluk ve gizlilik gereksinimlerini karşılamasını engelleyebileceği için kontroller erken aşamada tasarlanmalıdır (Goldman, 2017). Yeterli kontrol ortamının planlanması, iç denetimin geleneksel güvence rolünün ötesinde danışman rolüyle tavsiyelerde bulunabileceği bir alandır.

İç denetim, kullanılan teknolojinin güvence altına alınmasında önemli bir rol oynamaktadır. Bununla birlikte, iç denetim birincil sorumluluğa sahip değildir, ancak risk bazlı plana göre kontrollerin yeterli olduğunu ve uyum gerekliliklerinin yerine getirildiğini garanti etmelidir. Gerekli kontroller, bilgi otomasyonunun ne kadar hassas işlediğine ve bilgilerin düzenleme kapsamında olup olmadığına bağlıdır. Üçlü savunma hattı modeli dikkate alındığında, özellikle yeni teknoloji projelerinde üç savunma hattının da teknolojiden anlaması ve teknik becerilere sahip olması, aynı zamanda hatlar arası işbirliğinin artması, tüm hatlardan gelen uzmanlığın kullanılması gerektiği konusunda ortak bir anlayışa sahip olunması gerekmektedir. Dijital riskleri yönetmek için üç hattın hepsi birlikte sorunsuz çalışmalıdır. Ancak bu işbirliğinde aynı zamanda her bir savunma hattının rollerinin net olması önemlidir.

5.3. Kaynak Sağlama Modellerinin Çeşitliliği

İşletme süreçlerine ilişkin risklerin en aza indirilebilmesi için iç denetim planlamasının risk temelli olması ve temel olarak hiçbir şeyin yeterlilik sınırlamaları nedeniyle bir denetim alanı olarak iç denetimin sınırları dışında kalmaması gerekmektedir. Geçerli sonuçlara ulaşmak ve

yeterli tavsiyelerde bulunmak için iç denetimin denetim konusu etrafında yeterli yetkinliğe sahip olması sağlanmalıdır. Ancak akıllı teknolojilerin denetimi birçok uzmanlık alanı gerektirdiğinden iç denetim birimi için gereklilik koşullarının sağlanması geçmişe göre çok daha zordur. Bu alanlar veri analitik uzmanlığından yapay zeka algoritma uzmanlığına kadar uzanmaktadır. Teknik uzmanlığın ötesinde yasal düzenlemeler ile etik ve gizlilik konusu da denetim alanları kapsamındadır. Zaman veya diğer kaynak kısıtlamaları olmasa bile, organizasyondaki her alan veya teknoloji hakkında derin bilgiye sahip olmak imkansızdır. Özellikle küçük işletmelerde iç denetim birimlerinin, yeni teknolojilerin belirlediği tüm yeterlilik gerekliliklerine ayak uydurması hem zor hem de maliyetlidir.

İç denetim süreci için farklı beceri kombinasyonlarına ihtiyaç duyuldukça, kaynak sağlama modelleri de değişerek farklılaşmaktadır. Oldukça spesifik yetkinlikler gerektiren yeni teknolojiler ve işletmelerin hızla değişmesi nedeniyle, iç denetimin yeni duruma uyum sağlamak için esnek olması ve iç denetim birimi haricinde kurum içinden veya dışından desteğe ihtiyaç olup olmadığının sürekli olarak değerlendirilmesi gerekmektedir. İç denetimin iç denetim sürecinde gerekli uzmanlığa sahip olmaması durumunda, işletme içinden birim dışı uzmanlıklardan destek alınması, dışarıdan hizmet alımı veya akıllı sistemlerde bir tür ortak kaynak sağlama modeli gibi farklı alternatif çözümler üretilebilmektedir. Yeterli uzmanlığı sağlayan kaynak modeli seçimi ne olursa olsun iç denetim sürecinin bağımsızlık ve tarafsızlık ilkeleri mutlaka göz önünde bulundurulmalıdır.

