



T.C.

YÜKSEKÖĞRETİM KURULU

İÇ DENETİM BİRİMİ BAŞKANLIĞI

ARAŞTIRMA VE İNCELEME FAALİYETLERİ

Danışmanlık Raporu

Dijitalleşme Ve İç Denetimde Yapay Zekâ Kullanımı

İç Denetim Birimi Başkanlığı

İç Denetçiler

Selma SANCARBABA, 1162

Gözetim Sorumlusu

Suat AKSU, 1086

Rapor No: 2025/1162-1, 1086-1

Rapor Tarihi: 29.07.2025

İçindekiler Tablosu

RAPOR DAĞITIM LİSTESİ.....	5
DİJİTALLEŞME VE İÇ DENETİMDE YAPAY ZEKÂ KULLANIMI	6
1. GİRİŞ	6
1.1. Dijitalleşmenin Kamudaki Rolü.....	6
1.2. İç Denetimde Dijital Dönüşümün Önemi.....	6
1.3. Yapay Zekâ Kavramı ve Temel Bileşenleri	6
1.4. Araştırmanın Amacı ve Kapsamı.....	6
2. DİJİTALLEŞME, TEMEL KAVRAMLAR VE GELİŞİM SÜRECİ	7
2.1. Dijitalleşmenin Tanımı ve Evrimi	7
2.1.1. Dijitalleşme veya Sayısallaşma:	7
2.1.2. Dijital Dönüşüm:	7
2.2. Büyük Veri Analizinde Yapay Zekâ ve Makine Öğrenmesi Tekniklerinin Kullanımı	12
2.2.1. Kümeleme:	12
2.2.2. Sınıflandırma:	12
2.2.3.Yapay Sinir Ağları:.....	12
2.2.4. Metin ve Web Madenciliği:	12
2.2.5. Fikir Madenciliği (Duygu Analizi):	13
2.2.6. Değişik Alanlarda Kullanılan Bazı Yapay Zekâ ve Makine Öğrenmesi Uygulamaları:	13
2.3. Doğal Dil İşleme (NLP) Teknolojisi ve Otomatik Raporlama.....	15
2.4. Robotik Süreç Otomasyonu (RPA) ve İç Denetim.....	16
3. YAPAY ZEKÂ UYGULAMALARINDA KARŞILAŞILAN ZORLUKLAR VE ETİK SORUNLAR	17
3.1. Teknolojik Riskler.....	18
3.1.1. Algoritmaların Yanlış Davranması ve Şeffaflığın Sağlanamaması Riski.....	18
3.1.2. Algoritmalar Karşı Eleştirel Olmayan Güvenin Artması	18
3.2. Hesap Verebilirliğin Sağlanamaması	19
3.3. Düzenleme ve Gizlilik İle İlgili Riskler.....	19
3.4. Etik Riskler	19
3.5. Siber Riskler	20
3.6. Kurumsal Riskler	20
3.7. Akıllı Otomasyonun Benimsenmesi ve Finansal Riskler	21
4. GÜVENİLİR YAPAY ZEKÂ ARAYIŞI	22
5. İÇ DENETİMDE YAPAY ZEKÂ VE KULLANIM ALANLARI.....	24
5.1. İç Denetimde Dijital Dönüşümün Önemi.....	25
5.2. İç Denetim Fonksiyonunun Dijitalleşmeyle Değişimi	26

5.3. Dijital Dönüşümün İç Denetimde Sağladığı Fırsatlar ve Riskler ile Dikkat Edilmesi Gereken Hususlar	30
5.3.1.Fırsatlar.....	30
5.3.2.Riskler	31
5.3.3. Fırsat ve Risklerin Yönetimi İçin Dikkat Edilmesi Gereken Hususlar.....	31
5.4. Risk Değerlendirme ve Önceliklendirme	33
5.5. Süreç İzleme ve Anormallik Tespiti.....	34
5.6. Uygunluk ve Mevzuat Denetimi	35
5.6.1. Uygunluk Denetimi İçin Yapay Zekâ Temelli Örnek Algoritma Akış Şeması	35
5.6.2. Yurt Dışı Vaka Örneği: Estonya - Dijital Uygunluk Denetimi (e-Audit)	36
5.7. Finansal Denetim ve Sahtecilik Tespiti	36
5.7.1. Anomali Tespiti ve Şüpheli İşlem Analizi	37
5.7.2. Sahtecilik Risk Göstergelerinin Makine Öğrenmesiyle Tespiti	37
5.7.3. Blockchain ve YZ Tabanlı Denetim Entegrasyonları	37
5.7.4. Kamu Kurumları ve Yükseköğretim Bağlamında Yapılan Değerlendirme:	37
5.8. Performans Analizi ve İç Kontrol Süreçlerinin Güçlendirilmesi	39
5.8.1. Göstergelerin Dinamik Takibi ve Anlamlandırılması	39
5.8.2. İç Kontrol Bileşenlerinin Dijital Olarak İzlenmesi ve Güçlendirilmesi	39
5.8.3. Tahmine Dayalı Analitik ve Stratejik Öngörü.....	40
6. ULUSLARARASI UYGULAMALAR VE BAŞARILI ÖRNEKLER.....	42
6.1. Avrupa Birliği Ülkelerinde Yapay Zekâ Destekli İç Denetim.....	42
6.1.1. Hollanda: Tahmine Dayalı İç Denetim ve Anomali Algılama	42
6.1.2. Estonya: Dijitalleşmiş İç Denetim Çerçevesi.....	42
6.1.3. Danimarka: İç Denetim Süreçlerinde Makine Öğrenmesi Uygulamaları.....	42
6.1.4. Avrupa Komisyonu’nun Rehberliği ve Koordinasyonu	42
6.1.5. Stratejik Değerlendirme:	43
6.2. Amerika ve Asya’da Dijital İç Denetim Modelleri.....	43
6.2.1. Amerika Birleşik Devletleri: Entegre Dijital Denetim Ekosistemi	43
6.2.2. Japonya: Yüksek Otomasyon ve Sürekli Denetim.....	43
6.2.3. Singapur: Akıllı Denetim Altyapısı (Smart Audit Infrastructure)	44
6.2.4. Güney Kore: Kamu Bilişim Altyapısıyla Entegre Denetim.....	44
6.2.5. Genel Değerlendirme	44
6.3. Türkiye’de Dijitalleşme ve Yapay Zekâ Uygulamaları	44
6.3.1. Kamu Kurumlarında Veri Temelli Denetim Girişimleri	45
6.3.2. Yapay Zekâ Tabanlı Denetim Uygulamaları İçin Mevzuat ve Altyapı Hazırlıkları.....	45
6.3.3. Değerlendirme ve Gelişim Potansiyeli.....	45

7. GELECEĞE YÖNELİK TRENDLER VE İÇ DENETİMDE YAPAY ZEKÂ STRATEJİLERİ.....	46
7.1. Otonom Denetim Sistemleri ve Sürekli İzleme.....	46
7.1.1. Otonom Denetim Sistemleri (Autonomous Auditing Systems).....	46
7.1.2. Sürekli İzleme (Continuous Monitoring) ve Risk Tabanlı Uyarı Sistemleri	47
7.1.3. Stratejik Öneriler ve Uygulama Perspektifi	47
7.2. Yapay Zekâ ile Entegre İç Denetim Çözümleri	48
7.2.1. Entegre Denetim Platformları ve Modüler Yapay Zekâ Çözümleri.....	48
7.2.2. Kurum Sistemleriyle Uyumlu Entegrasyon	49
7.2.3. Akıllı Denetim Planlaması ve Kaynak Tahsisi	49
7.2.4. Karar Destek ve Otomatik Raporlama	49
7.2.5. Güvenlik, Etik ve Yapay Zekâ Yönetimi	50
7.3. İnsan-Makine İş Birliği ve Yetkinlik Gelişimi	51
7.3.1. Hibrit Denetim Ekosistemi: İnsan ve Yapay Zekâ Arasındaki Rol Dağılımı.....	51
7.3.2. Yeni Nesil Yetkinlik Alanları	51
7.3.3. Kamu ve Üniversite Denetim Birimlerine Özgü Eğitim ve Dönüşüm Stratejileri	52
7.3.4. Etik, Güven ve İnsan Odaklılık	52
7.4. Politika ve Strateji Önerileri.....	54
7.4.1. Ulusal Ölçekte Politikalar ve Mevzuat Uyumlaştırması	54
7.4.2. Kurumsal Düzeyde Uygulanabilir Stratejiler	55
8. DEĞERLENDİRME VE SONUÇ	56
8.1. Dijitalleşmenin İç Denetimdeki Dönüştürücü Etkisi	56
8.2. Yapay Zekâ Kullanımının Sürdürülebilirliği ve Gelecek Perspektifi	58
8.3. Öneriler ve İleri Araştırma Alanları.....	60
8.3.1. Öneriler.....	60
8.3.2. İleri Araştırma Alanları.....	60
KAYNAKÇA	62

RAPOR DAĞITIM LİSTESİ

Üst Yönetici	Prof. Dr. Erol ÖZVAR Yükseköğretim Kurulu Başkanı
İç Denetim Birimi Başkanlığı	Suat AKSU İç Denetim Birimi Başkanı
İlgili Merciler	İç Denetim Koordinasyon Kurulu

Selma SANCARBABA İç Denetçi	
Suat AKSU DGS / İç Denetim Birimi Başkanı	

DİJİTALLEŞME VE İÇ DENETİMDE YAPAY ZEKÂ KULLANIMI

1. GİRİŞ

1.1. Dijitalleşmenin Kamudaki Rolü

Teknolojide yaşanan ilerleme ve dönüşüm beraberinde kullanıma sunulan teknolojik araçların da hızlı bir şekilde değişimini getirmektedir. Bu hızlı dönüşümün ürünü olan teknolojik olanaklar, çağa ayak uydurmak isteyen tüm sektörlerde kullanılan araçlarda da hızlı bir dönüşüm ve değişimi zorunlu kılmakta, bu durum ise doğal olarak iş yapış şekilleri ile süreçlerini etkilemektedir.

Kamu kesiminde dijitalleşme, kamu hizmetlerinin etkinliği, şeffaflığı ve hesap verebilirliğini artırmak için stratejik bir araçtır. Özellikle kamu kurumlarının hizmet sunum süreçlerinin iyileştirilmesi, kaynakların verimli kullanımı ve vatandaş memnuniyetinin yükseltilmesi açısından kritik öneme sahiptir.

1.2. İç Denetimde Dijital Dönüşümün Önemi

İç denetim faaliyeti, kurumun risk yönetimi, kontrol ve yönetim süreçlerinin etkililiğini değerlendirerek geliştirmek amacıyla yönelik sistemli ve disiplinli bir yaklaşım getirerek, iç kontrol mekanizmalarını güçlendirmelerine katkı sağlar.

Bilişim teknolojilerinde yaşanan hızlı değişimin hayatın her alanındaki yansımaları, beraberinde iç denetimin fonksiyonunun da tekrar gözden geçilmesini ve yeni gelişmelere uyum sağlamasını zorunlu kılmaktadır. Bu gün artık dijital teknolojilerin denetim süreçlerine entegrasyonu ve iç denetçilerin dijital yetkinliklerinin artırılması gerekliliği, üzerinde durulması gereken çok önemli konular arasında yerini almıştır. Ancak bu alanda oluşan fırsatların yanında ortaya çıkan çeşitli zorluklarında bulunduğunu göz ardı etmemek gerekmektedir.

1.3. Yapay Zekâ Kavramı ve Temel Bileşenleri

Yapay zekâ (YZ), bilgisayarların insan benzeri bilişsel görevleri yerine getirebilmesini sağlayan algoritmalar ve modeller bütünüdür. Makine öğrenmesi, derin öğrenme, YZ ile otomasyonun birleştirildiği doğal dil işleme ve akıllı otomasyon sistemleri gibi alt alanlar, YZ'nin temel bileşenlerindendir.

1.4. Araştırmanın Amacı ve Kapsamı

Bu çalışmanın amacı, dijitalleşme sonucunda kullanımı yaygınlaşan akıllı otomasyon sistemlerinin kurumların faaliyetlerinde kullanımının getirdiği temel riskler ile bu risklerin iç denetim için ne tür zorluklar oluşturduğu, oluşabilecek risklerin önlenmesinde iç denetimin nasıl bir fonksiyon üstlenmesi gerektiği ve bu sistemlerin iç denetim faaliyetlerinde kullanımına ilişkin alanları değerlendirerek, iç denetimin yeni teknolojilere ayak uydurmak ve güncel kalabilmek için ne tür önlemler alması gerektiği konularını araştırmaktır.

Bu araştırma, dijitalleşmenin iç denetim süreçlerine etkisini incelemek ve yapay zekânın iç denetimdeki kullanım alanlarını ortaya koymak üzere hazırlanmıştır. Ayrıca uygulamadaki fırsatlar, zorluklar ve geleceğe yönelik stratejiler değerlendirilecektir.

2. DİJİTALLEŞME, TEMEL KAVRAMLAR VE GELİŞİM SÜRECİ

2.1. Dijitalleşmenin Tanımı ve Evrimi

2.1.1. Dijitalleşme veya Sayısallaşma:

Dijitalleşme veya sayısallaşma, ulaşılabilir bilgilerin herhangi bir bilgisayar tarafından okunabilecek şekilde dijital ortama aktarılması sürecine verilen addır. Özellikle mühendisler çeşitli fiziki görüntüleri bilgisayara aktarıp çalışmalar yapmak için kullanırlar.¹

Demirci'ye (Demirci, 2023) göre; “Dijitalleşme kavramı “0 ve 1 sembollerinin ikili sayı sistemine dayanarak işlenmesi” olarak ifade edilmektedir. Aksu' ya (Aksu, 2018) göre; Dijitalleşme sürecinin lokomotifleri olarak da “mikrocip, internet ve mobil iletişim” teknolojilerini sıralayabiliriz (Demirci, 2023; Aksu, 2018; aktaran Türkyılmaz, 2024)².

2.1.2. Dijital Dönüşüm:

Dijital dönüşüm, toplumsal ve sektörel ihtiyaçlara dijital teknolojilerin entegrasyonu ile çözüm bulmanın ve buna bağlı olarak iş akışlarının ve kültürün gelişmesi ve değişmesi sürecini tanımlayan bir kavramdır. Yaratıcılığı ve inovasyonu merkeze alan dijital dönüşüm, geleneksel metotlardan daha verimli sonuçlar elde etmek için ortaya çıkmıştır. Dijital dönüşüm, insan ve çevre odağında, teknolojinin sosyolojiyle etkileşiminden ortaya çıkan “yaratıcı yıkımla”, toplumsal olarak yeni bir yönetim, üretim ve yaşam sürecine geçiş olarak da ifade edilebilir.³

2.1.2.1. Dijital dönüşümün tarihi gelişimi:

Dijital Dönüşümün Tarihsel Gelişim Süreci Türkyılmaz (Türkyılmaz, 2024) tarafından oluşturulan tabloda yer alan verilerden yararlanılarak aşağıda özetlenmiştir.

- 17.yy (1679) -Leibenez ikili sayı sistemi “0-1”
- 18-19 yy. – Mekanik hesap makineleri Bilgi depolama yaklaşımları
- 1947 – Bell laboratuvarları ilk transistörün icadı
- 1950 – İnternetin resmi başlama tarihi
- 1971 – İlk mikrobilgisayar
- 1975 – İlk dijital kamera
- 1976 – Apple 1 ilk kişisel bilgisayar
- 1977 – İlk ATM
- 1981 – IBM PC Microsoft İşletim Sistemi
- 1989 – WWW (World Wide Web)
- 1990 – İnternet -Cep telefonu cihazları
- 1990-2000’li yıllar- İnternetin gelişimi –(VEDOP, MERNİS) Banka otomasyonları
- 2000 - WEB 2.0 Nesnelerin İnterneti
- 2004 - Facebook -You Tube – Wikipedia
- 2010- İnstagram – Blockchain ve kripto para – Hücresel taşıma sistemi

¹ <https://tr.wikipedia.org/wiki/Dijitalleşme> (Erişim Tarihi:05.05.2025)

² Türkyılmaz, S. (2024). DİJİTAL DÖNÜŞÜM: TARİHÇESİ, TANIMI VE İŞLETMELER ÜZERİNDEKİ ETKİSİ. Nişantaşı Üniversitesi Sosyal Bilimler Dergisi, 12(1), 276-297.

³ https://tr.wikipedia.org/wiki/Dijital_dönüşüm (Erişim Tarihi:05.05.2025)

- 2020 – Otonom Etkileşim ve Sanallaşma

2.1.2.2. Dijital dönüşüm ile birlikte hayatımıza giren kavramlar:

2.1.2.2.1. Büyük veri nedir ?

Büyük veri ya da İngilizce karşılığı olan "big data" geleneksel veri tabanı sistemleriyle depolanması, yönetilmesi ve analizi mümkün olmayan verilerdir. Büyük veri, analiz edilmesi ve verimliliği arttırması için toplanan, anlamlı ve işlenebilir veriler bütünüdür.⁴

2.1.2.2.2. Veri analitiği nedir?

Veri analitiği, gelecekteki eğilimleri tahmin etmek ve anlamlı öngörüler yapabilmek, bilinçli kararlar almak adına, büyük ve karmaşık veri gruplarını çeşitli algoritma ve uygulamalar aracılığı ile analiz ederek yorumlama ve sonuçlar çıkarma işlemidir.

Veri biliminden doğan ve günümüzün en kritik bilimlerinden biri haline gelen veri analitiği, oldukça geniş kapsamlı bir çalışma alanına sahiptir. Büyük verilerin (big data) incelenmesinde kullanılan veri analitiği sonuçları birçok farklı sektörün tercihlerinde yol gösterici olmaktadır.

Büyük Veri Analitiği⁵:

- Büyük veri analitiği, büyük ve çeşitli veri setleri üzerinde işlem yaparak gizli örüntüleri çıkarma, bilinmeyen ilişkileri keşfetme sürecidir.
- Kullanılan yöntemlerle elde edilen bilgi; firmalara, kurumlara veya ticari girişimlere yönelik önemli bilgiler sağlamaktadır.
- Büyük veri analitiği uygulamaları veri bilimcilere modelleri tahmin etme, istatistikçilere ve diğer analiz alanında çalışan profesyonellere büyüyen verileri kolay analiz etme yeteneği kazandırır. Büyük veri analitiği klasik yöntemlerle yönetilmesi çok zor olan çok büyük, yapılandırılmamış ve çok hızlı değişen veriyle uğraşır ve anlamlı örüntüler elde eder.
- Büyük veri analitiği yöntemleri veriyi saklamak, veriyi elde etmek ve analiz etmek için gelişmiş teknolojiyi kullanır.

2.1.2.2.3. Veri madenciliği nedir?

Bilgisayar sistemleri ile üretilen veriler tek başlarına bir anlam ifade etmez. Bu verilerin belli bir amaç doğrultusunda işlenmesi sonucunda elde edilen veriler ancak anlam ifade eden verilere dönüşmektedir. Veri madenciliği bir kurumda üretilen tüm verilerin, belirli yöntemler kullanarak var olan ya da gelecekte ortaya çıkabilecek gizli bilgiyi ortaya çıkarma süreci olarak değerlendirilmesidir. Veri madenciliği çalışmaları, sınıflandırma, ilişki kurma, kümeleme, regresyon, veri özetleme, değişikliklerin analizi, sapmaların tespiti gibi belirli sayıda teknik yaklaşımları içerir. Veri madenciliği ile ilgili diğer disiplinlere aşağıda yer verilmiştir.

VERİ MADENCİLİĞİ					
Veri Tabanı Sistemleri	Veri Görselliği	Yapay Sinir Ağları	İstatistik	Yapay Öğrenme	Diğer Disiplinler

⁴ <https://www.mysoft.com.tr/buyuk-veri-big-data> (Erişim Tarihi: 7.05.2025)

⁵ M. Ali Akcayol Gazi Üniversitesi Bilgisayar Mühendisliği Bölümü ders notları https://bigdata.gazi.edu.tr/akcayol/files/SLBD_L2BigData.pdf

2.1.2.2.4. Nesnelerin interneti (Internet of Things-IoT) nedir?

Yılmaz'a (2023) göre;

- “Nesnelerin İnterneti, internet bağlantısı olan cihazların makine öğrenmesi vasıtasıyla koordineli bir biçimde çalışmasını sağlayan sisteme verilen addır.
- Nesnelerin İnterneti; birbirleriyle iletişim kurabilen ve başka bilgisayarlar ile bilgi alışverişinde bulunabilen aygıtları ifade etmektedir.
- Nesnelerin İnterneti çok farklı şekilde tanımlansa da, insan ile insan arasında ya da insan ile bilgisayar arasında herhangi bir etkileşime gerek olmaksızın nesneler, sensörler tarafından toplanan verilerin ağ yoluyla otomatik olarak aktarılması yeteneği olarak ifade edilebilir. Nesneler tarafından toplanan veriler sıcaklık ve basınç gibi çevresel veriler olabileceği gibi insanlara ilişkin kişisel veriler de olabilmektedir. Nesnelerin İnterneti teknolojisi esas itibarıyla üç ögeden oluşmaktadır. Bunlar (Gonzales & Djurica, 2015, s.1):
 - ✓ Nesneler; veri yakalama, üretme, kaydetme yeteneği bulunan cihazlardır.
 - ✓ İletişim Ağı; nesnelerin birbirine bağlanmasını sağlayan ve genellikle kablosuz ağlardır.
 - ✓ Bilgisayar Sistemleri; nesneler tarafından yakalanan ve gönderilen verileri işleyen bilgisayar sistemleridir” (Yılmaz, 2023)⁶.

2.1.2.2.5. Yapay zekâ , makine öğrenimi ve derin öğrenme nedir?

Akın ve Şahin'e (2024) göre

“Yapay zekâ, makine öğrenmesi ve derin öğrenme mantık olarak aynı olsa da işlev bakımından birbirlerinden ayrılır. Yapay zekâ, sadece sisteme girilen yani öğretilen veriler doğrultusunda işlem yapabilirken makine öğrenmesi verilen veriler ve bu verilerden oluşturduğu ekstra bilgiler doğrultusunda çıkarım yapmaktadır. Denetimli makine öğreniminin bir alt dalı olan derin öğrenme ise beynin yapısından ve işlevinden ilham alan yapay sinir ağları algoritmalarını kullanarak işlemlerini gerçekleştirmektedir. Yapay zekâ ve makine öğrenmesine göre daha çok veriyi daha karmaşık bir şekilde kendi oluşturduğu algoritma zincirleri ile yinelemeli olarak öğrenebilen ve sürekli olarak öznelik değerlerini oluşturup oluşturduğu bu öz niteliklere göre çıkarımlar yapabilen bir sistemdir. En genel tanımıyla derin öğrenme; canlıların karmaşık problemler ve durumlar karşısında kullandığı gözlem, analiz, öğrenme ve karar verme gibi özgül davranışları, çok yüksek miktardaki verileri denetimli veya denetimsiz öğrenme algoritmalarında kullanarak öznelik çıkaran ve çıkardığı bu öz niteliklere dönüştürme ve sınıflandırma gibi işlemler uygulayarak taklit edebilen bir makine öğrenmesi yöntemidir” (Akın ve Şahin, 2024)⁷.

⁶ Yılmaz, R. K. (2023). KAMU YÖNETİMİNDE KULLANILABİLECEK NESNELERİN İNTERNETİ (IOT) UYGULAMALARI. Kamu Yönetimi Ve Teknoloji Dergisi, 5(1), 87-98.

⁷ Akın, E., & Şahin, M. E. (2024). Derin Öğrenme ve Yapay Sinir Ağı Modelleri Üzerine Bir İnceleme. EMO Bilimsel Dergi, 14(1), 27-38.

2.1.2.2.5.1.Yapay zekâ

Yapay Zekâ , 1950’lerde açığa çıkmıştır. En basit tanımı ile, insan zekâsının belli bir parçasını taklit etmeye çalışan sistemlerin genel adıdır. Bu açıdan bakıldığında, yapay zekâ dendiğinde aklımıza insanın zekâsını tamamen taklit edebilen veya amacı bu olan sistemler gelmemelidir.

2.1.2.2.5.2. Makine öğrenmesi

Makine öğrenmesi, 1980’lerde açığa çıkmış olup veri madenciliğın kullanılması ile beraber daha popüler hale gelmeye başlamıştır.

