



ENERJİ DAĞITIM ŞİRKETLERİNDE DİJİTAL DENETİM UYGULAMALARI VE OPERASYONEL RİSK YÖNETİMİ

Hüseyin SEVİM¹

¹ Bağımsız Araştırmacı, Türkiye, Diyarbakır; huseyinsevim355@gmail.com, ORCID:0000-0002-2565-0988

Özet

Enerji sektörü, Endüstri 4.0 ile birlikte köklü bir dijital dönüşüm sürecine girmiştir. Bu süreç, enerji dağıtım şirketlerinin operasyonel yapılarını karmaşılaştırırken, aynı zamanda denetim ve risk yönetimi süreçlerinde yeni fırsatlar sunmaktadır. Geleneksel denetim yöntemleri, büyük veri yığınlarını ve gerçek zamanlı operasyonel riskleri yönetmekte yetersiz kalmaktadır. Bu makale, enerji dağıtım şirketlerinde dijital denetim (Denetim 4.0) uygulamalarının nasıl yapılandırıldığını, nesnelerin interneti, yapay zeka ve büyük veri analitiği gibi teknolojilerin operasyonel risk yönetimindeki rolünü incelemektedir. Araştırma, dijital denetimin yalnızca bir verimlilik aracı değil, aynı zamanda operasyonel hataları ve suistimalleri önlemede stratejik bir mekanizma olduğunu ortaya koymaktadır.

Küresel enerji sektöründe dijitalleşme hız kazanırken kritik altyapı siber güvenlik tehditleri de derinleşmektedir. Bu çalışmada, enerji dağıtım şirketlerinde yapay zeka tabanlı suistimal tespiti, operasyonel risk yönetimi ve regülasyona uyum süreçlerinin bütünleşik bir çerçevede incelenmesi hedeflenmektedir. Yapay zeka verimlilik sağlarken aynı zamanda veri kalitesi, model açıklanabilirliği ve yasal uyum gereklilikleri gibi zorluklar doğurmaktadır. Akıllı şebekeler ve gelişmiş ölçüm altyapılarının getirdiği veri hacmi, klasik denetim yöntemlerinin yerini sürekli veriye dayalı denetime bırakmasını zorunlu kılmaktadır. Enerji dağıtım şirketlerinin siber güvenliğinin güçlendirilmesi, öngörücü analizlerle risklerin proaktif yönetimi ve regülasyon uyumunun otomatik denetimi, sürdürülebilir işletme pratikleri için kritik bir stratejik alan oluşturmaktadır.

Anahtar Kelimeler: Enerji Dağıtım Şirketleri, Dijital Denetim, Denetim 4.0, Operasyonel Risk Yönetimi, Yapay Zekâ

JEL Kodları: M40, M42, M49

DIGITAL AUDIT PRACTICES AND OPERATIONAL RISK MANAGEMENT IN ENERGY DISTRIBUTION COMPANIES

Abstract

The energy sector has embarked on a profound digital transformation process alongside Industry 4.0. Whilst this process has complicated the operational structures of energy distribution companies, it also presents new opportunities in audit and risk management processes. Traditional audit methods are proving inadequate for managing large volumes of data and real-time operational risks. This article examines how digital audit (Audit 4.0) applications are structured within energy distribution companies, and explores the role of technologies such as the Internet of Things, artificial intelligence and big data analytics in operational risk management. The research demonstrates that digital audit is not merely a tool for efficiency, but also a strategic mechanism for preventing operational errors and fraud.

As digitalisation gains momentum in the global energy sector, cyber security threats to critical infrastructure are also intensifying. This study aims to examine AI-based fraud detection, operational risk management and regulatory compliance processes within energy distribution companies within an integrated framework. Whilst artificial intelligence enhances efficiency, it also presents challenges such as data quality, model interpretability and legal compliance requirements.

The volume of data generated by smart grids and advanced metering infrastructure necessitates a shift from traditional audit methods to continuous data-driven auditing. Strengthening the cybersecurity of energy distribution companies, the proactive management of risks through predictive analytics, and the automated monitoring of regulatory compliance constitute a critical strategic area for sustainable business practices.

Keywords: Energy Distribution Companies, Digital Audit, Audit 4.0, Operational Risk Management, Artificial Intelligence

JEL Codes: M40, M42, M49

GİRİŞ

Enerji dağıtım sektörü, kritik altyapı statüsü nedeniyle yüksek düzeyde operasyonel risk ve düzenleyici baskı altındadır. Geleneksel denetim yaklaşımları genellikle geçmişe dönük ve örnekleme dayalıdır, bu da modern enerji şebekelerinin dinamik yapısında risklerin gözden kaçmasına neden olabilmektedir. Dijitalleşme, denetim mesleğini finansal tabloların doğrulanmasından, risk yönetimi ve kurumsal yönetişimi kapsayan daha geniş bir stratejik yapıya dönüştürmüştür (Kılıçarslan, 2024).

Günümüzde enerji dağıtım şirketleri, akıllı şebekeler ve gelişmiş ölçüm altyapıları üzerinden saniyeler içinde devasa miktarda veri üretmektedir. Bu veri yığınlarının manuel yöntemlerle analizi imkansız hale geldiği için, “Denetim 4.0” olarak adlandırılan yeni nesil denetim yaklaşımları zorunlu bir ihtiyaç haline gelmiştir (Erdoğan, 2019). Dijital denetim, enerji sistemlerindeki verimsizlikleri tespit etmekle kalmayıp, aynı zamanda teknik kayıpları ve ekipman arızalarını önceden tahmin ederek operasyonel sürekliliği desteklemektedir (Ashraf et al., 2025).