5.4. Veri Analitiğinin Kullanımı

Veri analitiği, veri madenciliği ve istatistiksel modelleme kullanarak verilerin toplanmasını, temizlenmesini, dönüştürülmesini ve analiz edilmesini içeren bir süreçtir (Batarseh ve Gonzales, 2018: 52). Veri analizi ile iç denetim, verileri analiz ederek ilişkileri, eğilimleri veya kalıpları ortaya çıkarmak için veri madenciliği tekniklerini ve prosedürlerini kullanmaktadır. Analizler yaparak, iç denetim, hata ve hile olasılıklarını belirleyebilir ve usulsüzlükleri daha detaylı araştırabilir.

Veri analitiğinin iç denetim alanındaki artan kullanımının ardında, veri analitiği ile iç denetimin örneklem kullanmak yerine faaliyetlerin tamamını test edebilmesinin sağlanması yatmaktadır. Doğal olarak bu, örneklem testine göre hataları, verimsizlikleri ve uygunsuzluğu belirleme olasılığının daha yüksek olduğu anlamına gelmektedir (Tang vd., 2017: 1126).

İç denetimin akıllı otomasyonu kapsamlı bir şekilde denetleyebilmesi için veri analitiğinin yararlı, hatta gerekli olduğu söylenebilir. Veri analitiği ile tüm verilerin incelenmesi mümkün olabilmektedir. Yapay zekanın veri üretme hızı düşünüldüğünde, analitiğin bu veriyi işleme ve olası sapmaları bulma gücünden mutlaka faydalanılmalıdır. Akıllı sistemler verileri çok hızlı üretip kullandığından, verilerin hatasız olduğundan ve yapay zekanın olması gerektiği gibi çalıştığından emin olmak için iç denetim sürecinde kaynak verilerden sonuçlara kadar veri analitiği kullanılmalıdır.

Veri analitiği iç denetim faaliyetlerinde bir odak alanı olmalı ve denetçilerin analitik yeterlilikleri düzenli eğitimlerle desteklenmelidir. Özellikle küçük iç denetim birimi olan işletmelerde ağ kurarak, fikir alışverişinde bulunarak ve eğitimlere katılarak değişime ayak uydurmak ve yetkinlikleri sürdürmek son derece önemlidir.

6. TARTIŞMA, SONUÇ ve ÖNERİLER

Son yıllarda bilgi teknolojilerinde önemli gelişmeler yaşanmış ve verimliliğin artırılması amacıyla yeni yollar arayan farklı sektörlerdeki birçok işletme iş süreçlerinde bu yeni teknolojileri benimsemiştir. Gelişen teknolojilerin kullanımı işletmeler için yeni fırsatlar yaratmakla birlikte birçok yeni risk alanını da beraberinde getirmiştir. İşletmelerin karar alma sürecinin bir parçası olarak risk yönetiminin rolü, özellikle yeni teknolojilerin sunduğu fırsatlar ve risklerin yarattığı belirsizlik neticesinde son derece önemli bir konu haline gelmiştir.

Günümüzde teknolojinin işletmeler üzerindeki etkisinin en güncel örneklerinden biri akıllı otomasyon sistemleridir. Akıllı otomasyon, RPA süreçlerinin yapay zeka teknolojileri kullanılarak geçmiş verilerden yola çıkarak öğrenebilme ve karar alabilme becerileri eklenmiş şekilde geliştirilmiş halidir. RPA, kesme, yapıştırma ve birleştirme gibi kurallara dayalı, tekrarlayan görevleri taklit edebilen bir yazılım programıdır ve basit BT görevlerini harici yazılımla otomatikleştirmek için kullanılmaktadır (Christofferson vd., 2018: 25).

Bilişsel beceriler gerektiren uçtan uca süreçleri otomatikleştirmek için yapay zeka yeteneklerinin RPA'ya entegre edilmesi gerekmektedir. Basitçe yapay zeka, makinelerin tahminlerde bulunma, verilerden öğrenme, resim ve seslerden anlam bulma gibi insan zekası gerektiren görevleri yerine getirebilmesi anlamına gelmektedir (Watson vd., 2019: 13). RPA'ya entegre edilen bilişsel teknolojilerin bu kombinasyonuna akıllı otomasyon denmektedir.