Makine öğrenimi, verilerden beslenerek yeni şeyler öğrenme sistemidir. Makine öğrenmesi, büyük veri guruplarının analiz edilerek sunulan verilerin içerdığı desenlerin öğrenilmesi ve elde edilen bu bilgilerle yeni veriler üzerinde çıkarımda bulunulması üzerine yapılan çalışmaları kapsayan sistem programları ile ilgilenen bir bilim dalıdır. Söz konusu sistemler, daha iyi tespitlerde bulunmasının yanında, programlananları da açığa çıkarabilen kendi kendini eğitebilen sistemlerdir. Bu sayede ihtiyaç duyulan veriler rahatlıkla depolanabilmekte, ihtiyaç duyulduğunda erişilebilmekte ve analiz için kullanılabilir. Bu sistemde belirli görevleri yerine getirmek amacıyla bilgisayarları açıkça programlamaya gerek bulunmamaktadır.

Makine öğrenmesi temelde denetimli (gözetimli) öğrenme, denetimsiz (gözetimsiz) öğrenme ve yarı denetimli öğrenme olmak üzere üç ana gruptan toplanabilir.

1. **Denetimli öğrenme:** Denetimli öğrenme, algoritmanın etiketli verilerle eğitildiği ve bir dizi girdinin bir dizi çıktıyla eşleştirildiği, makine öğreniminin bir dalıdır. Buradaki temel amaç ise sisteme yüklenen ve sonuçları bilinen veri setinden yapılan sınıflandırmadan yararlanarak, sonuçları bilinmeyen veri setine dair etkili tahminler elde etmektir. Bu yöntemin en olumsuz yönlerinden biri ise etiketli örnekler ile büyük veri kümelerini oluşturmanın çok zaman almasıdır.
2. **Denetimsiz öğrenme:** Denetimsiz öğrenmede kullanıcının sisteme herhangi bir müdahalesi söz konusu değildir. Sisteme sadece girdi verileri yüklenir. Denetimsiz öğrenme algoritmaları, girdileri içeren bu veri yığını yapısal olarak gruplar veya kümeler. Sistem etiketlenmemiş, sınıflandırılmamış veya kategorize edilmemiş test verilerinden yararlanarak keşifler yapar, ilişki ağını ortaya koymaya çalışır ve öğrenir. Denetimli öğrenmeye kıyasla denetimsiz öğrenme, makinelerin kendi kendilerine öğrenebilmelerine daha yakındır. Ancak bu öğrenmeyle ilgili en büyük sorun, sonucun genellikle tahmin edilemez olmasıdır.
3. **Yarı denetimli öğrenme:** Yarı denetimli öğrenme, denetimsiz öğrenme ve denetimli öğrenme arasında bir makine öğrenimi çeşididir. Az sayıdaki etiketlenmiş veriden hareketle, etiketlenmemiş veriler hakkında bilgi sahibi olmaya ve onları sınıflandırma yöntemine yarı denetimli öğrenme denir.

2.1.2.2.5.3. Derin öğrenme

Derin öğrenme, 2000’li yıllarda kullanılmaya başlanmıştır. Derin öğrenme makinenin yapay sinir ağıları vasıtasıyla büyük miktarda veriden öğrenme sürecini içermektedir. Diğer bir deyişle, derin öğrenme çok katmanlı yapay sinir ağıları aracılığıyla gerçekleştirilen öğrenmeyi ifade etmekte olup insan beyni temel alınarak modellenmiştir.

Derin öğrenme modelleri, doğru öngörü ve tahminler üretmek için karmaşık resimler, metinler, sesler ve diğer verilerdeki düzenleri tanımak, görüntüleri tasvir etmek veya bir ses dosyasını

metne dönüştürmek gibi insan zekâsı gerektiren birçok görevi otomatikleştirmek için kullanılabilmektedir.

2.1.2.2.6. Akıllı otomasyon nedir? Akıllı otomasyon kavramı ve bileşenleri nelerdir?

Akıllı otomasyon, iş süreçlerini iyileştirmek, kolaylaştırmak ve tekrarlayan görevleri otomatikleştirmek amacıyla, robotik süreç otomasyonu (RPA), makine öğrenimi (ML) ve doğal dil işleme (NLP) gibi teknikler kullanılarak, geçmiş verilerden öğrenebilme ve karar alabilme becerileri eklenerek geliştirilen, yapay zekâ (AI) ile otomasyonun birleştirildiği bir sistemdir.

Schoop'ye (2002: 2978) göre akıllı otomasyon; rutin iş süreci faaliyetleri ile birlikte karmaşık bilgi çalışmalarını otomatikleştirmek için veri ve analitik, robotik, bilişsel ve yapay zekâyı kullanan bir sistem olarak ifade edilebilmektedir (Schoop, vd., 2002: 2978; aktaran Kestane, 2021)⁸.

Kestane'ye (2021) göre akıllı otomasyon teknolojilerinin bileşenleri üç ana başlık altında toplanmıştır. Bunlar;

“Temel robotik süreç otomasyonu (RSO): Kural motorları, iş akışı ve ekran kazıma gibi yazılım ve uygulama tabanlı araçlardan oluşan RSO araçları, kayıtları karşılaştırma ve işlemleri yerine getirme gibi kesin kuralları izleyebilmekte, manuel ve rutin etkinlikleri otomatik hale getirmektedir (Huang ve Vasarhelyi, 2019: 1-2).

Gelişmiş süreç otomasyonu: İlgili teknolojiler, yapılandırılmamış verileri işleme, bilgi havuzları oluşturma ve kullanma ile deneyimlerden yararlanarak öğrenme yeteneğine sahiptir. Bahsedilen yetenekler, satın alma siparişlerini yerine getirme ve yeni çalışanları işe alma gibi bazı insani kararlar gerektiren daha karmaşık süreçlerin otomatikleştirmelerine olanak tanımaktadır.

Bilişsel otomasyon (BO): Üst düzey beceri, yargı ve eleştirel düşünme gerektiren faaliyetleri hedefleyen bilişsel otomasyon sistemleri (çıkarım yapma, duygusal ipuçlarını okuma, mantık yürütme, varsayım oluşturma ve insanlarla iletişim kurma gibi insan etkinliklerini taklit etmek gibi) doğal dil işleme, yapay zekâ, makine öğrenimi ve veri analitiği gibi gelişmiş teknolojileri bir araya getirmektedir. Bilişsel otomasyon araçları otomatikleştirme becerilerinin ötesine geçerek çalışanları daha bilinçli ve üretken hale getirerek gerçekleştirmiş oldukları faaliyetleri artırabilmektedir. Finansal yatırım rehberliği sağlayan bir "robot-danışman" ve bir çağrı merkezinde sorgulamaya yanıt veren, "sanal asistan" bugün var olan bilişsel otomasyonun gerçek dünyadaki örnekleridir”(Kestane, 2021).

Bugün artık akıllı otomasyon sistemleri ile tüm iş süreçlerini otomatikleştirmek neredeyse mümkün hale gelmiştir.

⁸ Kestane, A. (2021). İÇ DENETİMDE AKILLI OTOMASYON TEKNOLOJİLERİNİN KULLANIMI: ROBOTİK SÜREÇ OTOMASYONU VE BİLİŞSEL ZEKÂ. Journal of Accounting and Taxation Studies, 14(2), 813-835. <https://doi.org/10.29067/muvu.806426>

2.2. Büyük Veri Analizinde Yapay Zekâ ve Makine Öğrenmesi Tekniklerinin Kullanımı

Büyük veri kavramı, veri kümesinin olağanüstü boyutu yanında, yüksek veri oluşum hızı ve veri çeşitliliğini de içermektedir. Büyük verinin kullanımı beraberinde, bu verilerin depolanması, güvenlik ve mahremiyetinin sağlanması, doğru bir şekilde işlenerek analiz edilmesi ve veriye dayalı sağlıklı kararlar verilmesine ilişkin arayışları da getirmiştir.

Hacim, çeşitlilik, hız, değişkenlik gibi özellikleri yanında, mevcut ve hızla üretilmeye devam eden yapısal, yarı yapısal ve yapısal olmayan formlara sahip büyük verinin, geleneksel veri yönetim sistemleri ile işlenmesi mümkün değildir. Bu nedenle süreçte veri madenciliği, bilgisayar bilimi, makine öğrenmesi, veri tabanı yönetimi, matematiksel algoritmalar ve istatistiğin birlikte çalışması zorunlu hale gelmektedir.

Yapay zekâ, insan gibi düşünen ve davranan bilgisayar sistemleri olup makine öğrenmesi ise yapay zekânın son evresi olarak kabul edilmektedir.

Aşağıda veri madenciliği ve büyük veri analizinde makine öğrenmesi ve yapay zekâ yöntem ve tekniklerinin kullanımı; kümeleme, sınıflandırma, yapay sinir ağları, metin ve web madenciliği ve fikir madenciliği (duygu analizi) başlıkları altında gruplandırılarak, bunlara dair literatürde bulunan bazı uygulamalardan örnekler verilmiştir.

2.2.1. Kümeleme:

Denetimsiz öğrenme algoritması olan kümeleme analizinde, nesneler önceden belirlenmiş bir kritere göre gruplandırılmaktadır. Örnekler: satış hareketleri, çağrı merkezi kayıtları, örüntü tanıma, konuşma tanıma, görüntü ve ses işleme, işletmelerde müşterilerin tercihlerine, coğrafi durumlarına ve demografik yapılarına göre, satın alma davranışları gibi çeşitli özelliklerine göre gruplara ayrılması, sosyal ağ analizleri, anahtar kelime aramaları, taranan anahtar kelimelerin ilişkili olduğu kavramlara göre sıralanması, trend topiklerin ortaya çıkarılması vb.

2.2.2. Sınıflandırma:

Denetimli öğrenme algoritmaları olan sınıflandırma algoritmalarında, bir verinin sahip olduğu özellikler dikkate alınarak hangi gruba ait olduğu ve yeni eklenecek nesnelerin hangi sınıfta yer alacağı tahmin edilir. Örnekler: metin sınıflandırma, yüz ve ses tanıma, çağrı yönlendirme vb.

2.2.3. Yapay Sinir Ağları:

Yapay sinir ağları modeli ile aynı veri birbirinden bağımsız işlemcilerle ayrıştırılır ve her bir işlemci birbirinden bağımsız çalışır. Örnekler: yüz ve ses tanıma, doğal dil işleme, tercüme, lokasyon bazlı analizler, el yazısı tanıma, haritaların dijital ortamda işlenmesi, arkadaş-firma bulma, mekan bildirimi, işletmelerin finansal durumlarının derecelendirilmesi.

2.2.4. Metin ve Web Madenciliği:

Metin madenciliği, metin tabanlı çok büyük boyuttaki verilerin analiz edilerek, kavramlar arasındaki bağlantıların ve anlamlı bilgilerin ortaya çıkarılması, belgeler içerisindeki gizli kalıpların elde edilmesidir. Örnek: dilden dile yapılan çeviriler, arama motorlarında

kullanıcıların hatalı yazmış olduğu sözcüklerin bulunması ve doğrusunun önerilmesi, müşteri ilişkileri yönetimi, güvenlik ve istihbarat pazar araştırması.

Web madenciliği ise, web içerikleri ile ilişkili olan verinin analizini ifade etmektedir. Örnekler: web sitelerinin kullanıcıların geri dönüşlerine göre düzenlenmesi, tıklanma sayılarına göre reklam ücretlerinin belirlenmesi, müşteri kazanmak amacıyla lokasyon bilgileri tespit edilerek mesaj gönderilmesi, mobil cihazların internet ve GPS bağlantıları ile bağlantı kurması, sosyal ağlarla lokasyon bazlı servisler ile işlem yapması, trafik akışının düzenlenmesi, arkadaş arama vb.

2.2.5. Fikir Madenciliği (Duygu Analizi):

Fikir madenciliği (duygu analizi), metin madenciliğinin bir uygulama alanı olarak ortaya çıkmış olup bir konu üzerine görüş sahibinin fikrinin sınıflandırılması veya tanımlanması için istatistiksel model ve yazılımların kullanılmasıdır. Fikir madenciliği, kişilerin bir ürün, servis, kurum, olaylar ve diğer şahıslar hakkındaki duygu, fikir, görüş, yorum ve davranışlarını analiz ederken, yapılandırılmamış metinlerden bilgi ve içerdiği fikrin çıkarılmasını hedeflemektedir.

Örnekler: forum, blog ve haber sitelerindeki yorumların ve içinde geçen karşılaştırma cümlelerinin tespiti ve karşılaştırma ilişkilerinin sınıflandırılması, Twitter mesajlarının sınıflandırılması, biyomedikal literatüründeki atıf ve özetlerin karşılaştırılması, hangi ürün veya hizmetin diğerine göre tercih edildiğinin bulunması, sosyal medya verilerinden yapılan duygu durum analizine uygun reklam gönderimi, yazılan sosyal medya içerikleri değerlendirilerek seçim sonuçlarının tahmini.

2.2.6. Değişik Alanlarda Kullanılan Bazı Yapay Zekâ ve Makine Öğrenmesi Uygulamaları:

Aşağıda yükseköğretim, kamu yönetimi ve iç denetim alanlarında kullanılan bazı yapay zekâ ve makine öğrenmesi uygulamalarına yer verilmiştir.

Tablo 1. Yükseköğretim Alanında Kullanılan Bazı Yapay Zekâ ve Makine Öğrenmesi Uygulamaları

Uygulama Alanı	Açıklama	Örnek
Kişiselleştirilmiş Eğitim	Öğrenci performansına göre özelleştirilmiş içerik önerisi	YZ tabanlı öğrenme yönetim sistemleri (LMS)
Akademik Başarı Tahmini	Öğrenci notları, devam durumu, geçmiş başarılar üzerinden başarı tahmini	Mezuniyet risk analizi
Veriye Dayalı Karar Desteği	Akademik planlama ve kontenjan belirlemede veri analitiği	Bölüm açma-kapama kararlarında yapay zekâ
Akademik Sahtecilik Tespiti	Otomatik intihal kontrolü, sınav davranış analizleri	Kamera tabanlı sınav gözetim sistemleri

Yapay Zekâ ile Kütüphane Otomasyonu	Kullanıcı davranışına göre kaynak önerisi	Akıllı arama motorları ve otomatik sınıflandırıcılar
--	---	--

Tablo 2. Kamu Yönetimi Alanında Kullanılan Bazı Yapay Zekâ ve Makine Öğrenmesi Uygulamaları

Uygulama Alanı	Açıklama	Örnek
Politika Geliştirme	Sosyal medya, istatistiksel veriler ve geri bildirimlerle karar destek	Halk sağlığı veya ulaşım politikalarında simülasyon
e-Devlet Hizmetleri	Vatandaş sorularına otomatik yanıtlar	Chatbot destekli bilgi sistemleri
Kamu Kaynaklarının Tahsisinde Optimizasyon	Ödenek, personel ve hizmet dağılımında veriye dayalı kararlar	YZ ile bütçe planlama modelleri
Afet ve Kriz Yönetimi	Risk tahmini, erken uyarı sistemleri	Sel, deprem, yangın gibi afetlerde öngörü modelleri
Siber Güvenlik ve Veri Güvenliği	Anomali tespiti ve otomatik müdahale	YZ ile log verilerinin analizi ve saldırı tahmini

Tablo 3. İç Denetim Alanında Kullanılan Bazı Yapay Zekâ ve Makine Öğrenmesi Uygulamaları

Uygulama Alanı	Açıklama	Örnek
Anomali Tespiti	Harcama, ihale, personel verilerinde olağandışı durumların belirlenmesi	Taşınır kayıtlarında sapma analizi
Risk Tabanlı Denetim Planlaması	Öncelikli risk alanlarının otomatik olarak belirlenmesi	MÖ destekli dinamik risk skorlaması
Süreç Madenciliği (Process Mining)	Kurum içi iş akışlarının analiz edilerek uyumsuzlukların saptanması	İdari izin, satın alma veya maaş süreçlerinin izlenmesi
Metin Madenciliği ve Doğal Dil İşleme	Rapor, yazışma, sözleşme gibi metinlerde ihmal veya suistimal tespiti	Denetim raporlarının otomatik analiz edilmesi
Gerçek Zamanlı Denetim	Sürekli denetim sistemlerinin kurulması	Anlık finansal kontrol sistemleri (continuous auditing)

2.3. Doğal Dil İşleme (NLP) Teknolojisi ve Otomatik Raporlama

Bilgisayarların insanların dillerini anlaması, onlarla iletişime geçmeleri ancak doğal dil işleme biliminin kullanımı ile mümkündür.

Doğal dil işleme (NLP), bilgisayarların çeşitli amaçlarla doğal dildeki metni veya konuşmayı anlamak ve işlemek için nasıl kullanılabileceğini araştıran bir araştırma alanıdır. NLP araştırmacıları, bilgisayar sistemlerinin istenen görevleri gerçekleştirmek için doğal dilleri anlamasını ve manipüle etmesini sağlamak için bilgisayar bilimleri, yapay zekâ ve dilbilim aracılığıyla çeşitli araçlar ve teknikler geliştirmektedir⁹.

Doğal dil işlemenin kullanım alanlarının bazıları aşağıdaki gibidir:

- **Makine çevirisi:** Metinlerin bir dilden bir başka dile çevrilmesidir. Bu alandaki en büyük zorluk, kelimeleri doğrudan çevirmek yerine, anlamsal bütünlüğü koruyacak şekilde çevirebilmektir.
- **Metin kategorizasyonu:** Metnin, metin sınıflandırıcılar ile analiz edilmesi ve ardından içeriğine göre önceden tanımlanmış bir dizi kategori ile sınıflandırılmasıdır. Spam filtreleme çalışmaları, metin kategorizasyonu için örnek verilebilir.
- **Bilgi çıkarma:** Bilgi çıkarma, yapılandırılmış bilgilerin yapılandırılmamış veya yarı yapılandırılmış kaynaklardan otomatik olarak çıkarılmasıdır. Bu işlem ile adlar, yerler, olaylar ve tarihler gibi başka işlemlerde işlenebilecek veri metinden çıkarılarak, yapılandırılmamış veriyle hesaplama yapılabilir. Örneğin, bir web sayfasındaki önemli bilgilerin otomatik olarak tanınması, bir arama motorunun performansını oldukça artırabilir.
- **Özetleme:** Metin gibi bir veri setinin anlamını kaybetmeden boyutunun küçültülmesidir.

İç denetim faaliyeti sonucunda düzenlenen raporlar, genellikle kapsamlı veri analizi ve belge hazırlama sürecini gerektirmektedir. Günümüzde yapay zekâ destekli teknolojik araçlar bu süreçleri hızlandırarak, denetim raporlarının daha hızlı ve doğru bir şekilde oluşturulmasına katkı sağlamaktadır. Doğal dil işleme teknolojileri, denetim bulgularını analiz ederek özet raporlar oluşturabilmektedir.

Bugün artık sağlık alanında hizmet veren sektörlerde, iç denetim süreçlerinde kullanılan yapay zekâ teknolojileri ile hasta verileri analiz edilebilmekte ve sağlık hizmetlerinin kalitesi değerlendirilebilmektedir.

Ayrıca yapay zekâ ve doğal dil işleme (NLP) teknolojilerinin kullanıldığı bazı uygulamalar ise denetim sürecindeki verileri toplamakta, analitik araçlar kullanarak analiz etmekte, büyük veri setlerini tarayarak anomali tespiti yapmakta ve sonuçları özetleyerek otomatik olarak detaylı denetim raporları üretebilmektedir.

Bu uygulamalar denetim ekiplerinin daha hızlı ve doğru kararlar almasına katkı sağlamakta, aynı zamanda insan hatalarını azaltarak raporların kalitesini arttırmakta ve raporlama sürecini hızlandırmaktadır. Bu sayede denetimin verimliliği artarken zaman tasarrufu da sağlanmaktadır.

⁹ <https://nek.istanbul.edu.tr/ekos/TEZ/ET002645.pdf> (Erişim Tarihi:16.06.2025)

2.4. Robotik Süreç Otomasyonu (RPA) ve İç Denetim

Günümüzde artık şirketler yazılım robotlarını kullanarak, uygulamalar arasında veri kopyalama, yapıştırma, verileri bağdaştırma veya çapraz referanslama gibi manuel görevleri otomatikleştirebilmektedirler.

Huang ve Vasarhelyi'ye (2019: 1-2) göre: Kural motorları, iş akışı ve ekran kazıma gibi yazılım ve uygulama tabanlı araçlardan oluşan RSO araçları, kayıtları karşılaştırma ve işlemleri yerine getirme gibi kesin kuralları izleyebilmekte, manuel ve rutin etkinlikleri otomatik hale getirmektedir (Huang ve Vasarhelyi, 2019: 1-2; aktaran Kestane, 2021).

RPA, genellikle manüel, zaman alıcı işleri veya görevleri gerçekleştirmek için dijital **robotlar veya botlar** olarak da bilinen sanal yazılım robotlarını kullanan, bir iş süreci otomasyon teknolojisidir. Tekrarlayan görevleri ve anahtarlama hatalarını en aza indirerek, iş süreçlerini hızlandırmak suretiyle maliyetleri azaltır.

RPA, yapay zekâ (AI) ve makine öğrenimi teknolojileri ile mevcut yetenekleri geliştirir. Bu süreçte makine öğrenmesi modelleri ve doğal dil işleme (NLP) gibi yapay zekâ araçlarını kullanır. Bu gelişmeler RPA'nın bilgi ve yargıya dayalı iş aktivitelerini otomatikleştirmesine olanak sağlar.

RPA'nın temel avantajlarından en önemlisi kaliteli sonuçlar elde edebilmesidir. RPA robotları, sınırsız dikkat aralıklarına sahip olmaları ve mantığa dayalı çalışmaları nedeniyle, hesaplama hatalarını en aza indiren ve verimliliği arttıran uygulamalardır.

Bu uygulamalar, işi tam olarak öğrenildiği gibi yapar ve genellikle insanlardan daha hızlı çalışır, analizi mümkün kılan veriler üretir ve büyük veriler üzerinde gelişmiş veri analizi olanağı sağlar. Bu durum ise daha doğru kararlar alınmasına katkı sağlar.

Ayrıca, **RPA yazılımları tarafından gerçekleştirilen tüm eylemler kayıt altına almakta ve izlenmektedir.** Bu ise onları denetim izi oluşturan ve yasal uyumluluğun artmasına katkı sağlayan uygulamalar haline getirmektedir.

Büyük miktarlardaki veriyi analiz edebilme yeteneğine sahip yapay zekâ destekli araçlar, insanlar tarafından tespit edilmesi güç veya imkansız olan anormallikleri belirleyebilmekte, bu kapsamda veri ve tahminler üretebilmektedir.

İç denetim süreçlerinde RPA ve yapay zekâ uygulamalarının kullanılması ise, iç denetçilerin değerlendiremeyeceği boyuttaki büyük veri kümelerinin analiz edilmesini mümkün kılarak, fark edilemeyecek kayıplar ile anomalilerin, aykırı değerlerin ve dolandırıcılık girişimlerinin tespit edilmesine katkı sağlayacaktır. Ayrıca mutabakatlar, iç kontrol testleri, detay testler ve raporlama gibi manuel ve tekrar eden denetim görevlerinin otomatikleştirilmesi ve verimliliğin artırılması suretiyle daha doğru ve etkili kararlar alınması da mümkün olacaktır. Bu sayede risk ve kontrol değerlendirmesi süreçlerinin doğruluğu ve etkinliği de önemli ölçüde artabilecektir.

Doğru yönetim metodolojisi ile kurgulanan RPA, kurumların yönetim, risk yönetimi ve kontrollerinin etkinliğinin sürekli denetimini olanaklı kılarak, denetim maliyetlerinin düşürülmesine katkı sağlayacaktır.

Ayrıca, kurumların faaliyetlerinde yararlanmak üzere RPA uygulamasına yönelik bir girişimde bulunmaya karar verdiklerinde, bu sürece iç denetim ekibinin erken evrede dahil

edilmesi, genel yönetim çerçevesi ve süreç tasarımı hakkında dengeli bir risk değerlendirmesi gerçekleştirilmesine olanak sağlayacaktır.

3. YAPAY ZEKÂ UYGULAMALARINDA KARŞILAŞILAN ZORLUKLAR VE ETİK SORUNLAR

Bilişim teknolojilerinin etkin bir şekilde kullanımı, zaman içerisinde gerek tüm kullanıcı sektörler gerekse ülkeler ve toplumlar açısından büyük öneme sahip çok kritik ve çeşitli verilerin de dijital ortama taşınması sonucunu doğurmuştur. Dijital altyapılar kullanılarak yürütülmeye başlanan faaliyet ve hizmetler ile birlikte, mevcut tehdit ve riskler de boyut ve karakter değiştirmiştir. Siber tehdit ve saldırılar ise bu kapsamda her düzeyde büyük öneme sahip, karmaşık, hedef odaklı ve yıkıcı sonuçlar doğuran bir boyut kazanmıştır.

