THE JOURNAL OF TURKISH EDUCATIONAL SCIENCES
TÜRK EĞİTİM BİLİMLERİ DERGİSİ

Kamu Kurumlarında Bilgi Güvenliği Denetimi: İç Denetçilerin Kullanımı için LLM Destekli Bir Eğitim Modülü Önerisi

Information Security Auditing in Public Institutions: A Proposed LLM-Supported Training Module for Internal Auditors

Onur Ceran

Yazar Bilgileri

Onur Ceran
Dr. Öğr Üyesi, Gazi Üniversitesi,
onur.ceran@gazi.edu.tr

ÖZ

Kamu kurumlarında görev yapan iç denetçiler, mesleki yeterliliklerini genel yetenek, muhasebe, mevzuat ve iç kontrol alanlarındaki eğitimlerle sağlamaktadır. ISO 27001 sertifikasyonuna sahip olmalarına karşın, mevcut eğitim içeriğinin bilgi teknolojileri ve siber güvenlik konularında gereken teknik derinlikten yoksun olduğu değerlendirilmiştir. Bilgi ve iletişim güvenliği denetimlerinin yalnızca standart ve prosedür uyumluluğundan ibaret olmaması, aynı zamanda teknik altyapı, yazılım güvenliği ve ağ sistemleri gibi kritik bileşenleri de kapsaması gerekliliği, denetçilerin bu alanlarda daha kapsamlı bilgi ve becerilere sahip olmasını gerekli kılmaktadır. Bu durum, denetçilerin teknik uzmanlarla etkin iletişim kurma, kritik sorular yöneltme ve aldıkları yanıtların geçerliliğini değerlendirme kabiliyetlerini sınırlayabilmektedir. Bu çalışma, kamu iç denetçilerinin bilgi güvenliği denetimlerindeki teknik yeterliliklerini artıracak yenilikçi bir eğitim modülü geliştirmeyi amaçlamaktadır. Bu amaç doğrultusunda, özgün bir metodoloji benimsenmiştir: Bilgi güvenliği denetimi için gerekli teknik konuları ve öğrenim hedeflerini içeren bir eğitim içeriği taslağı, Büyük Dil Modelleri (LLM) kullanılarak oluşturulmuş, devamında ise, LLM'ler tarafından üretilen bu taslak içerik, alanında yetkin ve ISO 27001 sertifikasyonuna sahip kamu iç denetçilerinden oluşan bir uzman grubunun görüşüne sunulmuştur. Çalışmanın sonucunda, yapay zekâ ve insan uzmanlığının sentezine dayalı, kamu iç denetçilerinin ihtiyaçlarına özel olarak tasarlanmış, teknik odaklı bir bilgi güvenliği denetimi eğitim modülü önerisi sunulmuştur. Bu programın, kamu sektöründeki bilgi güvenliği denetimlerinin kalitesini, derinliğini ve katma değerini artırarak kurumların siber dayanıklılığına önemli bir katkı sağlaması hedeflenmektedir.

Makale Bilgileri

Anahtar Kelimeler
İç denetim
Bilgi güvenliği
Yapay zekâ
Büyük Dil Modeli

Keywords
Internal audit
Information security
Artificial intelligence
Large Language Model

Makale Geçmişi
Geliş: 11.08.2025
Kabul: 06.10.2025

ABSTRACT

Internal auditors within public institutions acquire their professional competencies through training in general skills, accounting, legislation, and internal control. Despite holding ISO 27001 certification, the current content of the training often lacks technical depth in information technology and cybersecurity. The requirement for information and communication security audits to address not only compliance with standards and procedures but also critical aspects such as technical infrastructure, software security, and network systems highlight the need for auditors to develop broader expertise in these domains. This deficiency may impair auditors' ability to effectively communicate with technical specialists, formulate pertinent technical inquiries, and accurately assess the validity of responses received. This research aims to develop an innovative training module to enhance the technical competencies of public internal auditors in information security audits. A unique methodology was employed: initially, a draft training module outlining essential technical topics and learning objectives for information security auditing was generated using Large Language Models (LLMs). Subsequently, this LLM-produced content was rigorously reviewed and validated by a panel of experienced and ISO 27001-certified public internal auditors. Finally, a proposal was presented for a technically oriented information security audit training module, designed specifically to meet the needs of public internal auditors and based on the synthesis of artificial intelligence and human expertise. The program is expected to make a significant contribution to the cyber resilience of public institutions by enhancing the quality, depth, and added value of information security audits in the public sector.

Makale Türü Araştırma

Önerilen Atıf Ceran, O. (2025). Kamu kurumlarında bilgi güvenliği denetimi: İç denetçilerin kullanımı için LLM destekli bir eğitim modülü önerisi. *TEBD*, *23*(3), 2211-2250. https://doi.org/10.37217/tebd.1762043

Giriş

Kamu kurum ve kuruluşları, vatandaşlara yönelik kritik hizmetleri yürüten, büyük miktarda kişisel ve kurumsal veri barındıran ve toplumun güvenliğini doğrudan etkileyen bilgi varlıklarına sahip yapılar olarak bilgi güvenliği açısından merkezi bir öneme sahiptir. Son dönemde hızlanan dijital dönüşüm hamleleri; e-devlet portalları, elektronik belge yönetim sistemleri, çevrim içi başvuru ve işlem platformları, yapay zekâ destekli hizmetler ve bulut bilişim altyapıları gibi yenilikçi uygulamalarla hizmet sunumunu önemli ölçüde hızlandırmıştır (Aksoy, 2024). Ancak bu dönüşüm, kurumların maruz kaldığı siber tehdit düzeyini de kayda değer ölçüde genişletmiştir (Tunçbilek, 2024). Özellikle kamu kuruluşları, siber saldırılara karşı yüksek değerli hedefler olmaları nedeniyle fidye yazılımları, DDoS (Dağıtık Servis Reddi) atakları, sistemlere sızma ve veri sızıntıları gibi tehditlerle karşılaşma riskiyle daha ciddi bir şekilde yüzleşmektedir (Hatipoğlu ve Tunacan, 2021). Bu durum, kamu kurumlarının sadece iş süreçlerini dijitalleştirmekle kalmayıp, aynı zamanda bu yeni ortamlarda bilgi güvenliğini proaktif ve kapsamlı bir şekilde sağlamalarını zorunlu kılmaktadır.

Kamu sektöründe bilgi güvenliği yalnızca teknik bir konu olmanın ötesinde, aynı zamanda yasal ve toplumsal bir zorunluluktur. Kişisel Verilerin Korunması Kanunu (KVKK) ve Genel Veri Koruma Tüzüğü (GDPR) gibi ulusal ve uluslararası düzenlemeler, kişisel verilerin korunmasına dair yükümlülükleri net bir şekilde tanımlamakta ve kamu kurumlarının bilgi güvenliğini sağlamak için belirli standartların ve denetimlerin uygulamasını zorunlu kılmaktadır (Güdek, 2023). Bu bağlamda, birçok kamu kurumu ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) uyum süreçlerini benimsemiş olmakla beraber bu süreçlerin odak noktası genellikle politika, prosedür ve standarda uyum düzeyinde kalmıştır. Oysa kamunun dijitalleşme süreci, sadece yönetimsel uygunlukla sınırlı kalmayıp, teknik altyapı, ağ sistemleri, yazılım güvenliği, siber olay müdahalesi gibi teknik boyutların da kapsamlı bir şekilde değerlendirilmesini elzem kılmaktadır (Uslu, 2023).

Bu gereklilik, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi (BİG Rehberi) ile daha da somutlaşmıştır. BİG Rehberi, kamu kurumlarının dijital varlıklarını siber tehditlere karşı koruması için kapsamlı bir çerçeve sunmakta ve bilgi güvenliği denetimlerinin sadece yüzeysel bir uygunluk kontrolü olmaktan çıkarak, teknik derinliği olan, sürekli ve risk odaklı bir sürece evirilmesini hedeflemektedir (Ünlü ve Çakmak, 2023). Rehber, kurumlara teknik güvenlik kontrolleri, siber olaylara müdahale planları, zafiyet yönetimi ve sızma testleri gibi alanlarda detaylı yol haritaları sunarak, kamu bilgi sistemlerinin dayanıklılığını artırmayı amaçlamaktadır. Diğer taraftan BİG Rehberi, bilgi güvenliğine yönelik bu denetimlerin ISO/IEC 27001 sertifikasına sahip iç denetçiler tarafından gerçekleştirmesini öngörmekte ise de mevcut ISO/IEC 27001 eğitim içeriğinin, BİG Rehberi'nde yer alan detaylı teknik incelemelerin yapılmasında iç denetçilere yeterli yetkinliği tam olarak sağlayamadığı görülmektedir (Ağdeniz,

2021). Bu bağlamda, CBDDO'nun bu rehberi yayımlaması, kamu iç denetçilerinin bilgi güvenliği denetimlerine yönelik bakış açısını ve yetkinliklerini dönüştürme ihtiyacını daha da belirgin hale getirmektedir. Zira rehberin öngördüğü teknik denetim gereksinimleri, ISO/IEC 27001 eğitimini tamamlayarak bu denetimleri gerçekleştiren iç denetçilerin bilgi güvenliği alanındaki eğitim programlarının bu yeni ve genişleyen beklentilere uygun şekilde güncellenmesini zorunlu kılmaktadır.

Kamu kurumlarında iç denetçiler, genel yetenek sınavları, muhasebe, mevzuat ve iç kontrol sistemlerine dayalı eğitim ve sınav süreçleriyle yetiştirilmektedir (ESY, 2005). Bilgi güvenliği iç denetçi eğitimleri kapsamında ISO 27001 standartları da öğretilmekle birlikte, mevcut programlarda teknik bilişim altyapısı ve siber güvenlik unsurlarına dair yeterli eğitim verilmediği görülmektedir. Gerçekleştirilen düzenlemeler, önleyici tedbirler içermek yerine ortaya çıkan durumlara yönelik tepkisel nitelikler barındırması, uygulamadaki etkinliklerini zayıflattığı yönünde eleştirilere maruz kalmakta iken (Kestane ve Kurt, 2024), etkin bir bilgi güvenliği denetiminde, savunma sistemlerinin yapısını anlama, güvenlik konfigürasyonlarını yorumlama, zafiyet raporlarını okuyup değerlendirmeye sokma, kritik soru sorma ve alınan teknik cevapların doğruluğunu sorgulama becerileri büyük önem taşımaktadır. Denetçilerin sadece politika ve prosedür uygunluğunu değil, aynı zamanda operasyonel ve teknik güvenlik kontrollerinin etkinliğini değerlendirebilmeleri, siber riskleri doğru bir şekilde tespit etmeleri ve kurumların siber güvenlik duruşunu güçlendirmeleri açısından hayati bir rol oynamaktadır (Selimoğlu ve Saldı, 2022). Denetçilerin teknik bilgi birikimini artırması, bilgi teknolojileri birimleriyle daha etkili bir iletişim kurmasını, siber olay çözümlemelerini daha iyi anlamasını ve bu bulgular ışığında değer yaratan tavsiyeler sunmasını kolaylaştıracaktır. Potansiyel güvenlik zafiyetlerinin gözden kaçması riski gelişen teknoloji ile artış gösterme potansiyeline de sahiptir. Bu bağlamda, teknolojinin durmaksızın ilerlemesiyle ortaya çıkan yeni riskleri yönetebilmek için denetim biriminin de bu değişime ayak uydurması önem arz edecektir (Arslan ve Özbilger, 2022). Sonuç olarak teknik denetim yetkinliğinin artırılması, kamu kurumlarını hem hukuki hem toplum güveni açısından zedeleyecek veri ihlalleri ve hizmet kesintileri gibi olumsuz sonuçlara karşı daha dirençli hale getirecektir.

Yapay zekâya dayalı sistemlerin gelişimi, eğitimden beklenen insan profilini, eğitim yapısını ve işleyişini değiştirmiş; günümüzde yapay zekâ uygulamaları, büyük veri kullanımıyla kişiselleştirilmiş eğitim programları, bireysel performans takibi, ders içeriği hazırlama ve öğretim modeli belirleme gibi işlemlerle eğitimin niteliğini yükseltmiştir. Yapay zekâ ve teknolojideki ilerlemeler, eğitimin zaman ve mekândan bağımsız hale gelmesini sağlamıştır. Dahası, yapay zekânın eğitim sistemleriyle entegrasyonu, serbest seçim, kişiselleştirilmiş öğrenme ve proje tabanlı öğrenme gibi yeni seçenekleri eğitim süreçlerine dâhil etmiştir (Coşkun ve Gülleroğlu, 2021). Devasa metin

verileri üzerinde eğitilerek insan dilini anlayabilen, işleyebilen ve insan benzeri metinler üretebilen bir yapay zekâ modeli olan (Chang vd., 2024) ve popüler örneklerini ChatGPT, Gemini, CoPilot'un oluşturduğu Büyük Dil Modellerinin hayatın her alanında kullanım senaryolarının oluşması ile öğrenme ve öğretme faaliyetleri kapsamında da araştırmalar hızla devam etmektedir (Boduroğlu ve Yigiter, 2024; Çetin ve Onan, 2025; Dündar vd., 2025; Özdemir vd., 2024). Bu çalışma ile kamu kurumlarında görev yapan iç denetçilerin bilgi güvenliği denetimleri süreçlerinde, yetkinliklerinin artırılmasına yaşam boyu öğrenme ilkeleri kapsamında katkıda bulunmayı hedeflemektedir. Büyük Dil Modeli kullanılarak oluşturulan eğitim modülleri ile iç denetçilerin bilgi güvenliği denetimlerinde daha etkin ve yetkin olmalarını sağlamak amaçlamaktadır. Çalışma, iç denetçilerin sadece mevzuat ve standartlara uyumu denetlemesinin ötesinde, siber güvenlik mimarilerini anlayarak siber olaylara karşı kurumların hazırlığını değerlendirebilen bir profil kazanmalarına yönelik Büyük Dil Modellerinin işe koşulduğu bir yol haritasını sunacaktır.

Bilgi Güvenliği

Bilgi güvenliği, günümüz dijital dünyasında bireyler, kurumlar ve devletler için hayati bir öneme sahiptir. En temel tanımıyla, bilginin; yetkisiz erişim, kullanım, açıklama, bozulma, değiştirme veya yok edilmesinden korunmasıdır. Bu koruma, sadece teknik tedbirlerle sınırlı kalmayıp, aynı zamanda yönetimsel, operasyonel ve fiziksel önlemleri de kapsayan bütüncül bir yaklaşımdır (Von Solms ve Van Niekerk, 2013). Bilgi güvenliğinin temel amacı, bilginin yaşam döngüsü boyunca üç ana niteliğini, yani gizlilik, bütünlük ve erişilebilirlik (CIA üçlüsü) ilkelerini sağlamaktır (Lundgren ve Möller, 2019). Gizlilik (Confidentiality), bilginin sadece yetkili kişilerin erişimine açık olmasını, yetkisiz kişilerin görüntülemesini engellemeyi ifade eder. Kamu kurumlarında vatandaşların kişisel verileri veya devlet sırları gibi hassas bilgileri gizlilik ilkesi kapsamında korunmalıdır; bunun sağlanması için şifreleme ve erişim kontrol mekanizmaları gibi yöntemler kullanılır. Bütünlük (Integrity), bilginin doğruluğunun, eksiksizliğinin ve güvenilirliğinin korunmasını, yetkisiz veya istem dışı değişikliklerden arındırılmasını amaçlar. Örneğin, e-Devlet üzerinden yapılan başvuruların veya kurumsal finansal kayıtların doğru ve tutarlı kalması bütünlük ilkesiyle güvence altına alınır; bu, hata kontrol mekanizmaları ve dijital imzalarla desteklenir. Erişilebilirlik (Availability) ise yetkili kullanıcıların ihtiyaç duydukları bilgilere ve bilgi sistemlerine istedikleri zaman, kesintisiz olarak ulaşabilmeleridir. Kamu hizmetlerinin sürekliliği ve acil durumlarda bilgiye hızlı şekilde erişim ihtiyacı bu ilkenin kritik önemini vurgular; yedekleme sistemleri ve felaket kurtarma planları erişilebilirliği sağlamak için elzemdir. Bu üç temel ilke, bilgi güvenliği yaklaşımlarının temelini oluşturur ve herhangi bir bilgi güvenlik stratejisi veya denetimi bu ilkelerin sağlanıp sağlanmadığını değerlendirmeyi hedefler (Stamp, 2011).