Akıllı otomasyon sistemleri ile tüm iş süreçlerini otomatikleştirmek neredeyse mümkün hale gelmiştir; çünkü yapay zeka, insan değerlendirmesi gerektiren görevleri de gerçekleştirebilmektedir. RPA, üretkenliği artırma, maliyeti düşürme ve çalışan deneyimini iyileştirme gibi birçok fayda sağlarken bilişsel yetenekleri RPA'ya entegre etmek bu faydaları daha da ileriye götürmektedir.

Çalışma ile akıllı otomasyon sistemlerinin işletmelerin risk yönetimi ve iç denetim süreçlerinde meydana getirdiği değişiklikler değerlendirilmektir. Bu amaçla akıllı otomasyon sistemlerinin temel riskleri üzerinde durularak, oluşan yeni riskler karşısında iç denetimin karşılaştığı zorlukların neler olduğu ve bu zorlukların nasıl aşılabileceği konularında değerlendirmelerde bulunulmaktadır.

Akıllı otomasyonun işletme faaliyetleri üzerinde oluşturduğu riskler; teknolojik riskler, düzenleme ve gizlilik riskleri, etik riskler, siber riskler, kurumsal riskler ve finansal riskler olmak üzere altı temel kategori altında incelenmiştir. İşletmelerin akıllı otomasyonun arkasındaki mantığın doğru olduğundan, hata risklerinin en aza indirildiğinden, verilerin güvence altına alındığından ve otomasyonun herhangi bir şekilde taraflı olabilecek sonuçlar sağlamadığından emin olması teknolojik risklerin konusunu oluşturmaktadır. Siber riskler bilgi teknolojilerinin gelişmesiyle oluşan siber ortamdan kaynaklı risklerdir. Algoritmaların kararlarında etik kuralları dikkate aldığından ve etik kurallarla tahminler yaptığından emin olmak zor olabileceğinden, algoritmaların bu konuda yeterince şeffaf olmaması akıllı otomasyonun kullanımında etik riskler yaratmaktadır. Yasal düzenlemelerin teknolojik gelişmelere gecikmeli olarak tepki vermesi ve özellikle büyük hacimli veri kullanan sistemler için gizlilik ile ilgili düzenlemelerin hayata geçirilmemiş olması bir diğer risk unsurudur. Kuruluş çapında geliştirilmiş bir risk kültürünün olmaması; kuruluşların riskleri ve bunlara yanıt verecek uygun stratejileri belirleme, mevcut risk ortamında faaliyetlerini sürdürebilme yetenekleri ile işletmelerin akıllı otomasyona geçişin istihdam ihtiyaçlarını nasıl etkileyeceğini anlamakta zorlanması bir takım kurumsal riskler ile sonuçlanmaktadır. Son olarak akıllı otomasyonun benimsenmesinin sağlanamaması işletmelerde çok büyük finansal sonuçlar ortaya çıkarabileceğinden finansal risk yaratmaktadır.

Geleneksel iç denetim süreçlerinin akıllı otomasyon sistemleri için tartışılan altı temel riski önleyici mekanizmalar geliştirmesinin önünde bir takım zorluklar bulunmaktadır. Bu zorlukların en büyüğü yetkinlik gereksinimleriyle ilgilidir. Özellikle teknik beceriler, düzenleme ve etik sorumluluk konularında değişen yeterliliklere ayak uydurmadaki zorluklar iç denetimin sağlıklı yürütülebilmesi açısından önemlidir. Tespit edilen ikinci zorluk, iç denetimin akıllı otomasyonun benimsenmesindeki konumu ve rolüyle ilgilidir. İç denetim akıllı otomasyonu benimseme sürecinin ilk aşamalarında yer almıyorsa, sonraki hata ve eksiklik tespitleri için yeterli sonuçlara varmak ve geçerli önerilerde bulunmak zor olmaktadır. Bir diğer zorluk ise, akıllı otomasyonu izleme ve kontrol yöntemlerinin, kısmen yeterlilik eksikliğinden ve aynı zamanda uygulanabilir araçların eksikliğinden kaynaklı olarak benimsenen teknolojilerin gerisinde kalmasıdır.