Bugün için özellikle ülkelerin ulusal güvenliğine yönelik olarak birer siber hedef haline gelen dijital altyapılar, öncelikli gündem konuları arasında yerini almaktadır.

Gelişmekte olan teknolojilerin sunduğu fırsatlar doğal olarak beraberinde önemli riskleri de getirmektedir. Bu kapsamda teknolojik olanakların kullanımı ile oluşacak yeni risklerin doğru bir şekilde belirlenmesi, yönetimine ilişkin uygun risk yönetim yaklaşım ve süreçlerinin geliştirilmesi zorunluluk olarak karşımıza çıkmaktadır.

Risk yönetimi, idarenin amaçlarına ve hedeflerine ulaşmasında karar mekanizmalarını güçlendiren bir yönetim aracıdır. Risk yönetimi ile kurumların hedeflerine ulaşmasına yardımcı olacak faaliyetleri etkileyebilecek her seviyedeki riskleri, belirli bir yöntemle sistematik olarak tespit etmek, değerlendirmek, izlemek ve alınan kontrol önlemleri yardımıyla yönetmek amaçlanmaktadır. Ayrıca bu süreçte makul fırsatların değerlendirilmesi suretiyle, kurumların hedeflerine ulaşmasına katkıda bulunmak da hedeflenmektedir.

Karacaer'e (2023) göre;

“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)

Tüm sektörlerdeki işletmeleri dönüştüren teknolojilerden biri de akıllı otomasyon sistemleridir. Robotik süreç otomasyonu (RPA) ile birleştirilen yapay zekâ 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. sektörlerle 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” (Karacaer, 2023)¹⁰.

Akıllı otomasyon teknolojilerinin işletmelere getirdiği yeni riskler literatürden ve önceki araştırmalardan yola çıkılarak ana hatlarıyla, teknolojik riskler, yasal düzenleme ve gizlilik ile ilgili riskler, etik riskler, siber riskler, kurumsal riskler ve finansal riskler şeklinde sınıflandırılabilir. Bu risklere aşağıda kısaca yer verilmiştir.

3.1. Teknolojik Riskler

3.1.1. Algoritmaların Yanlış Davranması ve Şeffaflığın Sağlanamaması Riski

Yapay zekâ sistemlerinin karar verme ilkeleri ve süreçleri genellikle şeffaf değildir. Bu durum ise değerlendirmeye esas teşkil eden objektif olmayan veriler, uygun olmayan modelleme teknikleri ve yanlış algoritmalar gibi riskler ile güvenlik açıklarının fark edilmesini, alınan uygun olmayan kararların izlenmesini zorlaştırmaktadır.

Yapay zekâ sistemlerinin kullanılmasında ki en büyük zafiyet, işletme operasyonları üzerinde büyük etkisi olabilecek, istenmeyen taraflı sonuçlar üretilebilmesi ve veri yönetiminin sağlanamaması riskidir.

Akıllı robotlar insan düşünme ve karar verme sürecini modelleyen öğretilen algoritmalarla çalışmaktadır. Farklı durumları ve koşulları yöneten, mantıklı ve analitik karar verebilen algoritmaların tasarlanması ise insan faktörü söz konusu olduğunda çok kolay olmamaktadır. Karar verme sürecinin mantığı net değilse, algoritmik kararlardaki hataları belirlemek de zorlaşmaktadır.

Kuşkusuz algoritmik şeffaflığın sağlanarak uygun olmayan karar modellerinin belirlenebilmesi, otomasyon sistemlerinde karar verme mantığını olumsuz etkileyen verilerin değerlendirilerek, güvenlik açıklarının giderilmesine ilişkin gerekli düzeltici önlemlerin alınmasına katkı sağlayacaktır.

3.1.2. Algoritmalarla Karşı Eleştirel Olmayan Güvenin Artması

Yeni teknolojilerin kullanımında insan faktörünün göz ardı edilmesi ve **algoritmaların doğruluğuna sorgusuz güvenmek**, özellikle tüm süreçlerin otomatikleştirilmesi için kullanılan akıllı otomasyon sistemlerinde büyük riskleri beraberinde getirmektedir.

Örneğin yazılımların amaçlanan hedeflere uygun çalışmaması, kullanılan algoritmaların karar verme mantığının ve iş süreçlerinin hatalı işlemesi geri dönülemez sonuçlara yol açacaktır. Bu etki süre uzadıkça katlanarak artacaktır.

Bu nedenle otomasyon sistemlerinin ürettiği sonuçların mutlak doğru olarak kabul edilmemesi, sürekli olarak izlenerek test edilmesi ve değerlendirilmesi gerekmektedir.

¹⁰ Karacaer, B. (2023). Akıllı Otomasyon Sistemlerinin Getirdiği Riskler ve İç Denetime Etkileri, İşletme Akademisi Dergisi, 4 (2): 155-173. <https://doi.org/10.26677/TR1010.2023.1248>

3.2. Hesap Verebilirliğin Sağlanamaması

Akıllı otomasyon sistemleri kullanılarak yürütülen iş süreçlerinde gelişen olumsuzluklara karşı sorumlu kimdir? Algoritmayı tasarlayan ve /veya satan tarafın mı, algoritmanın kararlarına güvenerek iş süreçlerinde kullanan taraf mı doğacak olumsuzluklara karşı sorumludur ve hesap verecektir?

Bu konu kurumlarda şeffaflığın ve hesap verilebilirliğin sağlanabilmesi açısından açıklığa kavuşturulması gereken en önemli sorunlar arasında yerini almaktadır.

3.3. Düzenleme ve Gizlilik İle İlgili Riskler

Akıllı otomasyon sistemini faaliyetlerinde kullanan kurumların, otomasyonun arkasındaki mantığın hedeflenen sonuçlara uyumlu ve doğru bir şekilde oluşturulduğundan, hata risklerinin en aza indirilmesine ilişkin önlemlerin alındığından, verilerin güvenliğinin sağlandığından ve otomasyon sisteminin önyargılı ve ayrımcı olabilecek sonuçlar sağlamadığından emin olması zorunludur. Bu zorunluluk, kurumların denetim süreçlerinde de birçok gerekliliği beraberinde getirmektedir.

Faaliyetlerini akıllı otomasyon sistemi kullanarak yürüten kurumlar açısından, başta bu sistemlerde kullanılan veriler olmak üzere, kurumsal veriler ile paydaşlara ait kişisel bilgilerin güvenliğinin ve gizliliğinin sağlanması da büyük önem arz etmektedir. Bu amaçla gerekli düzenlemelerin, değişen uygulamalara paralel olarak ivedilikle hayata geçirilmesi de bir zorunluluktur.

Türkiye’de bu kapsamda **6698 sayılı Kişisel Verilerin Korunması Kanunu** ile kişisel verilerin işlenmesinde, başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak amacıyla, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esaslar belirlenmiştir. Kanunda genel olarak kişisel bilgilerin kullanımına ilişkin pek çok düzenlemenin yanı sıra, özel olarak otomatik bilgi işlemeye ilişkin düzenlemelere de yer verilmiştir.

Ayrıca söz konusu Kanunda veri sorumlusu; kişisel verilerin işlenmesinin amaçlarını ve araçlarını belirleyerek, veri kayıt sisteminin oluşturulması ile yönetilmesinden sorumlu olan kişi şeklinde tanımlanmıştır. Yine veri sorumlusu, organizasyon içinde kişisel verilerin korunmasına ilişkin düzenlemelere uyumu sağlamak amacıyla denetimler yapmakla görevlendirilmiştir. Kanun ile verileri işleyen gerçek ve tüzel kişilerin sorumlulukları belirlenerek, kişisel veri gizliliğinin sağlanması güvence altına alınmaya çalışılmıştır.

3.4. Etik Riskler

Akıllı robotlar, insan düşünme ve karar verme sürecini modelleyen öğretilen algoritmalara göre çalışmaktadır. Doğal olarak insan davranışını belirleyen ahlaki ilkeler, algoritmaların davranışını da belirlemektedir. Buradaki en büyük sorun ise insanların ve toplumların etik konularda farklı düşünce ve değer yapısına sahip olmaları, bu nedenle de her zaman aynı fikirde olunamamasıdır.

Tüm yazılımların insanlar tarafından geliştirildiği değerlendirildiğinde, oluşumunda kültürel değer yargıları, insana ait olan sübjektif değerlendirmeler, önyargılı ve tarafsız yaklaşımlar, kişisel zafiyetler gibi unsurları barındırması ihtimali göz ardı edilemez bir gerçekliktir.

Bu kapsamda algoritmanın kararlarında her zaman etik kuralları dikkate aldığından ve etik kurallarla tahminler yaptığından emin olmak zordur ve algoritmanın bu konudaki opaklığı akıllı otomasyonun kullanımında karşılaşılan en büyük risklerden biridir.

Akıllı otomasyonlar üzerinde etik etkilerin yeterince yönetilememesi, verilen kararların karmaşıklığı ve şeffaflığın sağlanamaması kritik bazı sonuçların ortaya çıkmasına neden olabilir. Bunlardan bazıları aşağıda gösterilmiştir.

Akıllı otomasyonun kullanıldığı faaliyetlerde;

- Etik açıdan taraflı, önyargılı, ayrımcı ve opak yapıdaki yapay zekâ uygulamaları sonucunda, kurumların itibar ve müşteri kaybı yaşaması, yasal yaptırımlarla karşılaşması (Amazon'un iş başvurularını taramak için kullandığı yapay zekâ sisteminin kadınlara yönelik ayrımcı değerlendirmeleri).
- Kişisel verilerin korunamaması gibi nedenlerle kurumların itibar kaybı yaşaması, müşteri memnuniyetsizliği ve kaybı, iş fırsatlarından yararlanılamaması, yasal yaptırımlarla karşılaşılması.

3.5. Siber Riskler

Siber riskler, bilgi teknolojilerinin gelişmesiyle oluşan çok büyük miktarlardaki verilerin işlendiği siber ortamdan kaynaklanan risklerdir.

Yapay zekâ sistemlerinin kullanımı ile birlikte, gizli ve stratejik öneme sahip (devletlere, kurumlara veya kişilere ait) çok büyük miktardaki veri, bu sistemler tarafından işlenerek kayıt altına alınmaktadır. Ayrıca daha büyük ve esnek veri depolama talebinin artması ile birlikte bulut tabanlı depolama çözümlerinin benimsenmesi, veri güvenliği sorununu da beraberinde getirmektedir. Bu gelişmeler ise yapay zekâ sistemlerini ulusal ve uluslararası düzeyde siber saldırılara karşı açık hedef haline getirmektedir.

Bu doğrultuda, kurumların yeni teknolojileri ve akıllı otomasyon sistemini kullanıma alırken, verilerini güvende tutma adına sağlaması gereken ön koşul, **olası siber tehditlerin belirlenmesi, değerlendirilmesi ve siber ihlallere hızla yanıt verme yeteneğinin geliştirilmesi olmak zorundadır.**

Güvenli yazılım tasarımı ve geliştirilmesi süreci kullanılan sistemin yaşam döngüsü boyunca devam etmelidir. Doğru uygulanan güvenlik çözümleri, verilerin güvenliği ile birlikte etik riskler gibi diğer risklerin yönetilmesine de kuşkusuz katkı sağlayacaktır.

3.6. Kurumsal Riskler

Yeni teknolojilerin kullanılma alınması ve artan siber güvenlik ihtiyacı beraberinde yeni yeterlilikler ile teknik beceri gereksinimini de getirmektedir.

Dijital bir iş dönüşümü ile birlikte, otomasyonun getireceği teknik beceri gerekliliklerine uygun istihdam ihtiyacı, mevcut çalışanların durumundaki belirsizlikler ve ekonomik yansımaları, kurumların dijital dönüşüm tercihlerini doğrudan etkileyen faktörlerdir.

Mevcut çalışanların teknik beceri eksikliği, kurumların siber güvenlik tehditlerinin üstesinden gelme yeteneklerini de azaltan bir faktördür.

Yapay zekâ ve veri analitiği ile ilgili uygulamaların nitelikli personel takviyesini gerektirmesi, teknolojilerin benimsenmesinde gecikmelere ve devam eden projelerde aksamalara neden olan bir unsurdur.

Ayrıca istihdam edilen personelin mevcut teknolojiye uyumunu sağlamak da her zaman mümkün olamamaktadır. Bu nedenle dijital dönüşümün kurumların yapısına entegre edilerek, iş süreçlerinin bu dönüşüme uyumlu hale getirilmesi zahmetli ve zaman alıcı bir dönüşümdür. Kurumların yeterliliklerinin teknolojinin gerekliliklerini karşılamaması, akıllı otomasyon sistemlerinden kaçınmayı, başlamış projelerin sonuçlandırılmaması veya uygulanan sistemlerin güvenlik tehditlerine karşı savunmasız hale gelmeleri gibi sonuçlar doğurabilmektedir.

Bununla birlikte kurumların kullanılan otomasyon sistemlerini de kapsayacak şekilde geliştirilmiş bir risk kültürünün olmaması da, risklere yanıt verecek uygun kontrol önlemleri ile stratejilerin belirlenmesini zorlaştırmakta ve kurumları siber tehditlerde dahil olmak üzere birçok riske açık hale getirmektedir.

Bu gibi nedenler kurumların yeni teknolojilere karşı kültürel direnç göstermesi ve teknolojinin kullanılmasından sağlanacak faydanın göz ardı edilmesi gibi sonuçların ortaya çıkmasına neden olabilmektedir.

3.7. Akıllı Otomasyonun Benimsenmesi ve Finansal Riskler

Akıllı otomasyon sistemlerine ilişkin riskler (itibar kaybı, yasal yaptırımların oluşması, işe alım maliyetleri, ihtiyaca cevap vermeyen BT teknolojisi yatırımı gibi) kurumları farklı şekillerde etkilemekte ve oluşması halinde ciddi finansal sonuçları da beraberinde getirebilmektedir. Oluşacak risklere karşı etkin kontrollerin geliştirilmemesi ise otomasyon sistemlerinin kullanımı ile hedeflenen sonuçlara ulaşmanın önünde bir engel oluşturmaktadır.

Kurumların kullandığı akıllı otomasyon sistemlerinin başarısı için;

- Belirlenen stratejik hedefler ile akıllı otomasyon kullanımı ile hedeflenen sonuçların uyumlu olması,
- Akıllı otomasyon sistemlerinin planlanması ve uygulanmasında maliyet odaklı bir bakış açısı geliştirilmemesi, mutlaka tutarlılık, kalite ve doğruluk gibi kriterlerinde değerlendirmeye alınması,
- Oluşabilecek riskler ile görev çakışmalarını en aza indirmek ve yapılan yatırımlardan en üst düzeye fayda sağlamak için uygulamanın, akıllı robotik süreç otomasyonu (RPA) ile manuel olarak gerçekleştirilecek süreçler arasındaki dengenin doğru bir şekilde belirlenerek oluşturulması,
- Kullanılmasına karar verilen akıllı otomasyonlara bağlı süreçlere ait tüm kontrol ortamının yeniden tanımlanması, bu amaçla eski kontrol noktalarının gözden geçirilmesi ve gerekli olan yeni kontrollerin belirlenerek tasarlanması, uygulamasına devam edilecek eski kontrollerin dijitalleştirilmesi,
- Akıllı otomasyonun benimsenmesinin sağlanması,
- Otomasyonun planlanması sırasında doğru bir risk yönetim politikası oluşturulması, uygulamadaki değişikliklerin sürekli izlenerek günceliğinin korunması,

gerekmektedir.

4. GÜVENİLİR YAPAY ZEKÂ ARAYIŞI

Yapay zekâ uygulamaları günümüzde giderek daha fazla alanda kullanılmaya başlanmış olup günlük hayatımızın bir parçası haline gelmiştir. İnsan beyninin bir ürünü olan yapay zekâ uygulamalarının beraberinde getirdiği risklerde, doğal olarak her geçen gün değişerek artmaktadır. Yapay zekâ kullanımına ilişkin etik, yanlılık, veri güvenliği ve yasal eksiklikler gibi konularda yaşanacak risklere ilişkin olarak ciddi kaygılar yaşanmakta ve özellikle bu alanlarda son yıllarda ulusal ve uluslararası düzeyde yapay zekâ uygulamalarının nasıl daha güvenilir hale getirilebileceği sorusuna cevaplar aranarak, çözümler üretilmeye çalışılmaktadır.

Güvenilir yapay zekâ uygulaması ihtiyacına cevap vermek amacıyla geliştirilen bazı önemli uluslararası düzenleme ve çalışmalara aşağıda yer verilmiştir.

- AB üye ülkeleri arasında yapay zekâ için uyumlu bir düzenleyici çerçeve oluşturmayı amaçlayan "Avrupa Birliği Yapay Zekâ Yasası" (EU Artificial Intelligence Act) 14 Haziran 2023 yılında Avrupa Parlamentosu tarafından kabul edilmiştir.
- AB çalışmalarına öncülük eden YZ Üst Düzey Uzman Grubu (AI HLEG) tarafından Güvenilir Yapay Zekâ için Etik Kılavuz İlkeleri ve Değerlendirme Listesi yayımlanmıştır (Ulusal Yapay Zekâ Stratejisi, 2021, s.28).
- 2018 yılında, AB'ye üye devletler tarafından AB Yapay Zekâ Bildirgesi imzalanmıştır. Bu bildirme ile üye devletler için YZ alanında bir yol haritası belirlenmiş ve AB ülkelerinin YZ alanındaki lider ülkelerle yarışabilir konuma gelebilmesini sağlayacak hedefler ortaya koyulmuştur. İlgili bildirmede; teknolojik değişimin merkezinde görülen YZ'nin ekonomiye entegrasyonu, bilim ve eğitim alanlarında nasıl konumlandırılacağı, YZ etiği gibi kaygılardan bahsedilerek, bu hususlarda üye devletlere iş birliği çağrısı yapılmıştır (Ulusal Yapay Zekâ Stratejisi, 2021, s.29).
- Uluslararası düzeyde güvenilir YZ konusunda standartlaşma süreci de başlamıştır. ISO bünyesinde çalışmalar yürütülmekte olup bu kapsamda 2017 yılında "SC 42" alt komitesi kurulmuş ve 2020 yılında güvenilir YZ için ISO/IEC TR 24028:2020 standardı yayımlanmıştır (Ulusal Yapay Zekâ Stratejisi, 2021, s.29).
- Kanada'nın Yapay Zekâ Etik Yönergeleri: Kanada, adalet, şeffaflık, hesap verebilirlik ve güvenlik de dahil olmak üzere sorumlu yapay zekâ gelişimini teşvik etmek için yapay zekâ etik kuralları geliştirmiştir. 2018 yılında "Yapay Zekânın Sorumlu Geliştirilmesine İlişkin Montreal Deklarasyonu" ve 2023 yılında "Gelişmiş Üretken Yapay Zekâ Sistemlerinin Sorumlu Geliştirilmesi ve Yönetimine İlişkin Kurallar" adlı rehber yayınlanmıştır (Ulusal Yapay Zekâ Stratejisi, 2021, s.29).
- Yapay Zekâ Konusunda Küresel Ortaklık (GPAI), yapay zekânın sorumlu bir şekilde geliştirilmesini ve yaygınlaştırılmasını ilerletmek için hükümetleri ve uzmanları bir araya getiren uluslararası bir girişimdir. Yapay zekâ etiğine, politikasına ve en iyi uygulamalara odaklanmaktadır (Ulusal Yapay Zekâ Stratejisi, 2021, s.31).
- Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) Yapay Zekâ Kılavuzları: Etik ve demokratik değerleri dikkate alarak küresel yapay zekâ politikaları ekosistemini güçlendirmek amacıyla 2019 yılında yayımlanan OECD Yapay Zekâ Konsey Tavsiye Kararı, 2019 yılında G20 Yapay Zekâ İlkeleri adı ile kabul edilmiştir (Ulusal Yapay Zekâ Stratejisi, 2021, s.53).

Uluslararası kuruluşlar tarafından; insan hakları, demokratik değerler ve hukukun üstünlüğünü koruyan küresel bir politika ekosistemini güçlendirmeye yardımcı olmak ve ortaya çıkabilecek

toplumsal kaygıları azaltarak ortak bir tavır geliştirebilmek amacıyla yapay zekâ etik çerçeveleri yayımlanmıştır.

Ayrıca İç Denetçiler Enstitüsünün (İİA) 2017 yılında yayınladığı Yapay Zekâ Denetim Çerçevesi; Strateji (Siber Esneklik ve Yapay Zekâ Yetkinlikleri unsurları), Yönetişim (Veri Mimarisi & Altyapısı ve Veri Kalitesi unsurları) ve İnsan Faktörü (Etik ve Kara Kutu) olmak üzere üç kapsayıcı bileşenden oluşmaktadır (İİA, 2017). O zamandan bu güne önemi giderek artan bu önemli konu hakkında dönüm noktası niteliğinde bir düzenleme olan bu çerçeve, yapay zekâ ve iç denetim mesleği için dikkate alınması gereken önemli hususları içermekte ve bugüne kadar iç denetim alanında büyük ölçüde geçerli ve yararlı olmaya devam etmektedir.

Güvenilir yapay zekâ alanında Türkiye’de yapılan çalışmalara ise (mevzuat, politika, kurumlar) aşağıda yer verilmiştir.

- 2016 yılında TÜBİTAK BİLGEM Yazılım Teknolojileri Araştırma Enstitüsü tarafından başlatılan Dijital Olgunluk Modeli ve Rehberliği Projesi ile kamu kurumları ve sundukları hizmetlerde dijitalleşme kapasitesi ve yetkinliğinin belirlenmesine yönelik olarak, 2017 yılında Türkiye’ye özgü Dijital Olgunluk Modeli ile İşletim ve Bakım Rehberi oluşturulmuştur.
- 2019 yılında yayımlanan 48 sayılı Cumhurbaşkanlığı Kararnamesi ile 1 sayılı Kararname’ye eklenen maddelerle, ülkemizde “Kamuda öncelikli proje alanlarında yapay zekâ uygulamalarına öncülük etmek ve koordinasyonu sağlamak” temel göreviyle, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi bünyesinde “Büyük Veri ve Yapay Zekâ Uygulamaları Dairesi Başkanlığı” kurulmuştur.
- 2020 yılında 59 sayılı Cumhurbaşkanlığı Kararnamesi ile Sanayi ve Teknoloji Bakanlığının (STB) görevleri arasına “Ekonomik etki düzeyi yüksek ve birden çok sektörde gelişimi hızlandırma potansiyeline sahip ileri teknolojiler ile büyük veri, yapay zekâ, siber güvenlik gibi kritik alanlarda bireylerin ve işletmelerin AR-GE ve üretim yetkinliklerinin artırılması amacıyla politika önerileri ve stratejiler oluşturmak, belirlenen politika ve stratejilerin uygulanmasını sağlamak, ilgili alanlarda AR-GE ve yatırım faaliyetlerini ve girişimleri desteklemek, ilgili alanlara ve desteklere dair düzenleme ve denetlemeler yapmak” bendi eklenmiştir. Bu çerçevede yürütülecek çalışmalar için gerekli kurumsal kapasitenin oluşturulması amacıyla da STB bünyesinde Milli Teknoloji Genel Müdürlüğü (MTGM) kurulmuştur.
- 2020 yılında yapay zekâ teknolojilerinin yaygınlaştırılmasında katalizör olma hedefiyle TÜBİTAK Yapay Zekâ Enstitüsü kurulmuştur.
- Çeşitli ulusal politika belgelerinde öncelikli teknoloji alanı olarak belirlenen yapay zekâyâ yönelik uzun dönemli bir yol haritası oluşturmak amacıyla, On Birinci Kalkınma Planı doğrultusunda hazırlanan 2021 Yılı Cumhurbaşkanlığı Yıllık Programı’nda yer alan 473.1 No.lu tedbirle “Ulusal Yapay Zekâ Stratejisinin” hazırlanması görevi CBDDO ve STB’ye verilmiştir (Ulusal Yapay Zekâ Stratejisi, 2021, s.37).
- 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı: “Yapay zekâ, nesnelerin interneti, blok zincir, 5G gibi hayatımızda yer edinen yeni nesil teknolojilerin güvenlik kriterlerinin, yakın gelecekteki siber güvenlik planlamalarında öncelikli olarak yer alacağı” belirtilmiş ve “**yapay zekânın ve blok zincir teknolojilerinin siber güvenlik için kullanım alanlarının belirlenmesi ve geliştirilecek yerli ve millî teknolojiler ile katma değer oluşturulması**” amaçlanmıştır (Ulusal Yapay Zekâ Stratejisi, 2021, s.38).