Kamu kurumları, bilgi güvenliğini kâğıt üzerinde sağlamakla kalmayıp, çeşitli özel nedenlerle daha da ciddi ele almak zorundadır (Özdemir ve Uluyol, 2021). Öncelikle, vatandaşların kişisel verilerini ve hassas bilgilerini barındıran kamu kurumları, KVKK gibi yasal düzenlemelerle ağır sorumluluklar altındadır (Aydoğdu, 2021). Bilgi güvenliği ihlalleri, sadece yasal para cezalarına değil, aynı zamanda vatandaşın devlete olan güveninin sarsılmasına ve kamu imajının zedelenmesine de yol açar (Shandler ve Gomez, 2023). Güven, kamu hizmetlerinin benimsenmesi ve etkinliği için temel bir unsur olarak kabul edilir. İkinci olarak, enerji, su, ulaşım ve sağlık gibi kritik altyapı sistemleri genellikle kamuya aittir veya kamu denetimindedir. Bu sistemlere yönelik siber saldırılar, ulusal güvenliği doğrudan tehdit edebilir, toplumda kaosa neden olabilir ve geniş çaplı ekonomik zararlara yol açabilir (Daricili ve Çelik 2021). Bilgi güvenliği, bu stratejik sistemlerin korunmasında kilit rol oynar. Üçüncüsü, siber saldırılar, kamu kurumları için ciddi maliyetler doğurabilir; veri ihlalleri sonrası oluşan kurtarma maliyetleri, yasal süreçler, itibar kaybı ve hizmet kesintileri, kamu bütçesine önemli yükler getirebilir (Cobos ve Cakir, 2024). Etkin bilgi güvenliği, bu tür riskleri minimize ederek kamu kaynaklarının verimli kullanılmasını sağlar. Son olarak, dijitalleşen kamu hizmetlerinin vatandaşlara 7/24 kesintisiz sunulması gerekliliği, bilgi güvenliğini hizmet sürekliliği için vazgeçilmez kılmaktadır. Herhangi bir siber güvenlik olayı, bu hizmetlerin kesintiye uğramasına neden olarak vatandaş mağduriyetine yol açabilir ve kamu idaresinin işleyişini aksatabilir.

Kamu Kurumlarında Bilgi Güvenliği ve Denetimi

Dijital dönüşümün hız kesmeden devam ettiği günümüz dünyasında, bilginin korunması ve yönetimi, her türlü ve özellikle kamu kurumları için hayati bir gereklilik haline gelmiştir. Bu stratejik ihtiyaca yanıt olarak ortaya çıkan Bilgi Güvenliği Yönetim Sistemleri (BGYS), bir kurumun bilgi varlıklarını tüm yaşam döngüleri boyunca korumayı hedefleyen kapsamlı, sistematik ve sürekli iyileşmeye açık bir yaklaşımdır (Çetinkaya, 2008). Bir BGYS, sadece teknik güvenlik önlemlerinden ibaret olmayıp; aksine, insan unsurlarını, süreçleri ve teknolojiyi bütünsel bir çerçevede ele alarak bilgi güvenliğinin sağlanmasında çok yönlü bir rol oynamaktadır (Tekerek, 2008). Temelinde, bir kurumun sahip olduğu değerli bilgi varlıklarını doğru bir şekilde tanımlama, bu varlıkların maruz kalabileceği riskleri detaylıca değerlendirme ve tespit edilen bu riskleri kabul edilebilir seviyelere indirmek için uygun kontrolleri titizlikle uygulama felsefesi yatmaktadır.

Bir BGYS'nin en temel ve nihai amacı, bilginin üç ana özelliğini, yani gizlilik, bütünlük ve erişilebilirlik prensiplerini kesintisiz olarak güvence altına almaktır. BGYS'nin işleyişi, genellikle sürekli iyileşmeyi temel alan Planla-Uygula-Kontrol Et-Önlem Al (PUKÖ/PDCA) döngüsü prensibine dayanır (Ünlü ve Çakmak, 2023). Bu döngü, bilgi güvenliğinin tek seferlik bir proje değil, sürekli dinamik bir süreç olduğunu vurgular. İç denetim, kuruluşların operasyonel süreçlerini, finansal raporlama faaliyetlerini ve yasal düzenlemelere uyumunu takip eden önemli bir mekanizmadır.

Günümüzde iç denetim, sadece maliyet kontrolü sağlamanın ötesine geçerek, kuruluşların bilgi güvenliğini temin etmede de kritik bir rol üstlenmektedir (Köseoğlu, 2024). BGYS'nin başarılı bir şekilde uygulanabilmesi için kuruluşların etkili iç denetim süreçlerine sahip olması şarttır. İç denetim, güvenlik protokollerinin doğru bir şekilde uygulanıp uygulanmadığını ve risklere karşı alınan önlemlerin ne kadar etkili olduğunu düzenli olarak kontrol eder. Bu denetimler, kuruluşların bilgi güvenliği gerekliliklerine uyumunu belirlemede kritik bir rol oynar ve sürekli iyileştirme sürecinin önemli bir parçasıdır.

Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi (Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi, 2019) 6 Temmuz 2019'da yürürlüğe girmiş, kamu kurumları ve kritik altyapı hizmeti sunan işletmeler için önemli yükümlülükler getirmiştir. Bu genelgeyle, güvenlik risklerinin azaltılması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda ulusal güvenliği tehdit edebilecek veya kamu düzenini bozabilecek kritik verilerin korunması amaçlanmıştır. Genelge kapsamında, farklı güvenlik seviyelerinde tedbirleri içeren bir BİG Rehberi'nin CBDDO tarafından hazırlanması ve ilgili kurumların bu rehbere uyum sağlaması öngörülmüştür. Bu doğrultuda, Temmuz 2020 tarihinde BİG Rehberi (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2021) yayımlanarak kurumların uygulaması gereken gereklilikler belirlenmiştir. Kurumların rehbere uyum aşamasında atması gereken önemli adımlardan biri olan denetim sürecinin, bağımsız bir şekilde planlanması, yürütülmesi ve raporlanması konularında Kurumlara ve denetçilere yol göstermek amacıyla da Ekim 2021 tarihinde Bilgi ve İletişim Güvenliği Denetim Rehberi yayımlanmıştır (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2021).

Denetim Rehberi, kurumların ve denetçilerin bilgi teknolojileri denetiminde uymaları gereken usul ve esasları belirtmektedir. Denetim Rehberinde;

- "Kurumun denetime yönelik yapacağı hazırlık çalışmalarına ve denetimin dış hizmet alım yoluyla gerçekleştirmesi durumunda uyulması gereken yükümlülükler"
- "Denetim metodolojisinin nasıl uygulanması gerektiğine yönelik bir çerçeve"
- "Denetim sonuçlarının Kurum tarafından CBDDO'ya gönderilmesi ve denetim sonuçları üzerinden gerçekleştirilecek gözetim faaliyetlerine yönelik bilgi"

yer almaktadır. Ayrıca, anılan Rehberde denetimin yılda en az bir kez gerçekleştirilmesi amacıyla Kurumlar tarafından gerekli planlamaların yapılması gerektiği de belirtilmektedir.

Rehberde BT Denetim ekibinde yer alacak denetçilere ilişkin nitelikler de belirtilmiştir. Buna göre; denetimi yürütecek ekipte yer alacak denetçilerin sayısı ile sahip olmaları gereken uzmanlık alanları; kurumun bilgi varlıkları, iş süreçlerinin kapsamı ve bilgi sistemlerinin karmaşıklık düzeyi göz önünde bulundurularak belirlenmeli ve denetim ekibinde en az iki denetçi yer almalıdır. BT Denetiminde yer alacak iç denetçilerin;

- ISO/IEC 27001 (Bilgi güvenliği sistemi için gerekliliklerin belirtildiği standartlar bütünü) Başdenetçi sertifikası,
- CISA (Certified Information Systems Auditor - Sertifikalı Bilgi Sistemleri Denetçisi) sertifikası,
- Belgelendirme programı kapsamında yetkilendirilmiş denetçi veya baş denetçi olmaları,
- İç tetkik veya iç denetim faaliyetlerinde bulunmuş ve bilgi sistemleri denetimi alanında eğitim almaları yetkinliklerinden en az birini sağlamış olmaları aranmaktadır (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2021).

Rehbere göre oluşturulacak denetim programı, denetim hedefi doğrultusunda iki ana başlık üzerinden hazırlanmalıdır. "Hedef 1: Rehber Uygulama Sürecinin Etkinliğinin Değerlendirilmesi" başlıklı hedefte; "kurum varlık gruplarının rehbere uygun tanımlanması, tüm bilgi varlıklarının bir gruba dâhil edilmesi, bu çalışmaların varlık envanteri ile ilişkilendirilmesi, kritiklik derecelerine göre uygun tedbirlerin belirlenmesi, mevcut durum ve boşluk analizlerinin yapılması, telafi edici kontrollerin belgelenmesi ve uygulama yol haritasının oluşturulması" gibi unsurlar yer almaktadır. "Hedef 2: Varlık Gruplarına Uygulanan Tedbirlerin Etkinliğinin Değerlendirilmesi" olarak belirlenen ikinci hedef kapsamında ise; "denetim kapsamındaki varlık gruplarına yönelik tedbirlerin etkin uygulanıp uygulanmadığının ve yerine uygulanan telafi edici kontrollerin uygunluğu ile etkinliğinin değerlendirilmesi" gerektiği belirtilmektedir.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin yayımladığı, BİG Rehberinde varlık grubu ana başlıkları;

- Ağ ve Sistemler
- Uygulamalar
- Taşınabilir Cihaz ve Ortamlar
- Nesnelerin İnterneti (IoT) Cihazları
- Fiziksel Mekânlar
- Personel olarak belirlenmiştir (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2021).

Ayrıca Rehberde; varlık gruplarına yönelik güvenlik tedbirlerinin etkin bir şekilde uygulanabilmesi için "Tehdit ve Zafiyet Yönetimi, Kimlik Doğrulama ve Erişim Yönetimi, Siber Güvenlik Olay Yönetimi, Güvenli Yazılım Geliştirme, Veri Sızıntısı Önleme, Sızma Testleri ve Güvenlik Denetimleri, Zararlı Yazılımlardan Korunma, Sanallaştırma Güvenliği, Kötücül İşlemleri Engelleme, Felaket Kurtarma ve İş Sürekliliği Yönetimi, API ve Bağlantı Güvenliği" gibi yüksek düzeyde teknik bilgi, deneyim ve güncel bilgi güvenliği standartlarına hâkimiyet gerektiren ve

nitelikli bilgi güvenliği personeli tarafından yürütülmesi gereken kritik alanlara yönelik tedbirler yer almaktadır.

Söz konusu güvenlik tedbirlerinin teknik ve operasyonel açıdan yüksek düzeyde uzmanlık gerektirmesi nedeniyle, bu alanlarda denetim gerçekleştiren iç denetçilerin de bilgi güvenliği konusunda yeterli bilgi birikimine sahip olmaları büyük önem taşımaktadır. İç denetçinin, uygulayıcı personelle aynı teknik dili konuşabilmesi; denetim sürecinde etkili iletişim kurulmasını, doğru tespitlerin yapılmasını ve alınan önlemlerin yeterliliğinin gerçekçi bir şekilde değerlendirilmesini sağlar. Bu durum, iç denetimin hem kalitesini hem de kuruma sağlayacağı katma değeri doğrudan artırmaktadır.

İç Denetim

Avrupa Birliği müzakere süreci 32'nci fasıl kapsamında, Türkiye'de kamu kurum ve kuruluşlarında, uluslararası standartlara uygun olarak iç denetim birimlerinin kurulması konusu yer almış ve bu kapsamda, 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ile iç denetim mevzuatımıza girmiştir.

Kamu idarelerinde iç denetim, 5018 sayılı Kanunun 63'üncü maddesinde; "İç denetim, kamu idaresinin çalışmalarına değer katmak ve geliştirmek için kaynakların ekonomiklik, etkililik ve verimlilik esaslarına göre yönetilip yönetilmediğini değerlendirmek ve rehberlik yapmak amacıyla yapılan bağımsız, nesnel güvence sağlama ve danışmanlık faaliyeti" olarak tanımlandıktan sonra iç denetimin, iç denetçiler tarafından yapılacağı belirtilmiştir (Kamu Malî Yönetimi ve Kontrol Kanunu, 2003).

Aynı Kanunun 64'üncü maddesinde yer alan hükümler gereğince iç denetçinin görevleri arasında; kamu idarelerinin yönetim ve kontrol yapılarını değerlendirmek, kaynakların etkili, ekonomik ve verimli kullanılması bakımından incelemeler yapmak ve önerilerde bulunmak harcama sonrasında yasal uygunluk denetimi yapmak, idarenin harcamalarının mali denetimini yapmak, malî yönetim ve kontrol süreçlerinin sistem denetimini yapmak ve bu konularda önerilerde bulunmak, denetim sonuçları çerçevesinde iyileştirmelere yönelik önerilerde bulunmak yer almaktadır. Bu kapsamda iç denetçilerin denetim alanları; mali (finansal) denetim, uygunluk denetimi, performans denetimi, sistem denetimi ve bilgi teknolojisi denetimi olmak üzere beş ana başlıkta toplanmaktadır. İç denetçiler bu görevlerini, İç Denetim Koordinasyon Kurulu tarafından belirlenen ve uluslararası kabul görmüş kontrol ve denetim standartlarına uygun şekilde yerine getirir (Kamu Malî Yönetimi ve Kontrol Kanunu, 2003).

İç denetimin tanımı ve iç denetçilerin görevleri incelendiğinde iç denetimin klasik denetim anlayışından oldukça farklı bir bakış açısına sahip olduğu ortaya çıkmaktadır. Şöyle ki; klasik denetim anlayışı genellikle yapılan yanlışları ve eksiklikleri tespit etmeyi amaçlamakta ve daha çok kurumun

geçmişte gerçekleştirdiği iş ve işlemlerine odaklanmaktadır. İç denetim ise kuruma güvence sağlamayı ve süreçlerin geliştirilmesi ve daha iyiye taşınmasına yardımcı olmayı hedeflemektedir. Risk odaklı çalışan bu sistem geçmişteki hatalardan çok ileriye dönük iyileştirmelere yoğunlaşmaktadır (Baykara, 2016).

Bir kurumun iç kontrol sistemlerinin etkinliğini değerlendirmek, riskleri yönetmek ve süreçleri iyileştirmek gibi kritik öneme sahip görevleri üstlenen iç denetçilerin hem teknik bilgi ve becerileri hem de kişisel ve etik özellikleri kapsayan önemli niteliklere sahip olmaları gerekmektedir. Bu doğrultuda, Uluslararası İç Denetçiler Enstitüsünün (IIA) "Uluslararası İç Denetim Mesleki Uygulama Standartları" esas alınarak iç denetçilerin niteliklerini ve iç denetim faaliyetinde uygulanması gereken süreçleri belirlemek üzere Kamu İç Denetim Standartları belirlenmiştir. Bu kapsamda; "1210 – Yetkinlik" başlığı altında iç denetçilerin, kişisel sorumluluklarını yerine getirmek için gereken bilgi, beceri ve diğer niteliklere ve ayrıca asıl sorumluluğu bilgi teknolojileri denetimi olan denetçiler kadar uzmanlığa sahip olmaları beklenmemekle birlikte kilit bilgi teknolojisi riskleri ve kontrolleriyle ilgili yeterli bilgiye ve teknoloji tabanlı denetim tekniklerine sahip olmak zorunda oldukları belirtilmektedir (KIDS, 2017).

İç denetim faaliyetinin gerekli yetkinliğe sahip kişiler tarafından yürütülmesini sağlayabilmek adına; iç denetçilik eleme sınavına girebilmek için en az dört yıl süreli eğitim veren yükseköğretim kurumlarından birini bitirmek ve kariyer meslek grubunda, yönetici pozisyonunda veya öğretim elemanı olarak belirli bir süre çalışmakla birlikte belirli seviyede yabancı dil bilgisine sahip olma şartlarının yerine getirilmesi aranmaktadır. Ayrıca yabancı dil şartının sağlanması da gerekmektedir. Eleme sınavını geçen iç denetçi adaylarının mesleğe atanmak için gerekli olan sertifikayı almadan önce İç Denetim Koordinasyon Kurulu tarafından koordine edilen kapsamlı bir eğitim programı sonrasında yapılan sınavda başarılı olmaları gerekmektedir (İç Denetçi Adayları Belirleme, Eğitim ve Sertifika Yönetmeliği, 2005).

Ancak aday belirleme sınav konuları ve İç Denetim Koordinasyon Kurulu tarafından koordine edilen program incelendiğinde bilgi teknolojileri denetimine yönelik daha kapsamlı olabilecekleri değerlendirilmiştir. Aday belirleme sınav konuları genel yetenek ve genel kültür, genel muhasebe ve Türkiye ekonomisi gibi genellikle üniversitelerin iktisadi ve idari bilimler fakültelerinden mezun olan adaylara yönelik alanlardan oluşmaktadır. İç denetçi adaylarının eğitim programı da;

- Denetim yöntemi ve uygulamaları;
- Muhasebe ve
- Mevzuat ana başlıklarından oluşmakta olup eğitimde bilgi teknolojileri denetimi konusuna yer verilse bile denetim, bütçe, malî kontrol, kamu ihale mevzuatı, muhasebe,

personel mevzuatı, Avrupa Birliği mevzuatı ve mesleki diğer konularda yeterli bilgi verilecek şekilde hazırlanan çok geniş eğitim konuları içerisinde bu alana yönelik olarak kapsamlı ve yeterli ölçüde eğitim verilmesine imkân bulunmamaktadır (ESY, 2005).