Operasyonel risk yönetimi, enerji dağıtımında personelden ekipmana, çevresel faktörlerden yönetimsel eksikliklere kadar geniş bir yelpazeyi kapsar. Bu risklerin dijital araçlarla izlenmesi, şirketlerin finansal kayıplarını azaltırken yatırımcı ve kamu güvenini de artırmaktadır (Karlıdağ, 2021, Cornwell et al., 2023). Bu çalışma, dijital denetim araçlarının enerji sektöründeki operasyonel riskleri nasıl minimize ettiğini ve denetim döngüsünü nasıl sürekli hale getirdiğini detaylandırmaktadır.

Enerji Sektöründe Dijital Dönüşüm ve Denetim 4.0

Dijital dönüşüm, enerji sektöründe üretimden tüketime kadar olan tüm süreçleri etkileyerek maliyetleri düşürmekte ve müşteri deneyimini iyileştirmektedir. Bu dönüşümün temelinde IoT, yapay zeka ve bulut tabanlı platformlar yer almaktadır (Nazari ve Musilek, 2023). Enerji dağıtım şirketleri için dijitalleşme, şebeke planlamasından operasyonel mükemmelliğe kadar her aşamada veri odaklı kararlar alınmasını mümkün kılar (Aghahadi et al., 2024).

Denetim 4.0 kavramı, Endüstri 4.0 felsefesine uygun olarak finansal ve finansal olmayan verilerin entegre bir şekilde otomasyon sistemleri aracılığıyla denetlenmesini ifade eder. Bu yaklaşım, işletme içi ve dışı kontrol fonksiyonlarını hızlandırarak denetçilerin nesnelerin interneti üzerinden gerçek zamanlı verilere erişmesini sağlar (Erdoğan, 2019, Işık, 2024). Enerji dağıtımında bu durum, sayaç verilerinin veya trafo merkezlerindeki sensör verilerinin doğrudan denetim algoritmalarına aktarılması anlamına gelir.

Dijital teknolojilerin iç denetim süreçlerine entegrasyonu, denetimin rolünü geçmiş raporlayan bir birimden, geleceğe dair öngörüler sunan stratejik bir ortağa dönüştürmektedir. Yapay zeka destekli sistemler, denetim süreçlerinde hız ve doğruluk sağlayarak denetçilerin proaktif ve yönetim odaklı roller üstlenmesine imkan tanır (Kuş & Çıtak, 2025, Erişen & Erer, 2023). Bu dönüşüm, özellikle çok lokasyonlu ve karmaşık altyapıya sahip enerji şirketleri için kaynak verimliliği açısından kritik önemdedir.

Dijital Denetimde Veri Analitiği ve Büyük Veri Kullanımı

Büyük veri analitiği, denetçilerin milyonlarca işlemi filtreleyerek anomalileri belirlemesine ve yüksek risk taşıyan alanlara odaklanmasına olanak tanır. Küçük örneklemeler üzerinden yapılan geleneksel testler yerine, artık tüm veri popülasyonunun test edilebilmesi mümkün hale gelmektedir (Onay, 2020). Bu durum, enerji dağıtımındaki kaçak kullanım veya hatalı faturalandırma gibi sistemik sorunların tespit edilme olasılığını artırmaktadır.

Veri madenciliği ve makine öğrenmesi teknikleri, büyük veri yığınları içindeki gizli ilişkileri ve riskli durumları saniyeler içinde tarayabilir. Akıllı algoritmalar, geçmiş verilerdeki kalıpları inceleyerek gelecekte oluşabilecek riskli senaryolara karşı denetim kaynaklarını yönlendirmektedir (Sarıkaya et al., 2020). Enerji şirketlerinde bu teknikler, şebeke üzerindeki yük dengesizliklerini ve operasyonel verimsizlikleri tespit etmek için de kullanılmaktadır (Ashraf et al., 2025).

Dijital ikiz yöntemi gibi ileri teknolojiler, fiziksel varlıkların dijital kopyaları üzerinden denetim yapılmasını sağlar. Bu sayede denetçiler, karmaşık organizasyon yapılarını ve operasyonel süreçleri fiziksel müdahaleye gerek kalmadan inceleyebilir ve karar vericilere daha kaliteli bilgi üretebilir (Erturan & Ergin, 2018). Veri

analitiği ile desteklenen bu süreçler, denetim kalitesini artırırken bilgi asimetrisini de azaltmaktadır (Sayal et al., 2025).

Enerji dağıtım ağlarının genişlemesi, hat konfigürasyonlarını ve operasyonel karmaşıklığı artırarak güvenlik risklerini tetiklemektedir. Operasyonel risk yönetimi; personel, çevre, ekipman ve yönetsel eksikliklerden kaynaklanan risklerin ölçülebilir göstergelerle takip edilmesini gerektirir (Yang et al., 2024). Dijital denetim, bu göstergeleri sürekli izleyerek risklerin gerçekleşmeden önlenmesine yardımcı olur.