- 2020-2023 Ulusal Akıllı Ulaşım Sistemleri (AUS) Stratejisi Belgesi ve Eylem Planı: “AUS bileşenlerini içeren IoT ağına kurulması, bu bileşenlerden toplanan verilerin büyük veri ortamında saklanması ve analize uygun hale getirilerek yapay zekâ, derin öğrenme, haberleşme ve benzeri alanlardaki yenilikçi teknolojiler kullanılarak ulaşım altyapısının optimize edilmesi” hedeflenmiştir (Ulusal Yapay Zekâ Stratejisi, 2021, s.38).
- Ülkemiz, OECD, G20, AB ve UNESCO tarafından belirlenen insan odaklı yapay zekâ ilkelerinin paydaşı olup “**güvenilir ve sorumlu yapay zekâ**” değer ve ilkelerini benimsemektedir.
- Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ile T.C. Sanayi ve Teknoloji Bakanlığı tarafından 2021 yılı Ağustos ayında yayınlanan Türkiye Ulusal Yapay Zekâ Stratejisi ile Türkiye’nin güvenilir yapay zekâ alanında yapılan çalışmalara katılımının sağlanacağı ve bu alanda faaliyetler gerçekleştirileceği belirtilmiş ve çalışmada 8 adet güvenilir yapay zekâ ilkesi belirtilmiştir. Bu ilkeler aşağıda ki gibidir (Ulusal Yapay Zekâ Stratejisi, 2021, ss.60-61):
 - ✓ Ölçülülük,
 - ✓ Emniyet ve güvenlik,
 - ✓ Tarafsızlık,
 - ✓ Mahremiyet,
 - ✓ Şeffaflık ve açıklanabilirlik,
 - ✓ Sorumluluk ve hesap verebilirlik,
 - ✓ Veri egemenliği,
 - ✓ Çok paydaşlı yönetim.

5. İÇ DENETİMDE YAPAY ZEKÂ VE KULLANIM ALANLARI

Yapay zekâ tabanlı uygulamalar hız ve verimlilik gibi avantajlar sağlamakla birlikte, veri doğruluğu, güvenliği ve tarafsızlık gibi konularda ciddi riskleri de bünyesinde barındırmaktadır. Günümüzde kontrolsüz ve denetimsiz kullanılan yapay zekâ uygulamaları giderek daha büyük bir endişe kaynağı haline gelmeye başlamıştır.

Bilinçsiz çalışanlar tarafından kurumsal faaliyetlerin yürütülmesinde BT departmanın bilgisi ve onayı alınmadan kullanılan kontrolsüz ve denetimsiz teknolojik araçlar, uyumluluk sorunları, yanlış çıktılar elde edilmesi gibi sorunların yaşanmasına neden olmasının yanında, hassas kurumsal bilgilerin bu uygulamalara yüklenmesi gibi bir durumda da kurumları veri ihlali riski ile karşı karşıya bırakmaktadır.

Nitekim bir yapay zekâ uygulamasına yüklenen veriler sadece yükleyiciye ait olmaktan çıkmakta ve o sistemin belleğinde kalarak başka kullanıcılar tarafından dolaylı olarak kullanılabilir bir nitelik kazanmaktadır.

Akıllı robotlar, insan düşünme ve karar verme sürecini modelleyen öğretilen algoritmalara göre çalışmaktadır. Bu durum ise farklı eğitim modelleri kullanılarak üretilen yapay zekâ uygulamalarının, aynı girdiler ile birbirinden tamamen farklı çıktılar üretmesine neden olabilmekte ve üretilen verilerin doğruluğunu tartışmalı hale getirebilmektedir. Bu nedenle akıllı robotlar tarafından üretilen sonuçların koşulsuz kabul edilmesi doğru bir yaklaşım olarak kabul edilmemektedir.

Kurumsal kullanıcıların yapay zekâyı iş süreçlerinde kullanırken her zaman oluşabilecek riskleri göz önünde bulundurması, kurumları tarafından kabul edilerek onay verilen güvenilir ve etik değerlere sahip uygulamaları tercih etmeleri gerekmektedir.

Kurumlarda yürütülen faaliyetlerde verimliliğin artırılması çabaları, iş yapış şekilleri ve süreçlerinde de değişiklikleri beraberinde getirmektedir. Bu kapsamda iş süreçleri ve sorumlularının izlenmesi ve değerlendirilmesi ihtiyacı giderek artmış ve bu durum denetimden beklentileri de değiştirmiştir. Bu ihtiyaç 20'inci yüzyılın başlarında iç denetimin ortaya çıkmasına katkı sağlamıştır. İç Denetçiler Enstitüsü'nün (IIA) 1941 yılında kurulması ile iç denetim resmi bir nitelik kazanmıştır.

İç Denetim Enstitüsü'nün (IIA, 2024) tanımına göre iç denetim, bir kurumun faaliyetlerini geliştirmek ve değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. İç denetim, kurumun risk yönetimi, kontrol ve yönetim süreçlerinin etkililiğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur.

Bu bölümde yapay zekânın iç denetime etkileri, yapay zekâ ve iç denetim arasındaki ilişki analiz edilmeye ve yapay zekânın iç denetimdeki potansiyel uygulama alanları ile bu teknolojinin iç denetimde kullanılmasının oluşturacağı fırsatlar ve tehditler, bu fırsat ve tehditlerin sonuçları ve olası sonuçlarının nasıl yönetilebileceğine ilişkin sorulara cevap aranmıştır. Bu amaçla kapsamlı bir literatür taraması yapılarak yapay zekâ ve iç denetim üzerine yapılan çalışmalar incelenmiştir.

5.1. İç Denetimde Dijital Dönüşümün Önemi

Teknolojinin hızlı bir şekilde gelişmesi tüm sektörleri varlığını sürdürebilmek için iş yapış şekillerini gözden geçirerek günün şartlarına uyumlu hale getirmeye ve dijitalleşmeye zorlamaktadır. Bu değişim yeni mesleklerin ortaya çıkmasına vesile olduğu kadar, mevcut mesleklerde ve mesleki uygulamalarda da köklü değişikliklere gidilmesini zorunlu hale getirmiştir. Teknolojik değişiklikler bu olanaklardan yararlanan tüm kurumların uygulamaya yön veren düzenlemeler ile yetki ve sorumluluk alanlarının yeniden belirlenmesini zorunlu kılmaktadır.

Yeni teknolojiler kullanıcılarına şüphesiz sayısız fırsat sağlamaktadır. Ancak bu fırsatlar beraberinde önemli ve değişken yeni riskleri de getirmektedir. Teknolojik olanakların kullanımından sağlanacak faydanın en üst seviyeye ulaşması ancak taşıdığı yeni risklerin doğru bir şekilde yönetimi ile gerçekleştirilebilir.

Risk yönetimi ile işletmelerin faaliyetlerini etkileyebilecek risklerin belirlenmesi, izlenmesi, yönetilmesi ve risk iştahı açısından makul fırsatların değerlendirmesi suretiyle, belirlenen kurumsal hedeflere ulaşılması amaçlanır.

Uygulamaya alınan yeni teknolojilerin tamamı ise işletmelerin risk yönetimi, iç denetim planlaması ve yürütülmesi faaliyetlerini yeniden gözden geçirmesini zorunlu kılmaktadır.

İç denetim kritik bir yönetim kontrol aracıdır ve organizasyon içerisindeki risklere karşı geliştirilen kontrollerin etkinliğini ölçmeyi ve değerlendirmeyi amaçlar. Bu yönüyle de yönetim adına gerçekleştirilen bir denetim türü olarak diğer denetim türlerinden ayrılmaktadır.

Bu bağlamda, kurumların teknolojik dönüşümü ve iş yapış şekillerindeki değişikliklerin de iç denetim faaliyetini doğrudan etkilemesi kaçınılmaz bir durumdur. İç denetim faaliyetinin fonksiyonlarını doğru bir şekilde yerine getirebilmesi ve varlığını sürdürebilmesi de ancak iç denetçilerin günün koşullarına uygun olarak değişime uyum sağlaması, gerekli uzmanlık ve iş becerisini edinerek, sürekli olarak kendini geliştirmesi ile mümkündür.

Ayrıca yaşanan hızlı değişim karşısında ortaya çıkan yeni risklerin yönetimi konusunda da yeni yaklaşımların geliştirilmesi gerekmektedir.

Tüm sektörlerde risk yönetimi süreçlerinde yaygın olarak Uluslararası İç Denetçiler Enstitüsünün (The Institute of Internal Auditors-IIA) geliştirdiği yeni “Üçlü Hat Modeli” kullanılabilmektedir.

Riske dayalı karar vermenin, savunma hamleleriyle olduğu kadar fırsatların yakalanmasıyla da ilgili olduğunu kabul eden yeni Üçlü Hat Modeliyle, kuruluşların daha etkili bir uyum, işbirliği, hesap verebilirlik durumuna ve de daha etkili hedeflere ulaşmasında rol alan anahtar rollere ilişkin sorumluluklar ile etkileşimlerin daha iyi tanımlanmasına ve yapılandırılmasına yardımcı olacağı değerlendirilmektedir.

Bu model,

- Yönetişim organı ve yönetim kurulunun gözetim sorumluluğu da dahil olmak üzere, birinci ve ikinci seviye rollere ilişkin yönetim ve operasyonel liderlerin riske ve uyuma dair sorumluluklarını,
- İç denetimin üçüncü hat olarak verdiği bağımsız güvence de dahil olmak üzere kurum içindeki çeşitli lider pozisyonların rollerini,

açıkça belirtmektedir. Ayrıca, dış güvence sağlayıcılarının konumunu da ele almaktadır. Modelin büyüklük veya karmaşıklığından bağımsız olarak tüm kuruluşlar tarafından uygulanması mümkündür.

IIA’nın Üçlü Hat Model gereğince İç denetim,

- Kurumun amaçlarına ulaşmasını desteklemek ve sürekli gelişme ve iyileşmeyi teşvik etmek ve kolaylaştırmak amaçlarıyla, yönetim ve risk yönetiminin yeterliliği ve etkililiği hakkında bağımsız ve objektif güvence ve tavsiye sunar.
- Bunu sistemli ve disiplinli bir yaklaşımla süreçlerin, uzmanlığın ve içgörünün yetkin bir şekilde uygulanmasıyla yerine getirir. Sürekli gelişimi ve iyileşmeyi teşvik etmek amacıyla tespit ve önerilerini yönetim ve yönetim organına raporlar.

5.2. İç Denetim Fonksiyonunun Dijitalleşmeyle Değişimi

İç denetim bir kuruluşun iç kontrol sistemlerinin, kurumsal yönetim ve muhasebe süreçlerinin etkinliğini değerlendiren bağımsız bir denetim türüdür.

İç denetim faaliyeti kurumlarda aşağıda gösterilen beş temel fonksiyonu yerine getirmektedir.

- Kurumların karşılaştığı risklerin belirlenmesi, değerlendirilmesi ve yönetilmesi için stratejiler geliştirerek, potansiyel risklerin önceden tespit edilmesi ve gerekli önlemlerin alınmasına,
- İç kontrol sistemlerini değerlendirilerek, bu sistemlerin etkinliğinin artırılmasına ve örgütlerin yönetim süreçlerinin iyileştirilmesine,

- Yasal ve düzenleyici gerekliliklere uyumun sağlanmasına, finansal raporlama ve diğer düzenleyici gerekliliklerin yerine getirilmesine,
- Kurumların operasyonlarının etkinliğini ve verimliliğini değerlendirerek, iş süreçlerinin iyileştirilmesi ve maliyetlerin azaltılmasına,
- Bilgi güvenliği ve bilgi teknolojisi sistemlerinin güvenilirliğini ve bütünlüğünü de değerlendirmek, veri güvenliği ve siber güvenlik risklerinin yönetilmesine,

katkı sağlamak.

Denetim faaliyeti ile bir kurumun faaliyet ve işlemlerinin belirlenen amaç ve kurallara uygun olarak gerçekleştirilip gerçekleştirilmediğinin değerlendirilmesi hedeflenmektedir.

İç denetim kurumların faaliyet ve süreçlerini **risk esaslı bir yaklaşımla değerlendirmekte**, mevcut risklerin tespiti ile birlikte mevcut kontrollerin etkinliğinin test edilmesi, yürütülen faaliyetlerin mevzuata uygunluğunun belirlenmesi gibi faaliyetleri yürütmektedir.

İç denetim faaliyeti kapsamında iç denetçilerin, tüm iş süreçlerine ve verilerine dolayısıyla bulunduğu kurumun tüm bilgilerine erişim sağlama yetkisi bulunmaktadır. Denetim faaliyetinin özelliği gereği de özellikle yapılandırılmamış türde geniş bir veri setiyle (büyük veri) karşı karşıya kalmaktadır.

Dijital dönüşüm ve yapay zekâ uygulamaları denetim faaliyetlerini iki şekilde etkilemektedir. Bu etkiler;

- Yapay zekâ teknolojilerinin kullanıldığı kurumlarda, yapay zekâ ile ilişkili risk yönetimi, kontrol ve yönetim süreçlerinin etkinliğinin değerlendirilmesi ve iyileştirmeye yönelik faaliyetlerin yürütmesi, yani yapay zekâ uygulamasının denetimi.
- İç denetim faaliyetlerinin yürütülmesi sırasında, denetim faaliyetinin planlanması, denetime yönelik verilerin toplanması, yürütülmesi ve denetim raporunun hazırlanmasına kadar tüm aşamalarda yapay zekâ araçlarının kullanılması (örneğin; analitik inceleme prosedürleri ve risk değerlendirmelerinde yapay sinir ağlarının, işlem sınıflandırmalarına yardımcı olmak için yapay zekâ algoritmalarının, risk ve iç kontrol sistemlerinin değerlendirmeleri için uzman sistemlerin kullanılması gibi).

Denetim faaliyetleri sırasında değerlendirilen alanların daha iyi anlaşılabilmesi, kilit risk alanlarının doğru bir şekilde belirlenerek daha faydalı, hızlı ve fazla iş üretilebilmesi, geniş veri setlerinin doğru bir şekilde analiz edilmesi ile mümkündür. Bu kapsamda ise yeni teknik ve teknolojiler ile veri analitiği yöntemlerinin denetimlerde kullanılması bir zorunluluk olarak karşımıza çıkmaktadır.

Bilişim teknolojileri alanındaki hızlı gelişmeler kurumların kullanımında olan bilgi sistemlerine yönelik oluşan yeni risklere karşı mevcut kontrollerin yeterliliğinin ölçülmesini de zorunlu kılmıştır. Oluşan ihtiyaca binaen iç denetim alanında da Bilgi Teknolojileri (BT) denetimi adı altında bir alt uzmanlık alanı ortaya çıkmıştır. Bu denetim türünde, kurumların bilgilerini işleyen ve saklayan BT sistemlerinin değerlendirilmesi, finansal veriler, tüm paydaş verileri ve çalışanların kişisel verileri gibi kritik veriler ile BT kullanımının etkililiği ve verimliliğinin değerlendirilmesi hedeflenmiştir.

Denetim faaliyetinin fonksiyonlarını doğru bir şekilde yerine getirmesi ve varlığını devam ettirmesi ancak, görev yaptıkları kurumların yaşadığı teknolojik değişim ve iş yapış şekillerine uygun dönüşümü sağlaması ile mümkündür. Bu kapsamda da denetim elemanlarının mevcut

koşullara uygun uzmanlık ve iş becerisini edinerek, sürekli olarak kendisini geliştirmesi, kurumların iş süreçlerine uyumlu teknolojik araç ve analiz tekniklerini kullanmaları gerekmektedir.

Karacaer'e (2023) göre;

“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 yönetim süreçlerinin etkinliğini değerlendirerek ve iyileştirerek, kuruluşun gelişimini ve hedeflere ulaşmasını desteklemek için objektif bir değerlendirme, güvence ve danışmanlık sağlamaktır (www.iaa.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 yönetim 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, COSO1 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)” (Karacaer, 2023).

BT denetimi özel uzmanlık ve yetkinlik gerektiren bir denetim türüdür. Bu alanda veri hacmi ile işleme süresinin çok yüksek olması denetimdeki en büyük zorluklardan birisidir. Bu nedenle alan yazında, BT alanında gerçekleştirilecek denetimlerde etkinlik ve verimliliğin artırılması, maliyetlerin azaltılarak kalitenin sağlanması ve zamandan tasarruf sağlanabilmesi için BT denetçilerinin yapay zekâ uygulamalarından yararlanmasında fayda bulunduğu vurgulanmaktadır.

Bilgi Sistemleri Denetim ve Kontrol Derneği (ISACA), BT Denetçilerinin profesyonelleşmesi amacıyla bilişim teknolojilerinin (**bilgi teknolojisi, bilgisayar sistemleri, yazılım, programlama dilleri, veri ve bilgi işleme ve depolama alanlarını kapsayan**) yönetişimi, denetlenmesi ve risk alanlarına ilişkin merkezi bir bilgi kaynağı ve kılavuz oluşturmuştur.

Ayrıca ülkemizde iç denetim alanında merkezi uyumlaştırma görev ve fonksiyonu bulunana İç Denetim Koordinasyon Kurulu, 2014 yılı Ocak ayında kamu idarelerinde Bilgi Teknolojileri Denetimi gerçekleştirilmesi sırasında izlenmesi ve uygulanması gereken metodoloji ve denetim testleri ile ilgili yöntem sunmak amacıyla, **Kamu Bilgi Teknolojileri Denetim Rehberini** uygulamaya koymuştur.

Söz konusu Rehber 2021 Yılı Ekim ayında yerini, T.C. Dijital Dönüşüm Ofisi Başkanlığı tarafından denetim çalışmalarının yürütülmesi konusunda kurum ve kuruluşlara yol göstermesi amacıyla hazırlanan, **Bilgi ve İletişim Güvenliği Denetim Rehberine** bırakmıştır.

Denetim Rehberi, kurum ve kuruluşlara bilgi ve iletişim güvenliği uyum faaliyetlerinin denetiminde; denetimin planlanması, denetim prosedürlerinin uygulanması ve sonuçların raporlanması konusunda izlenmesi gereken metodolojiye yer vermektedir. Ayrıca Rehberde, tüm kurum ve kuruluşlarda denetim faaliyetlerinin öncelikli olarak iç denetim birimlerinde görev alan ve bilgi teknolojileri alanında denetim yapmak üzere görevlendirilen iç denetçiler tarafından gerçekleştirilmesi esası getirilmiştir.

Karaca'ya (2024) göre;

“İç denetimin bu fonksiyonları etkili bir şekilde yerine getirmesi çeşitli teknolojileri kullanmasını gerekli kılmaktadır. İç denetimde kullanılan teknolojiler arasında YZ, makine öğrenimi, robotik süreç otomasyonu ve veri analitiği gibi araçlar bulunmaktadır. Bu teknolojiler, denetim süreçlerini daha hızlı, doğru ve verimli hale getirebilmekte ve denetçilere daha fazla bilginin toplanması ve analizi imkanını sağlayabilmektedir. YZ ve iç denetim arasındaki ilişki, YZ'nin denetim süreçlerindeki verimliliği ve etkinliği artırma potansiyeli ile belirginleşmektedir. YZ araçları, hem kuruluş içi hem de dışı bilgileri dikkate alarak denetçilerin büyük veri yığınları arasından daha önce gözden kaçırmış olabileceği bulguları belirlemelerine yardımcı olabilmektedir. Fedele tarafından hazırlanan Deloitte'un raporuna göre, YZ tabanlı süreçler, iç denetim ekiplerinin günlük operasyonlarına daha yüksek kalite, güvence ve üretkenlik getirmektedir. Ayrıca, Kluwer tarafından yayınlanan bir makalede, YZ'nin iç denetimdeki uygulamalarının, denetim yaşam döngüsünün her aşamasında etkili olabileceği belirtilmektedir (Fedele, 2021; ISACA; 2021; Kluwer, 2024).

YZ'nin iç denetimdeki önemi, denetim süreçlerinin her aşamasında fayda sağlamasıyla ortaya çıkmaktadır. Planlama ve kapsam belirlemeden saha çalışmasına ve bilgi raporlamasına kadar YZ, denetim kalitesini ve bilgilerini artırmakta ve finansal raporlamanın kalitesini iyileştirmekte önemli bir rol oynamaktadır. Bu nedenle, YZ'nin iç denetimde aşağıdaki süreçlerde kullanımı, kuruluşların yönetim, risk yönetimi ve iç kontrol süreçlerini güçlendirmelerine olanak tanımaktadır (Fedele; 2021; ISACA; 2021; Kluwer, 2024; Mach, 2024):

- ✓ **Planlama ve Kapsam Belirleme Süreci:** YZ, risk değerlendirmeleri ve kapsam belirlemede kullanılarak, en kritik risklere odaklanan daha kapsamlı bir plan oluşturulmasına yardımcı olmaktadır. Farklı kaynaklardan gelen verilerin daha hızlı ve nitelikli bir şekilde analiz edilmesi suretiyle denetim evreni ve örneklemin kapsamının belirlenmesinde YZ'den yararlanılmaktadır.
- ✓ **Risk Değerlendirme Süreci:** Geçmişte risk değerlendirmesi süreci genellikle zaman alıcı, özellikle yüz yüze görüşmelere dayalı subjektif verilere dayanmaktaydı. İç denetçiler veri toplama sürecini daha verimli hale getirmek ve somut veri kaynaklarını sürece dahil etmek için bu görüşmelere katkı sunacak ikincil veri kaynaklarını değerlendirme sürecinde YZ'yi aktif olarak kullanmıştır. İşte bu süreçte YZ ile denetim planlaması, denetçilere büyük veri setlerini analiz ederek potansiyel riskleri belirleme ve odak alanlarını önceliklendirmelerine yardımcı olmaktadır.
- ✓ **Denetim Saha Çalışması Süreci:** YZ'nin saha çalışmasında kullanımı, verimliliği ve otomasyonu artırmakta, risk tanımlama ve tespitini geliştirmekte ve denetim kalitesi ile içgörülerini iyileştirmektedir.

- ✓ **Raporlama Süreci:** YZ, denetim raporlamasını hızlandırmak, dilin basitleştirilmesi ve özetlerin oluşturulması gibi süreçlerde kullanılarak profesyonellerin işlerini daha verimli bir şekilde yapmalarına olanak tanımaktadır” (Karaca, 2024)¹¹.

5.3. Dijital Dönüşümün İç Denetimde Sağladığı Fırsatlar ve Riskler ile Dikkat Edilmesi Gereken Hususlar

5.3.1.Fırsatlar

İç denetim süreçlerinde yapay zekânın kullanımı, iç denetçilere ve kurumlara çok önemli fırsatlar sağlamaktadır. Bu fırsatlar aşağıda gösterilmiştir.

- **Kaynak Kullanımında Etkinliği Artırma ve Zaman Tasarrufu:** Yapay zekâ teknolojisi denetim süreçlerinde maliyetleri düşürmekte, zaman tasarrufu sağlamakta, kaynakların tam ve etkin kullanımına katkı sunmakta ve denetçilerin daha stratejik görevlerle ilgilenmesine olanak tanımaktadır
- **Büyük Veri Analizi ve Etkili Karar Alma:** Tüm örgütler; iç ve dış paydaşlarına ait veriler, iş süreçlerinden gelen veriler, finansal bilgiler gibi büyük miktarda veriyi yönetmek zorundadır. Bu verilerin etkin bir şekilde analiz edilmesi, örgütlerin daha iyi kararlar almasına yardımcı olmaktadır. Büyük veri analizi için YZ kullanımı, manuel yöntemlere göre daha hızlı ve doğru sonuç vermektedir. Özellikle veri hacmi arttıkça, YZ'nin avantajları daha da belirgin hale gelmektedir. Zira YZ algoritmaları, veri setlerini hızlı ve hassas bir şekilde işleyebilmektedir. Örneğin, stok yönetimi, fiyatlandırma ve tedarik zinciri optimizasyonunda ve denetiminde büyük veri analizlerinin kullanılması gerekmektedir. YZ, bu verileri analiz ederek iç denetçilere daha iyi kararlar almaları için önerilerde bulunabilmektedir. Böylece iç denetçilerin geleneksel örnekleme tekniklerinin ötesine geçmeleri ve tüm işlem veya veri kümesi popülasyonlarının kapsamlı analizlerini gerçekleştirmeleri mümkün olmakta, elde edilen doğru sonuçlarla getirilen önerilerle kurumların daha doğru kararlar almaları sağlanabilmektedir.
- **Hata Oranlarının Azalması, Etkili Raporlama ve İletişim:** Yapılan araştırmalarda; yapay zekâ algoritmalarının insan hatalarını azalttığı, finansal raporlamalar başta olmak üzere veri analizindeki hata oranlarını minimize ederek daha güvenilir sonuçlar elde edilmesine katkı sağladığı, yapay zekâ uygulamalarıyla yapılan denetimlerde ise daha az hata yapıldığı ve doğru veri üretmenin yanı sıra, yapay zekâ destekli araçlarla üretilen özlu, ihtiyaçlara göre uyarlanmış iç denetim raporlarının kurumlar genelinde bilinçli karar almayı kolaylaştırarak, sürekli iyileştirmeye katkı sağladığı ifade edilmektedir.
- **Daha Kolay ve Hızlı Anomali Tespiti:** Yapay zekâ destekli araçlar, büyük veri setlerini ele alarak tüm işlem veya veri kümesi popülasyonlarının kapsamlı analizlerini gerçekleştirebilmekte, anormallikler, düzensizlikler, fark edilmeyebilecek kalıplar ile aykırı değerleri belirleyebilmekte, dolandırıcılık tespiti, risk değerlendirmesi ve kontrol değerlendirmesinin doğruluğunu ve etkinliğini önemli ölçüde artırarak iç denetim faaliyetlerine önemli ölçüde katkı sağlaması mümkün olmaktadır.