En az iki ay süreli olmak üzere verilen bu eğitimlerin tek başına diğer denetim alanlarında da adayların iç denetim faaliyetini yerine getirmelerinde yeterli olması beklenilmemektedir. Ancak çoğunluğunu iktisadi idari bilimler fakültesinden mezun olanların oluşturduğu iç denetçilerin almış oldukları eğitimler ve kariyer meslek mensubu olarak geçirmiş oldukları süreler; mali (finansal), mevzuat, kurumsal yönetim, risk yönetimi ve iç kontrol konularında belirli bir bilgi ve deneyime sahip olmalarına olanak sağlamaktadır. Ayrıca bu adaylar eleme sınavına tabi tutulurken muhasebe ve Türkiye ekonomisi gibi kendi uzmanlık alanlarını ilgilendiren konulardaki yeterlilikleri ölçülmektedir.

Bilgi teknolojileri denetimi ise bu konulardan bağımsız, tamamen kendine özgü nitelikler gerektiren bir alandır. Kamu iç denetçisi alımlarında bilgi teknolojileri alanından da personel istihdam edildiği görülmekte olup, bu kapsamda alınan adayların ilgili alandaki bilgi ve becerilerinin değerlendirilmesi önem taşımaktadır. Çünkü bilgi teknolojisi kapsamında başvuru hakkı tanınanlar, lisans mezuniyeti; Elektrik-Elektronik Mühendisliği, Bilgisayar Mühendisliği, Yazılım Mühendisliği, Endüstri Mühendisliği, Elektronik ve Haberleşme Mühendisliği, Haberleşme Mühendisliği, Matematik Mühendisliği, Kontrol ve Sistem Mühendisliği olanlardır (Hazine ve Maliye Bakanlığı, 2022). Bu durumdan, bu kapsamda elemeye tabi tutulan adayların tamamının uzmanlıklarının doğrudan bilgi teknolojileri alanında olmadığı anlaşılmaktadır. Ayrıca, İç Denetçilerin Çalışma Usul ve Esasları Hakkında Yönetmelikte (2006) bilgi teknolojileri denetimi alanına özgü ayrı aday belirleme sınavı yapılabileceği belirtilmekle birlikte bu kişiler de diğer adaylarla aynı konularda kendi uzmanlıkları ile ilgisi olmayan alanlarda elemeye tabi tutulmakta ve bilgi teknolojileri konusundaki yeterlilikleri eleme sınavında ölçülmemektedir. Ayrıca oldukça yeni bir alan olan BT denetimi konusunda kamu kurum ve kuruluşlarında da yeterli sayıda tecrübeye sahip iç denetçi bulunmamaktadır. Bu nedenle kurumlara yeni atanan iç denetçilerin büyük çoğunluğunun, kıdemli iç denetçilerin bu konudaki tecrübe ve bilgi birikiminden faydalanarak işe başladıktan sonra işi işte öğrenme gibi bir imkânı da bulunmamaktadır.

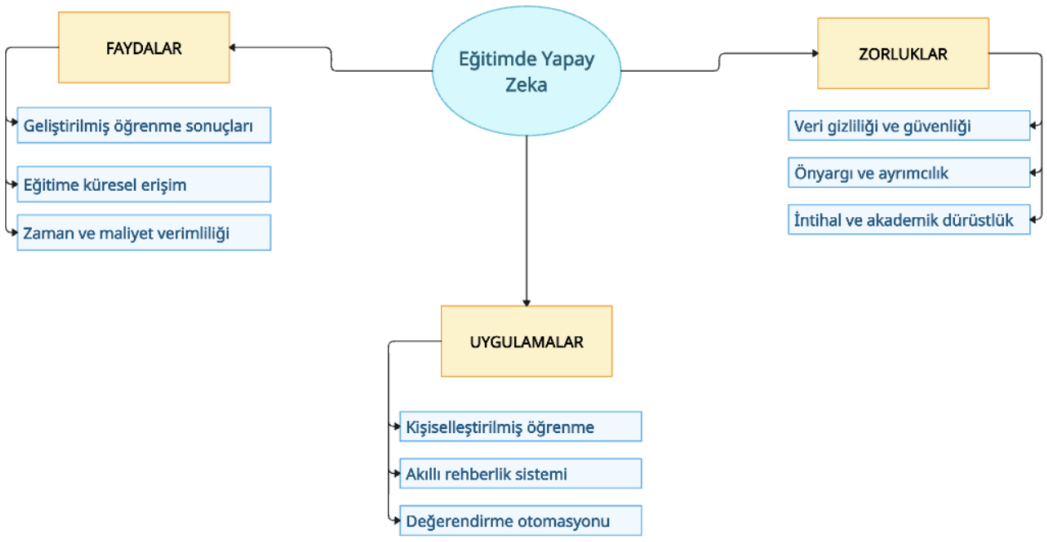
Bu doğrultuda, kapsamlı ve çok fazla konuda kısa bir süre zarfında bilgilendirme yapılmaya çalışılan sertifika eğitiminde BGYS eğitimine yeterli zamanın ayrılmasına imkân bulunmadığı da göz önünde bulundurularak; sertifika sahibi tüm iç denetçi adaylarına olmasa bile kamu kurumlarına iç denetçi olarak ataması yapılan ve fiilin bu mesleği icra eden iç denetçilere öğrenme desteği sunmak elzem durumdadır.

Yapay Zekâ ve Büyük Dil Modelleri

Yirminci yüzyılın ortalarında dijital hesap makinelerinin eğitim sistemine entegrasyonu, matematik öğretiminde önemli dönüşümler meydana getirmiştir. Bu teknolojik yeniliğin başlangıçtaki kabulleniliş süreci, eğitim camiasında farklı görüşlerin ortaya çıkmasına neden olmuştur. Bir grup eğitimci ve matematikçi, hesap makinelerinin öğrencilerin temel aritmetik becerilerini ve matematiksel kavramları kavrama kapasitelerini olumsuz yönde etkileyebileceği yönünde endişeler dile getirmişlerdir. Buna karşın, diğer akademisyenler ise hesap makinelerini, öğrencilerin matematiksel anlayışını derinleştirme ve daha karmaşık problemleri çözme yeteneklerini geliştirme potansiyeli taşıyan değerli bir araç olarak değerlendirmişlerdir. Matematik eğitiminde hesap makinelerinin kullanımına yönelik süregelen bu tartışmalara rağmen, söz konusu teknoloji küresel ölçekte sınıf ortamlarında yaygın bir kabul görmüş ve matematik öğreniminin her düzeyindeki öğrenciler için vazgeçilmez bir araç konumuna gelmiştir (Ellis ve Slade, 2023).

Benzer bir durum olarak yapay zekâ uygulamaları da günümüzde tartışma konusu haline gelmiştir. 2022 yılının sonlarında ChatGPT'nin piyasaya sürülmesi ile genel popülasyona yapay zekâdan faydalanma konusunda benzersiz bir fırsat sunulmuştur. OpenAI tarafından geliştirilen bu yapay zekâ tabanlı sohbet robotu ana akım topluma henüz yeni girmiş olmasına rağmen, yükseköğretim alanında büyük yankı uyandırmış, güncel eğitim yöntemlerini köklü bir şekilde dönüştürecek ve demode kabul edilen yaklaşımlara yeni bir soluk getirecek "çığır açıcı" bir teknoloji olarak değerlendirilmiştir (Maric vd., 2025). Yapay zekânın eğitim alanına entegrasyonunun, öğretmenler, öğrenciler ve akademik personel nezdinde bilgiye erişilebilirliği kayda değer ölçüde artırma potansiyeli taşıdığının savunulmasının yanında (Matalka vd., 2024), çeşitli çekinceleri de ortaya çıkarmıştır. Yeni nesil yapay zekâ araçlarının eğitim süreçlerine entegrasyonu, akademik dürüstlük, intihal ve öğrenci öğreniminde hesap verebilirlik başta olmak üzere çeşitli potansiyel zorlukları ve etik meseleleri beraberinde getirmek konusunda da eleştiriler almıştır (Alasadi ve Baiz, 2023). Geleneksel öğretim dinamiklerini değiştirebileceği, dolayısıyla sınıflarda yapay zekâ uygulamasına yönelik dengeli bir yaklaşımın gerekliliği savunulmuştur (Salloum, 2024).

Yapay zekânın (YZ) eğitimdeki kullanımına odaklanarak, özellikle işbirlikçi öğretmen-öğrenci öğrenimi, akıllı öğretim sistemleri, otomatik değerlendirme ve kişiselleştirilmiş öğrenme alanlarındaki uygulamalarını alanyazında inceleyen (Kamalov vd., 2023), Şekil 1 üzerinde gösterilen fayda-zarar durumunu ortaya koymuştur.



Şekil 1. Eğitimde yapay zekâ

Büyük Dil Modelleri (LLM), doğal dil söylemini anlama ve üretme yetenekleriyle Yapay Zekâ alanında bir devrim yaratmış, bu durum, LLM'lerin müzik, sanat ve hikâye anlatımı gibi çeşitli yaratıcı alanlarda kullanılmasına yol açmıştır. LLM'lerin hem insanlardan hem de makinelerden sürekli gelişen bir yaratıcı çıktı döngüsü oluşturabileceği ileri sürülmektedir. Yapay zekâ sohbet robotları, LLM'leri eğitmek ve kullanıcı girdilerine yanıt olarak yeni içerik (bilgi) üretmek için verilere yoğun şekilde bağımlı olup ChatGPT'nin ortaya çıkışıyla, LLM tabanlı sohbet robotları yapay zekâ camiasında yeni standartlar belirlemiştir (Dam vd., 2024). LLM'lerin eğitim alanındaki potansiyeli, özellikle içerik üretimi ve öğretim tasarımı bağlamında akademik araştırmaların odak noktası haline gelmiştir. Yan vd. (2024) tarafından gerçekleştirilen sistematik derleme, LLM'lerin öğrenci profillemeden otomatik değerlendirmeye, öğretmen desteğinden içerik oluşturma ve öneri sistemlerine kadar dokuz ana kategoride kullanıldığını ortaya koymuştur. Bu bağlamda içerik üretimi, soru hazırlama, ders özeti oluşturma ve kişisel öğrenme desteği öne çıkan uygulama alanları olmuştur. Eğitimde kişiselleştirilmiş içerik sunumu açısından da LLM'ler önemli fırsatlar yaratmaktadır. Uyarlanabilir öğrenme sistemlerine entegre edilen modeller, öğrencinin bilgi düzeyine göre içerik oluşturabilmekte, böylece farklılaştırılmış öğretim mümkün hale gelmektedir (Wen vd., 2024). Ayrıca ders materyali, program taslağı veya teknik eğitim modülleri geliştirme süreçlerinde, öğretmenlere taslak içerik sunma becerisiyle zaman kazandırmaktadır (Sallam, 2023). LLM'lerin insan benzeri konuşmaları taklit etme ve doğal dil işlemeyi destekleme yeteneği sayesinde öğretim yaklaşımlarını dönüştüreceğine inanılmaktadır. Bu durum, eğitmenlere öğretim görevlerini daha verimli bir şekilde yönetmelerinde yardımcı olurken, aynı zamanda öğrencilere kişiselleştirilmiş öğrenme fırsatları sunmakta, zamanında geri bildirim sağlamakta, öz-yönelimli öğrenmeyi teşvik etmekte ve işbirlikçi problem tabanlı öğrenme aracılığıyla gerçek zamanlı etkileşimi artırmaktadır (Chen vd., 2025).

Ancak oluşturulan içerik kalitesi açısından da dikkatli olunması gerektiği vurgulanmaktadır. Üretilen materyallerin pedagojik uygunluğu, bilgi doğruluğu ve ölçme geçerliliği insan uzmanlar tarafından değerlendirilmelidir (Lee vd., 2025; Meissner vd., 2024). Bu nedenle LLM çıktılarının etkin kullanımı için yönlendirilmiş istemler (prompt engineering) (Cain, 2024) ve insan geri bildirimiyle pekiştirme (RLHF) gibi teknikler önerilmektedir (Yao vd., 2023).

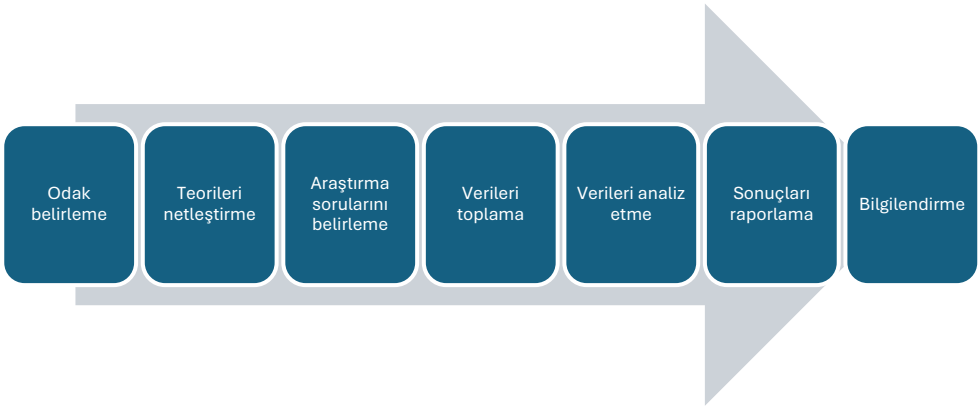
Araştırmanın Amacı

Bu çalışmanın amacı ISO 27001 belgesine sahip kamu iç denetim birimlerinde görev yapan iç denetçilerin, gerçekleştirdikleri bilgi güvenliği denetimi sürecinde teknik uzmanlarla etkin iletişim kurma, kritik sorular yöneltme ve aldıkları yanıtların geçerliliğini değerlendirme konusunda ve denetlemeye konu tedbir maddesi kapsamında bilmesi gereken teknik konuları anlama ve öğrenmeleri konusunda LLM'lerin yapacağı katkının incelenmesidir. Teşkilat yapısında uzmanlık alanlarına göre birimlere ayrılan ve farklı bilgi ve yetenekte personelin istihdam edildiği Bilgi İşlem Daire Başkanlıklarında gerçekleştirilen denetimlerde, iç denetçiler tarafından iletilen mülakat sorularına tek bir personelin değil ilgili uzmanların cevap vermesine karşılık değerlendirmenin soruyu soran iç denetçi tarafından yapılıyor olması iç deneticinin teknik bir konu hakkında bilgi eksikliğinin bulunmasını doğal kılmaktadır. Ancak ayrıntılarına önceki bölümlerde değinildiği üzere, bu durum aynı zamanda denetim faaliyetlerinin etkinliğini en üst düzeye çıkarmak için gerçekleştirilebilecek iyileştirmelerin kaynağını oluşturmaktadır. Bu çalışma esnasında gerçekleştirilen uygulamaların denetim esnasında konuya özgü teknik bilgi eksikliği bulunan iç denetçilerin bu problemlerini gidermede bir rehber olacağı, bu konuda çalışma gerçekleştirmek isteyen araştırmacılar için örnek teşkil edeceği düşünülmektedir. Bu araştırmada "Bilgi güvenliği denetimleri kapsamında, iç denetçilerin tedbir konusunda özgü teknik bilgi eksikliğini gidermesinde oluşturulacak eğitim modülüne Büyük Dil Modellerinin katkısı nedir?" sorusuna yanıt aranmaktadır.

Yöntem

Bu çalışmanın gerçekleştirilmesinde eylem araştırması yöntemi izlenmiştir. Eylem araştırması, eğitimciler gibi uygulamacıların kendi uygulamalarını geliştirmeleri, karşılaştıkları sorunlara çözüm bulmaları ve kurumsal değişim yaratmaları amacıyla kullandıkları bir araştırma yöntemidir (Mills, 2000). Yıldırım ve Şimşek (2013) eylem araştırmasını, uygulayıcıların kendi mesleki pratiklerini mercek altına aldıkları bir araştırma yöntemi olarak tarif etmiş, uygulayıcıların tek başlarına ya da bir araştırmacıyla iş birliği içinde, uygulama esnasında beliren veya zaten var olan sorunları tespit etmek, anlamak ve çözmek için veri toplayıp analiz ettiklerini belirtmişlerdir. Tezcan vd. (2016), eylem araştırmasının temelinde, katılımcıların üzerinde çalışılan duruma dair sahip oldukları pratik deneyimler ve eleştirel bakış açılarının yattığını vurgular. Bu yaklaşım, araştırmacıları da içeren bir çalışma grubuyla birlikte, insanların kendi kendilerine ve en iyi şekilde nasıl öğrenebilecekleri

sorusuna odaklanır. Sagor (2000) eylem araştırmasının Şekil 2 üzerinde gösterildiği şekliyle bir süreç izlediğini belirtmiştir.