Türkiye’deki enerji sektörü üzerinde yapılan araştırmalar, risk odaklı iç denetim ile operasyonel süreçlerdeki suistimallerin tespiti arasında güçlü ve pozitif bir ilişki olduğunu göstermektedir. Denetim birimleri, risk düzeylerini analiz ederek suistimale açık hususları üst yönetime raporlamakta ve böylece finansal kayıpları minimize etmektedir (Karlıdağ, 2021). Operasyonel risk yönetimi stratejilerinin veri temelli olarak kurgulanması, şirketin finansal dayanıklılığı ve karar kalitesi üzerinde de doğrudan etki yaratmaktadır (Cornwell et al., 2023).

Geleneksel, statik ve kalitatif risk yönetimi uygulamaları modern enerji sektörünün karmaşıklığı karşısında verimsiz kalmaktadır. Veri analitiği, bu risklerin objektif ve dinamik bir şekilde yönetilmesini sağlayarak kurumların maliyetlerini düşürür (Cornwell et al., 2023). Enerji altyapı projeleri gibi büyük ölçekli ve şeffaflığın kritik olduğu alanlarda, dijital denetim araçları yolsuzluk ve verimsizlikleri erken aşamada tespit ederek kurumsal bütünlüğü desteklemektedir (Dworzecki & Szkurlat, 2022).

Teknolojik Araçlar: AI, IoT ve Sürekli Denetim

Enerji denetiminde IoT tabanlı cihazlar, bina ve şebeke yönetiminde gerçek zamanlı izleme yaparak enerji tüketimini optimize eder. Yapay zeka ile birleşen bu sistemler, sürekli denetime elverişli dijital kontrol altyapıları oluşturmaktadır (Abidin et al., 2025). Sürekli denetim yaklaşımı ise denetimin yılda birkaç kez yapılan bir faaliyetten ziyade 7/24 işleyen bir kontrol mekanizmasına dönüşmesini sağlamaktadır (Sarıkaya et al., 2020).

Makine öğrenmesi modelleri, yük sınıflandırması ve performans kıyaslaması yaparak enerji tasarrufu potansiyellerini belirleyebilir. Akıllı izleme sistemleri sayesinde enerji tasarrufunun ve sistem davranışının daha hassas biçimde modellenbildiği örnekler mevcuttur (Ashraf et al., 2025). Denetçiler bu teknolojileri kullanarak operasyonel hataları tahmin edebilir ve verimlilik önerilerini gerçek zamanlı olarak sunabilir.

Güç şebekesi projelerinin yönetiminde yaşam döngüsü denetimi modeli, projenin başlangıcından bitişine kadar tüm aşamaların dijital platformlar üzerinden izlenmesini sağlar. Bu model, gerçek zamanlı izleme ve proaktif risk azaltma yoluyla geleneksel yöntemlerin sınırlamalarını aşarak projenin sürdürülebilirliğini desteklemektedir (Zhou et al., 2025). Dijital denetim platformları, veri entegrasyonu sayesinde projelerdeki gecikmeleri ve bütçe aşımalarını anında raporlayabilmektedir.

Dijitalleşme büyük avantajlar sunsa da beraberinde teknoloji kaynaklı belirsizlikler ve yeni riskler de getirmektedir. Bilgi teknolojileri risklerinin yönetilememesi, kurumların kaynak israfına ve yenilikçi teknolojilerden vazgeçmesine neden olabilmektedir (Kharisova et al., 2023). Bu nedenle, dijital denetim süreçlerinin kendisi de güçlü bir siber güvenlik ve BT risk yönetimi çerçevesine sahip olmalıdır.

İç denetçiler arasında yapılan araştırmalar, dijital farkındalığın ve yetkinliğin reel sektörde henüz istenilen düzeyde olmadığını göstermektedir. Denetçilerin yapay zeka, blokzincir ve robotik süreç otomasyonu gibi alanlarda bilgi düzeylerini artırmaları, dijital dönüşüme uyum sağlamaları açısından kritiktir (Erişen & Erer, 2023). Ayrıca, yapay zeka algoritmalarının kara kutu doğası, denetim sonuçlarının açıklanabilirliğini zorlaştırarak kalite eleştirilerine yol açabilmektedir (Sayal et al., 2025).

Büyük veri yönetimi, verilerin çok kısa aralıklarla ve devasa boyutlarda üretilmesi nedeniyle ölçeklenebilirlik ve erişilebilirlik sorunları yaratabilmektedir. Geleneksel veri tabanlarının bu yükü kaldıramaması, analiz süreçlerinde darboğazlara yol açarak dijital denetimin etkinliğini kısıtlayabilir (Mwinuka et al., 2026). Bu zorlukların aşılması için enerji şirketlerinin bulut tabanlı ve NoSQL gibi modern veri yönetimi çözümlerine yatırım yapması gerekmektedir.

Enerji Dağıtımında Dijital İç Denetimin Dönüşümü

Denetim 4.0 olarak tanımlanan yeni nesil iç denetim, finansal tabloların doğrulanmasının ötesinde risk yönetimi, kurumsal yönetim ve etik ilkeleri de kapsayan bütüncül bir yapıya dönüşmektedir (Kılıçarslan, 2024). Geleneksel örnekleme dayalı yaklaşımlar, modern enerji şebekelerinin karmaşık ve dinamik yapısında riskleri zamanında tespit etmekte yetersiz kalırken; nesnelerin interneti ile donatılan işletme içi ve dışı sistemler üzerinden anlık kontrol imkanı sağlanmaktadır (Işık, 2024). Yapay zeka ve büyük veri analitiği, denetçilerin proaktif ve yönetim odaklı roller üstlenmesine olanak tanırken denetimin hız ve doğruluk algısını da güçlendirmektedir (Kuş & Çıtak, 2025).