¹¹ Karaca, M. (2024). Yapay Zekanın İç Denetime Etkileri Fırsatların Yakalanması ve Tehditlerin Yönetilmesi. Denetışim(31), 86-101. <https://doi.org/10.58348/denetisim.1526298>

- **Doğru Öngörü ve Analiz Yeteneği:** “Araştırmalarda YZ tabanlı sistemlerin; potansiyel riskleri tespit etmede başarılı olduğu, belirli trendleri analiz ederek şirketlerin finansal risklerini önceden tahmin edebildiği ve bu sayede erken müdahale imkanının oluştuğu, ayrıca bazı sektörlerde gelecekteki arz-talep dengesizliklerini tahmin edebildiği ve bu tahminler doğrultusunda operasyonel stratejilerinin oluşturulabildiği belirtilmektedir (Bose vd., 2023, ss. 32-51; Chu ve Yong, 2021, ss. 42-52; Narayanan vd., 2023, ss. 65-78)” (Aktaran Karaca, 2024).
- Yapay zekâ çeşitli kaynaklardan (sosyal medya, haber akışları ve sektör yayınları vb.) elde ettiği yapılandırılmış ve yapılandırılmamış verileri analiz ederek ürettiği bilgilerle, iç denetçilerin ortaya çıkan riskleri ve eğilimleri belirlemelerine yardımcı olmaktadır. Bu sayede kurumlara yönelik potansiyel tehditler belirlenebilmekte, önceden önlem almak ve oluşabilecek potansiyel kayıpların önüne geçilmek suretiyle itibar riskinin en aza indirilmesi mümkün olabilmektedir.

5.3.2.Riskler

Yapay zekânın iç denetimde kullanımı örgütler için aşağıda belirtilen bazı riskleri içerisinde barındırmaktadır.

- **Veri Güvenirliği ve Gizliliği Riski:** Yapay zekâ destekli araçlar, çeşitli kaynaklardan elde edilen yapılandırılmış ve yapılandırılmamış büyük veri setlerini ele alarak değerlendirmekte ve bilgi üretmektedir. Ancak kullanılan bu verilerin doğruluğu, güvenliği, gizliliği ve muhafazası gibi konular çok önemli tehditleri içerisinde barındırmaktadır. Araştırmalar, **yapay zekâ uygulamalarının veri ihlali riskini artırdığını göstermektedir.** Bu nedenle bu tür uygulamalar kullanılırken veri gizliliği ve güvenirliliği riskini artıran faktörlerin tespiti ve gerekli önlemlerin alınması büyük önem taşımaktadır.
- **Algoritmik Önyargı Riski:** Yapay zekâ sistemlerinin, eğitim verilerindeki önyargıları yansıtmaları sonucu ortaya çıkan durum algoritmik önyargı olarak ifade edilmektedir. Yapay zekâ sistemlerinin karar verme süreçlerinde farklı nedenlerle oluşan algoritmik önyargılar, denetim süreçlerinde de hatalı değerlendirme ve kararların oluşmasına, etik ve güvenilirlik sorunlarının yaşanmasına yol açabilmektedir. Algoritmik önyargılar, yapay zekâ tabanlı denetim sistemlerinin güvenilirliği ve etkinliğini de sorgulanabilir hale getirebilmektedir.
- **YZ Teknolojileri Konusunda Yetenekli Personel İhtiyacı ile Birlikte İş Gücü Değişimine İlişkin Riskler:** Denetim faaliyetlerinin yürütülmesinde yapay zekâ sistemlerinin kullanımı, analitik düşünme yeteneği ihtiyacını arttırmakta ve bazı görevlerin bu sistemler tarafından yürütülmesi sonucunda iş gücü gereksinimlerinde değişikliklere neden olabilmektedir. Bu nedenle bu uygulamadan yararlanan sektörlerde denetim elemanlarının rol ve sorumluluklarının yeniden tanımlanması ve mevcut çalışanların yetkinliklerinin artırılması veya yeni gerekliliklere uygun personel istihdamı zorunlu hale gelmektedir.

5.3.3. Fırsat ve Risklerin Yönetimi İçin Dikkat Edilmesi Gereken Hususlar

Yapay zekâ teknolojisinin iç denetimde oluşturduğu fırsat ve risklerin yönetimi için dikkat edilmesi gereken hususlar ise aşağıdaki gibi tasnif edilebilir.

- **Ulusal Dil Modeline Sahip YZ ve Güçlü Teknik Altyapısının Oluşturulması:** Kurumların ulusal dil modeline sahip yapay zekâ kullanımı, önemli avantajların yanında bazı güvenlik risklerini de bertaraf etmektedir. Bulunduğu ülkenin kültürünü ve hassasiyetlerini dikkate alarak tasarlanmış bir yapay zekâ uygulaması, hizmet verdiği coğrafyanın değerlerine uygun hareket ederek kararlar alacaktır. Ayrıca YZ sistemlerinin güvenilir veri üretmesi ve sürekliliğinin sağlanması güçlü bir teknik altyapının oluşturulmasına, yüksek kapasiteli sunucular ve güvenilir veri depolama çözümleri kullanılmasına bağlıdır. Bu ise yazılım ve donanım yatırımlarını gerektirmektedir. Günümüzde ülkelerin YZ uygulamalarını desteklemek için bulut tabanlı veri işleme hizmetlerine yatırım yapmaları bir zorunluluk olarak ortaya çıkmaktadır.
- **Veri Güvenliği Protokollerinin Güçlendirilmesi:** Veri güvenliği tehditlerini minimize etmek için öncelikle en güncel güvenlik yazılımlarıyla şifreleme tekniklerinin kullanıldığı ve veri anonimleştirme tekniklerinin uygulandığı güçlü güvenlik protokollerinin belirlenmesi ve uygulanması gerekmektedir.
- **Algoritma Şeffaflığı ve İzlenebilirliği:** Eğitim verileri, önyargılardan arındırılmalı ve farklı grupların temsili sağlanarak algoritmik önyargıların etkileri azaltılmalıdır. Algoritmaların karar verme süreçleri incelenerek, YZ sistemlerinin nasıl çalıştığına dair şeffaflık sağlanmalı ve sürekli olarak izlenerek performans değerlendirmesi gerçekleştirilmelidir. Ayrıca algoritmaların şeffaflığını sağlamak amacıyla uygulamaların sürekli izlenmesi, denetim algoritmalarının düzenli olarak gözden geçirilmesi ve bağımsız denetçiler tarafından değerlendirilmesi, bağımsız denetim komitelerinin kurulması ve bunların aktif olarak çalışmalarının sağlanması, algoritma şeffaflığını artırmak için önerilen önlemler arasında yer almaktadır. Bu kapsamda iç denetim ekiplerinin algoritmik önyargılar konusunda eğitilmesi ve konu hakkında farkındalığın artırılması, denetim süreçlerinde daha bilinçli kararlar alınmasına yardımcı olacaktır.
- **Sürekli Eğitim ve Bilgilendirme:** Denetim elemanlarının yapay zekâ teknolojileri konusunda bilgilendirilmesi, sürekli eğitilmesi ve yapay zekâ uygulamalarının etkin bir şekilde kullanımının sağlanması, sisteme ilişkin mevcut riskler ile kontrollerin yeterliliğinin doğru bir şekilde değerlendirilerek, gerekli önlemlerin zamanında alınmasına ve bildirimlerin zamanında yapılmasına katkı sağlayacaktır.
- **Yapay Zekâ Tabanlı Risk Yönetim Modeli Oluşturulması ve Kapsamlı Risk Yönetim Çerçevesi:** Kurumların yapay zekâ tabanlı risk yönetim modeline geçmesi ile birlikte bu sistemin kurulumu ve yönetiminin yanında, YZ'nin iç denetime getirdiği fırsatlar ve tehditleri yönetmek için kapsamlı bir risk yönetim çerçevesi oluşturmak bir gereklilik olarak karşımıza çıkmaktadır. Bu çerçeve oluşturulurken denetim birimleri tarafından;
 - ✓ Yapay zekâyla ilgili veri güvenliği, algoritmik yanlılık, şeffaflığın sağlanamaması, hukuki uyum, etik gibi riskleri içeren riskler belirlemelidir.
 - ✓ Her riskin olasılığı ve etkisi analiz edilerek değerlendirmelidir.
 - ✓ Değerlendirme sonrası yapay zekânın iç denetimde kullanımında hangi risklerin iş süreçlerini en çok etkilediğini ve hangi risklerin öncelikli olarak ele alınması gerektiğini anlamak adına paydaşlarla iletişime geçilmeli, alınacak görüşler değerlendirilerek ihtiyaçlar belirlenmeli, elde edilen bilgiler değerlendirilerek risk değerlendirmesinde dikkate alınmalıdır.

- ✓ Risk matrisi oluşturularak, önceliklendirilen riskler başta olmak üzere tüm riskler için riskleri azaltmak veya yönetmek için alınacak adımları içeren bir eylem planı oluşturmalıdır.

5.4. Risk Değerlendirme ve Önceliklendirme

İç denetim faaliyetlerinin planlanmasında esas alınan risk odaklı denetim anlayışı ile kurumların önemli düzeyde riskli görülen alanlarda güvence ve danışmanlık hizmetinin sağlıklı bir şekilde yürütülmesi hedeflenmektedir. Bu sürecin doğru bir şekilde yönetilmesi, iç denetçilerin risk ve risk yönetimi ile ilgili temel kavramlar, çerçeveler, araçlar ve teknikler hakkında yeterli bilgiye sahip olmasını gerektirmektedir.

Bozkurt’a (2024) göre;

“IIA’nın en son 2017 yılında güncellediği Uluslararası İç Denetim Standartlarında 2010 Kodlu Planlama Standardına göre iç denetim birimi sorumlusu işletme hedeflerini dikkate alarak iç denetim sürecindeki öncelikleri tespit eden risk odaklı denetim planı hazırlamalıdır. Standardın A1 paragrafına göre iç denetim faaliyet planı yılda en az bir kez yapılacak yazılı bir risk değerlendirmesini temel almalıdır. A2 paragrafına göre iç denetim birimi sorumlusu iç denetim görüşleri açısından tüm paydaşları göz önünde bulundurmalıdır. C1 paragrafına göre ise iç denetim birimi sorumlusu risk yönetimini etkin kılma, fayda sağlama ve faaliyetleri geliştirmek için kendini değerlendirerek danışmanlık görevini kabul edip etmeyeceğine karar vermelidir (TİDE, 2017a).

IIA tarafından 2020 yılında risk odaklı denetim planının geliştirilmesi kapsamında uygulama kılavuzu yayımlanmıştır. Bu uygulama kılavuzu, risk temelli bir yönetim oluşturma ve sürdürmeye yönelik sistematik bir yaklaşımı içermektedir. Kılavuza göre iç denetim birimi sorumluları iç denetim planı hazırlarken aşağıdaki hususları dikkate almalıdır (IIA,2020a):

- İşletmenin tanınması,
- Risklerin belirlenmesi, değerlendirilmesi ve önceliklendirilmesi,
- İç ve dış kaynak sağlayıcıları ile iş birliği yapılması,
- Kaynakların hesaplanması,
- İç denetim planının önerilmesi ve geri bildirim talebi,
- Planın sonlandırması ve iletilmesi,
- Risklerin sürekli değerlendirmesi,
- Planın güncellenmesi ve güncellemelerin iletilmesi vb.

Günümüzde iç denetim işlem ve uygunluk odaklı değil, sistem ve risk odaklıdır (Kaya, 2020, s.159). IIA standartları esas alınarak hazırlanan risk odaklı denetim sürecinin planlaması üç temel aşamadan oluşmaktadır. Bunlar risk değerlendirme, dönemsel denetim planlaması ve denetim görevlerinin belirlenmesidir (Selimoğlu ve Özbek, 2018:164). Risk odaklı denetimde yüksek riskli alanlara daha çok zaman ayrılır. Risklere karşı daha çok tespit yapılırken, denetim alanı genişletilir. Bu denetimde düzeltici yaklaşım yerine, önleyici yaklaşım uygulanmaktadır (Tanç ve Çardak, 2021, s.333). Bu yöntemin diğerlerinden farkı yönetimin iç değerlendirme sürecini anlama ve analiz etmeye odaklanmasıdır (Kaya,2020:161). Risk odaklı denetimin riskleri önceden

tespit etme ve makul seviyeye indirmek için planlama yapan öneren ve bunları değerlendiren süreç olduğu söylenebilir.

İç denetimin odaklanması gereken risk unsurları, işletmelerin dinamik bir çevrede faaliyette bulunmaları nedeniyle sürekli değişiklik göstermektedir. Bunun içindir ki doğru zamanda doğru risk unsurlarına odaklanması için risk değerlendirmeleri sürekli güncel tutulmalıdır (Tanç ve Çardak, 2021, s.350). Esasen risk odaklı denetimin başlangıç noktası organizasyonel iş hedefleri, odak noktası ise bu hedeflere ulaşmayı engelleyen risklerdir (Kaya, 2020, s.170). Bu yüzden değişen koşullar çerçevesinde işletmeler gerekli önlemleri alabilmek için gerekli değerlendirmeleri yapmalıdırlar. Örneğin; Tanç ve Çardak tarafından 2021 yılında yapılan çalışmada COVID 19 salgını ile işletmelerin ve iç denetim birimlerinin odaklanması gereken risk unsurlarından birisi de tedarik zinciri kesintileri olduğu belirtilmiştir (Tanç ve Çardak, 2021, s.350)” (Bozkurt, 2024)¹².

Denetim faaliyetleri sırasında kullanılan yapay zekâ uygulamaları, büyük veri setlerini hızlı ve doğru bir şekilde analiz ederek, iç denetim süreçlerine önemli katkılar sağlamaktadır. Bu analizler sırasında elde edilen veriler yapay zekâ algoritmaları tarafından değerlendirilerek, verilerdeki olağandışı kalıplar izlenmek suretiyle anomali tespiti gerçekleştirilmekte ve kurumların potansiyel riskleri belirlenebilmektedir. Yapay zekâ destekli tahmin modelleri ile değerlendirilen veriler esas alınarak oluşturulan risk senaryolarıyla, kurumların olası risklere karşı hazırlıklı olması da sağlanabilmektedir. Ayrıca yapay zekâ uygulamaları ile uygulayıcılara belirlenen bu risk faktörlerine karşı etkili çözümler geliştirilmesi ve stratejik kararlar alınması kapsamında da katkı sağlanmaktadır. Bu tür yapay zekâ uygulamaları, iç denetim ekiplerine veri tabanlı stratejik kararlar alma noktasında yardımcı olmaktadır.

Ancak kurumların ve iç denetim birimlerinin yapay zekâ uygulamalarından yararlanırken gözden kaçırmaması gereken en önemli konu, kullanılan akıllı otomasyon sistemlerinin çalışmasına ilişkin mantığın doğru ve hata risklerini en aza indirecek şekilde kurgulandığından, şeffaflığın sağlandığından, verilerin güvence altına alındığından ve otomasyonun herhangi bir şekilde taraflı olabilecek sonuçlar üretmediğinden emin olunması gerekliliğidir.

5.5. Süreç İzleme ve Anormallik Tespiti

Yapay zekâ uygulamaları, iç denetim faaliyetinin yürütülmesi sırasında büyük verilerin değerlendirilmesini sağlayarak, küçük hatalarda dahil anormal ve dolandırıcılık şüphesi olan durumların tespitinde önemli ve vazgeçilmez araçlar olarak karşımıza çıkmaktadır.

Bugün artık anomali tespiti algoritmaları, finansal işlemler ve diğer verilerdeki olağandışı faaliyetler ile muhtemel dolandırıcılık veya usulsüzlük içeren işlemleri erken evrede belirleyebilme olanağı sağlamaktadır. Bu uygulamalar büyük veri setlerinin analizini çok kısa sürelerde gerçekleştirerek, olağandışı işlem desenlerini belirlemekte ve denetim ekiplerini uyaramaktadır.

Geleneksel yöntemlerle yapılacak denetimler de ise, bu kadar kısa sürede bu büyüklükteki veri kümelerinin incelenerek değerlendirilmesi mümkün değildir.

¹² Bozkurt Yazar, B. (2024). KÜRESEL GELİŞMELER IŞIĞINDA İÇ DENETİM FAALİYETİNDE YAŞANAN DEĞİŞİMLERİN DEĞERLENDİRİLMESİ. Denetişim(29), 97-111. <https://doi.org/10.58348/denetisim.1391796>

5.6. Uygunluk ve Mevzuat Denetimi

Kamu kurumlarında iç denetimin temel işlevlerinden biri olan uygunluk denetimi, faaliyetlerin yürürlükteki mevzuata, politika belgelerine ve iç düzenlemelere ne ölçüde uygun olduğunu tespit etmeye yönelik sistematik bir süreçtir. Dijitalleşmenin hız kazanmasıyla birlikte bu denetim türü, büyük veri analitiği ve yapay zekâ tabanlı teknolojilerin desteğiyle daha etkin, bütüncül ve öngörücü bir yapıya kavuşmaktadır.

Yapay zekâ, uygunluk denetiminde üç temel düzeyde katma değer sunmaktadır:

a. Mevzuat Takibi ve Otomatik Güncelleme

Yapay zekâ destekli sistemler, mevzuat değişikliklerini gerçek zamanlı izleyerek kurum içi politika ve prosedürlerle karşılaştırabilir. Bu sayede denetim ekipleri, güncel olmayan uygulamaları erken safhada tespit edebilir. Ayrıca doğal dil işleme (NLP) algoritmaları kullanılarak mevzuat metinleri otomatik olarak analiz edilip, kurumsal faaliyetlerle ilişkili risk alanları çıkarılabilir.

b. Otomatik Uygunluk Taramaları (Compliance Scanning)

Yapay zekâ sistemleri, milyonlarca satırlık işlem ve belgeden oluşan veri kümelerini kısa sürede analiz ederek mevzuata aykırılık olasılığı taşıyan işlemleri işaretleyebilir. Bu durum, özellikle mali işlemlerde, satın alma süreçlerinde ve insan kaynakları uygulamalarında yüksek hacimli veri üzerinden riskli örüntülerin yakalanmasına olanak tanır.

b. Kural Motorları ve Öğrenen Sistemler

Gelişmiş YZ çözümleri, belirli mevzuat hükümlerini içeren kural motorları ile entegre edilerek, denetlenen birimin faaliyetlerini otomatik biçimde kontrol edebilir. Bunun yanı sıra, makine öğrenmesi algoritmaları geçmiş denetim verilerinden öğrenerek, gelecekteki potansiyel uygunsuzlukları tahmin edebilir ve denetim planlamasını bu doğrultuda optimize edebilir.

Kamu yükseköğretim kurumları özelinde değerlendirildiğinde, öğrenci işleri, akademik atamalar, proje harcamaları ve döner sermaye işlemleri gibi alanlarda mevzuata uygunluğun denetimi, yapay zekâ desteğiyle daha sistematik, objektif ve izlenebilir bir yapıya kavuşabilir. Bu gelişme, iç denetim birimlerinin yalnızca tespit eden değil; aynı zamanda proaktif biçimde yönlendiren bir konuma evrilmesini sağlayacaktır.

5.6.1. Uygunluk Denetimi İçin Yapay Zekâ Temelli Örnek Algoritma Akış Şeması

Amaç: Kurumsal faaliyetlerin ilgili mevzuata uygunluğunu denetlemek için yapay zekâ destekli otomatik tarama ve analiz süreci.

[1] Mevzuat Veri Tabanı Güncellemesi

↓

[2] Kurum Politikaları ve Süreç Dokümantasyonunun Yüklenmesi

↓

[3] İşlem Verilerinin Toplanması (muhasabe, satın alma, atama vb.)

↓

[4] NLP Tabanlı Mevzuat-Anlam Eşleştirmesi



[5] Kural Motoru ile Uyum Analizi



[6] Uygunsuzluk Risk Skolama (ML ile)



[7] Riskli Alanların Otomatik Raporlanması



[8] Denetçi Tarafından İncelenmesi ve Önceliklendirmesi



[9] Tavsiye Üretimi ve Otomatik Uyum Takip Sistemiyle Entegrasyon

Bu akış, özellikle kamu kurumlarında sık karşılaşılan “mevzuat dışı ödeme”, “mevzuata aykırı atama”, “usulsüz görevlendirme” gibi risklerin erken safhada tespiti için son derece işlevseldir.

5.6.2. Yurt Dışı Vaka Örneği: Estonya - Dijital Uygunluk Denetimi (e-Audit)

Ülke: Estonya

Kuruluş: Estonya Ulusal Denetim Ofisi (NAO – Riigikontroll)

Uygulama: e-Audit – Mevzuat Uyumunun Otomatik Takibi

Estonya'da geliştirilen e-Audit sistemi, kamu kurumlarının yürüttüğü faaliyetlerin ülke mevzuatına uygunluğunu yapay zekâ destekli olarak izlemektedir. Sistem, her kamu kurumunun sunduğu işlemsel verileri (ihale sonuçları, harcama detayları, personel atamaları vb.) merkezi olarak toplar. NLP algoritmaları sayesinde Estonya mevzuatı ile bu işlem verileri eşleştirilir.

Yapay zekâ, potansiyel mevzuat ihlallerini skorlar ve bunları görsel raporlarla denetçiye sunar. Örneğin, bir üniversitenin personel görevlendirmelerindeki tutarsızlıklar veya ödenek üstü harcamalar sistem tarafından otomatik uyarı ile işaretlenir. Böylece denetim süreci sadece geçmişe dönük bir kontrol olmaktan çıkar ve proaktif bir yönetim aracına dönüşür.

Sonuç:

Estonya örneği, mevzuatın dijitalleştirilmesi ile işlem verilerinin entegrasyonunun nasıl etkili bir denetim aracına dönüştürülebileceğini göstermektedir. Türkiye’de kamu kurumlarının benzer pilot uygulamalara yönelmesi mümkündür.

5.7. Finansal Denetim ve Sahtecilik Tespiti

Finansal denetim süreçleri, kamu kaynaklarının etkili, ekonomik ve mevzuata uygun kullanımının değerlendirilmesini amaçlar. Ancak işlem hacminin büyümesi, verinin çeşitlenmesi ve klasik denetim yöntemlerinin sınırlılıkları, denetçilerin özellikle **sahtecilik ve usulsüzlükleri tespit etme kapasitesini zorlamaktadır**. Bu noktada **yapay zekâ destekli**

finansal denetim araçları, iç denetimin kapsamını genişletmekte, zaman ve kaynak verimliliğini artırmakta ve risk odaklı denetim anlayışını güçlendirmektedir.

5.7.1. Anomali Tespiti ve Şüpheli İşlem Analizi

Yapay zekâ sistemleri, muhasebe, harcama ve satın alma verileri gibi çok boyutlu finansal veri kümelerinde **alışılmıřın dıřında örüntüleri (anomalileri)** tespit edebilir. Bu örüntüler, genellikle insan denetçiler tarafından fark edilemeyen karmařık sapmalardır. Örneğın:

- Aynı tedarikçiye yapılan tekrar eden ödemeler,
- Olağandışı zamanlarda (örneğin resmi tatil günleri) gerçekleştirilen harcamalar,
- Belirli personele yönelmiş alışılmadık ödeme kalıpları,
- İhale süreçlerinde teklif benzerliğı gibi yapay kalıplar.
- Bu tür anomaliler, makine öğrenmesi modelleriyle “risk skoru” verilerek önceliklendirilir ve denetçiye yönlendirilir.