Şekil 2. Eylem araştırması süreci

Çalışma Grubu

Bu çalışma, bir kamu kurumunun İç Denetim Birim Başkanlığında görev yapan ve ISO27001 belgesine sahip dört iç denetçinin katılımı ile gerçekleştirilmiştir.

Veri Toplama Araçları

Araştırma Günlüğü

Bu araştırmada araştırmacı; planlama, tasarım, uygulama ve raporlama aşamalarının tamamında etkin bir rol oynamıştır. Araştırmacı, siber güvenlik uzmanı kimliğiyle bilgi güvenliği denetlemelerinde denetlenen konumunda yer almakla birlikte, nitel araştırma deneyimi sayesinde sürecin her adımında aktif rol almıştır. Bu durum, araştırmanın güvenilirliğini artırmak adına gerekli etik ilkelere özen gösterilmesini sağlamıştır. Araştırmacı, araştırma konusunun belirlenmesinden alanyazın taramasına, eylem araştırması sorularının oluşturulmasından veri toplama araçlarının seçimine kadar her aşamada bizzat sorumluluk üstlenmiştir. Araştırma günlükleri, araştırmacının kendi öznel farkındalığını geliştirmesine yardımcı olurken, aynı zamanda araştırma bulgularını çok daha derinlemesine ve kapsamlı bir biçimde yorumlamayı destekleyen önemli bir araçtır (Aslan, 2025). Araştırmacı bir kamu kurumu bünyesinde bilgi işlem personeli olarak görev yapmıştır. Görev sürecinde farklı dönemlerde farklı iç denetçiler tarafından gerçekleştirilen bilgi güvenliği denetimine katılmıştır. Araştırmacı bu süreçlerde oluşan sorunlarla ilgili günlükler tutmuştur. Uygulama alanından gelen bir profesyonelin araştırmayı gerçekleştirmiş olması bağlama özgü bilgilerin elde edilmesine, alan dışı biri tarafından anlaşılmayacak örüntülerin kavranmasına katkı sağlamıştır. Yıldırım ve Şimşek (2013) araştırma günlüklerini bireyin kendine özgü görüşlerine, duygusal tepkilerine, davranışlarına ve bunları anlamlandırma biçimine ulaşmak için yararlı bir araç olarak tanımlasa da bu durum aynı zamanda öznel bir bakış açısı riski de taşımaktadır. Nitel araştırmada öznelliğin bilimselliği yok etmeden ortaya konulması, araştırmacının duruşunu belirtmesinden

geçmektedir. Araştırmacı günlüklerinin veri kaynağı olarak kullanılması, hem çalışmanın bütünlüğünü ve derinliğini artırmakta hem de araştırmacının sonrasında bu notları eleştirel bir üst bakışla değerlendirmesine ve bulgularını sürekli gözden geçirmesine olanak tanımaktadır (Fındıklı ve Saygın, 2023).

Bilgi Güvenliği Denetim Rehberi

Kamu iç denetçilerinin gerçekleştirmekle görevlendirildikleri bilgi güvenliği denetimleri CBDDO tarafından yayınlanan Bilgi Güvenliği Denetim Rehberi kapsamında gerçekleştirildiğinden ilgili rehber içeriğindeki tedbir maddeleri üzerinde çalışma gerçekleştirilmiştir.

Yapılandırılmamış Görüşme Formu

Etnografik görüşme olarak da adlandırılan yapılandırılmamış görüşme, gidişatın daha çok cevaplayıcının verdiği bilgilere göre şekillendiği, sohbet şeklinde ilerleyen, araştırma alanı hakkında gerekli ön bilginin yeterli olmadığı durumlarda esneklik sağlama avantajı oluşturan bir görüşme türüdür (Akman-Dömbekci ve Erişen, 2022). LLM'lerin iç denetçilerin teknik bilgi kapasitelerini geliştirmek için ortaya koyulacak olan eğitim modülüne olan katkısını çok yönlü olarak değerlendirebilmek, işe koşulan LLM'lerin her bir tedbir maddesi için sabit ve aynı kategori altında toplanabilecek yanıtlar üretmediği için, katılımcılardan daha çok veri toplayabilmek için geniş bir uygulama alanına sahip olan yapılandırılmamış görüşmeler uygun olarak belirlenmiştir.

Uygulama

Araştırmanın yürütülmesi adına Gazi Üniversitesi Etik Kurul başvurusu yapılmıştır. Başvuru kapsamında Gazi Üniversitesi Kurulundan 2025-1244 araştırma kod nolu etik kurul izni alınmıştır. Etik kurul izninin ardından gönüllülük onam formu ve eğitim modülleri katılımcılar ile paylaşılmış, elde edilen verilerin analizi yapılmıştır.

Uygulama Süreci

Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin yayımladığı, BİG Rehberinde varlık grubu ana başlıkları;

- Ağ ve Sistemler
- Uygulamalar
- Taşınabilir Cihaz ve Ortamlar
- Nesnelerin İnterneti (IoT) Cihazları
- Fiziksel Mekânlar
- Personel olarak belirlenmiştir. Her bir varlık grubu ana başlığı altında değişken sayıda ele alınan güvenlik tedbirleri alt başlıkları bulunmaktadır. Rehber her bir alt başlık için üç ayrı seviyede alınması gereken tedbir maddelerini sıralamış, tanımını yapmış, denetim

yöntemi ve denetim soruları için önerilerde bulunmuştur. Örneğin; "Ağ ve Sistemler" ana varlık grubu altında tanımlanan "Donanın Varlıklarının Envanter Yönetimi" alt başlığı bulunmaktadır. Bu alt başlık altında seviyesi 1 olan "Donanın Envanter İçeriğinin Yönetimi" tedbiri bulunmaktadır. Bu tedbir için önerilen denetim sorularından biri de "Donanım envanterinde; her bir donanım için ağ adresi, donanım adresi, makine adı, seri numarası, marka, model, donanımın sorumlusu ve donanımın kurum tarafından onaylı olup olmadığı bilgisi tutulmakta mıdır?" şeklindedir.

Öncelikle her bir ana varlık grubundan birer alt başlık ve her bir başlık altından da üç farklı seviyede (1, 2, 3) tedbir seçilmiş, Tablo 1 üzerinde gösterilmiştir. Seçim yapılırken bilgi güvenliği denetiminde bulunmuş olan iki iç denetçinin görüşleri araştırmacının tutmuş olduğu günlüklerdeki notlarla istişare edilerek alınmış, teknik kavramların yoğun bulunduğu alt başlıklar seçilmiştir. Personel ana varlık grubu altında bulunan tedbirler genel denetimle benzer olduğundan kapsam dışında tutulmuştur.

Tablo 1. Bilgi Güvenliği Denetim Rehberinden Çalışmaya Dahil Edilen Tedbirler

Ana Varlık Grubu	*Güvenlik Tedbiri Alt Başlığı*	*Tedbir Seviyesi*	*Önerilen Denetim Soruları*
Ağ ve Sistemler	Donanım Varlıklarının Envanter Yönetimi	1	Donanım envanterinde; her bir donanım için ağ adresi, donanım adresi, makine adı, seri numarası, marka, model, donanımın sorumlusu ve donanımın kurum tarafından onaylı olup olmadığı bilgisi tutulmakta mıdır?
		2	Cihazların veri depolama ünitelerini güvenli silmek amacıyla hangi yöntemler kullanılmaktadır?
		3	Kuruma ait güvenli ağlara bağlanan hangi donanımlar için istemci sertifikası ile kimlik doğrulaması yapılmaktadır?
Uygulamalar	Veri Tabanı ve Kayıt Yönetimi	1	Geliştirme ve/veya test ortamlarında bulunan veri tabanı, gerçek veri barındırıyor mu?
		2	Periyodik olarak kritik veri tabanı tabloları ve görüntüleri (view) üzerinde yetkilere sahip olan kullanıcılar/roller analiz ediliyor mu?
		3	Hangi verilerin maskelenerek kullanılacağı dokümante edilmiş midir?
Taşınabilir Cihaz ve Ortamlar	Akıllı Telefon ve Tablet Güvenliği	1	Mobil cihaz kullanım politikasında root veya jailbreak yapılmış cihazlar için hangi önlemler tanımlanmıştır?
		2	Mobil cihaz kullanım politikasında kurum çalışanlarının cihazlarını uzaktan fabrika ayarlarına döndürmelerini sağlayacak ayarları yapmaları istenmekte midir?
		3	Kurumun güvenlik ihtiyaçlarına göre bir mobil cihaz parola politikası belirlenmiş midir?
Nesnelerin İnterneti (IoT) Cihazları	Ağ Servisleri ve İletişimi	1	Cihazın ağ portları ve servisleri internet üzerinden erişilebilir midir?
		2	Cihazların kablosuz erişim noktalarına erişimleri güvenli erişim protokolleri ile desteklenmekte midir?
		3	Cihazlardan gönderilen kritik veri şifreli gönderilmekte midir?
Fiziksel Mekânlar	Sistem Odası/Veri Merkezine Yönelik Güvenlik Tedbirleri	1	Kablolama güvenliğini sağlamak için ne gibi kontroller uygulanmaktadır?
		2	Sistem odası/veri merkezi su, nem, sıcaklık ve duman kontrolü için üretilen veri gerçek zamanlı izlenebilmekte midir?
		3	Sistem odası/veri merkezi iklimlendirmesi için ne tip klima kullanılmaktadır?

Tablo 1 üzerinde belirlenen varlık grupları altında yer alan tedbirlerin denetlenebilmesi için önerilen soruların, iç denetçi tarafından ilgililerine yönetilmesi sonucu alacağı yanıtları etkin bir şekilde irdeleyebilmesi, doğru ekstra sorular sorabilmesi, kendisine sunulan kanıtların (log kaydı, ekran görüntüsü, rapor, kullanım kılavuzu vb.) geçerliliğini ve yeterliliğini değerlendirebilmesi için bilmesi gereken teknik içeriği (terim, çalışma mekanizması, muadili, alt dalı vb.) ona sunabilmek için LLM'lerden Gemini 2.5 flash versiyonu kullanılmıştır.

Ek-1 üzerinde şekilsel olarak gösterildiği üzere, LLM'nin istenen çıktıyı üretebilmesi için dört adım izlenmiştir.

- Birinci adımda LLM Modeli'nin bir iç denetim uzamanı çalışma prensibine göre düşünmesi için persona tanımı gerçekleştirilmiştir. Çalışma alanı fark etmeksizin her bir iç denetim uzmanının üniversite mezunu olmasından dolayı temel bilgi teknolojilerine hâkim olduğu, bilgi güvenliği denetimi yapabilmesinin ön şartı olan ISO27001 eğitimini tamamladığı model için ayrıntılandırılmıştır. Bu sayede içeriğin en basit seviyede bilgi içermesinin önüne geçilmesi amaçlanmıştır.
- İkinci adımda eğitim modülünün çıktısının belirli bir düzende olması için boş bir şablon dokümanı ve doküman üzerinde bulunan alanların açıklamalarını, birbiri ile olan bağlantılarını içeren şablon açıklama dokümanı sunulmuştur. Doküman şablonu Millî Eğitim Bakanlığı, Hayat Boyu Öğrenme Genel Müdürlüğü e-yaygın sistemi üzerinde bulunan Bilişim Teknolojileri kurs alanında bulunan içerikten uyarlanmıştır. Bu şablonun seçilmesinin temel amacı iç denetim uzmanının kendi kendine öğrenme oluşturmasını sağlamak adına Hayat Boyu Öğrenme Genel Müdürlüğü yetkinlik ve tecrübesinden faydalanmaktır. Çıktıdaki içeriğin kavramsal ve terminolojik uyumu ve tutarlılığı için CBDDO Bilgi Güvenliği Rehberi de LLM Modeli'ne öğrenmesi için sunulmuştur.
- Üçüncü adımda LLM Modeli'nin çıktıda oluşturacağı içeriğe bir sınır koyulabilmesi adına istenen derinlik seviyesi açıklanmıştır. Bu kapsamda öğrenilmesi gereken kavramlar ve kavramların birbiri ile ilgili ilişkileri, soru ile ilgili pratik uygulamalar, iki yönlü değerlendirme yapılabilmesi için risk ve zafiyetler içerik üretiminin derinliğini belirtmiştir.
- Dördüncü adım ise ilk üç adımda gerçekleştirilen LLM Modeli'nin eğitilmesi işlemlerinin istenen çıktıya dönüşmesi için gerekli talimatları içermektedir. Bir sonraki aşamada kullanıcıdan istenecek olan tetikleyici konuya (iç denetim uzmanının denetim esnasında soracağı soru) özel olarak LLM Modeli üzerinde eğitilen referans dokümanlara göre bir eğitim modülü oluşturulan aşamadır.

Bulgular

Her bir varlık grubuna ait 15 farklı denetim sorusu önerisi, oluşturulan komut modelinde tetikleyici konu olarak işleme tabi tutulmuş, her bir çıktı kayıt altına alınmıştır. Tüm çıktılar OSF https://osf.io/d6nm2/?view_only=2f7fd4d4d02b41a6a9b571cc56422c30 adresinden erişilebilir konumdadır. Ayrıntıları Ek-2 de verilen örnek eğitim modeli, Ağ ve Sistemler ana varlık grubu altında, Donanım Varlıklarının Envanter Yönetimi alt başlığı altında 2. kritiklik seviyesinde bulunan bir varlık için yöneltilen "Cihazların veri depolama ünitelerini güvenli silmek amacıyla hangi yöntemler kullanılmaktadır?" soru önerisine karşı oluşturulmuş eğitim modülünü göstermektedir.

Belirtilen eğitim modeli içerik açısından iç denetim uzmanının görüşüne sunulmuş ve aşağıda belirtilen bilgilendirme alınmıştır.

Uzman Görüşmesi-1

> İç denetim uzmanı-1: "*Öncelikle uzman görüşüme sunulan bu içerik her durumda benim konuya ilişkin bir fikir edinmemi sağlıyor. Teknik bir disiplinden eğitim almama rağmen içeriğinde kolayca anlayabileceğim ve ayırt edebileceğim kavramlar verilmiş. Kısa cümlelerle anlatılan bu konular hakkında arama motorlarında tekrar arama yaptığımda konunun daha detaylı açıklamalarına erişebileceğime inanıyorum. Ancak bazı konular LLM tarafından yanlış algılanmış olabilir ya da algılanmamış olabilir. Öğrenme kazanımları arasında yer alan "Güvenli veri silme süreçlerine ilişkin pratik uygulama adımları ve denetim senaryoları geliştirebilme." şeklinde bir kazanımdan bahsedilmiş. İç denetçinin temel rolü, süreçleri veya teknik adımları oluşturmak ya da uygulamak değil, mevcut veya olması gereken süreçleri denetlemek, sorgulamak, değerlendirmek ve doğrulamaktır. İç denetçi, operasyonel süreçlerin veya uygulama adımlarının fiilen oluşturulması veya tasarlanmasıyla doğrudan sorumlu değildir. Bu genellikle ilgili birimlerin (örneğin IT departmanları) görevidir. İç denetçi, bir geliştirici veya uygulayıcı değil, bir değerlendiricidir. İkinci bir konu ise veri üzerine yazma yaklaşımlarını ilk defa duydum. Bu benim için iyi bir şey. Ancak bu soruyu "hangi yöntemi kullanıyorsunuz?" şeklinde ilerletebilirim ancak. O an silinecek bir donanım olmayabilir."*
>
> Araştırmacı: "*İşlemi yapan kişi bir form tutuyorsa bu işlemle ilgili?"*
>
> İç denetim uzmanı-1: "*Tabi, silme işlemi için uygulanan bir politika ve prosedür olması gerekiyor. Orada silme işleminin yapılma yöntemini sorgular duruma gelirim.*"
>
> Araştırmacı: "*Başka ne söylemek istersiniz?"*
>
> İç denetim uzmanı-1: "*Stratejik önem başlığı altında yazanlar teknik içerikten daha çok zaten hali hazırda yapıyor olduğumuz denetimin özünü oluşturuyor. Dolayısıyla burada bulunmasının bir zararı yok ancak faydası da yok. Genel olarak da iç denetçinin her şeyi bilmek gibi bir misyonu yoktur. Yapılan denetim illa bir bulgu bulunacak niyeti ile gerçekleştirilmez. Amacımız denetimi yapılan iş ve işlemin 3. bir göz olarak nasıl daha iyi bir noktaya getirilebileceği çabasıdır. Burada sunulan her bilgi bu amaca hizmet edecek ve bizim için kıymetli diye düşünüyorum."*

Uzman, sunulan içeriğin konuya ilişkin fikir edinmesini sağladığını, teknik bir disiplinden gelmemesine rağmen kavramların kolay anlaşılır olduğunu belirtmiştir. Bu durum, makalenin temel amacı olan "iç denetçilerin bilgi güvenliği denetimlerindeki teknik yeterliliklerini artıracak yenilikçi bir eğitim içeriği geliştirmek" hedefiyle örtüşmektedir. Uzman, kısa cümlelerle anlatılan konuların detaylı araştırma için başlangıç noktası olabileceğine inanmaktadır. Uzman "Güvenli veri silme

süreçlerine ilişkin pratik uygulama adımları ve denetim senaryoları geliştirebilme" kazanımının, iç denetçinin rolüyle çeliştiğini belirtmiştir. İç denetçinin rolünün süreçleri veya teknik adımları oluşturmak değil, mevcut süreçleri denetlemek, sorgulamak, değerlendirmek ve doğrulamak olduğunu vurgulamıştır. Bu görüş, LLM destekli eğitim modülünün kazanım tanımlarının iç denetçi rolüyle daha uyumlu hale getirilmesi gerektiğini göstermektedir. Ayrıca "veri üzerine yazma yaklaşımlarını (disk üzerindeki verilerin geri döndürülemez şekilde silinmesi için kullanılan yöntem (Çil ve Demirci, 2024)) ilk defa duydum" demesi, modülün iç denetçide eksikliği bulunan bir teknik konu hakkında bilgilendirme yaptığını kanıtlamaktadır. Stratejik önem başlığının faydası olmadığını, ancak zararının da olmadığını belirtmesi, modül içeriğinin sadeleştirilebileceği veya ana denetim hedeflerine daha fazla odaklanabileceği anlamına gelmektedir. Uzman, iç denetçinin her şeyi bilmek gibi bir misyonu olmadığını ve amacın iş ve işlemleri daha iyi bir noktaya getirmek olduğunu ifade ederek, LLM destekli modülün bu amaca hizmet ettiğini doğrulamaktadır.