Dijital dönüşümün enerji dağıtım şirketlerindeki pratik karşılığı, sayaçlar, trafo merkezleri ve şebeke sensörlerinden gelen devasa veri akışlarının gerçek zamanlı işlenmesidir. Bu veriler, operasyonel verimsizliklerin, teknik kayıpların ve kaçak kullanımın tespitinde kilit bir kaynak oluşturmaktadır. Yapay zeka destekli risk değerlendirme sistemleri, büyük hacimli finansal ve operasyonel verileri analiz ederek dolandırıcılıkla ilişkili örüntüleri belirlemekte ve denetçilere yüksek riskli işlemler hakkında detaylı bilgiler sunmaktadır (Şentürk, 2025). Bu sayede denetim süreçleri daha verimli hale gelmekte, dolandırıcılık girişimlerine karşı daha etkili önlemler alınmakta ve şirketlerin mali güvenliği güçlenmektedir.

Enerji dağıtımında dijital iç denetimin hedeflerinden biri de denetim döngüsünü yıllık veya dönemlik bir faaliyet olmaktan çıkarıp 7/24 işleyen bir kontrol mekanizmasına dönüştürmektir. Bu çerçevede, teknoloji yatırımlarının maliyet-fayda analizi, veri güvenliği önlemlerinin etkinliği ve operasyonel risklerin dinamik takibi, iç denetim portföyünün merkezini oluşturmaktadır.

Enerji hırsızlığı veya enerji düzensizlikleri, akıllı sayaçların sağladığı tüketim verilerinin konum, tarife tipi ve tüketim paterni ile çaprazlanarak önceliklendirilmiş risk puanları üretildiği yapay zeka tabanlı sistemlerle tespit edilmektedir (Benabed, 2023). Bu sistemler, potansiyel suistimal riski taşıyan kullanıcıları gruplar halinde belirlemekte ve şirketlerin fiziksel denetim kaynaklarını yüksek riskli alanlara yönlendirmesine yardımcı olmaktadır. Bu sayede dağıtım şirketleri, enerji kayıplarını minimize ederken finansal kayıpların da önüne geçebilmektedir.

Akıllı şebekelerde yapay zeka kullanımı enerji izleme yeteneklerini artırmakta, anomali tespit modelleri düzensiz tüketim örüntülerini tespit ederek enerji dağıtım ağlarının güvenilirliğini ve verimliliğini iyileştirmektedir (Gresoi et al., 2025). Enerji hırsızlığının otomatik tespiti, gerçek zamanlı ölçüm ve hızlı haberleşme gerektirir; bu nedenle veri iletişim altyapısının ve analitik yeteneklerinin kurumsal düzeyde entegrasyonu kritik bir başarı faktörüdür (Stracqualursi et al., 2023). Öngörücü analitik ve gerçek zamanlı izleme yeteneklerine sahip yapay zeka tabanlı dolandırıcılık tespit sistemleri, enerji dağıtımının operasyonel güvenliğini ve sürdürülebilirliğini desteklemektedir.

Enerji hırsızlığının tespitinde evrişimli sinir ağları ve uzun kısa vadeli hafıza gibi derin öğrenme algoritmaları kullanılmakta; akıllı şebekelerden elde edilen tüketim verilerinden soyut özellikler çıkarılarak tüketici bazlı hırsızlık tespit doğruluğu artırılmaktadır (Elshennawy et al., 2025). Veri setlerinin eksikliği ve sınıflar arası dengesizlik gibi veri kalitesi sorunları, uygun veri çoğaltma ve dengeleme teknikleriyle giderilerek model performansı daha da güçlendirilebilmektedir (Elshennawy et al., 2025).

Denetim faaliyetlerinde dijital dönüşümün etkisi, özellikle iç denetim süreçlerinde daha görünür hale gelmiştir. Geleneksel denetim teknikleri çoğu zaman sınırlı teknoloji kullanımıyla yürütülürken, yeni denetim anlayışı yapay zeka destekli sistemler ve dijital altyapılar üzerinden şekillenmektedir. Bu dönüşüm, denetçilerin çalışma biçimini değiştirmekte; risklerin daha erken tespit edilmesine, finansal raporlamanın güvenilirliğinin artırılmasına ve hata ile usulsüzlüklerin daha kısa sürede belirlenmesine katkı sağlamaktadır. Ayrıca denetçilerin rutin ve zaman alıcı işlemlerden uzaklaşarak daha fazla katma değer üreten faaliyetlere yönelmesine imkân vermektedir (Gökoğlu, Sevim & Kılıç, 2025).

Operasyonel Risk ve Kritik Altyapı Siber Güvenliği

Enerji dağıtım ağlarının sürekli genişlemesi, hat konfigürasyonlarının karmaşıklaşması ve operasyonel karmaşıklığın artması; personel, operasyonel çevre, ekipman ve yönetsel eksikliklerle ilişkili risklerin ölçülebilir göstergelerle kategorize edilmesini zorunlu hale getirmektedir (Yang et al., 2024). Özellikle pandemi sürecinde ulus devletlerden siber suçlulara kadar geniş bir yelpazede faaliyet gösteren aktörlerin enerji sektörüne yönelik saldırı kapasiteleri artmış, evden çalışmanın yaygınlaşması da siber tehditleri derinleştirmiştir (Sheehan, 2023). Ayrıca, Amerika Birleşik Devletleri bağlamında elektrik şebekesinin

üretim ve iletim kısımlarına odaklanan ulusal siber güvenlik yaklaşımının dağıtım sistemlerine yeterince yoğunlaşmaması, son kullanıcıya elektriği ileten bu yapıları daha kırılgan hale getirmektedir (Sheehan, 2023).