5.7.2. Sahtecilik Risk Göstergelerinin Makine Öğrenmesiyle Tespiti

Makine öğrenmesi algoritmaları, geçmişte tespit edilmiş **sahtecilik vakalarından öğrenerek** benzer örüntüleri yeni veri kümelerinde tanımlayabilir. Bu yaklaşımla sistem hem **öğrenen hem de uyarlanan** bir denetim aracı haline gelir. Kamu yükseköğretim kurumlarında bu teknoloji:

- Usulsüz fatura düzenlemeleri,
- Gerçekleşmemiş mal/hizmet alımları,
- Yanıltıcı bordro hareketleri,
- Bağlantılı kişi veya şirketler üzerinden yapılan işlemler

gibi sahteciliğe açık alanlarda erken uyarı mekanizması sağlayabilir.

5.7.3. Blockchain ve YZ Tabanlı Denetim Entegrasyonları

Gelişmiş uygulamalarda yapay zekâ, blockchain tabanlı muhasebe sistemleriyle entegre çalışarak **her işlem adımının şeffaflık içinde ve değiştirilemez biçimde kaydedilmesini** sağlar. YZ ise bu kayıtlar arasında **tutarsızlık, gecikme, çakışma** gibi hususları tespit ederek denetçilere otomatik raporlar sunar. Bu tür sistemler, güvenli finansal denetimin dijital geleceğini şekillendirmektedir.

5.7.4. Kamu Kurumları ve Yükseköğretim Bağlamında Yapılan Değerlendirme:

Özellikle döner sermaye işletmeleri, proje bütçeleri ve dış kaynaklı fonlar gibi hassas finansal alanlar, **YZ destekli sürekli denetim sistemleriyle izlenebilir hale getirilebilir**. Bu sayede hem Sayıştay hem de iç denetim birimleri, klasik "tespit edici" rolün ötesine geçerek "öngören ve yönlendiren" bir denetim yapısına ulaşabilir.

Vaka Örneğı – ABD Sayıştay & Hazine Bakanlığı: “Do Not Pay” Analitik Platformu

Ülke: Amerika Birleşik Devletleri

Kuruluş: U.S. Department of the Treasury & Government Accountability Office (GAO)

Uygulama: Do Not Pay (DNP) Fraud Analytics Platform

ABD federal kurumları, kamu ödemelerinde hata, israf ve dolandırıcılığı önlemek için **“Do Not Pay”** adlı yapay zekâ destekli bir analiz platformu geliştirmiştir. Sistem, kamu kurumlarının yapacağı ödemeleri **risk analizinden geçirerek** ödemeden önce olası usulsüzlükleri işaretler.

Nasıl Çalışır?

- Yapay zekâ, geçmişte yapılmış binlerce hatalı veya sahte ödemeden “öğrenerek” potansiyel sahtecilik örüntülerini tanımlar.
- Kurumlar, ödeme yapmadan önce verileri DNP sistemine entegre eder.
- Sistem, şüpheli ödemelere “uyarı puanı” verir; bu puanlar karar vericilere sunulur.
- GAO, bu sistemle yılda milyonlarca dolar tasarruf edildiğini raporlamaktadır.

Uygulamanın Kamu Kurumları ve Yükseköğretim İçin Uyarlanabilirliği:

Türkiye'deki kamu kurumları ve üniversiteler de döner sermaye, dış kaynaklı projeler ve taşeron hizmet alımları gibi alanlarda bu tür bir erken uyarı ve analiz platformunu hayata geçirebilir.

Karar Destek Sistemi: YZ Tabanlı Finansal Sahtecilik Risk Değerlendirme Akışı

Aşağıdaki süreç, bir iç denetim biriminin yapay zekâ destekli dolandırıcılık taraması yaparken izleyebileceği örnek akış şemasıdır:

[1] Finansal İşlem Verilerinin Toplanması

(Harcama, bordro, fatura, satın alma vb.)



[2] Veri Temizleme ve Sınıflandırma

(Farklı kaynaklardan gelen verilerin standardize edilmesi)



[3] Makine Öğrenmesi ile Anomali Tespiti

(Olağandışı ödeme desenleri, gecikmeler, tekrar eden işlemler)



[4] Sahtecilik Risk Skoru Üretimi

(Her işlem veya tedarikçiye özel risk puanı)



[5] Uyarı Sistemi ve Görsel Raporlama

(Renk kodlamalı risk haritaları, grafikler)



[6] Denetçi Değerlendirmesi ve Geri Bildirim

(İnsan müdahalesiyle model doğruluğunun artırılması)



[7] Öğrenen Sistem Geliştirmesi

(Yeni tespit edilen vakalardan modelin sürekli öğrenmesi)

Bu tür sistemlerin uygulanması, kamu yükseköğretim kurumlarında sadece usulsüzlüklerin tespiti değil, aynı zamanda **finansal şeffaflık ve kaynak yönetiminde kalite güvencesi** sağlar.

5.8. Performans Analizi ve İç Kontrol Süreçlerinin Güçlendirilmesi

Kamu kurumlarında etkinlik, etkililik ve ekonomiklik ilkelerine dayalı performans denetimi, iç denetim fonksiyonunun stratejik düzeydeki en önemli araçlarından biridir. Ancak performans göstergelerinin doğru belirlenmesi, veriye dayalı izlenmesi ve gerçekçi biçimde değerlendirilmesi; büyük veri hacmi ve süreçler arası karmaşıklık nedeniyle geleneksel yöntemlerle sınırlı kalabilmektedir. Bu noktada **yapay zekâ destekli analitik teknolojiler**, iç denetimin performansa dayalı yönetim kabiliyetini belirgin biçimde artırmaktadır.

5.8.1. Göstergelerin Dinamik Takibi ve Anlamlandırılması

Yapay zekâ sistemleri, kamu kurumlarının belirlediği performans göstergelerini (KPI'lar) içeren çok çeşitli verileri (akademik başarı, bütçe kullanım oranı, hizmet sunum süresi, proje tamamlama süresi vb.) eş zamanlı analiz edebilir. Bu analizlerde:

- Zaman serileri üzerinden sapma analizi,
- Performans düşüklüğüne neden olan yapısal darboğazların tespiti,
- Kurum içi birimler arasında karşılaştırmalı verimlilik analizi,

yapılabilir.

Yapay zekâ bu sayede yalnızca veriyi izlemekle kalmaz, **nedensel ilişkiler kurarak denetçiye içgörü üretir**.

5.8.2. İç Kontrol Bileşenlerinin Dijital Olarak İzlenmesi ve Güçlendirilmesi

COSO modelinin öngördüğü iç kontrol bileşenleri (kontrol ortamı, risk değerlendirme, kontrol faaliyetleri, bilgi ve iletişim, izleme faaliyetleri), YZ tabanlı sistemlerle **ölçülebilir, izlenebilir ve optimize edilebilir hale gelir**. Örneğin:

Kontrol ortamı: Personel davranışlarındaki örüntülerden etik riskler tespit edilebilir.

Risk değerlendirme: YZ algoritmaları olasılık ve etki bazlı otomatik risk skorlaması yapabilir.

Kontrol faaliyetleri: Sistemler, prosedür dışına çıkan işlemleri işaretleyerek iç kontrollerin etkinliğini test eder.

Bilgi ve iletişim: Kurum içi bilgi akışının yavaşladığı veya tıklandığı noktalar haritalanabilir.

İzleme faaliyetleri: İç kontrol matrisleri dijital ortamda sürekli test edilerek zayıf noktalar belirlenebilir.

5.8.3. Tahmine Dayalı Analitik ve Stratejik Öngörü

Yapay zekâ destekli tahmine dayalı analitik araçlar, geçmiş performans verilerinden yola çıkarak **gelecekteki olası başarısızlık alanlarını** önceden işaretleyebilir. Bu öngörü:

- İç kontrol önlemlerinin proaktif şekilde alınmasını,
- Performans hedeflerinin revize edilmesini,
- Denetim kaynaklarının riskli alanlara yönlendirilmesini sağlar.

Bu yönüyle iç denetim, sadece geçmişe dönük tespit yapan bir yapı olmaktan çıkar, **kurumsal öğrenmeye katkı sunan stratejik bir danışma fonksiyonu** haline gelir.

Yükseköğretim kurumları özelinde değerlendirme:

Akademik başarı, öğrenci memnuniyeti, bütçe gerçekleştirmeleri, araştırma verimliliği, idari işlem süreleri gibi çok boyutlu göstergeler YZ algoritmaları ile izlenerek hem iç denetimin hem de iç kontrol sisteminin etkinliği artırılabilir. Bu sayede denetim, sadece hata arayan bir mekanizma değil, **kurumun kendini sürekli geliştirmesini sağlayan bir yönetim ortağı** rolünü üstlenebilir.

YZ Tabanlı Performans Denetimi: Örnek Algoritmik Süreç Akışı

Amaç: Kurumun belirlenen stratejik ve operasyonel performans göstergeleri üzerinden veriye dayalı analiz yapılması ve iç kontrol sisteminin bu analiz doğrultusunda yönlendirilmesi.

[1] Performans Göstergelerinin Tanımlanması

- Akademik (örn. yayın sayısı, mezuniyet oranı)
- İdari (örn. işlem süresi, bütçe kullanım oranı)
- Stratejik (örn. araştırma projeleri, dış fon çekme kapasitesi)

↓

[2] İlgili Verilerin Toplanması

- Akademik bilgi sistemi
- Stratejik plan izleme raporları
- Bütçe sistemleri
- Anketler (öğrenci, personel memnuniyeti)
- ERP/SAP entegrasyonu (varsa)

↓

[3] Veri Temizleme ve Standardizasyon

- Eksik, tutarsız ya da yanlış formatlanmış verilerin işlenmesi
- Tüm verilerin karşılaştırılabilir hâle getirilmesi

↓

[4] Zaman Serisi ve Benchmark Analizi (YZ Destekli)

- Her gösterge için yıllık/aylık deęişim trendi
- İ birimler arası ve benzer kurumlarla karşılaştırma
- “Outlier” analizleri (normalden sapan deęerler)



[5] Sapma Analizi ve Neden-Sonuç Modelleme

- Hedeflenen performans ile gerekleşen sonuçlar karşılaştırılır
- Makine öğrenmesi modelleri, sapmaya neden olan faktörleri analiz eder
- Örnek: Personel yetersizlięi → işlem süresinde gecikme



[6] Tahmine Dayalı Performans Simülasyonu

- “Eęer řu yapılırsa ne olur?” sorusuna yanıt veren modelleme
- Kaynak artışı, süreç sadeleştirme gibi senaryolar test edilir



[7] İ Kontrol Sistemine Otomatik Geri Bildirim

- Zayıf kontrol noktaları sistem tarafından işaretlenir
- Kontrol faaliyetlerinin yeterlilięi test edilir ve öneri sunulur



[8] Karar Destek Paneline Raporlama

- Renk kodlu gösterge panelleri (dashboard)
- Denetiye özel uyarı sistemi: “Yüksek Sapma – Müdahale Gerekli”

Uygulama Potansiyeli – Kamu Üniversiteleri İin:

Bölüm düzeyinde performans denetimi: Akademik çıktıların YZ ile analiz edilmesi (örneğin yayın-performans oranı, öğretim yükü dağılımı).

Destek hizmetlerinin verimlilik analizi: Öğrenci işleri, idari süreçler, kütüphane, BT hizmetleri gibi alanlarda işlem sürelerinin izlenmesi.

Proje yönetimi: Araştırma projelerinde büte gerekleşmeleri, zaman planlaması ve çıktı düzeyi analiz edilebilir.

İ kontrol geri beslemesi: Örneğin, sürekli sapma yaşanan göstergelere karşılık sistem, yeni kontrol noktası önerisinde bulunabilir.

6. ULUSLARARASI UYGULAMALAR VE BAŞARILI ÖRNEKLER

6.1. Avrupa Birliği Ülkelerinde Yapay Zekâ Destekli İç Denetim

Avrupa Birliği (AB), dijital dönüşüm politikalarını kamu yönetiminde şeffaflık, hesap verebilirlik ve etkililiği artırma hedefiyle bütünleştirmiştir. Bu bağlamda, **yapay zekâ destekli iç denetim sistemleri**, birçok AB üyesi ülkede hem merkezi yönetim hem de yerel/kamusal hizmet sunan kurumlar düzeyinde kullanılmaya başlanmıştır. AB'nin 2021-2027 Dijital Avrupa Programı (Digital Europe Programme) ve Avrupa Sayıştaylar Birliği (EUROSAI) çerçevesindeki işbirlikleri, iç denetimde YZ uygulamalarının geliştirilmesini kurumsal düzeyde desteklemektedir.

6.1.1. Hollanda: Tahmine Dayalı İç Denetim ve Anomali Algılama

Hollanda İçişleri ve Krallık İlişkileri Bakanlığı, kamu harcamalarının izlenmesinde yapay zekâ temelli denetim modelleri kullanmaktadır. Bu modeller, harcama verileri üzerinde sürekli çalışan **anomali tespit algoritmaları** ile olası yolsuzluk risklerini önceden belirleyerek iç denetçileri bilgilendirmektedir. Ayrıca, tahmine dayalı analizlerle, yıl sonu bütçe sapmaları önceden kestirilmekte ve iç kontrol sistemleri bu doğrultuda güncellenmektedir.

6.1.2. Estonya: Dijitalleşmiş İç Denetim Çerçevesi

Dijital devlet altyapısıyla öncü konumda bulunan **Estonya**, iç denetimi tamamen dijital platformlarla bütünleştirmiştir. Ulusal Denetim Ofisi (Riigikontroll), kamu kurumlarının performans ve uygunluk göstergelerini gerçek zamanlı izleyen bir **yapay zekâ destekli e-Denetim platformu** kullanmaktadır. Sistem, iç kontrol zafiyetlerini tespit ettiğinde otomatik uyarılar üretmekte, mevzuata uyumsuzlukları işaretlemektedir. Bu sistemin temel avantajı, denetimin sürekliliği ve dinamik öğrenme kapasitesidir.

6.1.3. Danimarka: İç Denetim Süreçlerinde Makine Öğrenmesi Uygulamaları

Danimarka Devlet Denetim Ofisi (Rigsrevisionen), kamuya ait sözleşmelerin, tedarik zinciri verilerinin ve ödeme sistemlerinin denetiminde **makine öğrenmesi algoritmalarını** kullanmaktadır. Bu sayede sahtecilik, çıkar çatışması, olağandışı ödeme akışları gibi durumlar erken aşamada tespit edilebilmektedir. Ayrıca sistem, geçmiş verilerden öğrenerek denetim planlarını sürekli optimize etmektedir.

6.1.4. Avrupa Komisyonu'nun Rehberliği ve Koordinasyonu

Avrupa Komisyonu, 2020'de yayımladığı "**Yapay Zekâ İçin Güvenli ve Etik Rehber**" (Ethics Guidelines for Trustworthy AI) ile kamu kurumlarında yapay zekâ kullanımına dair ilkeleri belirlemiş; bu doğrultuda iç denetim ve kamu finans yönetimi sistemlerine entegre YZ uygulamalarının **etik, denetlenebilir ve insan denetimiyle desteklenmiş** olması gerektiğini vurgulamıştır. Komisyon ayrıca, Horizon Europe kapsamında iç denetimde dijitalleşmeye yönelik projelere finansal destek sunmaktadır.

6.1.5. Stratejik Değerlendirme:

AB ülkelerindeki bu uygulamalar, iç denetimin veri odaklı, önleyici ve rehberlik edici rolünü güçlendiren örnekler sunmaktadır. Türkiye’de yükseköğretim kurumları özelinde düşünüldüğünde, bu modellerin pilot düzeyde uygulanabilirliği (örneğin döner sermaye işlemlerinde, performans göstergelerinde, mali disiplin kontrollerinde) son derece yüksektir. Özellikle YÖK ile Sayıştay iş birliğiyle geliştirilecek rehberler ve dijital denetim çerçeveleri, AB ile uyumlu ve ileri düzey bir iç denetim mimarisi oluşturulmasına katkı sağlayacaktır.

6.2. Amerika ve Asya’da Dijital İç Denetim Modelleri

Kamu yönetiminde yapay zekâ destekli iç denetim uygulamaları, Amerika ve Asya kıtasında özellikle veri yoğunluğu yüksek sektörlerde ve stratejik kamu hizmetlerinde yaygınlık kazanmıştır. Bu bölgelerde iç denetim, sadece kontrol ve tespit işleviyle sınırlı kalmayıp; risk odaklı, öngörücü ve karar destekleyici bir sistem olarak yeniden kurgulanmıştır. Aşağıda öne çıkan bazı ülke modelleri ve uygulama örnekleri sunulmaktadır.

6.2.1. Amerika Birleşik Devletleri: Entegre Dijital Denetim Ekosistemi

ABD’de iç denetim sistemleri, federal düzeyde **veri analitiği, tahmine dayalı modelleme ve algoritmik risk skorlaması** üzerine inşa edilmiştir. Öne çıkan uygulamalardan bazıları:

“Do Not Pay” (DNP) Platformu: Hazine Bakanlığı tarafından geliştirilen bu sistem, kamuya yapılan ödemeleri yapay zekâ ile tarayarak hatalı, mükerrer veya dolandırıcılığa açık işlemleri anında işaretlemektedir. İç denetim birimleri bu verilerle gerçek zamanlı risk analizleri yürütmektedir.

GAO’nun (Government Accountability Office) Veri Madenciliği Tabanlı Denetimleri: GAO, yapay zekâ ile desteklenen denetimlerde federal program harcamalarını analiz ederek verimsizlikleri ve yolsuzluk eğilimlerini erken aşamada ortaya koymaktadır.

Savunma Bakanlığı (DoD) Risk Değerlendirme Modeli: Harcama, tedarik ve insan kaynakları süreçlerinde milyonlarca veri noktasını analiz eden yapay zekâ algoritmaları sayesinde iç denetçiler hedefli denetimler yürütebilmektedir.

6.2.2. Japonya: Yüksek Otomasyon ve Sürekli Denetim

Japon kamu yönetiminde, iç denetim süreçleri yapay zekâ ve robotik süreç otomasyonu (RPA) ile entegre şekilde çalışmaktadır:

Eğitim ve Bilim Bakanlığı, üniversitelere yönelik denetimlerinde araştırma fonlarının kullanımını makine öğrenmesi ile izleyen sistemler kullanmaktadır. Bu sistemler, proje bütçelerinin öngörülen hedeflerle uyumunu denetleyerek uygunsuz harcama eğilimlerini tespit etmektedir.

Sürekli Denetim Yaklaşımı (Continuous Auditing): Yüksek hacimli kamu projelerinde, YZ tabanlı sistemler aracılığıyla her işlem gerçek zamanlı olarak denetlenmekte; sistem, iç kontrol noktalarında otomatik alarm üretmektedir. Bu yapı, denetimin sadece dönemsel değil sürekli bir süreç olarak işlemlerini sağlamaktadır.

6.2.3. Singapur: Akıllı Denetim Altyapısı (Smart Audit Infrastructure)

Singapur Sayıştay'ı (Auditor-General's Office) tarafından geliştirilen “**Smart Audit**” modeli, kamu kurumlarından gelen verileri merkezi bir veri ambarında toplayarak YZ algoritmalarıyla analiz etmektedir. Sistem;

- Yüksek riskli işlemleri işaretler,
- Performans sapmalarına dayalı erken uyarılar üretir,
- Kurumlara özel “denetim profili” oluşturarak hedefli denetim sağlar.

Ayrıca, denetim bulgularının sınıflandırılması ve önceliklendirilmesi de doğal dil işleme (NLP) teknolojileri ile otomatikleştirilmektedir.

6.2.4. Güney Kore: Kamu Bilişim Altyapısıyla Entegre Denetim

Güney Kore, e-Devlet uygulamalarındaki başarısını iç denetim sistemlerine de entegre etmiştir. Özellikle:

e-Audit Platformu, kamu kurumlarının işlem verilerini merkezi olarak toplayarak risk skorları oluşturmaktadır.

Kore Sayıştay Başkanlığı (Board of Audit and Inspection – BAI), yapay zekâ destekli denetim yazılımları ile çok sayıda kurumu aynı anda ve sürekli biçimde denetleyebilmektedir.

Ayrıca kamu üniversiteleri ve araştırma merkezlerine yönelik projelerde, harcama verileri yapay zekâ algoritmalarıyla anlık analiz edilmekte, sistem dışı işlemler için otomatik uyarı sistemi devreye girmektedir.

6.2.5. Genel Değerlendirme

Amerika ve Asya ülkeleri, yapay zekânın iç denetim süreçlerine entegrasyonunu büyük veri analizi, erken uyarı sistemleri, sürekli denetim ve öngörüye dayalı karar destek mekanizmaları üzerinden şekillendirmiştir. Bu ülkelerde iç denetim, yalnızca hata arayan bir süreç değil, **stratejik karar alma sürecinin bir girdisi** haline gelmiştir.

Türkiye’de yükseköğretim kurumları bu modellerden esinlenerek; araştırma fonlarının kullanımı, bütçe gerçekleştirmeleri, performans göstergeleri ve mevzuata uyum konularında **YZ tabanlı iç denetim modülleri** geliştirebilir. Bu gelişim, sadece denetim kapasitesini değil, aynı zamanda yönetim kalitesini de önemli ölçüde artıracaktır.

6.3. Türkiye’de Dijitalleşme ve Yapay Zekâ Uygulamaları

Türkiye’de kamu yönetiminde dijitalleşme süreci, son on yılda özellikle e-Devlet altyapısının güçlendirilmesi, kamu mali yönetimi bilgi sistemlerinin yaygınlaştırılması ve veri merkezli yönetim anlayışının benimsenmesiyle ivme kazanmıştır. Ancak bu gelişmelere rağmen iç denetim fonksiyonunun yapay zekâ destekli, proaktif ve bütünleşik bir yapıya evrilmesi henüz kurumsal düzeyde sistematik bir uygulama alanı bulamamıştır.

Yine de son yıllarda çeşitli kamu kurumlarında atılan adımlar, **iç denetimin dijital dönüşümüne zemin hazırlamakta ve yapay zekâ uygulamaları için uygun veri altyapısını oluşturmaktadır.**

6.3.1. Kamu Kurumlarında Veri Temelli Denetim Girişimleri

Sayıştay Başkanlığı,

Son dönemde yayımladığı denetim rehberlerinde **veri analitiğine dayalı denetim tekniklerinin** kullanımını teşvik etmektedir.

Özellikle büyük veri setlerinin anlamlandırılmasına yönelik yazılımlarla desteklenen denetimlerde; tekrar eden ödemeler, bütçe sapmaları ve usulsüzlük ihtimali taşıyan işlemler öncelikli olarak analiz edilmektedir.

Hazine ve Maliye Bakanlığı – Kamu İç Denetim Koordinasyon Kurulu (KİDKK),

2024-2026 İç Denetim Strateji Belgesi’nde;

- Bilgi teknolojileri (BT) denetimi gerçekleştirebilecek niteliğe sahip iç denetçilerin istihdam edilmesinin destekleneceği ve iç denetçi eğitimlerinde BT denetimi alanının ağırlığının arttırılacağı,
- Performans ve bilgi teknolojileri denetimleri konusunda kapasite geliştirici faaliyetlere yeterli denetim kaynağının ayrılmasının sağlanacağı,
- İç denetçilerin başta bilgi teknolojileri alanı olmak üzere ulusal/uluslararası geçerliliği olan sertifikaları almalarının destekleneceği,

vurgusu yapılmış ve iç denetçilerin dijital denetim yetkinliğini artıracak uygulamalara öncelik tanınmıştır.

TÜBİTAK ve Dijital Dönüşüm Ofisi

Öncülüğünde yürütülen bazı projelerde (örneğin: yapay zekâ destekli karar destek sistemleri, anomali tespiti için algoritmalar) denetim süreçlerine dolaylı katkı sunabilecek bileşenler geliştirilmektedir.

6.3.2. Yapay Zekâ Tabanlı Denetim Uygulamaları İçin Mevzuat ve Altyapı Hazırlıkları

Yapay Zekâ Stratejisi (2021-2025) kapsamında kamu sektöründe yapay zekâ uygulamalarının yaygınlaştırılması hedeflenmiş; bu bağlamda **denetim ve risk yönetimi uygulamaları** öncelikli alanlar arasında değerlendirilmiştir.

5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ile oluşturulan iç denetim çerçevesi, dijital ve yapay zekâ destekli araçların kullanımına engel teşkil etmemekte, aksine “risk odaklı denetim” anlayışına geçişi mümkün kılmaktadır.

Üniversiteler özelinde ise, **Yükseköğretim Kalite Kurulu (YÖKAK)** tarafından belirlenen kurumsal iç kalite güvencesi kriterleri, dijital veri analitiğine dayalı sürekli izleme ve iç değerlendirme sistemlerinin kurulmasını teşvik etmektedir.