Uzman Görüşmesi-2

> İç denetim uzmanı-2: "*Görüşüm sorulan konu ile ilgili olarak "root" ve "jailbreak" kavramlarını ilk defa duydum. Normalde denetlemeye başlamadan önce denetimle ilgili kavramları internetten kendim araştırıp, bilgi sahibi olup o şekilde katılırım. Bu çıktı bana neyi öğrenmem veya bilmem gerekiyor konusunu toplu olarak gösteriyor olması güzel olmuş. Teknik bir disiplinden gelmiyorum. ISO 27001 eğitimini almaya başladığımda teknik bilgi birikimimi artıracağımı düşünmüştüm ancak o eğitimde de metodoloji öğretiliyor. Teknik detayların anlaşılması için bir içerik yok. Dolayısıyla böyle bir içeriğe erişebiliyor olmam açısından bu belge iyi olmuş. Belge içerisinde MDM/EMM terimleri de geçiyor. Bu kavramların ne olduğunu bilmiyorum. Bu sebeple internetten araştırmam gerekiyor. Bazı bölümler çok detaylı olmuş. Gördüğüm kadarı ile (eğitimci değilim ancak) bu bir müfredat değil. Bu içeriği oku da direk denetime gir şeklinde bir şey vadetmiyor. Bu sebeple daha da basit olabilir içerik. Risk ve zafiyet analizi başlığı altında yazanlar denetimde uyguladığımız "Bulgu- önem düzeyi – nedeni-risk ve etkileri" sıralamasındaki "risk ve etkileri" adımını oluşturmuş. Yapay zekâ konuya hâkim olmuş. Bu kısım bana bir bakış açısı sağlar. Bulunmasının bir zararı yok dokümanda ancak denetimde ilgili bölümü yazmak için ben bu alanı açıp okumam.*"

Uzman, "root" ve "jailbreak" kavramlarını (mobil cihazlarda üreticiler tarafından uygulanan kısıtlamaları aşarak cihaza tam yönetim yetkisi -sistemin "süper kullanıcısı" olma yetkisi- kazanmak anlamına gelmektedir. "Root" android işletim sistemli cihazlar için kullanılırken, "jailbreak" ios işletim sistemli cihazlar için kullanılmaktadır.) ilk defa duyduğunu ve normalde bu tür kavramları denetime başlamadan önce kendisinin araştırdığını belirtmiştir. Bu durum, çalışmanın belirttiği gibi, iç denetçilerin mevcut eğitim içeriklerinin bilgi teknolojileri ve siber güvenlik konularında arzu edilen teknik derinlikte olmadığı değerlendirmesini desteklemektedir. Uzman, modül çıktısının "neyi öğrenmem veya bilmem gerekiyor konusunu toplu olarak göstermesinin" güzel olduğunu ifade etmiştir. Ayrıca ISO 27001 eğitiminin metodoloji öğrettiğini ancak teknik detayların anlaşılması için bir içerik sunmadığını belirtmesi, LLM destekli modülün bu boşluğu doldurduğunu göstermektedir. Uzman, MDM/EMM (Bir organizasyonun mobil cihazlarını ve uygulamalarını merkezi olarak

yönetmek ve güvence altına almak için kullanılan çözümleri temsil etmektedir.) terimlerini bilmediğini ve internetten araştırma ihtiyacı duyduğunu belirtmiştir. Bu durum uzman tarafından bir eksiklik olarak görülse de modülün nihai amacı konu hakkında bir eğitim programı oluşturmak değil, yol gösterici olmasıdır. Bu durum uzmanın ilerleyen bölümde sunduğu "Bazı bölümlerin çok detaylı olduğunu ve modülün bir program olmadığını, daha basit olabileceğini" ifade etmesi ile de örtüşmektedir. Risk ve zafiyet analizi başlığının, denetim işlemlerinin "risk ve etkileri" adımını oluşturduğunu ve yapay zekânın konuya hâkim olduğunu, bir bakış açısı sağladığını ancak denetimde bu alanı açıp okumayacağını belirtmiştir. Bu geri bildirimler, modülün içerik derinliğinin ve sunumunun iç denetçilerin ihtiyaçlarına göre daha optimize edilebileceğini göstermektedir.

Uzman Görüşmesi-3

> İç denetim uzmanı-3: "*İç denetim görevinde verilen bilginin doğruluğu ön kabul oluyor. Çünkü bizim işimiz yapılan denetimle ilgili konuyu nasıl daha iyi bir yere taşıyabiliriz ile ilgili. Ancak adı denetleme olduğu için sanırım denetlenecek yerde size karşı doğal bir karşı durma olabiliyor. Bu sebeple böyle bir konuda sorduğunuz soruları ve aldığınız cevapları anlamadığınız durumda madara olma daha ilerisi mesleğin saygınlığına da zarar verme gibi durumlar ortaya çıkabilir. Sadece 27001 belgesi olduğu için bilgi güvenliği denetimi yapan, teknik bilgisi iyi olmayan bir iç denetçi için, rehberdeki denetimle alakalı sorduğu şeylerin neler olduğunu, ne ile ilgili olduğunu anlayarak sormasına yardımcı olacağını düşünüyorum. Belge içerisinde bazı markalar verilmiş. Ben denetimde olsam marka var mı diye değil böyle bir çözüm var mı diye bakarım. Birden fazla önlem verilmiş konu ile ilgili. Alınan önlemin biri geçilirse risk ne olur nasıl tedbir alınıyor ya da olmalı diye sorabilirim. Bağlamsal ilişkiler başlığı olmasa da olur belgede. Olursa da bir zararı olmaz. Belge 8 sayfadan oluşuyor. Yaklaşık 800 tedbir var ve her bir tedbir için belge hazırlansa büyük bir el kitabı gibi oluyor. Ancak belgenin çok yol gösterici olduğunu düşünüyorum. Teknik konuda ihtiyaç duyan kullanabilir."*

Uzman, denetimde verilen bilginin doğruluğunun ön kabul olduğunu ve işlerinin denetlenen konuyu daha iyi bir yere taşımakla ilgili olduğunu belirtmiştir. Ancak denetim sürecinde denetlenenlerin doğal bir karşı duruş sergileyebileceğini ve bu durumda soruları ve cevapları anlamamanın mesleğin saygınlığına zarar verebileceğini vurgulamıştır. Bu durum, çalışmanın "denetçilerin teknik uzmanlarla etkin iletişim kurma, kritik sorular yöneltme ve aldıkları yanıtların geçerliliğini değerlendirme kabiliyetlerini sınırlayabilmektedir" değerlendirmesini doğrulamaktadır. Uzman, sadece ISO 27001 belgesi olduğu için bilgi güvenliği denetimi yapan, teknik bilgisi iyi olmayan bir iç denetçi için modülün, rehberdeki denetimle alakalı soruları anlayarak sormasına yardımcı olacağını düşünmektedir. Uzman, modül içerisinde bazı markaların verilmesinin denetim açısından gereksiz olduğunu, önemli olanın çözümün var olup olmadığı olduğunu belirtmiştir. Ayrıca "bağlamsal ilişkiler" başlığının olmasa da olacağını ve belgenin yaklaşık 800 tedbir için hazırlanması durumunda büyük bir el kitabı olacağını, ancak modülün teknik konuda ihtiyaç duyanlar için yol gösterici olduğunu ifade etmiştir. Bu görüşler, modülün pratik kullanımda daha odaklı ve özelleştirilmiş olabileceğini göstermektedir.

Uzman Görüşmesi-4

> İç denetim uzmanı-4: "*Sistem Odası/Veri Merkezlerinde Çevresel Kontrol Verilerinin Gerçek Zamanlı İzlenmesi ve Denetimi Modülü, amacı ve kazanımları açısından iç denetçiler için önemli bir rehber niteliğinde. Söz konusu modül, denetim sürecinde ihtiyaç duyulacak bilgi, beceri ve yetkinlikleri açık bir şekilde ortaya koymakta; denetim sırasında karşılaşılabilecek olası senaryolara ilişkin örnekler sunarak odaklanılması gereken kritik alanları somutlaştırmakta. Bu çerçevede, modülde yer alan yönergeler hem denetim planlamasında hem de saha çalışmaları sırasında denetçiye sistematik bir yaklaşım kazandırmakta; özellikle çevresel risklerin tespiti, kontrol önlemlerinin yeterliliği ve sürekliliğin sağlanması gibi alanlarda yönlendirici olmaktadır. Dolayısıyla, bu modülün iç denetim faaliyetlerinde hem teknik hem de metodolojik açıdan önemli bir destek sağlayacağı ve denetim kalitesini artıracağı değerlendirilmektedir.*"

Uzman, incelediği modülün iç denetçiler için önemli bir rehber niteliğinde olduğunu ve denetim sürecinde ihtiyaç duyulacak bilgi, beceri ve yetkinlikleri açık bir şekilde ortaya koyduğunu belirtmiştir. Ayrıca modülün olası senaryolara ilişkin örnekler sunarak odaklanılması gereken kritik alanları somutlaştırdığını ifade etmiştir. Uzman, modülde yer alan yönergelerin hem denetim planlamasında hem de saha çalışmaları sırasında denetçiye sistematik bir yaklaşım kazandırdığını ve özellikle çevresel risklerin tespiti, kontrol önlemlerinin yeterliliği ve sürekliliğin sağlanması gibi alanlarda yönlendirici olduğunu vurgulamıştır. Sonuç olarak bu modülün iç denetim faaliyetlerinde hem teknik hem de metodolojik açıdan önemli bir destek sağlayacağını ve denetim kalitesini artıracağını değerlendirmiştir. Bu görüş, makalenin LLM destekli modülün iç denetim faaliyetlerine getireceği faydalar konusundaki iddialarını güçlü bir şekilde desteklemektedir.

Tartışma

Bu çalışmada, kamu iç denetçilerinin bilgi güvenliği denetimlerindeki teknik bilgi birikimlerini ve kapasitelerini güçlendirmek amacıyla LLM destekli bir eğitim modülü geliştirilmiş ve bu modelin etkinliği uzman görüşleri aracılığıyla değerlendirilmiştir. Araştırmanın temel odağını ISO 27001 sertifikasına sahip olmalarına rağmen kamu iç denetçilerinin, CBDDO tarafından yayımlanan BİG Rehberi'nin gerektirdiği teknik derinlik ve detay seviyesindeki denetimleri gerçekleştirebilmeleri için mevcut bilgi birikimlerini ve araçlarını nasıl daha ileri taşıyabilecekleri oluşturmaktadır.

Uzman görüşmeleri, LLM tarafından üretilen eğitim modüllerinin, denetçilerin teknik konulara hâkimiyetini artırmada önemli bir rol oynayabileceğini göstermiştir. Katılımcıların "root/jailbreak", "veri üzerine yazma yaklaşımları" gibi daha önce duymadıkları teknik kavramlarla bu modül sayesinde tanışmaları, mevcut eğitimlerin bu alandaki yetersizliğini ve modelin bu boşluğu doldurma potansiyelini açıkça ortaya koymaktadır. Zastudil vd. (2023) yapmış oldukları çalışmalarında öğrenenlerin LLM'leri ihtiyaç duydukları öğrenme materyalleri bulmak ve özet bilgiyi almak için geçen zamanı azaltmak için kullandıklarını belirtmişlerdir. İç denetim uzmanları da modülün denetime başlamadan önce "neyi öğrenmek veya bilmek gerektiğini toplu olarak göstermesinin" ve karmaşık konuları anlaşılır bir dille sunmasının en değerli yönleri olduğunu

vurgulamışlardır. Bu durum, LLM'nin, yoğun mevzuat ve prosedür bilgisiyle donatılmış ancak teknik altyapısı sınırlı olan denetçiler için bir "tercüman" veya "hızlandırılmış öğrenme" aracı işlevi görebileceğini düşündürmektedir. Modülün bir "program" değil, denetim anında yol gösterici bir "el kitabı" veya "rehber" olarak konumlandırılması, bu aracın en doğru kullanım senaryosunu da tanımlamaktadır. Kim vd.'ne (2023) göre LLM'ler bilimsel makalelerde yazar olarak değerlendirilmemelidir; zira tüm makaleyi üretebilecek kapasitede olsa dahi, onu kullanan yazarların en azından LLM'nin ne olduğu hakkında temel bir bilgiye sahip olmaları ve modelin ürettiği içeriği doğrulamaları, düzenlemeleri ve geliştirmeleri gerekmektedir. Dolayısıyla oluşturulan içeriğin program olarak algılanmaması bu açıdan önemlidir.

Bununla birlikte, tartışılması gereken en kritik noktalardan biri, LLM'nin bir "iç denetçi" rolünü tam olarak kavrayamamasıdır. Uzman-1'in, modülde yer alan "denetim senaryoları geliştirebilme" kazanımının denetçinin asli göreviyle (değerlendirme, doğrulama) çeliştiğini belirtmesi, yapay zekâ çıktılarının insan uzmanlığıyla doğrulanmasının ve rafine edilmesinin mutlak zorunluluğunu göstermektedir. LLM, içerik üretmede son derece yetenekli olsa da bu içeriğin mesleki rol ve sorumluluklarla tam uyumlu hale getirilmesi için insan geri bildirimine dayalı pekiştirmeli öğrenme (RLHF) gibi tekniklerin (Shypula vd., 2025) ve uzman denetiminin ne kadar hayati olduğunu (Tan vd., 2025) kanıtlamaktadır. Qu vd. (2024) genel amaçlı LLM'lerin, genel doğal dil işleme görevlerinde olağanüstü bir performans sergilemiş olsalar da kapsamlı uzmanlık bilgisi gerektiren dikey alanlarda çoğu zaman yetersiz kaldığını belirtmiş, bu sebeple alan-özel LLM'lere olan araştırma ilgisinin arttığını belirtmişlerdir. LLM'nin yanıtlarının genellikle ayrıntılı, iyi yapılandırılmış ve bilgilendirici olsa da bütüncül tanı gibi birçok tıbbi açıdan bir hekim düzeyinde performans sergilemediğini belirten Zhang vd. (2023), gerçek dünyadaki doktor-hasta etkileşimlerinin yanıt tarzlarından, hekimlerin gerçek tıbbi danışmanlıklarını öğrenip üretilecek içeriğin kalitesini artıran bir model önermişlerdir. Bu durum alanyazında belirtilen, üretilen materyallerin pedagojik ve mesleki uygunluğunun insan uzmanlar tarafından değerlendirilmesi gerektiği yönündeki uyarılarla paralellik göstermektedir. Wu vd. (2025), bir simülasyonun amacının belirsiz olduğunda, neyin doğru veya yanlış kabul edileceği, hangi senaryoların gerçek dünyayı temsil ettiği ve çıktıların beklenen sonuçlarla ne kadar eşleştiğinin net olmayacağını; bu durumun, simülasyonun sonuçlarının geçerliliğini sorgulatacağını ve pratikteki uygulanabilirliğini sınırlayacağını belirtmişlerdir. Dolayısıyla güçlü ve güvenilir simülasyonlar inşa etmek için başlangıçta hedeflerin çok iyi belirlenmesi esastır. Bu çalışma kapsamında LLM'nin uzman denetçinin görev sınırını tam olarak belirleyememesinin, sadece kitabi tanımının kendisine öğretilmiş olmasından kaynaklanmış olabileceğinin bir göstergesi olmuştur.