MOSAR yöntemi ile elektrik enerji sisteminin sürekliliğini sağlamaya yönelik en kritik riskler arasında siber saldırılar, bilgi teknolojisi sistemlerinin kullanılabilirliği, kritik personel kayıpları ve ağ sorunları öne çıkmaktadır (Foşner et al., 2024). Bu risklerin yönetimi için enerjinin zamanında ve yüksek standartta iletilmesi, müşteri taleplerine hızlı yanıt verilmesi, teknik standartların uygulanması ve kişisel ile çevresel koruma önlemlerinin gözetilmesi gerekmektedir (Foşner et al., 2024).

Enerji altyapısındaki siber saldırılara karşı güvenliği artırmak için stres testlerinin ve tehdit tespit sistemlerinin düzenli bir şekilde uygulanması önerilmektedir (Aköz & Süruri, 2025). Türkiye’de 2016 yılında enerji altyapısına yönelik gerçekleştirilen siber saldırının, elektrik dağıtım sistemlerinin işlevini geçici süreyle durdurduğu ve bu altyapıların savunmasızlığını açık biçimde ortaya koyduğu belirtilmektedir (Aköz & Süruri, 2025). Dağıtık enerji kaynaklarının akıllı şebekelerle entegre olması, enerji sürdürülebilirliği, verimliliği ve dayanıklılığını desteklerken bilgi teknolojilerine artan bağımlılık güç sistemlerini siber saldırılara karşı daha savunmasız hale getirmektedir (Chen et al., 2025).

Regülasyon Uyumu ve Denetim Analitiği Stratejileri

Yüksek büyüme oranlı enerji piyasalarında büyük ölçekli altyapı projeleri karmaşık yönetim yapıları ve finansal opaklık riskleri barındırmaktadır. Bu nedenle denetim analitiği çerçevelerinin tahminsel analiz, tedarikçi yönetimi, kontrol bayrakları ve uyum izleme bileşenlerini birlikte ele alması gerekmektedir (Sayal et al., 2025; Cornwell et al., 2023). Bu araçlar kurumsal denetim sistemlerine gömüldüğünde, denetimin geriye dönük bir kontrol sürecinden sürekli ve veriye dayalı bir yönetim mekanizmasına evrilmesine katkı sağlamaktadır (Kuş & Çıtak, 2025, Şahin & Evdilek, 2025).

Lojistik ve enerji sektörlerinde dijital dönüşümün stratejik çerçeveleri, enerji şirketlerinin veri gizliliği, çevresel etki ve güvenliğe ilişkin yasal standartlara uyumunu zorunlu kılmaktadır (Attah et al., 2024). Bu düzenleyici çerçevelere uyum için dijital teknolojilere ilişkin normların derinlemesine anlaşılması gerekir. Akıllı şebekeler ve IoT cihazları gibi yeni teknolojilerin mevcut düzenlemelerle her zaman tam uyum göstermemesi nedeniyle, entegrasyon sürecinde regülatörlerle proaktif diyalog kurulması ve iç yönetim modelinin açık şekilde tanımlanması kritik önemdedir (Attah et al., 2024). Enerji dağıtım şirketlerinin uyum süreçlerinde sektördeki paydaşlarla iş birliği yapması ve endüstriler arası standart belirleme örgütlerine katılması, regülasyon uyumunu güçlendiren bir stratejidir (Attah et al., 2024).

Enerji altyapısındaki dağıtık enerji kaynağı sistemlerinin siber güvenliği, risk değerlendirmesi, tehdit ve açıklıkların belirlenmesi ve kapsamlı bir derinlemesine savunma çerçevesinin geliştirilmesini gerektirmektedir (Chen et al., 2025). Bu çerçeve, çeşitli paydaşların verimli koordinasyonunu ve güç sistemlerinin operasyonel performansını siber saldırılara karşı güvence altına almayı hedefler. Enerji dağıtım şirketleri, regülasyon uyumunu otomatik denetim platformlarına entegre ederek yasal gerekliliklerin gerçek zamanlı izlenmesini ve sapmaların hızlı biçimde tespit edilmesini sağlayabilir.

Dijital dönüşümün denetim alanındaki bir diğer önemli sonucu, veri odaklı denetim anlayışının güç kazanmasıdır. Yapay zekâ, büyük veri ve makine öğrenmesi gibi teknolojiler sayesinde denetim artık yalnızca geçmiş işlemlerin incelenmesine dayalı bir faaliyet olmaktan çıkmakta; ileriye dönük tahmin, gerçek zamanlı analiz ve kapsamlı risk değerlendirmesi sağlayan bir yapıya dönüşmektedir. Bu durum, denetçilerin yalnızca muhasebe ve kontrol bilgisiyle yetinmesini değil, aynı zamanda teknolojik sistemleri anlayabilen, algoritmik sonuçları yorumlayabilen ve veri temelli denetim süreçlerine uyum sağlayabilen yeni bir yetkinlik seti geliştirmesini zorunlu kılmaktadır (Gökoğlu et al., 2025).