6.3.3. Değerlendirme ve Gelişim Potansiyeli

Türkiye’de iç denetimin dijitalleşmesine yönelik güçlü bir altyapı ve stratejik yönelim bulunsa da, **yapay zekâ destekli denetim sistemlerinin kurumsal düzeyde yaygınlaşması için aşağıdaki adımlar gereklidir:**

- Veri yönetimi, iç kontrol ve denetim sistemleri arasında **teknolojik entegrasyonun** sağlanması,
- İç denetçilerin veri analitiği, algoritmik analiz ve dijital denetim araçları konusunda **yetkinleştirilmesi**,
- Kamu üniversitelerinde **pilot dijital iç denetim uygulamalarının** YÖK-Sayıştay-İDKK işbirliğiyle geliştirilmesi,
- Denetim bulgularının raporlanmasında **görselleştirme, tahmine dayalı analiz ve karar destek panellerinin** devreye alınması.

Sonuç olarak; Türkiye’de dijitalleşme süreci, iç denetim fonksiyonunun yeniden tanımlanması için büyük bir fırsat sunmaktadır. Kamu yükseköğretim kurumları bu dönüşümde öncü rol üstlenerek, yapay zekâ destekli denetim uygulamalarının etik, güvenilir ve etkili biçimde nasıl işleyeceğine dair **model oluşturan kurumlar** haline gelebilir. Bu doğrultuda, ileriye dönük olarak dijital denetim araçlarının **kurumsal yönetim sistemine entegre edilmesi**, sadece iç denetimin değil, yükseköğretimin bütünsel kalitesinin artırılmasına katkı sağlayacaktır.

7. GELECEĞE YÖNELİK TRENDLER VE İÇ DENETİMDE YAPAY ZEKÂ STRATEJİLERİ

7.1. Otonom Denetim Sistemleri ve Sürekli İzleme

Dijitalleşmenin ivme kazandığı günümüzde, iç denetim fonksiyonlarının manuel ve dönemsel yapısından uzaklaşarak, gerçek zamanlı ve otonom yapılandırılmış sistemlere yönelmesi, kurumların risk yönetimi ve iç kontrol etkinliğini artırmakta kritik rol oynamaktadır. Bu kapsamda, **otonom denetim sistemleri** ve **sürekli izleme (continuous monitoring)** mekanizmaları, iç denetimin geleceğini şekillendiren iki temel yapı taşı olarak öne çıkmaktadır.

7.1.1. Otonom Denetim Sistemleri (Autonomous Auditing Systems)

Otonom denetim sistemleri, denetim süreçlerinin insan müdahalesi olmaksızın, yapay zekâ ve makine öğrenmesi algoritmaları ile otomatik olarak yürütüldüğü sistemlerdir. Bu sistemler, büyük veri kümeleri üzerinde örüntü tanıma, sapma tespiti ve risk analizi gibi görevleri sürekli şekilde yerine getirebilmektedir.

Yapay Zekâ Tabanlı Denetim Motorları: Denetim evrenine giren verileri otomatik olarak analiz eden ve denetim kapsamına girmesi gereken anormal işlemleri belirleyen algoritmalar geliştirilmiştir.

Makine Öğrenmesi ile Gelişen Uyarılama Yeteneği: Sistem, geçmiş denetim bulgularından ve sonuçlarından öğrenerek kendini geliştirmekte, böylece denetim süreçleri zamanla daha hedefe yönelik ve etkili hâle gelmektedir.

Otonomluk Seviyeleri: Başlangıç seviyesinde veri toplama ve analiz süreçleri otomatikleşirken, ileri aşamada denetim planlaması, kanıt toplama ve hatta ön bulgu üretme işlemleri de otonom hâle gelmektedir.

Bu tür sistemler, özellikle yüksek işlem hacmine sahip kamu kurumlarında (örneğin vergi idareleri, sosyal güvenlik kurumları, büyük üniversite hastaneleri) denetim performansını artırmada büyük potansiyel taşımaktadır.

7.1.2. Sürekli İzleme (Continuous Monitoring) ve Risk Tabanlı Uyarı Sistemleri

Sürekli izleme, iç denetimin artık yalnızca belirli aralıklarla yapılan bir faaliyet olmaktan çıkıp, **kurumun bilgi sistemleriyle entegre bir şekilde 7/24 çalışan** bir yapı hâline gelmesini ifade eder. Bu sistemler sayesinde:

Kontrol Göstergeleri Anlık İzlenebilir: Önemli risk göstergeleri (KRI'lar) ve iç kontrol noktaları sürekli takip edilir.

Gerçek Zamanlı Uyarı ve Müdahale: Sistem, olağandışı bir işlem veya potansiyel suiistimal tespit ettiğinde iç denetim birimini anlık olarak uyarabilir.

Proaktif Denetim İmkânı: Riskler gerçekleşmeden önce tespit edilerek önleyici aksiyonlar alınabilir.

Bu sistemler, özellikle kamu sektöründe şeffaflık ve hesap verebilirlik ilkelerinin güçlendirilmesi bakımından önemlidir. Yükseköğretim kurumlarında da öğrenci işleri otomasyonları, bütçe harcamaları ve akademik performans verilerinin sürekli izlenmesi yoluyla risk temelli erken uyarı sistemleri oluşturulabilir.

7.1.3. Stratejik Öneriler ve Uygulama Perspektifi

Veri Entegrasyonu Altyapısının Kurulması: Otonom sistemlerin etkin çalışabilmesi için denetimle ilgili tüm veri kaynaklarının merkezi bir platformda toplanması gerekir.

İç Denetim Meslek Mensuplarının Dijital Yetkinliklerinin Artırılması: Yeni sistemlerin benimsenebilmesi için denetçilerin veri analitiği, yapay zekâ ve etik algoritmalar konusunda yetkinleştirilmesi şarttır.

Hibrit Denetim Modelleri: İnsan denetçilerin sezgisel ve bağlamsal değerlendirmeleri ile yapay zekânın sistematik analitik gücünün entegre edilmesi, en etkili sonuçları doğuracaktır.

Tablo 4. Otonom Denetim Sistemlerinin Gelişim Aşamaları

Aşama	Özellikler	Kullanılan Teknolojiler	İç Denetimde Uygulama Örnekleri
1. Otomasyon	Rutin işlerin yazılım ile yapılması	RPA (Robotik Süreç Otomasyonu)	Harcama belgelerinin sınıflandırılması
2. Akıllı Otomasyon	Kurallar ve eşiklere dayalı karar verme	Kural tabanlı sistemler	İhale dosyalarının ön kontrolü
3. Yarı-Otonom Sistem	Veriye dayalı önerilerde bulunma	Makine öğrenmesi, veri madenciliği	Riskli işlemlerin işaretlenmesi
4. Tam Otonom Sistem	Denetim sürecini baştan sona kendisi yürütme	NLP, Derin öğrenme, AI motorları	Anlık sahtecilik tespiti, öngörüsül denetim

Tablo 5. Sürekli İzleme Sistemlerinin Faydaları ve Örnek Kullanım Alanları

Faydalar	Açıklama	Uygulama (Kamu/Üniversite) Örneği
Gerçek zamanlı risk tespiti	Anlık veri analizi ile potansiyel risklerin belirlenmesi	Öğrenci kayıt sisteminde usulsüz kredi işlemi tespiti
Süreç performansı ölçümü	İç kontrol noktalarının etkinliğinin sürekli ölçülmesi	Harcama sürecinde işlem gecikmelerinin takibi
Erken uyarı mekanizması	Olası suiistimaller için ön sinyallerin izlenmesi	Akademik atamalarda olağan dışı puanlamaların uyarılması
Hesap verebilirliği artırma	Şeffaflığı ve raporlanabilirliği güçlendirme	BAP (Bilimsel Araştırma Projesi) ödeneklerinin izlenmesi

Tablo 6. İç Denetimde Yapay Zekâ ile Geleneksel Yaklaşımların Karşılaştırılması

Kriter	Geleneksel İç Denetim	Yapay Zekâ Destekli İç Denetim
Zamanlama	Dönemsel (yıllık planlara bağlı)	Anlık / Gerçek zamanlı
Kapsam	Örnekleme	Tüm veri evreni
Hata Tespiti	Geriye dönük	Anında / Tahmine dayalı
Müdahale Süresi	Gecikmeli	Anında
Maliyet	Yüksek (insan gücüne dayalı)	Uzun vadede düşük
İnsan Faktörü	Denetçi yorumuna dayalı	Algoritmik analiz + denetçi onayı

7.2. Yapay Zekâ ile Entegre İç Denetim Çözümleri

Günümüzde iç denetim fonksiyonları, yalnızca kontrol mekanizmalarının değerlendirilmesiyle sınırlı kalmayıp, kurumsal yönetimi, risk yönetimini ve stratejik karar alma süreçlerini destekleyen bir yapıya dönüşmektedir. Bu dönüşümün itici gücü ise, yapay zekâ (YZ) ile entegre edilmiş iç denetim çözümleridir. Söz konusu çözümler, iç denetimin **veriye dayalı, sürekli, öngörülü ve yüksek doğrulukla çalışan** bir sistem haline gelmesini mümkün kılmaktadır.

7.2.1. Entegre Denetim Platformları ve Modüler Yapay Zekâ Çözümleri

Yapay zekâ ile entegre iç denetim uygulamaları genellikle merkezi bir denetim platformu altında toplanan ve farklı teknolojik modüllerden oluşan sistemlerdir. Bu sistemler:

- **Veri analitiği ve görselleştirme modülleri** (özellikle büyük veri kümelerinde örüntü tespiti),

- **Makine öğrenmesi ile anomali tespit sistemleri** (önceki işlemlerden öğrenerek normal dışı işlemleri belirleme),
- **NLP (Doğal Dil İşleme) destekli belge analizi** (sözleşmeler, yönetmelikler, satın alma dosyalarının otomatik değerlendirilmesi),
- **Tahmine dayalı risk analiz motorları** (gelecekteki olası risk alanlarını belirleyen algoritmalar),

şeklinde işlevsel bileşenlere sahiptir.

Bu yapı sayesinde iç denetim, sadece geçmişin denetimi değil aynı zamanda **geleceğin risklerine hazırlık** işlevi kazanır.

7.2.2. Kurum Sistemleriyle Uyumlu Entegrasyon

YZ ile entegre çözümler yalnızca iç denetim birimine özel değil; **muhasabe, insan kaynakları, satın alma, öğrenci işleri, akademik bilgi sistemleri gibi kurumsal veri kaynaklarıyla senkronize** çalışır. Böylece:

- Tüm kurumsal süreçler bütünsel olarak izlenebilir,
- Kurum içi veri silo problemi¹³ aşılar,
- Farklı sistemlerde meydana gelen çapraz riskler daha kolay tespit edilir.

Örneğin, bir üniversitede araştırma projeleri bütçesi ile fatura girişleri arasında yapay zekâ destekli tutarsızlık tespiti yapılabilir.

7.2.3. Akıllı Denetim Planlaması ve Kaynak Tahsisi

YZ tabanlı sistemler, kurumsal risk haritalarını analiz ederek hangi birim veya süreçlerin **yüksek risk taşıdığını öngörebilir**. Bu veriler doğrultusunda:

- **Dinamik denetim planları** hazırlanabilir,
- Denetim ekiplerinin daha etkili ve öncelikli alanlara yönlendirilmesi sağlanabilir,
- Denetim kaynakları optimize edilerek zaman ve insan gücü verimliliği artırılabilir.

Bu yaklaşım, özellikle kamu kaynaklarının etkin kullanımı açısından stratejik önem taşır.

7.2.4. Karar Destek ve Otomatik Raporlama

YZ sistemleri, elde edilen bulgulara ilişkin:

- Denetim sonuçlarının özetlenmesi,
- Politika önerileri üretilmesi,
- Yöneticilere özgü karar destek raporlarının hazırlanması,

gibi işlevleri otomatik olarak gerçekleştirebilir.

¹³ Bir kuruluş içindeki farklı departmanlar veya bölümler veri sistemlerini bağımsız olarak tedarik edip yönettiklerinde, genellikle veri siloları oluşturur. Bunlar, kendilerini oluşturan iş birimi için yararlı olan ancak tuttukları verilerden yararlanabilecek diğer ekipler için erişilemez olan bilgi havuzlarıdır.

Bu sayede iç denetim raporları yalnızca tespitlere değil, aynı zamanda **karar alıcılar için öngörü ve çözüm önerilerine** dayalı bir yapıya dönüşmektedir.

7.2.5. Güvenlik, Etik ve Yapay Zekâ Yönetimi

YZ ile entegre çözümler geliştirilirken dikkate alınması gereken önemli bir unsur da **veri gizliliği, algoritmik şeffaflık ve etik denetim ilkeleridir**. Kurumlar, bu sistemleri devreye alırken:

- YZ kararlarının nasıl alındığını izleyebilir şekilde dokümanete etmeli,
- Olası algoritmik önyargılara karşı bağımsız denetim mekanizmaları kurmalı,
- Denetim süreçlerinde insan denetçilerin nihai kararda yer aldığı **hibrit modeller** oluşturmalıdır.

SWOT Analizi: Yapay Zekâ ile Entegre İç Denetim Çözümleri

Güçlü Yönler (Strengths)	Zayıf Yönler (Weaknesses)
Büyük veri analiziyle yüksek doğrulukta tespit kapasitesi	Kurum içi yapay zekâ okuryazarlığının sınırlı olması
Sürekli izleme ve gerçek zamanlı risk farkındalığı	Veri kalitesi ve bütünlüğü sorunları sistem etkinliğini düşürebilir
Kurum genelinde sistemler arası entegrasyon ve çapraz kontrol	Yapay zekâ kararlarının açıklanabilirliği (transparanlık) sınırlı olabilir
Denetim planlamasında otomasyon ve kaynak optimizasyonu	Uyarılma ve entegrasyon maliyetleri başlangıçta yüksek olabilir
Tahmine dayalı analizlerle önleyici denetim imkânı	Yapay zekâyâ aşırı güven, insan denetçinin rolünü zayıflatabilir

Fırsatlar (Opportunities)	Tehditler (Threats)
Dijital dönüşüm stratejileriyle uyumlu ulusal politikaların varlığı (e-Devlet, Dijital Türkiye, Yapay Zekâ Stratejisi 2021–2025)	Siber güvenlik riskleri ve veri mahremiyetine ilişkin açıklar
Yükseköğretim ve kamu sektöründe artan veri hacmi ve çeşitliliği	Algoritmik önyargılar ve etik dışı YZ kararlarının denetim sonuçlarını etkilemesi
Kamu-özel iş birliğiyle geliştirilebilecek yerli denetim yazılımları	Yasal ve düzenleyici çerçevenin yapay zekâ uygulamalarına tam uyumlu olmaması
YZ destekli karar destek sistemleriyle yönetsel etki gücünün artması	Denetim bulgularının otomasyonuna karşı iç direnç (kurum içi adaptasyon sorunu)

Uluslararası iyi uygulamalar ve fon destekli dönüşüm projeleri (OECD, EU, Dünya Bankası vb.)	Denetim algoritmalarının dış kaynaklı olması durumunda bağımsızlık riskleri
--	---

Yorum ve Stratejik Öneri:

Bu SWOT tablosu ışığında, kamu kurumları ve yükseköğretim yapıları için:

- YZ sistemlerinin uyarlanabilirliğini artıracak pilot uygulamalar başlatılması,
- Denetçiler için veri ve YZ okuryazarlığına yönelik eğitim programlarının oluşturulması,
- Etik yapay zekâ denetim çerçevesinin geliştirilmesi,
- Ulusal düzeyde yerli YZ destekli denetim yazılım platformlarının desteklenmesi,

gibi adımlar bu entegrasyonun sürdürülebilir ve denetim etiğine uygun biçimde gerçekleştirilmesini sağlayacaktır.

7.3. İnsan-Makine İş Birliği ve Yetkinlik Gelişimi

Dijitalleşme ve yapay zekâ teknolojilerinin iç denetim alanına entegrasyonu, denetim süreçlerinin otomasyonunu ve analitik derinliğini artırmakla kalmamış; aynı zamanda iç denetçilerin rollerini ve gerekli yetkinlik setlerini köklü biçimde dönüştürmüştür. Bu dönüşüm, klasik “insan merkezli denetim” yaklaşımının yerine, **insan-makine iş birliğine dayalı hibrit bir denetim modelini** getirmektedir. Bu modelde, yapay zekâ sistemleri operasyonel ve analitik işlevleri üstlenirken, denetçilerin uzmanlığı; değerlendirme, etik karar alma, yorumlama ve iletişim becerilerine odaklanmaktadır.

7.3.1. Hibrit Denetim Ekosistemi: İnsan ve Yapay Zekâ Arasındaki Rol Dağılımı

İç denetimin geleceğinde, insan-makine iş birliğine dayalı yeni bir iş bölümü ortaya çıkmaktadır:

Görev Türü	İnsan Denetçi	Yapay Zekâ
Stratejik denetim planlaması	☑	○
Büyük veri analizi ve örüntü tanıma	○	☑
Anomali tespiti ve ön bulgu üretimi	○	☑
Bulguların yorumlanması ve raporlaştırılması	☑	○
Etik değerlendirme ve yönetime öneri sunma	☑	○

Bu iş bölümünde, yapay zekâ “yardımcı denetçi” rolüyle süreci hızlandırırken, nihai yargı ve yönetsel tavsiyeler insan denetçinin sorumluluğunda kalmaktadır.

7.3.2. Yeni Nesil Yetkinlik Alanları

Yapay zekâ ile entegre denetim süreçlerinde iç denetçilerin sahip olması gereken yetkinlik seti genişlemekte ve çeşitlenmektedir. **Geleneksel denetim bilgi ve becerilerine ek olarak aşağıdaki alanlarda yetkinlik gelişimi kaçınılmazdır:**

- Veri analitiği ve temel istatistik bilgisi
- Makine öğrenmesi ve algoritma mantığına aşinalık
- İş zekâsı (Business Intelligence) araçlarını kullanabilme (Power BI¹⁴, Tableau¹⁵ vb.)
- Veri güvenliği ve mahremiyet farkındalığı
- Etik yapay zekâ değerlendirmesi ve dijital sorumluluk
- İnsan-makine etkileşim psikolojisi ve teknoloji adaptasyonu

Bu yetkinlikler iç denetçiyi yalnızca bir "uygulayıcı" değil, aynı zamanda **teknolojiyle entegre çalışan stratejik bir aktör** hâline getirmektedir.

7.3.3. Kamu ve Üniversite Denetim Birimlerine Özgü Eğitim ve Dönüşüm Stratejileri

Yükseköğretim kurumları ve kamu idarelerinde insan-makine iş birliğine geçiş süreci, sistematik bir değişim yönetimi ve kapasite geliştirme planı gerektirir. Bu bağlamda önerilen stratejiler şunlardır:

İç denetçiler için dijital beceri geliştirme programları düzenlenmeli (YZ, veri analitiği, yapay zekâ okuryazarlığı).

Denetim ekiplerinde teknik danışman pozisyonları (veri bilimci, sistem analisti) ihdas edilmeli.

Mentor destekli geçiş modelleri uygulanmalı (tecrübeli denetçiler ile teknoloji uzmanları eşleştirilmeli).

Kurumsal dijital olgunluk düzeyine göre aşamalı uyum planları hazırlanmalı.

7.3.4. Etik, Güven ve İnsan Odaklılık

İnsan-makine iş birliğinde **güven** en kritik unsurdur. Yapay zekâ destekli kararların kabul görmesi, bu sistemlerin şeffaflık, izlenebilirlik ve insan denetçinin sürece müdahale hakkı çerçevesinde işlemesine bağlıdır. Bu nedenle:

- YZ sistemlerinin denetlenebilirliği güvence altına alınmalı,
- Karar alma süreçlerinde **“insan merkezli kontrol noktaları”** korunmalı,
- İnsan denetçilerin “teknolojik edilgen” değil, **aktif stratejik ortak** olarak konumlanması sağlanmalıdır.

İç denetim, teknolojik gelişmelerle sadece dijitalleşen değil, aynı zamanda insan faktörünün niteliğini dönüştüren bir meslek hâline gelmektedir. Bu dönüşümün başarılı olması, **insan-makine sinerjisini dengeleyen, etik temelli ve yetkinlik odaklı bir değişim yönetimi stratejisine** bağlıdır.

¹⁴ Microsoft Power BI, işletmeler ve profesyoneller tarafından her gün kullanılan bir veri görselleştirme ve raporlama platformudur. Platform genellikle iş analistleri tarafından kullanılsa da, herhangi bir özel veri bilgisi olmayanlar için de kolayca erişilebilir olacak şekilde tasarlanmıştır.

¹⁵ Tableau, etkileşimli grafikler, raporlar ve panolar oluşturarak veri odaklı seçimler yapmanıza olanak tanıyan popüler bir İş Zekâsı çözümüdür. Tableau'nun kapsamlı Şablon ve Widget seti, Tableau çalışma alanına aktarılan veri kümelerini kolayca analiz etmenizi ve görselleştirmenizi sağlar.

1. Yetkinlik Haritası: Yapay Zekâ Destekli İç Denetimde Geliştirilmesi Gereken Yetkinlik Alanları

Yetkinlik Kategorisi	Spesifik Yetkinlikler ve Açıklamalar	Gelişim Düzeyi	Önerilen Eğitim ve Kaynaklar
Temel Dijital Okuryazarlık	Bilgi sistemleri, veri güvenliği, yazılım okuryazarlığı	Orta – Zorunlu	E-Devlet, e-imza, veri erişimi eğitimleri
Veri Analitiği Yetkinliği	Veri temizleme, analiz, görselleştirme (Excel PowerQuery, Power BI, Tableau)	Başlangıç – Orta	İç denetçilere özel veri analizi atölyeleri
Yapay Zekâ Farkındalığı	Algoritma mantığı, makine öğrenmesi nedir, nasıl çalışır	Temel	YZ okuryazarlığı seminerleri, MOOC (Coursera, Enocta)
İleri Düzey Denetim Bilgisi	Risk odaklılık, iç kontrol sistemleri, bulgu oluşturma	İleri – Uzmanlık	Sayıştay, COSO ve INTOSAI ¹⁶ rehberleri
Yorumlama ve Eleştirel Düşünme	YZ çıktılarının bağlamsal analizi ve denetim bulgularına dönüştürülmesi	İleri	Vaka analizleri, stratejik denetim eğitimi
Etik ve Sorumlu Teknoloji Kullanımı	YZ etiği, veri mahremiyeti, algoritmik önyargı farkındalığı	Temel – Orta	Kamu Etik Kurulu ve OECD kaynakları
İletişim ve İş Birliği	Teknik personelle iletişim, raporlaştırma, yönetime öneri sunma	İleri	Denetim raporu yazım eğitimi, liderlik seminerleri

Not: Bu harita, kamu kurumlarının iç denetim birimleri için iç eğitim planı veya meslek içi gelişim programı temeli olarak kullanılabilir.

2. Hibrit Denetim Roller Matrisi: İnsan ve Yapay Zekâ İş Bölümü

Denetim Faaliyeti	İnsan Denetçi Rolü	YZ/Algoritma Rolü	Açıklama
Denetim Planlaması	Stratejik öncelikleri belirler	Geçmiş verilerden risk analiz önerisi sunar	İnsan denetçi karar vericidir
Veri Toplama ve Hazırlık	Süreçleri tanımlar, anlamlandırır	Otomatik veri toplar, temizler, sınıflandırır	Zaman tasarrufu sağlar

¹⁶ Uluslararası Yüksek Denetim Kurumları Teşkilatı

Anomali ve Risk Tespiti	Bulguları değerlendirir, bağlamsal analiz yapar	İşlem örüntüsü, eşik dışı hareketleri tespit eder	YZ destekli risk işaretleme
İç Kontrol Değerlendirmesi	Kontrol ortamını yorumlar	Standartlara göre kontrolleri tarar	Kriter bazlı analiz
Kanıt Toplama ve Belgelendirme	Fiziki ve bağlamsal kanıt toplar	Sistemsal delilleri otomatik loglar	Çift kaynaklı belgeleme
Raporlama ve Öneri Geliştirme	Yönetim diliyle öneri sunar	Taslak bulgu özetleri üretir	YZ öneri sunmaz, veri sağlar
Etik ve Yargısal Değerlendirme	Nihai kararı verir	Süreci destekler	YZ etik karar alamaz
Eğilim ve Risk Tahmini (Predictive)	Bulgularla stratejik yönlendirme yapar	Risk skorları ve senaryo üretir	Geleceğe dair içgörü sağlar

Kritik Nokta: İnsan denetçi her zaman nihai otorite ve karar verici pozisyonunda kalmalı; YZ ise **analitik ortak** olarak destekleyici rolde çalışmalıdır.