Akıllı otomasyonu benimseyen işletmelerin iç denetim faaliyetleriyle ilgili oluşan denetim zorluklarıyla mücadele edebilmesi için bir takım güncellemeler yapması gerekmektedir. Bunun için çalışmada kritik olduğu düşünülen dört hususta tavsiyelerde bulunulmuştur. Öncelikle akıllı otomasyonu benimseyen işletmelerin iç denetim faaliyetlerini yeni teknolojilere uyumlu şekilde yürütebilmesi için en uygun kaynak bulma seçeneklerini sürekli olarak değerlendirmesi ve yeni teknolojilere yönelik eğitimler ile yeterlilik boşluklarını doldurmaları gerekmektedir. Özellikle küçük işletmelerde iç denetim için dışarıdan kaynak sağlama gibi alternatiflerin çeşitliliğinin artmasının muhtemel olduğu düşünülmektedir. İç denetim, akıllı otomasyonu benimseme sürecinin başından itibaren danışmanlık rolünde olabileceği, ancak aynı zamanda örgütsel yapı içerisinde bağımsızlığını koruyabileceği bir konumda bulunmalıdır. Son olarak, iç denetim birimleri, yeni teknolojik süreçlerin denetiminde hız ve veri büyüklüğü avantajını yakalayabilmek için veri analizi yeteneklerini geliştirmeli ve bu yeteneklerini akıllı otomasyon sistemlerinin denetiminde kullanmalıdır.

KAYNAKÇA

Albinson, N., Thomas, C., Rohrig, M. and Chu, Y. (2019). *Future of Risk in the Digital Era*. Deloitte.

Batarseh, F. and Gonzales, A. (2018). Predicting Failures in Agile Software Development Through Data Analytics. *In Software Quality Journal*, 26 (1), 49-66.

Celayir, D. ve Celayir, C. (2020), Dijitalleşmenin Denetim Mesleğine Yansımaları. *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi*, 7(6): 128-148.

Christofferson, S., Murray M., McKnight L. and Go, R. (2018). *2019 Audit Plan Hotspots*. Gartner.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2015). *COSO in the Cyber Age*. [Online] http://www.coso.org > [Erişim Tarihi: 10.02.2023].

Datta, A., Sen, S. and Zick, Y. (2016). *Algorithmic Transparency via Quantitative Input Influence: Theory and Experiments with Learning Systems*. Carnegie Mellon University, Pittsburgh, USA.

Deloitte. (2018). *Adopting Automation in İnternal Audit: Using Robotic Process Automation and Cognitive İntelligence to Fortify the Third Line of Defense*. [Online] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/adopting-robotic-process-automation-in-internal-audit.pdf> [Erişim Tarihi: 18.03.2023].

European Confederation of Institutes of Internal Audit (ECIIA). (2019). *Risk in Focus 2020*. [Online] http://www.iia.org.uk> [Erişim Tarihi: 05.03.2023].

Fraser, J. and Simkins, B. (2010). *Enterprise Risk Management*. (1st edition). ABD: Wiley.

Ganite, T. ve Uçma Uysal, T. (2015). Siber Riskler ve COSO İç Kontrol Bütünleşik Çerçevesi. *Muhasebe ve Denetime Bakış Dergisi*, 15 (46), 1-10.

Goldman, S. (2017). *The Role of Risk Management and Governance in Intelligent Automation*. [Online] https://www.cio.com/article/3242246/the-role-of-risk-management-and-governance-in intelligent-automation.html> [Erişim Tarihi: 18.02.2023].

Hatherell, T. (2018). *In Forging Internal Audit's Path to Greater İmpact and İnfluence*. (Foreword). Global Chief Audit Executive Research Survey. Deloitte.

Institute of Internal Auditors (IIA). (2013a). *The Three Lines of Defense in Effective Risk Management and Control*.

Institute of Internal Auditors (IIA). (2013b). *The IIA Global Internal Audit Competency Framework*.

Joseph, A. (2018). *Robotics and İntelligent Automation - Combining The Power of Human and Machine*. Ernst & Young.

Kananen, H. and Puolitaival, H. (2019). *Artificial İntelligence: New Tools for Business*. Helsinki: Alma Talent Oy.

Kokina, J. and Davenport, T.H. (2017). The Emergence of Artificial İntelligence: How Automation İs Changing Auditing? *Journal of Emerging Technologies in Accounting*, 14 (1), 115-122. [Online] doi: 10.2308/jeta-51730> [Erişim Tarihi: 18.03.2023].