Veri Kalitesi, Model Açıklanabilirliği ve Deneysel Çalışma Bağlamı

Yapay zeka tabanlı suistimal ve dolandırıcılık tespit sistemlerinde veri kalitesi ve akıllı sayaçların geniş kapsamda temin edilebilirliği, model performansını doğrudan etkilemektedir. Enerji hırsızlığının tespitinde yapay zeka tabanlı genelleştirilebilir yöntemlerin geliştirilmesi, gerçek zamanlı ölçüm ve hızlı haberleşme altyapısını zorunlu kılmaktadır (Stracqualursi et al., 2023). Tek yöntemle kapsamlı bir tespit sistemi geliştirmek yerine, çeşitli yapay zeka yöntemlerinin güçlü ve zayıf yönlerinin karşılaştırıldığı hibrit çözümler geliştirilmesi önerilmektedir (Stracqualursi et al., 2023).

Yapay zeka tabanlı dolandırıcılık tespitinde öngörücü analizler, olağandışılık tespiti ve gerçek zamanlı izleme gibi imkanlar finansal raporlamanın otomasyonuna, operasyonel maliyetlerin düşürülmesine ve yanlış pozitiflerin minimize edilmesine yardımcı olur (Erkan et al., 2025). Ancak yapay zeka uygulamaları veri kalitesi, model açıklanabilirliği, regülasyon gereklilikleri ve teknik operasyonel riskler gibi zorluklarla da karşı karşıya kalabilir. Bu nedenle şirketler, etkili bir dolandırıcılık savunması için klasik yöntemlerle yapay zeka teknolojisinin entegre kullanımına başvurmalıdır (Erkan et al., 2025).

Denetim süreçlerinde kullanılan veri analitiği tekniklerinin ileri düzeye taşınması, yapay zeka tabanlı sistemlerin dolandırıcılığı önleme konusunda daha etkili olacağını göstermektedir. Derin öğrenme ve karar ağaçları gibi yöntemlerin yüksek doğruluk oranlarıyla dolandırıcılık tespiti yapabildiği vurgulanmaktadır (Işık et al., 2023, Terzi, 2025). Enerji dağıtım şirketlerinde deneysel çalışmalar çoğunlukla simülasyon ortamlarında gerçekleştirilmektedir; ancak bu çalışmaların gerçek saha verileriyle doğrulanması, yönetim süreçlerini iyileştirmenin yanı sıra operasyonel risk profilinin daha net ortaya konulmasına da katkı sağlamaktadır.

Gelişimin en kritik aşaması, derin öğrenme (deep learning) ve yapay sinir ağlarının yaygınlaşmasıdır. Makine öğrenimi verileri analiz ederek tahminlerde bulunurken, derin öğrenme bu süreci insan beyninin çalışma prensiplerine benzer katmanlı yapılarla gerçekleştirir (Gökoğlu ve Sevim, 2024). Bu teknolojik sıçrama, yapay zekanın karmaşık finansal verileri yorumlamasından tıbbi teşhislere kadar geniş bir yelpazede kullanılmasını sağlamıştır (Gökoğlu & Sevim, 2024).

SONUÇ

Enerji dağıtım şirketlerinde dijital denetim ve operasyonel risk yönetimi, artık birbirinden ayrılmaz bir bütün haline gelmiştir. Dijital araçlar, denetimi yalnızca bir kontrol mekanizması olmaktan çıkarıp operasyonel verimliliği artıran ve stratejik karar alma süreçlerini destekleyen bir fonksiyona dönüştürmüştür (Kuş & Çıtak, 2025). Veri analitiği ve sürekli izleme sayesinde, enerji şebekelerindeki riskler daha şeffaf ve yönetilebilir hale gelmiştir.

Gelecekte, yapay zeka ve nesnelerin interneti gibi teknolojilerin daha derin entegrasyonu ile otonom denetim süreçlerinin yaygınlaşması beklenmektedir. Ancak bu süreçte denetçilerin dijital yetkinliklerini geliştirmeleri ve veri güvenliği risklerini önceliklendirmeleri başarının anahtarı olacaktır (Erişen & Erer, 2023; Şentürk, 2025). Enerji sektöründeki karmaşık altyapı projeleri ve operasyonel süreçler, ancak teknoloji ile denetim uzmanlığının birleştiği bir modelle sürdürülebilir kılınabilir.

Sonuç olarak, dijital denetim uygulamaları enerji dağıtım şirketlerine sadece hata tespiti değil, aynı zamanda operasyonel risklerin proaktif yönetimi yoluyla uzun vadeli finansal istikrar ve rekabet avantajı sağlamaktadır (Dworzecki & Szkurlat, 2022). Dijital dönüşümün getirdiği bu yeni düzen, denetimi kurumsal yönetişimin en güçlü halkalarından biri haline getirmektedir.

Enerji dağıtım şirketlerinde yapay zeka destekli dijital denetim ve operasyonel risk yönetimi, şirketlere yalnızca hızlı ve doğru bir kontrol mekanizması sağlamakla kalmayıp, regülasyon uyumunu güçlendiren ve sürdürülebilir güvenlik stratejileri oluşturan kritik bir yetkinlik alanı olarak ortaya çıkmaktadır. Denetimin statik bir yapıdan sürekli veriye dayalı bir yönetim mekanizmasına dönüşmesi, enerji altyapı projelerinin karmaşık risk manzarasının aşılmasına yardımcı olmaktadır. Kritik altyapı siber güvenliği, enerji dağıtım süreçlerinin sürekliliği ve müşteri güveninin korunması için, şirketlerin teknoloji ve denetim uzmanlığını birleştirmesi gerekmektedir.