7.4. Politika ve Strateji Önerileri

Yapay zekâ (YZ) teknolojilerinin iç denetim süreçlerine entegrasyonu sadece teknik bir dönüşüm değil, aynı zamanda yönetim, etik, mevzuat ve kurumsal kapasite açısından çok katmanlı bir dönüşüm sürecidir. Bu süreçte kamu idareleri ve yükseköğretim kurumları düzeyinde başarılı bir dijital dönüşüm için, **ulusal politikalarla uyumlu, veri odaklı ve insan merkezli** stratejiler geliştirilmesi gerekmektedir.

7.4.1. Ulusal Ölçekte Politikalar ve Mevzuat Uyumlaştırması

Ulusal Dijitalleşme ve Yapay Zekâ Stratejilerine Entegrasyon: İç denetim fonksiyonlarının, Türkiye Ulusal Yapay Zekâ Stratejisi (2021–2025)¹⁷, Dijital Türkiye Platformu¹⁸ ve e-Devlet projeleriyle entegre olacak biçimde yeniden yapılandırılması önerilmektedir.

Etik Yapay Zekâ Rehberliği ve Denetim Standardı Oluşturulması: Kamu kurumlarında iç denetimde kullanılacak YZ destekli algoritmaların şeffaf, izlenebilir ve tarafsız olması için **etik ilkeler seti** ve **uluslararası uyumlu standartlar** belirlenmelidir (örneğin: OECD YZ İlkeleri¹⁹, INTOSAI YZ Kılavuzları).

¹⁷ <https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf>

¹⁸ <https://dijitalturkiyeplatformu.org/>

¹⁹ 22 Mayıs 2019 tarihinde Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) tarafından benimsenen ve dünyada ilk kez hükümetler arası bir kuruluş tarafından onaylanan **uluslararası yapay zekâ ilkeleridir**. Bu ilkeler, yapay zekânın güvenli, adil, şeffaf ve insan merkezli bir şekilde geliştirilmesi ve uygulanmasını teşvik etmeyi amaçlar.

Denetim Mevzuatının Güncellenmesi: 5018 sayılı Kanun, iç denetim yönetmelikleri ve ilgili usul esaslara YZ destekli denetim araçlarının kullanımına açıklık getiren hükümlerin eklenmesi önerilir.

7.4.2. Kurumsal Düzeyde Uygulanabilir Stratejiler

a. Veri Yönetimi ve Altyapı Geliştirme

Denetim Odaklı Veri Mimarisinin Oluşturulması: Kurumsal verilerin YZ sistemlerinde anlamlı analizlere konu olabilmesi için bütüncül, güncel, erişilebilir ve temiz bir **veri yönetim stratejisi** oluşturulmalıdır.

Denetim Bilgi Sistemleri Entegrasyonu: İç denetim birimlerinin kullandığı araçların, ERP, e-Bütçe, e-Taşınır, KBS, Üniversite Bilgi Yönetim Sistemleri gibi platformlarla **çift yönlü veri akışına** uygun hale getirilmesi gerekir.

b. İnsan Kaynağı ve Yetkinlik Dönüşümü

Yeni Nesil Denetçi Profili Geliştirme: Veri analitiği, yapay zekâ okuryazarlığı ve dijital etik konularında yetkinliğe sahip hibrit denetçiler yetiştirilmeli, mevcut denetçilere bu alanlarda eğitim verilmelidir.

Çok Disiplinli Denetim Ekipleri: İç denetim birimleri, veri bilimcisi, algoritma uzmanı ve denetçiden oluşan **çok disiplinli takımlar** ile güçlendirilmelidir.

c. Pilot Projeler ve Kademeli Uygulama Modeli

Kamu Kurumlarında Pilot Denetim Uygulamaları: Mali işlemlerin, satın alma süreçlerinin, taşınır işlemlerinin veya burs ödemelerinin yapay zekâ destekli denetimi için **pilot projeler** hayata geçirilmelidir.

Kademeli Geçiş Stratejisi: Kurumlar, dijital olgunluk seviyesine göre 3 aşamalı bir geçiş modeli benimsemelidir:

- **Aşama 1:** Veri temelli geleneksel denetim
- **Aşama 2:** Yarı otonom YZ destekli denetim
- **Aşama 3:** Sürekli izleme ve tahmine dayalı denetim

d. Güvenlik ve Etik Çerçeve

Algoritmik Etik Kurullarının Oluşturulması: YZ sistemlerinin denetim kararlarını nasıl etkilediği izlenmeli ve kurum içi “algoritmik karar denetim kurulları” teşkil edilmelidir.

Siber Güvenlik Önceliği: YZ tabanlı denetim sistemleri yüksek düzeyde veri erişimi içerdiğinden, güçlü güvenlik protokolleri, log takibi ve kimlik doğrulama sistemleri kullanılmalıdır.

Stratejik Vizyon: YZ ile Dönüşen Denetim Ekosistemi

İç denetimin geleceği, teknolojik yeteneklerin kurumsal etikle, stratejik denetim vizyonunun insan-makine iş birliğiyle bütünleştirildiği bir “**akıllı denetim ekosistemi**” inşa edilmesine bağlıdır.

Bu bağlamda önerilen stratejiler, Türkiye’de hem iç denetim mesleğinin itibarını artıracak hem de kurumsal yönetim yapılarının dijital çağın gereklerine uygun şekilde evrilmesini sağlayacaktır.

8. DEĞERLENDİRME VE SONUÇ

8.1. Dijitalleşmenin İç Denetimdeki Dönüştürücü Etkisi

Günümüzün hızla dijitalleşen dünyasında, iç denetim fonksiyonları da teknolojik gelişmelerin etkisiyle köklü bir dönüşüm yaşamaktadır. Dijitalleşme, iç denetimin metodolojisini, araçlarını ve çalışma biçimini yeniden şekillendirerek, daha etkin, şeffaf ve dinamik bir denetim süreci oluşturulmasına olanak tanımaktadır.

İç denetimde dijitalleşmenin dönüştürücü etkileri başlıca şu şekildedir:

- **Süreçlerin Otomasyonu ve Verimlilik Artışı:** Rutin ve zaman alan görevlerin yapay zekâ destekli otomasyonlarla gerçekleştirilmesi, denetçilerin daha stratejik ve analitik görevlere odaklanmasını sağlar. Böylece iç denetim süreçlerinde hız, doğruluk ve verimlilik artar.

- **Veri Odaklı ve Sürekli Denetim Yaklaşımı:** Dijitalleşme, büyük veri analitiği ve gerçek zamanlı izleme teknolojilerinin iç denetim faaliyetlerine entegre edilmesini mümkün kılar. Bu sayede denetimler sadece dönemsel kontroller olmaktan çıkarak, sürekli izlemeye ve proaktif risk yönetimine dönüşür.

- **Gelişmiş Risk Tespiti ve Analizi:** Yapay zekâ algoritmaları, karmaşık veri setlerinde anormallikleri, trendleri ve potansiyel riskleri hızlıca tespit ederek, denetim odaklarının daha isabetli belirlenmesini sağlar. Bu da risk odaklı denetim anlayışını güçlendirir.

- **Şeffaflık ve Hesap Verebilirlik:** Dijital araçlar, denetim bulgularının belgelenmesini, raporlanmasını ve takip edilmesini kolaylaştırır. Bu da hem iç hem dış paydaşlar nezdinde şeffaflığı artırır ve hesap verebilirlik mekanizmalarının etkinleşmesini sağlar.

- **İnsan-Makine İş Birliği:** Dijitalleşme, denetçilerin yapay zekâ ile iş birliği içinde çalışmasına olanak verir. Bu hibrit model, denetimin kalitesini yükseltirken etik ve profesyonel standartların korunmasını da temin eder.

- **Kültürel ve Yetkinlik Dönüşümü:** Dijitalleşme, iç denetim profesyonellerinden yeni yetkinlikler ve dijital okuryazarlık talep eder. Bu durum, sürekli eğitim, adaptasyon ve değişime açıklık kültürünü zorunlu kılar.

Sonuç olarak, dijitalleşme iç denetimde sadece teknolojik bir yenilik değil, aynı zamanda süreçlerin, insan kaynağının ve organizasyon kültürünün bütünsel olarak dönüşümüdür. Bu dönüşüm, iç denetimin kurumsal yönetim ve risk yönetimindeki stratejik rolünü güçlendirirken, kamu kaynaklarının etkin kullanımı ve hesap verebilirliğin sağlanmasında yeni fırsatlar yaratmaktadır.

Tablo 7. Dijitalleşmenin İç Denetime Etkileri ve Sağladığı Katma Değer

Dönüştürücü Etki	Açıklama	İç Denetime Katkısı
Süreç Otomasyonu	Rutin işleri yapay zekâ ile otomatikleştirme	Zaman tasarrufu, hata azalma, hız artışı
Sürekli Denetim	Gerçek zamanlı veri analizi ve izleme	Risklerin proaktif tespiti, kesintisiz kontrol

Gelişmiş Risk Tespiti	Büyük veri ve yapay zekâ algoritmalarıyla anormallik tespiti	Risk odaklı denetim, önceliklendirme
Şeffaflık ve Hesap Verebilirlik	Dijital dokümantasyon ve raporlama	İzlenebilirlik, paydaş güveni
İnsan-Makine İş Birliği	Denetçi ve yapay zekânın birlikte çalışması	Denetim kalitesinde artış, etik denetim sağlama
Yetkinlik ve Kültür Dönüşümü	Dijital yetkinlik gelişimi ve adaptasyon kültürü	Sürekli eğitim, yeniliklere açıklık

Tablo 8. Dijitalleşme Öncesi ve Sonrası İç Denetim Faaliyetinin Karşılaştırılması

Kriter	Dijitalleşme Öncesi	Dijitalleşme Sonrası
Denetim Süresi	Uzun ve yoğun manuel çalışma	Kısalan, otomatik ve hızlanan süreçler
Veri Analizi	Sınırlı, örneklem bazlı	Kapsamlı, gerçek zamanlı ve sürekli
Risk Tespiti	Geçmişe yönelik, dönemsel	Proaktif, tahmine dayalı
Raporlama	Manuel, statik raporlar	Otomatik, dinamik ve interaktif
Denetçi Rolü	Sadece karar verici	İnsan-makine iş birliğiyle karar destekçisi
İzlenebilirlik	Sınırlı denetim izi	Tam dijital kayıt ve takip

Tablo 9. Dijitalleşmenin İç Denetimin Boyutlarında Sağladığı Dönüşüm

Boyut	Değişim Öncesi Durum	Dijitalleşme Sonrası Durum	Katma Değer / Fırsatlar
Teknoloji Kullanımı	Geleneksel yöntemler	Yapay zekâ, büyük veri, otomasyon	Verimlilik, hız, kapsam artışı
İnsan Kaynağı	Sınırlı dijital beceri	Hibrit yetkinlikler, dijital eğitim	Yetkinlik gelişimi, yeni iş tanımları
Süreç Yönetimi	Periyodik denetimler	Sürekli denetim ve izleme	Risk odaklılık, anlık müdahale
Raporlama ve İletişim	Statik ve sınırlı paydaş	Dinamik, interaktif, çok kanallı	Şeffaflık, daha iyi karar alma
Etik ve Güvenlik	Geleneksel denetim protokolleri	Algoritmik etik ve veri güvenliği	Hesap verebilirlik, güven artırma

8.2. Yapay Zekâ Kullanımının Sürdürülebilirliği ve Gelecek Perspektifi

Yapay zekâ (YZ) teknolojilerinin iç denetimde etkin kullanımı, kurumların sadece bugünkü ihtiyaçlarına cevap vermekle kalmayıp, uzun vadede sürdürülebilirlik hedeflerine ulaşmalarına da katkı sağlamaktadır. Ancak YZ uygulamalarının sürdürülebilirliği, teknolojik yeniliklerin hızına uyum sağlamanın yanı sıra, kurumsal yapıların, insan kaynağının ve etik standartların da eşzamanlı gelişimine bağlıdır.

Sürdürülebilirlik İçin Temel Unsurlar

- **Sürekli İnovasyon ve Teknoloji Takibi:**

YZ teknolojilerindeki hızlı değişim ve gelişmeler, iç denetim birimlerinin bu yenilikleri takip ederek sistemlerini güncel tutmasını zorunlu kılar. Ar-Ge yatırımları, pilot uygulamalar ve iş birlikleri sürdürülebilirlik için temel teşkil eder.

- **İnsan ve Yetkinlik Gelişimi:**

YZ destekli iç denetimin kalıcı başarısı, denetçilerin dijital okuryazarlık ve yapay zekâ alanında sürekli eğitimlerle donatılmasına bağlıdır. Bu süreçte, insan-makine iş birliği yetkinliklerinin geliştirilmesi, mesleki gelişimin ayrılmaz bir parçası haline gelmelidir.

- **Etik ve Hukuki Çerçeve:**

Sürdürülebilir YZ kullanımı, etik standartların ve hukuki düzenlemelerin sağlandığı bir ortamda mümkündür. Veri güvenliği, algoritmik şeffaflık ve hesap verebilirlik ilkelerinin kurumsal kültüre yerleştirilmesi, teknolojinin toplum nezdindeki meşruiyetini artırır.

- **Kurumsal Entegrasyon ve Yönetim Desteği:**

YZ uygulamalarının sürdürülebilirliği için üst yönetimin vizyonu ve desteği kritik öneme sahiptir. Kurumsal stratejilerle uyumlu, kaynak planlaması ve performans izleme mekanizmaları içeren entegre yaklaşımlar gereklidir.

Gelecek Perspektifi

- **Tahmine Dayalı ve Proaktif Denetim:**

YZ'nin gelişimiyle birlikte, denetim sistemleri sadece geçmişe dönük kontroller yapmakla kalmayacak, gelecekte ortaya çıkabilecek riskleri önceden tespit eden, proaktif ve öngörüsül denetim modelleri geliştirilecektir.

- **Otonom Denetim Sistemleri:**

İnsan denetçilerin rolünü destekleyen, ancak belirli süreçlerde kendi kendine karar verebilen otonom denetim mekanizmaları yaygınlaşacaktır. Bu sistemler, sürekli izleme ve anlık müdahale kapasitesine sahip olacaktır.

- **Veri Ekosistemi ve Çok Kaynaklı Analiz:**

İç denetim süreçleri, farklı veri kaynaklarının (kurumsal veriler, sosyal medya, açık veri vb.) entegre edilmesiyle daha zengin ve kapsamlı analizlere imkân tanıyacak, böylece denetim kalitesi artacaktır.

- **Yapay Zekâ ve İnsan Etkileşiminin Evrimi:**

İnsan ile yapay zekâ arasındaki iş birliği, etik ve karar alma süreçlerinde yeni standartlara ulaşacak, denetçilerin rolü daha çok denetim stratejisi belirleme, etik denetim ve kompleks problem çözme üzerine yoğunlaşacaktır.

- **Uluslararası Standartlaşma ve İş Birliği:**

YZ destekli iç denetimde uluslararası standartlar ve karşılıklı bilgi paylaşımı artacak, bu durum hem kaliteyi yükseltecek hem de küresel uyumu güçlendirecektir.

Sonuç olarak, yapay zekâ kullanımının iç denetimde sürdürülebilirliği, teknolojik altyapı, insan kaynağı, etik-hukuki düzenlemeler ve kurumsal stratejilerin uyum içinde ilerlemesine bağlıdır. Bu alanlarda sağlanacak sinerji, yükseköğretim ve kamu sektöründe iç denetim uygulamalarının gelecekte de etkin ve güvenilir kalmasını garanti edecektir.

SWOT Analizi: Yapay Zekâ Kullanımının Sürdürülebilirliği ve Gelecek Perspektifi

Güçlü Yönler (Strengths)	Zayıf Yönler (Weaknesses)
- Artan denetim verimliliği ve hız	- İnsan kaynağında dijital yetkinlik eksiklikleri
- Proaktif ve tahmine dayalı risk yönetimi	- YZ algoritmalarının şeffaf olmaması ve karmaşıklığı
- Sürekli izleme ve gerçek zamanlı veri analizi	- Veri güvenliği ve mahremiyet konularında riskler
- İnsan-makine iş birliği ile artırılmış karar kalitesi	- YZ uygulamalarının yüksek maliyetli altyapı gereksinimi
- Kurumsal strateji ve dijitalleşme uyumu	- Kurumsal direnç ve değişime adaptasyon zorlukları
Fırsatlar (Opportunities)	Tehditler (Threats)
- Teknoloji gelişmeleriyle sürekli yenilik imkanları	- Hızlı değişen teknoloji nedeniyle güncelliğin kaybedilmesi
- Uluslararası standartlar ve iş birliği imkanları	- Etik ve hukuki düzenlemelerde gecikmeler veya uyumsuzluklar
- Veri ekosistemi ve çok kaynaklı analizlerin yükselişi	- Siber güvenlik tehditleri ve veri ihlalleri riski
- İnsan-makine hibrit modellerinin yaygınlaşması	- YZ'ye aşırı bağımlılık ve insan faktörünün göz ardı edilmesi
- Kurumsal kültürde dijital dönüşüm ve eğitim fırsatları	- Toplumda YZ kullanımı ve denetim süreçlerine yönelik güven kaybı

Bu SWOT analizi, YÖK ve benzeri yükseköğretim kurumlarının iç denetim birimlerinin yapay zekâ kullanımı konusunda stratejik kararlar alırken dikkate alması gereken kritik unsurları kapsamaktadır.

8.3. Öneriler ve İleri Araştırma Alanları

Dijitalleşmenin ve yapay zekânın iç denetimde kullanımı, yükseköğretim kurumları başta olmak üzere kamu sektöründe kalite, etkinlik ve şeffaflık açısından önemli fırsatlar sunmaktadır. Ancak, bu teknolojilerin verimli bir şekilde kullanılması ve sürdürülebilir fayda sağlaması için stratejik, etik ve teknik boyutlarda dikkatli planlama yapılması ve sürekli geliştirilmesi gerekmektedir.

8.3.1. Öneriler

- **Kurumsal Dijital Dönüşüm Stratejilerinin Güçlendirilmesi:**

Yükseköğretim kurumları ve YÖK gibi üst düzey kurullar, iç denetimde dijitalleşmeyi stratejik öncelik haline getirmeli, altyapı yatırımları, insan kaynağı gelişimi ve süreç iyileştirme için kapsamlı planlar oluşturmalıdır.

- **Yapay Zekâ Destekli Risk Yönetim Sistemlerinin Yaygınlaştırılması:**

Risk tespiti ve analizinde yapay zekâ tabanlı modellerin kullanımı artırılmalı, bu modeller kurumlara özgü veri setleriyle sürekli olarak güncellenmeli ve optimize edilmelidir.

- **Etik ve Hukuki Çerçevenin Güçlendirilmesi:**

İç denetimde yapay zekâ kullanımına ilişkin etik ilkeler ve mevzuat netleştirilmeli, uyum süreçleri düzenli izlenmeli, etik eğitim programları yaygınlaştırılmalıdır.

- **İnsan-Makine İş Birliği Modellerinin Geliştirilmesi:**

Denetim süreçlerinde insan denetçilerin yetkinlikleri yapay zekâ ile tamamlanmalı, bu iş birliği modelleri için özel eğitimler ve adaptasyon destek programları tasarlanmalıdır.

- **Veri Kalitesi ve Güvenliğine Yatırım:**

Yapay zekâ sistemlerinin etkinliği, kaliteli ve güvenilir veri kaynaklarına bağlıdır. Kurumlarda veri yönetimi, bütünlüğü ve güvenliği için sürekli iyileştirme mekanizmaları oluşturulmalıdır.

- **Sürekli İzleme ve Performans Değerlendirme Sistemleri Kurulması:**

Yapay zekâ destekli iç denetim süreçleri düzenli olarak izlenmeli, performans göstergeleri doğrultusunda değerlendirilip geliştirilmelidir.

8.3.2. İleri Araştırma Alanları

- **Yapay Zekâ Algoritmalarında Şeffaflık ve Açıklanabilirlik:**

Siyah kutu algoritmalarının neden olduğu karar belirsizliklerini azaltmaya yönelik yöntemlerin geliştirilmesi; açıklanabilir yapay zekâ (Explainable AI) modellerinin iç denetimde uygulanabilirliği.

- **YZ Destekli Otonom Denetim Sistemleri:**

İnsan müdahalesi gerektirmeden belirli denetim görevlerini yürütebilen otonom denetim sistemlerinin tasarımı, prototip geliştirilmesi ve saha uygulamalarının incelenmesi.

- **Etik ve Sosyal Etkiler:**

Yapay zekâ uygulamalarının iç denetimde etik, hukuki ve sosyal sonuçlarının sistematik analizi; toplum ve paydaş algısının ölçülmesi.

- **Çok Kaynaklı Veri Entegrasyonu ve Analizi:**

Farklı kurumlar ve sistemlerden gelen veri setlerinin entegre edilmesiyle oluşturulan kapsamlı iç denetim veri ekosistemlerinin modellenmesi ve performansının değerlendirilmesi.

- **Yapay Zekâ ve İnsan Faktörü Arasındaki Etkileşim Modelleri:**

İnsan ve yapay zekâ iş birliğinin en etkin nasıl sağlanabileceği, rol dağılımı, karar alma süreçlerindeki optimum denge ve bu alandaki eğitim metodolojileri.

- **Siber Güvenlik ve Veri Gizliliği:**

İç denetim alanında yapay zekâ kullanımına özgü siber güvenlik tehditlerinin tespiti ve önlenmesi; veri gizliliği ve KVKK uyumu bağlamında yeni teknolojik çözümlerin araştırılması.

Bu öneri ve araştırma alanları, YÖK ve yükseköğretim kurumlarının dijital dönüşüm vizyonuna katkı sağlamakla kalmayıp, iç denetim süreçlerinin geleceğe hazır, esnek ve güvenilir hale gelmesini destekleyecektir.

KAYNAKÇA

- <https://tr.wikipedia.org/wiki/Dijitalle%C5%9Fme> (Erişim Tarihi:05.05.2025)
- https://tr.wikipedia.org/wiki/Dijital_d%C3%B6n%C3%BC%C5%9F%C3%BCm(Erişim Tarihi:05.05.2025)
- Turkyılmaz, S. (2024). DİJİTAL DÖNÜŞÜM: TARİHÇESİ, TANIMI VE İŞLETMELER ÜZERİNDEKİ ETKİSİ. Nişantaşı Üniversitesi Sosyal Bilimler Dergisi, 12(1), 276-297.
- Yılmaz, R. K. (2023). KAMU YÖNETİMİNDE KULLANILABİLECEK NESNELERİN İNTERNETİ (IOT) UYGULAMALARI. Kamu Yönetimi Ve Teknoloji Dergisi, 5(1), 87-98.
- <https://www.mysoft.com.tr/buyuk-veri-big-data> (Erişim Tarihi: 7.05.2025)
- M. Ali Akcayol Gazi Üniversitesi Bilgisayar Mühendisliği Bölümü ders notları https://bigdata.gazi.edu.tr/akcayol/files/SLBD_L2BigData.pdf
- Akın, E., & Şahin, M. E. (2024). Derin Öğrenme ve Yapay Sinir Ağı Modelleri Üzerine Bir İnceleme. EMO Bilimsel Dergi, 14(1), 27-38.
- Kestane, A. (2021). İÇ DENETİMDE AKILLI OTOMASYON TEKNOLOJİLERİNİN KULLANIMI: ROBOTİK SÜREÇ OTOMASYONU VE BİLİŞSEL ZEKÂ. Journal of Accounting and Taxation Studies, 14(2), 813-835. <https://doi.org/10.29067/muvu.806426>
- <https://nek.istanbul.edu.tr/ekos/TEZ/ET002645.pdf> (Erişim Tarihi:16.06.2025)
- Karacaer, B. (2023). Akıllı Otomasyon Sistemlerinin Getirdiği Riskler ve İç Denetime Etkileri, İşletme Akademisi Dergisi, 4 (2): 155-173. <https://doi.org/10.26677/TR1010.2023.1248>
- Karaca, M. (2024). Yapay Zekanın İç Denetime Etkileri Fırsatların Yakalanması ve Tehditlerin Yönetilmesi. Denetişim(31), 86-101. <https://doi.org/10.58348/denetisim.1526298>
- Bozkurt Yazar, B. (2024). KÜRESEL GELİŞMELER IŞIĞINDA İÇ DENETİM FAALİYETİNDE YAŞANAN DEĞİŞİMLERİN DEĞERLENDİRİLMESİ. Denetişim(29), 97-111. <https://doi.org/10.58348/denetisim.1391796>
- İç Denetçiler Enstitüsünün (İIA) 2017 yılında yayınladığı Yapay Zekâ Denetim Çerçevesi
- Türkiye Ulusal Yapay Zekâ Stratejisi (2021–2025)
- OECD YZ İlkeleri
- <https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf>
- <https://dijitalturkiyeplatformu.org/>