Bir diğer önemli tartışma konusu, modülün içeriğinin kapsamı ve derinliğidir. Uzmanlar, "Stratejik Önem" ve "Bağlamsal İlişkiler" gibi bazı başlıkların faydalı olmakla birlikte zorunlu olmadığını, içeriğin daha sade ve odaklı olabileceğini ve marka ismi gibi gereksiz detaylardan arındırılması gerektiğini ifade etmişlerdir. Bu geri bildirimler, LLM'ye sunulan talimatların (prompt engineering) daha da geliştirilerek, denetçinin pratik ihtiyaçlarına tam olarak odaklanan, daha "minimalist" ve etkili çıktılar üretilebileceğini göstermektedir. Zhang vd. (2024), LLM'leri arzu edilmeyen bir şekilde yeterli parametrik bilgileri olmadığı durumlarda belirsiz çıktılar oluşturabilmesini eleştirmiş, Pornprasit ve Tantithamthavorn (2024), talimat tasarımının LLM performansını olumlu yönde etkileyeceğini belirtmişlerdir. Razafinirina vd. (2024), LLM'lerin en ufak komut varyasyonlarına dahi yüksek hassasiyet gösterebileceğini, bu konuda istenen öğrenme hedefleriyle uyum sağlamak ve istenmeyen sonuçları engellemek için dikkatli bir komut tasarımının gerekliliğini vurgulamaktadır. Küçük bir kelime değişikliği, noktalama işareti farkı veya cümlenin yapısındaki ince bir ayarlamanın bile LLM'lerin ürettiği çıktıyı önemli ölçüde değiştirebildiğini, bu hassasiyetin bir yandan modellerin esnekliğini gösterirken, diğer yandan da doğru ve tutarlı sonuçlar elde etmek için kullanıcıdan veya geliştiriciden hassas bir yönlendirme beklentisi yarattığını belirtmektedirler.

Sonuç olarak bu çalışma, yapay zekânın ve insan uzmanlığının güçlü bir sentezini sunarak, kamu iç denetçilerinin mevcut teknik bilgi birikimlerini üst seviyelere taşıma ihtiyacına yenilikçi bir çözüm önermektedir. Bulgular, LLM destekli modülün, denetçilerin teknik özgüvenini artırarak daha etkin sorular sormalarına, aldıkları yanıtları daha iyi değerlendirmelerine ve nihayetinde denetimin kalitesini ve katma değerini yükseltmelerine yardımcı olacağını göstermektedir. Ancak bu potansiyelin tam olarak hayata geçirilmesi, modelin denetçinin rolüne uygun şekilde sürekli iyileştirilmesine ve bir "yardımcı pilot" olarak konumlandırılmasına bağlıdır. Mevcut araştırmalar, Büyük Dil Modellerinin (LLM'ler) öğretim sürecinin karmaşıklıklarını anlamada ve çeşitli öğretim içerikleri üretmede hâlâ geliştirmeye ihtiyaç duyduğunu ortaya koymaktadır (Hu vd., 2025).

Sonuç ve Öneriler

Kamu kurumlarında dijital dönüşümün hızlanması, bilgi güvenliği denetimlerinin hem kapsamını hem de önemini artırmıştır. Ancak bu kurumların denetiminden sorumlu iç denetçilerin, mevcut eğitim modellerini destekleyerek bilgi teknolojileri ve siber güvenlik alanında hedeflenen teknik derinliğe ulaşması, denetim faaliyetlerinin etkinliğini en üst seviyeye taşımak adına önemli bir gereklilik olarak değerlendirilmektedir. Bu çalışmanın temel amacı, Büyük Dil Modelleri kullanılarak geliştirilen yenilikçi bir eğitim modülü aracılığıyla kamu iç denetçilerinin teknik yeterliliklerini artırmak ve bu sayede denetim kalitesini yükseltmektir.

Araştırma sonucunda elde edilen bulgular, LLM destekli eğitim modülünün, iç denetçilerin bilgi güvenliği denetimlerine yönelik teknik bilgi eksikliklerini gidermede etkili bir araç olduğunu ortaya koymuştur. Çalışma, yapay zekâ ve insan uzmanlığının birleşimine dayanan bu hibrit modelin, denetçilere "yaşam boyu öğrenme" ilkesi doğrultusunda, ihtiyaç duydukları anda ve denetleyecekleri konuya özel olarak teknik bilgi desteği sunabildiğini kanıtlamıştır. Bununla birlikte LLM tarafından üretilen içeriğin, denetçinin rolü ve sorumlulukları ile tam uyumlu hale getirilmesi için mutlaka insan uzman (kıdemli denetçi veya alan uzmanı) tarafından gözden geçirilmesi ve rafine edilmesi gerektiği de önemli bir sonuç olarak öne çıkmıştır.

Çalışmanın sonuçları ve tartışma bölümünde yapılan değerlendirmeler ışığında, uygulayıcılara, modelin geliştirilmesine ve gelecek araştırmalara yönelik aşağıdaki öneriler sunulmuştur:

Uygulayıcılara (Kamu İç Denetçileri ve İlgili Kurumlar) Yönelik Öneriler

1. Sürekli Mesleki Gelişim Aracı Olarak Kullanım: Kamu İç Denetim birimleri, bu çalışmada önerilen modeli, denetçilerin sürekli mesleki gelişim programlarına bir "just-in-time" (tam zamanında) öğrenme aracı olarak entegre edebilir. Denetçiler, denetim planlama aşamasında, denetleyecekleri spesifik BİG Rehberi maddeleri için bu modeli kullanarak ön hazırlık yapabilirler.
2. Kritik Düşünme ve Doğrulama: Denetçiler, LLM tarafından üretilen içerikleri nihai bir doğru olarak kabul etmek yerine, bir başlangıç noktası ve araştırma rehberi olarak kullanmalıdır. Özellikle modelin önerdiği denetim kanıtları ve risk senaryoları, kurumun kendi bağlamı içinde eleştirel bir süzgeçten geçirilmelidir.

Modelin Geliştirilmesine Yönelik Öneriler

1. Rol Odaklı Talimat (Prompt) İyileştirmesi: LLM'ye verilen başlangıç talimatları, uzman görüşlerinden elde edilen geri bildirimler doğrultusunda iyileştirilmelidir. Özellikle "iç denetçinin rolünün süreç geliştirmek değil, mevcut süreci değerlendirmek, doğrulamak ve güvence sağlamak olduğu" konusunda ayrıca uzman görüşüne başvurularak LLM'nin daha isabetli kazanımlar ve içerikler üretmesi sağlanmalıdır.
2. Merkezi ve Etkileşimli Bir Platform Oluşturulması: Üretilen modüllerin statik dokümanlar olarak kalması yerine, kamu iç denetçilerinin ortak kullanımına açık, web tabanlı ve etkileşimli bir platform geliştirilebilir. Bu platformda denetçiler, denetim maddesine göre modül üretebilir, üretilen modülleri oylayabilir ve geri bildirim bırakarak modelin sürekli iyileşmesine (RLHF) katkıda bulunabilirler.

3. Çıktı Formatının Sadeleştirilmesi: Modül şablonu, uzmanların "olmasa da olur" şeklinde belirttiği "Stratejik Önem", "Bağlamsal İlişkiler" gibi bölümlerin isteğe bağlı olarak üretileceği şekilde daha esnek ve sade bir yapıda yeniden tasarlanabilir.

Gelecek Araştırmalara Yönelik Öneriler

1. Geniş Ölçekli Uygulama ve Etki Analizi: Bu çalışma, dört iç denetçi ile sınırlı bir uzman grubunu kapsamaktadır. Gelecek araştırmalar, farklı kamu kurumlarından daha geniş bir denetçi kitlesinin katılımıyla gerçekleştirilebilir. Ayrıca modelin kullanımının denetim raporlarına (bulgu sayısı, kalitesi vb.) olan nicel etkisini ölçen karşılaştırmalı çalışmalar tasarlanabilir.
2. Farklı LLM'lerin Karşılaştırılması: Bu çalışmada Gemini 2.5 flash modeli kullanılmıştır. Farklı LLM'lerin (örn. GPT-4, Llama serisi vb.) aynı talimatlarla ne tür içerikler ürettiği ve hangi modelin iç denetim bağlamında daha başarılı sonuçlar verdiği karşılaştırmalı olarak analiz edilebilir.
3. Otomatik Güncelleme Mekanizması: BİG Rehberi gibi düzenlemeler zamanla güncellenmektedir. Gelecek çalışmalarda, LLM'nin bu güncel dokümanları otomatik olarak takip edip eğitim modüllerini en son versiyona göre üretebilmesini sağlayacak teknik altyapılar araştırılabilir.

Kaynaklar

Ağdeniz, Ş. (2021). Bilgi ve iletişim güvenliği denetiminde kamu iç denetçilerinin rolü ve yetkinliklerine ilişkin bir araştırma. *Alanya Akademik Bakış*, *5*(2), 525-545. https://doi.org/10.29023/alanyaakademik.869215

Akman-Dömbekci, H. & Erişen, M. A. (2022). Nitel araştırmalarda görüşme tekniği. *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, *22*[Özel Sayı 2], 141-160. https://doi.org/10.18037/ausbd.1227330

Aksoy, C. (2024). İşletmelerin dijital dönüşümü ve dijital liderlik yaklaşımı. *Kalite ve Strateji Yönetimi Dergisi*, *4*(1), 1-29. https://doi.org/10.56682/ksydergi.1364569

Alasadi, E. A. & Baiz, C. R. (2023). Generative AI in education and research: Opportunities, concerns, and solutions. *Journal of Chemical Education*, *100*(8), 2965-2971. https://doi.org/10.1021/acs.jchemed.3c00323

Arslan, Y. & Özbilger, H. İ. (2022). Ulusal mevzuat perspektifinde bilgi işlem birimlerinin iç denetiminde bir kontrol listesi önerisi. *Denetişim*, *26*[Ek Sayı], 1-12.

Aslan, S. (2025). Eylem araştırması ile matematik öğretmen adaylarının dönüşümü: Klinik danışmanlık modeliyle ders planı hazırlama ve mesleki yeterlilik geliştirme. *Türk Eğitim Bilimleri Dergisi*, *23*(1), 173-224. https://doi.org/10.37217/tebd.1601026

Aydoğdu, Y. (2021). Kamu idaresinde kişisel verilerin korunması. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, *29*(1), 263-293. https://doi.org/10.15337/suhfd.808608

Baykara, S. T. (2016). OECD ülkelerinde iç denetim. *Denetişim*(14), 42-58.

Bilgi ve İletişim Güvenliği Tedbirleri Konulu Cumhurbaşkanlığı Genelgesi. (2019). https://cbddo.gov.tr/mevzuat/2019-12-sayili-bilgi-guvenligi-tedbirleri-cumhurbaskanligi-genelgesi/ sayfasından erişilmiştir.

Boduroğlu, E. & Yigiter, M. S. (2024). Öğretmen yapımı testler için yapay zekâ destekli geribildirim. *Journal of Applied Measurement and Assessment*, *1*(2), 50-58.

Cain, W. (2024). Prompting change: Exploring prompt engineering in large language model AI and its potential to transform education. *TechTrends*, *68*(1), 47-57. https://doi.org/10.1007/s11528-023-00896-0

Chang, Y., Wang, X., Wang, J., Wu, Y., Yang, L., Zhu, K., ..., & Xie, X. (2024). A survey on evaluation of large language models. *Acm Transactions on Intelligent Systems and Technology*, *15*(3), 1-45. https://doi.org/10.1145/3641289

Chen, X., Lin, X., Zou, D., Xie, H., & Wang, F. L. (2025). Understanding influential factors for college instructors' adoption of LLM-based applications using analytic hierarchy process. *Journal of Computers in Education*. https://doi.org/10.1007/s40692-025-00363-0

Cobos, E. V. & Cakir, S. (2024). A Review of the Economic Costs of Cyber Incidents [Advisory Services & Analytics]. World Bank Group. https://policycommons.net/artifacts/16847422/a-review-of-the-economic-costs-of-cyber-incidents-english/17732306/ sayfasından erişilmiştir.

Coşkun, F. & Gülleroğlu, H. D. (2021). Geçmişten günümüze yapay zekanın gelişimi ve eğitim alanında kullanılması. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi*, *54*(3), 947-966. https://doi.org/10.30964/auebfd.916220

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2021). *Bilgi ve İletişim Güvenliği Denetim Rehberi*. https://cbddo.gov.tr/SharedFolderServer/Projeler/File/BG_Denetim_Rehberi.pdf sayfasından erişilmiştir.

Çetin, P. & Onan, A. (2025). Büyük dil modellerinin tıp eğitimde soru yanıtlama sistemlerinde kullanımı: potansiyel, zorluklar ve gelecek yönelimleri. *Fen, Matematik ve Bilgisayar Eğitiminde Yenilikler Dergisi*, *1*(1), Article 1.

Çetinkaya, M. (2008). *Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin uygulanması*. Akademik Bilişim 2008 Konferansı'nda sunulmuş bildiri, Çanakkale Onsekiz Mart Üniversitesi, Çanakkale. https://ab.org.tr/ab08/kitap/Bildiriler/MCetinkaya_AB08.pdf sayfasından erişilmiştir.

Çil, A. & Demirci, M. (2024). Ağ adli bilişimi süreç gereksinimlerinin belirlenmesi ve yazılım tanımlı ağlarda incelenmesi. *Politeknik Dergisi*, *27*(2), 665-679. https://doi.org/10.2339/politeknik.1141107

Dam, S. K., Hong, C. S., Qiao, Y., & Zhang, C. (2024). *A complete survey on LLM-based AI chatbots* (arXiv:2406.16937). arXiv. https://doi.org/10.48550/arXiv.2406.16937

Daricili, A. B. & Çelik, S. (2021). National security 2.0: The cyber security of critical ınfrastructure. *National Security*, *26*(2), 259-276.

Dündar, R., Yeşilyurt, S., Demir, R. Z., & Yeşilyurt, A. G. (2025). Üretken yapay zekâ araçları ile sosyal bilgiler öğretimi: Avantajlar ve dezavantajlar. *Disiplinlerarası Eğitim Araştırmaları Dergisi*, *9*(20), 1-16. https://doi.org/10.57135/jier.1594253

Ellis, A. R. & Slade, E. (2023). A new era of learning: Considerations for ChatGPT as a tool to enhance statistics and data science education. *Journal of Statistics and Data Science Education*, *31*(2), 128-133. https://doi.org/10.1080/26939169.2023.2223609

ESY. (2005). İç Denetçi Adayları Belirleme, Eğitim ve Sertifika Yönetmeliği. https://ms.hmb.gov.tr/uploads/2019/09/icdenegisinseryon.pdf#page=1.00&gsr=0 sayfasından erişilmiştir.

Fındıklı, S. & Saygın, E. P. (2023). Nitel araştırmalarda araştırmacının rolü ve araştırmacı günlükleri. *Tujom*, *8*(2), 64-74. https://doi.org/10.30685/tujom.v8i2.184

Güdek, B. (2023). Kamu sektöründe etik yönetime ilişkin politikaların uygulanması: KVKK ve veri etiği. *Politik Ekonomik Kuram*, *7*(2), 237-251. https://doi.org/10.30586/pek.1325605

Hatipoğlu, C. & Tunacan, T. (2021). Türkiye'de siber saldırı ve tespit yöntemleri: Bir literatür taraması. *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi*, *8*(1), 430-445. https://doi.org/10.35193/bseufbd.838732

Hazine ve Maliye Bakanlığı. (2022). *2022 İç Denetçi Aday Belirleme Sınavı İlanı ve Başvuru Kılavuzu—T.C. Hazine ve Maliye Bakanlığı*. https://www.hmb.gov.tr/duyuru/2022-ic-denetci-aday-belirleme-sinavi-ilani sayfasından erişilmiştir.

Hu, B., Zhu, J., Pei, Y., & Gu, X. (2025). Exploring the potential of LLM to enhance teaching plans through teaching simulation. *Npj Science of Learning*, *10*(1), 1-12. https://doi.org/10.1038/s41539-025-00300-x

İç Denetçi Adayları Belirleme, Eğitim ve Sertifika Yönetmeliği. (2005). https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=9510&MevzuatTur=7&MevzuatTertip=5 sayfasından erişilmiştir.