Gelecekte, enerji dağıtım şirketlerinin regülasyon uyumunu otomatik denetime katması, yapay zeka uygulamalarında veri kalitesini ve etik standartları geliştirmesi ve çok paydaşlı derinlemesine savunma çerçevelerini güçlendirmesi, enerji altyapılarının güvenilirliğini ve sürdürülebilirliğini destekleyecektir. Bu bağlamda, insan faktörü ile makine entegrasyonunun denetim süreçlerine dengeli biçimde yansıtılması; yapay zeka tabanlı sistemlerin denetçilerin yerini alan değil, denetçilerin operasyonel etkinliğini artıran araçlar olarak konumlandırılmasını gerektirmektedir (Şahin & Evdilek, 2025; Şentürk, 2025).

KAYNAKÇA

- Abidin, A. Z., Enriko, I. K. A. & Pramudita, A. A. (2025). Leveraging IoT, digital twin and machine learning for smart energy audit in office building: A systematic literature review and recommendations. *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, 14, Article 101124. <https://doi.org/10.1016/j.prime.2025.101124>
- Aghahadi, M., Bosisio, A., Merlo, M., Berizzi, A., Pegoianni, A. & Forciniti, S. (2024). Digitalization processes in distribution grids: A comprehensive review of strategies and challenges. *Applied Sciences*, 14(11), Article 4528. <https://doi.org/10.3390/app14114528>
- Aköz, S. & Süruri, H. (2025). Cybersecurity in critical infrastructures and cyber terrorism: A strategic analysis on Türkiye. *Journal of Terrorism and Radicalization Studies*, 4(2), 223-265. <https://doi.org/10.61314/traddergi.1618580>
- Ashraf, S., Zarie, M. M. & Abdellatif, S. O. (2025). Towards autonomous energy management: Machine learning for effective auditing and optimization. *Scientific Reports*, 15, Article 39368. <https://doi.org/10.1038/s41598-025-24513-7>
- Attah, R. U., Garba, B. M. P., Gil-Ozoudeh, I. & Iwuanyanwu, O. (2024). Strategic frameworks for digital transformation across logistics and energy sectors: Bridging technology with business strategy. *Open Access Research Journal of Science and Technology*, 12(2), 70-80. <https://doi.org/10.53022/oarjst.2024.12.2.0142>
- Benabed, A. (2023). Artificial intelligence's relevance for energy optimization, companies and business internationalization. In D. Vasiliu ve L. Tăchiciu (Ed.), *Proceedings of the 9th BASIQ International Conference on New Trends in Sustainable Business and Consumption* (ss. 183-191). ASE. <https://doi.org/10.24818/BASIQ/2023/09/075>
- Chen, J., Yan, J., Kemmeugne, A., Kassouf, M. & Debbabi, M. (2025). Cybersecurity of distributed energy resource systems in the smart grid: A survey. *Applied Energy*, 383, Article 125364. <https://doi.org/10.1016/j.apenergy.2025.125364>
- Cornwell, N., Bilson, C., Gepp, A., Stern, S. & Vanstone, B. J. (2023). The role of data analytics within operational risk management: A systematic review from the financial services and energy sectors. *Journal of the Operational Research Society*, 74(1), 374-402. <https://doi.org/10.1080/01605682.2022.2041373>
- Dworzecki, J. & Szkurlat, I. (2022). Audit as a tool affecting the management of economic security of companies in the Polish energy sector: A research report. *European Research Studies Journal*, 25(4), 112-143. <https://doi.org/10.35808/ersj/3071>
- Elshennawy, N. M., Ibrahim, D. M. & Gab Allah, A. M. (2025). An efficient electricity theft detection based on deep learning. *Scientific Reports*, 15, Article 12866. <https://doi.org/10.1038/s41598-025-93140-z>
- Erdoğan, M. (2019). Denetim 4.0 ve ötesi. *Muhasebe ve Vergi Uygulamaları Dergisi*, 12(3), 809-834. <https://doi.org/10.29067/muvu.479247>
- Erişen, O. & Erer, M. (2023). Exploring the impacts of digitalization on the internal audit profession. *Journal of Research in Business*, 8(1), 171-190. <https://doi.org/10.54452/jrb.1182813>
- Erkan, M., Özdemir, İ. & Erkasap, A. (2025). İşletmelerde, hile tespiti ve önlenmesi süreçlerinde yapay zekâ uygulamalarıyla verimliliğin artırılması. *Paradoks Ekonomi, Sosyoloji ve Politika Dergisi*, 21(1), 62-86.
- Erturan, İ. E. & Ergin, E. (2018). Dijital denetim ve dijital ikiz yöntemi. *Muhasebe Bilim Dünyası Dergisi*, 20(4), 810-830. <https://doi.org/10.31460/mbdd.395261>
- Fošner, A., Bertoneclj, B., Poznič, T. & Fink, L. (2024). Risk analysis of critical infrastructure with the MOSAR method. *Heliyon*, 10(4), Article e26439. <https://doi.org/10.1016/j.heliyon.2024.e26439>
- Gökoğlan, K., & Sevim, H. (2024). The Impact Of Artificial Intelligence Recommendations On Individual Investor Decisions. (146-148).