Kovanen, A. (2020). *Risks of Intelligent Automatıon and Their Impact on Internal Audit*. (Master's Thesis), Tampere University / Faculty of Management and Business, Finland.

Köse, H. Ö., Polat, N. (2021). Dijital Dönüşüm ve Denetimin Geleceğine Etkisi. *Sayıştay Dergisi*, 32 (123): 9-41. [Online] https://doi.org/10.52836/sayistay.1068328> [Erişim Tarihi: 18.03.2023].

KPMG. (2017). IT *Internal Audit: Multiplying Risks Amid Scarce Resources*. [Online] https://assets.kpmg.com/content/dam/kpmg/ch/pdf/it-internal-audit-en.pdf> [Erişim Tarihi: 15.02.2023].

KPMG. (2018a). *Intelligent Automation and Internal Audit*. [Online] https://assets.kpmg.com/content/dam/kpmg/ch/pdf/intelligent-automation-and-internal-audit.pdf> [Erişim Tarihi: 15.02.2023].

KPMG. (2018b). *Internal Audit and Robotic Process Automation*. [Online] https://assets.kpmg/content/dam/kpmg/nl/pdf/2018/advisory/internal-audit-and-robotic-process-automation.pdf.> [Erişim Tarihi: 19.02.2023].

KPMG. (2021). *Dijitalleşme Yolunda Türkiye Raporu*. [Online] https://assets.kpmg.com/content/dam/kpmg/tr/pdf/2021/04/dijitallesme-yolunda-turkiye-raporu-2021.pdf> [Erişim Tarihi: 02.03.2023].

Laurent, P., Chollet T. and Herzberg E. (2015). *Intelligent Automation Entering the Business World*. Holt, Rinehart & Winston, ABD.

Lehto, Martti. 2017. Artificial Intelligence and Cyber Security. *In: Future*, 36 (2), 6-14.

Moffitt K C., Rozario A. M. and Vasarhelyi M.A. (2018). Robotic Process Automation for Auditing. *Journal of Emerging Technologies in Accounting*, 15 (1): 1-10. [Online] http://dx.doi: 10.2308/jeta-10589> [Erişim Tarihi: 18.03.2023].

Niemi, P. (2018). *Internal Audit in Practice*. Helsinki: Alma Talent.

Nunes, T., Leite, J. and Pedrosa, I. (2020). Intelligent Process Automation: An Overview Over the Future of Auditing. Conference Paper. *15th Iberian Conference on Information Systems and Technologies (CISTI)*. [Online] http://dx.doi.org/10.23919/CISTI49556.2020.9140969> [Erişim Tarihi: 18.03.2023].

Ollila, M. (2019). The Ethics of Artificial İntelligence. Otava.

Osoba, O. and Welser, W. (2017). An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence. Rand Corporation, ABD.

Özyürek, H. (2021), Dijitalleşme Sürecinde Denetim. İ. Erdoğan Tarakçı,İ., Göktaş, B. (Ed.). *Dijital Gelecek Dijital Dönüşüm 2021* içinde (ss.45-71), İstanbul: Efe Akademi.

Patel, P. (2018). *Compelling Benefits, Common Misconceptions – Putting İntelligent Automation to Work for Federal*. Accenture Federal Services, U.S.

Tang, F., Norman S. and Vendrzyk, V. (2017). Exploring Perceptions of Data Analytics in The İnternal Audit Function. *In Behaviour and Information Technology Journal*, 36 (11), 1125-1136.

Türkiye Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı. [Online] https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm> [Erişim Tarihi: 20.03.2023].

Wang, Y. and Kogan, A. (2018). Designing Confidentiality-Preserving Blockchain-Based Transaction Processing Systems. *International Journal of Accounting Information Systems*, 30(1):1-18.

Watson, J., Hatfield, S., Wright, D., Howard, M., Witherick, D., Coe, L. and Horton, R. (2018). *Automation With İntelligence - Reimagining the Organization in the 'Age of With'*. Deloitte Insights.

Zhang, C. (2019). Intelligent Process Automation in Audit. *Journal of Emerging Technologies in Accounting*, 16 (2): 69-88. [Online] http://dx.doi: 10.2308/jeta-52653> [Erişim Tarihi: 25.02.2023].