İç Denetçilerin Çalışma Usul ve Esasları Hakkında Yönetmelik. (2006). https://mevzuat.gov.tr/MevzuatMetin/21.5.200610654.pdf sayfasından erişilmiştir.

Kamalov, F., Santandreu-Calonge, D., & Gurrib, I. (2023). New era of artificial intelligence in education: Towards a sustainable multifaceted revolution. *Sustainability*, *15*(16), 12451. https://doi.org/10.3390/su151612451

Kamu Malî Yönetimi ve Kontrol Kanunu. (2003). https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5018&MevzuatTur=1&MevzuatTertip=5 sayfasından erişilmiştir.

Kestane, A. & Kurt, G. (2024). Bulut güvenlik denetimi: Bulut siber güvenlik uygulamalarında iç denetim. *Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *17*(3), 667-690. https://doi.org/10.25287/ohuiibf.1482734

KIDS. (2017). *Kamu İç Denetim Standartları*. https://ms.hmb.gov.tr/uploads/2019/09/kamu_ic_denetim_standartlari.pdf sayfasından erişilmiştir.

Kim, J. K., Chua, M., Rickard, M., & Lorenzo, A. (2023). ChatGPT and Large Language Model (LLM) chatbots: The current state of acceptability and a proposal for guidelines on utilization in academic medicine. *Journal of Pediatric Urology*, *19*(5), 598-604. https://doi.org/10.1016/j.jpurol.2023.05.018

Köseoğlu, İ. (2024). Türk kamu yönetiminde iç denetimin gelişimi üzerine bir inceleme. *Denetişim*(30), 65-81. https://doi.org/10.58348/denetisim.1455190

Lee, D., Kim, D., Loeser, M., & Seo, K. (2025). How large language models are transforming teachers' assessment of student competency: A case study on LLM-based report writing. *2025 International Conference on Electronics, Information, and Communication (ICEIC)* içinde (s. 1-4). https://doi.org/10.1109/iceic64972.2025.10879736

Lundgren, B. & Möller, N. (2019). Defining information security. *Science and Engineering Ethics*, *25*(2), 419-441. https://doi.org/10.1007/s11948-017-9992-1

Maric, S., Maric, S., & Maric, L. (2025). *Chat-GPT: An AI based educational revolution* (arXiv:2503.04758; Versiyon 2). arXiv. https://doi.org/10.48550/arXiv.2503.04758

Matalka, M. A., Badir, R., Ahmad, A. Y. A. B., Al-Said, K., Nassar, H. T. I., Alzoubi, S., & Alzoubi, M. (2024). The adoption of ChatGPT marks the beginning of a new era in educational platforms. *International Journal of Data and Network Science*, *8*(3), 1941-1946. https://doi.org/10.5267/j.ijdns.2024.1.019

Meissner, R., Pögelt, A., Ihsberner, K., Grüttmüller, M., Tornack, S., Thor, A., Pengel, N., Wollersheim, H.-W., & Hardt, W. (2024). LLM-generated competence-based e-assessment items for higher education mathematics: Methodology and evaluation. *Frontiers in Education*, *9*, 1-13. https://doi.org/10.3389/feduc.2024.1427502

Mills, G. E. (2000). *Action research: A guide for the teacher researcher*. Pearson.

Özdemir, A. & Uluyol, Ç. (2021). Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı. *Türkiye Sosyal Araştırmalar Dergisi*, *25*(3), 649-666. https://doi.org/10.20296/tsadergisi.815635

Özdemir, F. S., Bengü, H., & Turan, E. (2024). Artificial intelligence in accounting education: Identifying learning styles and assessing individual differences. *Niğde Ömer Halisdemir Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *6*(2), 417-436. https://doi.org/10.56574/nohusosbil.1604719

Pornprasit, C. & Tantithamthavorn, C. (2024). Fine-tuning and prompt engineering for large language models-based code review automation. *Information and Software Technology*, *175*, 107523. https://doi.org/10.1016/j.infsof.2024.107523

Qu, Z., Yin, L., Yu, Z., Wang, W., & Zhang, X. (2024). *CourseGPT-zh: An educational large language model based on knowledge distillation incorporating prompt optimization* (arXiv:2405.04781). arXiv. https://doi.org/10.48550/arXiv.2405.04781

Razafinirina, M. A., Dimbisoa, W. G., & Mahatody, T. (2024). Pedagogical alignment of Large Language Models (LLM) for personalized learning: A survey, trends and challenges. *Journal of Intelligent Learning Systems and Applications*, *16*(04), 448-480. https://doi.org/10.4236/jilsa.2024.164023

Sagor, R. (2000). *Guiding school improvement with action research*. ASCD.

Sallam, M. (2023). ChatGPT utility in healthcare education, research, and practice: Systematic review on the promising perspectives and valid concerns. *Healthcare*, *11*(6), 1-20. https://doi.org/10.3390/healthcare11060887

Salloum, S. A. (2024). AI perils in education: Exploring ethical concerns. A. Al-Marzouqi, S. A. Salloum, M. Al-Saidat, A. Aburayya, & B. Gupta (Ed.), *Artificial intelligence in education: The power and dangers of ChatGPT in the classroom* (c. 144) içinde (s. 669-675). Springer, Cham. https://doi.org/10.1007/978-3-031-52280-2_43

Selimoğlu, S. K. & Saldı, M. H. (2022). Türk bankacılık sektöründe iç denetim yoluyla siber güvenlik yönetişimi. *İşletme Akademisi Dergisi*, *3*(2), 161-187.

Shandler, R. & Gomez, M. A. (2023). The hidden threat of cyber-attacks – undermining public confidence in government. *Journal of Information Technology & Politics*, *20*(4), 359-374. https://doi.org/10.1080/19331681.2022.2112796

Shypula, A., Li, S., Zhang, B., Padmakumar, V., Yin, K., & Bastani, O. (2025). *Evaluating the diversity and quality of LLM generated content* (Versiyon 1). arXiv. https://doi.org/10.48550/ARXIV.2504.12522

Stamp, M. (2011). *Information security: Principles and practice*. John Wiley & Sons.

Tan, K., Yao, J., Pang, T., Fan, C., & Song, Y. (2025). ELF: Educational LLM framework of improving and evaluating AI generated content for classroom teaching. *Journal of Data and Information Quality*, *17*(3), 1-23. https://doi.org/10.1145/3712065

Tekerek, M. (2008). Bilgi güvenliği yönetimi. *KSÜ Doğa Bilimleri Dergisi*, *11*(1), Article 1.

Tezcan, Ö., Ada, S., & Baysal, Z. N. (2016). Eğitim alanında eylem araştırmaları. *Kocaeli Üniversitesi Sosyal Bilimler Dergisi*, *32*, Article 32.

Tunçbilek, M. (2024). 2022 yılında yaşanan gelişmeler doğrultusunda bilgi güvenliğinde risk yönetiminin artan önemine ilişkin bir değerlendirme. *Bilgi ve İletişim Teknolojileri Dergisi*, *6*(1), 36-56. https://doi.org/10.53694/bited.1282138

Uslu, H. (2023). Dijital dönüşüm ve kamu hizmetleri yönetimde yenilikçi yaklaşımlar ve zorluklar. *International Journal of Political Studies*, *17*(1), 453-475. https://doi.org/10.25272/icps.1354693

Ünlü, A. M. & Çakmak, T. (2023). Kamu sektöründe kurumlar arasında bilgi paylaşımı: Türkiye'deki politika ve yasal düzenlemelere yönelik bir değerlendirme. *Bilgi Yönetimi*, *6*(1), 1-20. https://doi.org/10.33721/by.1251635

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Wen, Q., Liang, J., Sierra, C., Luckin, R., Tong, R., Liu, Z., …, & Tang, J. (2024). AI for Education (AI4EDU): Advancing personalized education with LLM and adaptive learning. *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining* içinde (s. 6743-6744). Association for Computing Machinery. https://doi.org/10.1145/3637528.3671498

Wu, Z., Peng, R., Ito, T., & Xiao, C. (2025). *LLM-based social simulations require a boundary* (Versiyon 1). arXiv. https://doi.org/10.48550/ARXIV.2506.19806

Yan, L., Sha, L., Zhao, L., Li, Y., Martinez-Maldonado, R., Chen, G., …, & Gašević, D. (2024). Practical and ethical challenges of large language models in education: A systematic scoping review. *British Journal of Educational Technology*, *55*(1), 90-112. https://doi.org/10.1111/bjet.13370

Yao, Z., Aminabadi, R. Y., Ruwase, O., Rajbhandari, S., Wu, X., Awan, A. A., …, & He, Y. (2023). *DeepSpeed-Chat: Easy, fast and affordable RLHF training of ChatGPT-like models at all scales* (Versiyon 1). arXiv. https://doi.org/10.48550/ARXIV.2308.01320

Yıldırım, A. & Şimşek, H. (2013). *Sosyal bilimlerde nitel araştırma yöntemleri.* Seçkin.

Zastudil, C., Rogalska, M., Kapp, C., Vaughn, J., & MacNeil, S. (2023). Generative AI in computing education: Perspectives of students and instructors. *2023 IEEE Frontiers in Education Conference (FIE)* içinde (s. 1-9). College Station. https://doi.org/10.1109/fie58773.2023.10343467

Zhang, H., Chen, J., Jiang, F., Yu, F., Chen, Z., Li, J., …, & Li, H. (2023). *HuatuoGPT, towards Taming Language Model to be a doctor* (Versiyon 1). arXiv. https://doi.org/10.48550/ARXIV.2305.15075

Zhang, W., Xu, Z., & Cai, H. (2024). *Defining boundaries: A spectrum of task feasibility for Large Language Models* (Versiyon 2). arXiv. https://doi.org/10.48550/ARXIV.2408.05873

Extended Summary

This study presents a novel approach to addressing a critical competency gap among public internal auditors in Türkiye. As Turkish public institutions accelerate their digital transformation, adopting e-government services and data-driven processes, their exposure to sophisticated cyber threats has significantly increased. In response, regulatory frameworks have been established, most notably the "Information and Communication Security Guide" (ICSG) published by the Presidential Digital Transformation Office (CBDDO). This guide mandates rigorous, technically-oriented information security audits to ensure the resilience of public digital infrastructure. The study highlights a notable gap between the expectations of these technical audits and the professional development needs of the internal auditors who carry them out. While these auditors are required to hold certifications like the ISO/IEC 27001 Lead Auditor, their foundational training and professional backgrounds are predominantly in non-technical fields such as law, accounting, and public administration. Consequently, the standard ISO 27001 training, which focuses on management systems and procedural compliance, fails to provide the necessary technical depth to audit complex areas like network security, secure software development, or threat management as stipulated by the ICSG. This knowledge gap limits their ability to engage in meaningful dialogue with IT specialists, ask critical follow-up questions, and accurately assess the validity of technical evidence, thereby compromising the overall effectiveness and value of the security audits.

To address the knowledge gap, the study aims to develop and evaluate an innovative, "just-in-time" training model that leverages Large Language Models (LLMs) to bridge this technical divide. The core research question is: "What is the contribution of Large Language Models to an educational module created to address the specific technical knowledge gaps of internal auditors within the scope of information security audits?". The research employed an action research methodology, a practical

and iterative approach where the researcher, a cybersecurity specialist who has experienced these audits from the auditee's perspective, actively seeks to solve a problem within their own professional context. The study was conducted with a focus group of four internal auditors, all of whom were ISO 27001 certified. The innovative application process involved several distinct steps. First, a set of technically-demanding audit questions was selected from the ICSG, covering diverse asset groups such as Networks and Systems, Applications, Mobile Devices, IoT, and Physical Spaces. The study then utilized the Gemini 2.5 flash LLM to generate a specific educational module for each selected audit question. To ensure the output was relevant and structured, the LLM was primed with a carefully crafted set of instructions and reference materials. This included a persona defining the target user as an internal auditor with a university degree and ISO 27001 certification but lacking deep technical expertise, preventing the content from being overly simplistic. It also included a template adapted from the Turkish Ministry of National Education's lifelong learning curriculum framework to promote self-directed learning and the ICSG itself to ensure terminological consistency. Finally, these AI-generated modules were presented to the expert auditors, and data on their perceptions of the modules' utility, accuracy, and relevance was collected through unstructured, in-depth interviews.

The feedback from the expert auditors overwhelmingly validated the potential of the proposed model, while also highlighting key areas for refinement. The auditors consistently affirmed that the modules were a highly valuable resource. A key finding was the module's ability to introduce them to previously unknown technical concepts. For example, auditors explicitly mentioned learning about terms like “root/jailbreak” and “data overwriting approaches” for the first time through the modules. This directly confirmed the existence of the knowledge gap the study set out to address. The auditors praised the modules for providing a concise and accessible overview of what they “need to know” before an audit, serving as an excellent starting point for further research. They noted that this filled a significant void left by standard ISO 27001 training, which is primarily methodological rather than technical. Furthermore, auditors felt that being equipped with this knowledge would enhance their ability to ask more insightful questions and understand technical responses, thereby boosting the quality of the audit and upholding their professional credibility. One expert summarized the tool as an “important guide” that provides a “systematic approach” to both planning and fieldwork.

However, the expert feedback also provided crucial critical insights. The most significant critique was the LLM's occasional failure to grasp the nuanced role of an internal auditor. One expert pointed out that a learning outcome suggesting the auditor would “develop... denetim senaryoları” (develop... audit scenarios) was incorrect; an auditor's role was to evaluate existing processes, not create them. This highlights the indispensable need for human expert oversight to ensure the AI-generated content is professionally and pedagogically sound, a finding that aligns with existing

literature on the limitations of AI in education. Other critiques were related to content optimization. Auditors suggested that sections like “Strategic Importance” and “Contextual Relationships” were redundant and that the inclusion of specific brand names was unhelpful. They also noted that if a module were generated for all 800+ controls in the ICSG, it would result in an impractically large manual, suggesting a need for a more dynamic delivery platform.

Ultimately, the study successfully demonstrated that a hybrid model combining the rapid content generation capabilities of LLMs with the contextual expertise of human auditors could provide a powerful solution to a persistent problem in public sector governance. The LLM acted as a “technical translator” or “cognitive accelerator”, quickly providing auditors with the foundational knowledge needed to navigate complex IT environments. The findings confirmed that the model was not a replacement for the auditor but rather a “support tool” or “just-in-time” learning aid. Critical feedback underscored that AI-generated content could not be used off-the-shelf and required a “human-in-the-loop” approach, where experts refined prompts and validated outputs to align them with the specific roles and responsibilities of the profession. In conclusion, this research proposed a practical and effective model to enhance the technical competencies of public internal auditors. By enabling them to conduct more informed and in-depth security audits, this approach has the potential to significantly improve the quality and impact of public sector audits, thereby contributing to the overall cyber resilience and security of Türkiye’s national digital infrastructure. The study's recommendations include the formal adoption of this model in continuous professional development programs, the refinement of LLM prompts to be more role-specific, the development of a centralized web platform for module generation and sharing, and further research to quantify the model's impact on audit quality and compare the efficacy of different LLMs.

Ekler

EK-1: LLM’nin Eğitilmesi Esnasında Uygulanan Komutlar

Sana öğrenmen için gerekli olan 4 adımı sırasıyla vereceğim. 5. adımda ilk 4 adımı uygulaman için tetikleyici konuyu vereceğim. Buna göre Ana görevi gerçekleştireceksin.

ADIM 1: PERSONA TANIMLAMASI

Rolüm: “Bir İç Denetim Uzmanı”

ISO 27001 Eğitimini tamamladın. Temel bilgi teknolojileri konularını biliyorsun. Bu rol çerçevesinde düşünecek, bu rolün bilgi seviyesine ve bakış açısına uygun bir dil ve içerik üreteceksin.

ADIM 2: REFERANS DOKÜMANLARI ÖĞRENME

Sana üç adet referans doküman sunacağım. Göreve başlamadan önce bu üç dokümanın yapısını ve içeriğini detaylarıyla öğrenmelisin.

1. **Referans Doküman 1 (Şablon Doküman):** Bu doküman, oluşturulacak nihai çıktının **yapısal şablonunu** belirler.

Şablon Doküman Adı: şablon.docx

2. **Referans Doküman 2 (Şablon Açıklama Dokümanı):** Bu doküman, "**Referans Doküman 1"** içerisinde bulunan alanların açıklamalarını içermektedir.

Şablon Doküman Adı: şablon_açıklama.docx

3. **Referans Doküman 3 (İçerik ve Bağlam Dokümanı):** Bu doküman, uzmanlık alanının **bilgi kaynağını ve bağlamını** oluşturur. Bu dokümanın içeriğine tamamen hâkim olmalı ve bir uzman gibi davranmalısın. Çıktıdaki içerik, bu dokümandaki kavramlar ve terminoloji ile tutarlı olmalıdır.