- Gökoğlu, K., Sevim, H. & Kılıç, S. (2025). Digital transformation and artificial intelligence-assisted auditing: The role of technology in internal audit processes in 2025. *Dynamics in Social Sciences and Humanities*, 6(1), 25-33. <https://doi.org/10.62425/dssh.1647929>
- Gresoi, S., Stămătescu, G. & Făgărășan, I. (2025). Advanced methodology for fraud detection in energy using machine learning algorithms. *Applied Sciences*, 15(6), Article 3361. <https://doi.org/10.3390/app15063361>
- Işık, S. (2024). Yapay zekâ ve denetim ile ilgili yapılan uluslararası çalışmaların bibliyometrik analizi. *Quantrade Journal of Complex Systems in Social Sciences*, 6(2), 201-216. <https://doi.org/10.5281/zenodo.14577904>
- Işık, Y., Kefe, İ. & Sağlar, J. (2023). Detection of fraudulent transactions using artificial neural networks and decision tree methods. *Business and Management Studies: An International Journal*, 11(2), 451-467. <https://doi.org/10.15295/bmij.v11i2.2200>
- Karlıdağ, G. Ö. (2021). Türkiye'deki enerji sektörü çalışanlarının risk odaklı iç denetimle ilgili görüşlerine ilişkin bir araştırma. *Journal of Accounting Institute*, 64, 59-70. <https://doi.org/10.26650/MED.826908>
- Kharisova, F. I., Efimova, O. V., Sabirova, A. I., Umarov, H. S. & Dashin, A. S. (2023). Energy-efficient internal audit for IT-risks in municipal facilities and environmental technologies. *E3S Web of Conferences*, 458, Article 01001. <https://doi.org/10.1051/e3sconf/202345801001>
- Kılıçarslan, Ş. (2024). Denetimde dijital dönüşüm konusunda yapılan çalışmaların bibliyometrik analizi. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 29(3), 211-224.
- Kuş, M. & Çıtak, N. (2025). Yapay zekâ destekli iç denetim ve uygulamalı bir model yaklaşımı [AI-driven internal audit and an applied model approach]. *Denetışim*, 33, 213-237. <https://doi.org/10.58348/denetisim.1713359>
- Mwinuka, L. J., Cafaro, M., Pereira, L. & Morais, H. (2026). Big data energy systems: A survey of practices and associated challenges. *Computer Science Review*, 49, Article 100927. <https://doi.org/10.1016/j.cosrev.2026.100927>
- Nazari, Z. & Musilek, P. (2023). Impact of digital transformation on the energy sector: A review. *Algorithms*, 16(4), Article 211. <https://doi.org/10.3390/a16040211>
- Onay, A. (2020). Büyük veri çağında iç denetimin dönüşümü. *Muhasebe Bilim Dünyası Dergisi*, 22(1), 127-163. <https://doi.org/10.31460/mbdd.620837>
- Şahin, O. N. & Evdilek, N. (2025). Digital transformation in audit: Opportunities and challenges of artificial intelligence in audit. *Denetim ve Güvence Hizmetleri Dergisi*, 5(1), 49-61.
- Sarıkaya, R., Orman, R. & Özgel, Ç. (2020). An application for continuous auditing in Turkish public sector: E-auditor. *Denetışim*, 21, 53-65.
- Sayal, A., Johri, A., Chaithra, N., Alhumoudi, H. & Alatawi, Z. (2025). Optimizing audit processes through open innovation: Leveraging emerging technologies for enhanced accuracy and efficiency. *Journal of Open Innovation: Technology, Market, and Complexity*, 11(3), Article 100573. <https://doi.org/10.1016/j.joitmc.2025.100573>
- Şentürk, Ö. (2025). İnsan faktörü ve makine: Yapay zekâ iç denetçilerin yerini alabilir mi? *TİDE Academia Research*, 7(1), 11-52.
- Sheehan, J. (2023). Beyond lip-service: Content clouds, 10-K filings, cyber risk and the electric grid. In K. J. Engemann, C. F. Lavery ve J. Sheehan (Ed.), *Volume IV Socio-Political Risk Management: Assessing and Managing Global Insecurity* (ss. 51-72). De Gruyter. <https://doi.org/10.1515/9783110731217-004>
- Stracqualursi, E., Rosato, A., Di Lorenzo, G., Panella, M. & Araneo, R. (2023). Systematic review of energy theft practices and autonomous detection through artificial intelligence methods. *Renewable and Sustainable Energy Reviews*, 184, Article 113544. <https://doi.org/10.1016/j.rser.2023.113544>
- Terzi, A. K. (2025). Yapay zekâ ve denetim: Scopus veritabanındaki yayınların bibliyometrik analizi. *Çalışma İlişkileri Dergisi*, 16(2), 1-38.

- Yang, Y., Zhao, X., Han, T., Xu, M. & Li, C. (2024). Enhancing operational risk management in distribution networks: A comprehensive framework. *Fluctuation and Noise Letters*, 23(5), Article 2450044. <https://doi.org/10.1142/S0219477524500445>
- Zhou, M., Chen, Y. & Zhou, L. (2025). Strengthening power grid projects' governance and sustainability through lifecycle auditing. *Scientific Reports*, 15, Article 36442. <https://doi.org/10.1038/s41598-025-20389-9>