İçerik Doküman Adı: bg_rehber.pdf

ADIM 3: İSTENEN DERİNLİK SEVİYESİ

Seviye: İleri Seviye (Derinlemesine)

Bu seviyede içerik üretilirken aşağıdaki hususlara dikkat edilmelidir:

- **Kavramların Detaylandırılması:** Sadece kavramın tanımı değil, alt bileşenleri, türleri (örn: IP Adresi için IPv4/IPv6, Statik/Dinamik) ve teknik çalışma prensipleri de açıklanmalıdır.
- **Pratik Uygulama:** Konuyla ilgili pratik uygulama adımları, komut satırı örnekleri veya denetim senaryoları sunulmalıdır.
- **Risk ve Zafiyet Analizi:** Konuyla ilgili potansiyel riskler, zafiyetler veya yanlış yapılandırma senaryoları belirtilmelidir.
- **Bağlamsal İlişki:** Farklı kavramların birbiriyle olan teknik veya mantıksal ilişkisi (örn: IP, MAC ve Hostname ilişkisi) kurulmalıdır.

ADIM 4: ANA GÖREV TANIMI

Oluşturulacak Çıktı: Bir eğitim modülü.

Tetikleyici Konu:

Aşağıda, Referans Doküman 3'ten alınmış olan spesifik bir konu/soru/madde yer almaktadır. Oluşturulacak tüm modül, bu konuyu açıklamak üzerine kurulacaktır:

Modülün Amacı:

Oluşturulacak eğitim modülünün temel amacı, yukarıdaki 'Tetikleyici Konu'da geçen kavramları, bir uzmanın (bkz. Persona) bu konuyu denetleyebilmesi, sorgulayabilmesi veya kendisine verilen cevapların doğruluğunu değerlendirebilmesi için gereken tüm teknik ve idari derinlikle açıklamaktır.

Yapısal Kısıtlama:

Oluşturulacak modül, birebir olarak Referans Doküman 1'in yapısını (başlıklar, tablolar, bölümler) kullanmalıdır.

İçerik Kısıtlaması:

İçerik, 'Tetikleyici Konu'yu açıklamak için özgün olarak oluşturulmalı ve Referans Doküman 3'teki bağlama uygun olmalıdır. İçerik Referans Doküman 2'de belirtilen açıklamalara göre yapılandırılmalıdır.

Örnek Kullanım

Tetikleyici Konu:

Cihazların veri depolama ünitelerini güvenli silmek amacıyla hangi yöntemler kullanılmaktadır?

EK-2: Örnek Eğitim Modülü

MODÜL BİLGİ SAYFASI

MODÜL ADI: Cihazların Veri Depolama Ünitelerini Güvenli Silme Yöntemleri ve İç Denetim Perspektifi

MODÜLÜN SÜRESİ: 6 Ders Saati

MODÜLÜN AMACI:

Bu modül, cihazların veri depolama ünitelerinin güvenli bir şekilde silinmesi için kullanılan yöntemleri, teknik detayları, stratejik önemini, pratik uygulamalarını, potansiyel risklerini ve bağlamsal ilişkilerini "İç Denetim Uzmanı" perspektifinden derinlemesine açıklamayı amaçlamaktadır. Modül sonunda katılımcılar, ilgili süreçleri denetleyebilme, sorgulayabilme ve verilen cevapların doğruluğunu değerlendirebilme yetkinliğine sahip olacaklardır.

ÖĞRENME KAZANIMLARI:

A. Veri depolama ünitelerini güvenli silme yöntemlerini ve teknik çalışma prensiplerini ileri düzeyde açıklayabilme.

B. Güvenli veri silmenin bilgi güvenliği ve denetim süreçleri açısından stratejik önemini analiz edebilme.

C. Güvenli veri silme süreçlerine ilişkin pratik uygulama adımları ve denetim senaryoları geliştirebilme.

D. Güvenli veri silme süreçlerindeki potansiyel riskleri, zafiyetleri ve yanlış yapılandırma senaryolarını tespit edebilme.

E. Veri silme yöntemlerinin ilgili bilgi güvenliği kavramları ve yasal düzenlemelerle bağlamını kurabilme.

KAZANIM / BAŞARIM ÖLÇÜTLERİ:

KAZANIM	*BİLGİ*	*BECERİ*
A	1. Fiziksel imha, manyetik imha (degaussing) ve veri üzerine yazma (overwrite) yöntemlerinin temel prensiplerini ve teknik işleyişini açıklar. 2. Yazılımsal veri üzerine yazma yöntemlerinde kullanılan farklı paternleri (örn: Gutmann, DoD 5220.22-M, Heri) ve bunların güvenilirlik seviyelerini karşılaştırır. 3. SSD'ler (Katı Hal Sürücüleri) için güvenli silme yöntemlerinin (örn: Secure Erase, Crypto Erase) HDD'lerden farklılıklarını ve gerekçelerini ifade eder.	1. Belirli bir senaryo için en uygun güvenli veri silme yöntemini belirleyebilir. 2. Farklı veri silme yöntemlerinin potansiyel veri kurtarma risklerini değerlendirebilir.
B	1. Güvenli veri silmenin KVKK/GDPR gibi veri koruma mevzuatlarına uyum açısından önemini detaylandırır. 2. Güvenli veri silmenin kurumun itibar yönetimi, hukuki sorumlulukları ve siber güvenlik olaylarına müdahale süreçlerindeki yerini analiz eder. 3. Veri yaşam döngüsü yönetiminde güvenli veri silmenin kritik aşama olduğunu gerekçeleriyle açıklar.	1. Kurum içindeki veri imha politikalarının mevzuata ve en iyi uygulamalara uygunluğunu denetleyebilir. 2. Veri sızıntısı riskini azaltmada güvenli veri silmenin rolünü açıklayan bir senaryo sunabilir.
C	1. Linux ortamında shred, dd ve wipe gibi komut satırı araçlarının veri silme amaçlı kullanımını ve parametrelerini açıklar. 2. Ticari veri silme yazılımlarının (örn: DBAN, Blancco) özelliklerini ve kurumsal kullanım senaryolarını karşılaştırır. 3. Fiziksel imha süreçlerinde kullanılan cihazların (öğütücü, parçalayıcı) teknik standartlarını ve kapasitelerini tanımlar.	1. Veri silme sürecinin denetimi için bir kontrol listesi oluşturabilir. 2. Bir denetim senaryosunda, veri silme işleminin doğru uygulandığını doğrulamak için yapılması gereken adımları (örn: log inceleme, rastgele kontrol) belirleyebilir. 3. Veri depolama birimi imha sertifikalarının içeriğini ve geçerliliğini değerlendirebilir.

D	1. Yetersiz veya yanlış uygulanan veri silme yöntemlerinin veri kurtarma risklerini (örn: adli bilişim teknikleri) analiz eder. 2. Manyetik imha (degaussing) sonrası kalan artık manyetizma risklerini ve doğrulanması gerektiğini açıklar. 3. Yazılımsal silme yöntemlerinde bypass edilebilecek zafiyetleri (örn: SSD aşınma dengeleme, dosya sistemi meta verileri) ve alınabilecek önlemleri tartışır.	1. Kurumun veri imha süreçlerindeki olası zafiyetleri ve yanlış yapılandırmaları tespit edebilir. 2. Belirlenen risklere karşı düzeltici ve önleyici denetim bulguları önerebilir.
E	1. "Veri yaşam döngüsü yönetimi" ve "güvenli veri silme" arasındaki ilişkiyi açıklar. 2. "Envanter yönetimi" ile "güvenli veri silme" süreçlerinin bütünsel önemini analiz eder. 3. "Olay müdahale planı" kapsamında güvenli veri silmenin rolünü ve zamanlamasını belirler.	1. Güvenli veri silme politikalarının, kurumun genel bilgi güvenliği politikalarıyla uyumunu değerlendirebilir. 2. Bir varlık elden çıkarma senaryosunda, veri silme sürecinin diğer bilgi güvenliği süreçleriyle entegrasyonunu açıklayabilir.

UYGULAMAYA İLİŞKİN AÇIKLAMALAR:

1. **Kavramların Detaylandırılması: Veri Silme Yöntemleri**
   - **Veri Üzerine Yazma (Overwrite):** Bu yöntem, depolama birimindeki mevcut verilerin üzerine rastgele veya belirli paternlerde yeni veriler (genellikle sıfırlar veya birler) yazılarak eski verilerin okunamaz hale getirilmesidir. Tek seferlik yazmadan çok geçişli yazmaya kadar farklı yaklaşımları vardır.
     - **Tek Geçişli Yazma:** Verinin üzerine sadece bir kez sıfır veya rastgele karakter yazılır. Hızlıdır ancak modern veri kurtarma tekniklerine karşı daha zayıf kalabilir.
     - **Çok Geçişli Yazma:** Verinin üzerine birden fazla kez farklı paternlerde (örn: 0x00, 0xFF, rastgele karakterler) yazma işlemi uygulanır. Daha güvenlidir ancak daha uzun sürer. En bilinen standartlar şunlardır:
       - **DoD 5220.22-M:** ABD Savunma Bakanlığı standardı. Genellikle üç geçişli bir algoritma kullanır (birinci geçiş 0x00, ikinci geçiş 0xFF, üçüncü geçiş rastgele karakter ve son doğrulama). Bazı versiyonları yedi geçişe kadar çıkabilir.
       - **Gutmann Yöntemi:** 35 geçişli, oldukça yavaş ancak çok güvenli bir yöntemdir. Özellikle eski depolama teknolojileri için geliştirilmiştir. Artık modern sürücüler için çoğu zaman gereksiz görülse de, maksimum güvenlik arayışında hala referans alınır.
       - **Heri Temizleme:** 9 geçişli bir yöntemdir.
     - **Teknik Çalışma Prensibi:** Bu yöntem, manyetik disklerin (HDD) sektörlerindeki manyetik kutupları değiştirerek veriyi siler. Bir verinin üzerine yeni bir veri yazıldığında, eski manyetik izler tamamen bozulur. Ancak, çok eski ve özel donanımlar kullanılarak zayıf yöntemlerle yazılmış verilerin "gölge" verileri üzerinden kısmi kurtarılması teorik olarak mümkündür, bu yüzden çok geçişli yöntemler tercih edilir.
     - **Uygulama Alanları:** Çalışır durumdaki HDD'ler, USB bellekler, SD kartlar.
   - **Manyetik İmha (Degaussing):** Bu yöntem, güçlü bir manyetik alan (degausser) oluşturarak manyetik depolama ortamlarındaki (HDD, manyetik bantlar) verileri okunamaz hale getirir. Manyetik alan, disk plakalarındaki manyetik alanların yönünü rastgeleleştirerek depolanan verileri bozar.
     - **Türleri:**
       - **Darbe Degaussing:** Kısa ve yüksek yoğunluklu manyetik darbe gönderir.
       - **Sürekli Degaussing:** Sürekli manyetik alan oluşturur.
     - **Teknik Çalışma Prensibi:** Manyetik ortamların fiziksel yapısını değiştirmez, ancak manyetik domenlerin hizalanmasını kalıcı olarak bozar. Degaussing işlemi sonrası diskler genellikle tekrar kullanılamaz hale gelir (çünkü düşük seviyeli formatlama bilgileri de bozulur).

- **Uygulama Alanları:** HDD'ler, manyetik bantlar, floppy diskler. SSD'ler için etkili değildir çünkü NAND tabanlı bellekler manyetik prensiple çalışmaz.

- **Fiziksel İmha:** Depolama biriminin fiziksel olarak kullanılamaz hale getirilmesidir. Bu, öğütme (shredding), parçalama (disintegration), yakma (incineration) veya eritme (melting) gibi yöntemlerle yapılabilir.
  - **Teknik Çalışma Prensibi:** Veri depolanan plakaların, yongaların veya diğer bileşenlerin fiziksel bütünlüğünü yok ederek veriye erişimi imkânsız kılar.
  - **Uygulama Alanları:** Tüm depolama birimleri (HDD, SSD, CD/DVD, USB bellekler, cep telefonları vb.). Genellikle en güvenli yöntem kabul edilir.
- **SSD'ler için Güvenli Silme (Secure Erase/Crypto Erase):** SSD'ler, HDD'lerden farklı olarak Wear Leveling (aşınma dengeleme) ve Over-Provisioning gibi teknolojiler kullanır. Bu durum, üzerine yazma yöntemlerinin her zaman tüm verilere ulaşamayabileceği anlamına gelir.
  - **Secure Erase (ATA Secure Erase):** SSD'lerin kontrolcüsü tarafından desteklenen bir komuttur. Bu komut, tüm NAND bellek hücrelerini elektriksel olarak sıfırlayarak veya depolanan verileri kriptografik olarak yok ederek fabrika ayarlarına döndürür. Verimli ve hızlıdır, ayrıca tüm depolama alanının silindiğinden emin olunmasını sağlar.
  - **Crypto Erase:** Eğer SSD donanımsal şifrelemeye sahipse (self-encrypting drive - SED), depolanan veri aslında her zaman şifrelenmiş durumdadır. Bu durumda, kriptografik anahtarın silinmesi (crypto erase) veriyi anında erişilemez hale getirir. Bu, en hızlı ve çoğu zaman en güvenli yöntemlerden biridir.

2. **Stratejik Önem:**
   - **Veri Gizliliği ve KVKK/GDPR Uyum:** Kurumların elden çıkardığı veya kullanım ömrü biten cihazlardaki kişisel verilerin, hassas bilgilerin veya ticari sırların kötü niyetli kişilerin eline geçmesini engellemek kritik öneme sahiptir. Güvenli veri silme, Kanun Hükmünde Kararname (KVKK) ve Genel Veri Koruma Tüzüğü (GDPR) gibi yasal düzenlemelerin getirdiği "veri ihlali" risklerini minimize ederek hukuki uyumluluğu sağlar. Aksi takdirde, ciddi para cezaları ve itibar kaybı yaşanabilir.
   - **Kurumsal İtibar ve Güven:** Veri sızıntıları, kurumların kamuoyundaki imajını ciddi şekilde zedeleyebilir, müşteri güvenini sarsabilir ve uzun vadeli iş ilişkilerine zarar verebilir. Güvenli veri silme, bu tür olumsuz senaryoları önleyerek kurumun itibarını korur.
   - **Siber Güvenlik Postürü:** Cihazların elden çıkarılması veya yeniden kullanılması durumunda, eski verilerin kalması siber saldırganlar için bir zafiyet noktası oluşturabilir. Güvenli silme, bu tür arka kapıları kapatarak kurumun genel siber güvenlik postürünü güçlendirir. Özellikle Bilgi ve İletişim Güvenliği Rehberi kapsamında belirtilen "Varlık Gruplarına Yönelik Güvenlik Tedbirleri" başlığı altında "Taşınabilir Cihaz ve Ortam Güvenliği" ve "Fiziksel Mekanların Güvenliği" gibi konularla doğrudan ilişkilidir.

3. **Pratik Uygulama ve Denetim Senaryoları:**
   - **Yazılımsal Uygulama Örnekleri (Linux):**
     - **shred komutu:** Dosyaların veya disklerin üzerine birden fazla kez yazarak güvenli bir şekilde silinmesini sağlar.

       Bash
       ```
       shred -v -n 3 -z /dev/sda  # /dev/sda diskini 3 kez rastgele veriyle üzerine yazar, son olarak sıfırlarla doldurur ve ilerlemeyi gösterir.
       shred -u -n 1 /path/to/file.txt # Dosyayı 1 kez rastgele veriyle üzerine yazar ve ardından siler.
       ```

- **dd komutu ile sıfırlama:** Diskin tamamını sıfırlarla doldurmak için kullanılabilir. Daha hızlıdır ancak shred kadar güvenli değildir.

  Bash
  ```
  dd if=/dev/zero of=/dev/sda bs=1M status=progress # /dev/sda diskini tamamen sıfırlarla doldurur.
  ```

- **wipe aracı:** Çeşitli veri silme paternlerini destekleyen bir araçtır.

  Bash
  ```
  sudo apt-get install wipe # Kurulum (Debian/Ubuntu tabanlı sistemlerde)
  wipe -r -f /dev/sdb # /dev/sdb diskini güvenli bir şekilde siler (varsayılan paternlerle)
  ```

- **Kurumsal Çözümler:**
  - **DBAN (Darik's Boot and Nuke):** Açık kaynaklı, önyüklenebilir bir araçtır. Bilgisayarın tüm disklerini güvenli bir şekilde silmek için kullanılır. Çeşitli silme algoritmalarını (DoD, Gutmann vb.) destekler.
  - **Blancco/Certus Erasure:** Ticari çözümler olup, denetlenebilir ve sertifikalı veri silme hizmetleri sunar. Büyük ölçekli kurumsal veri imha süreçleri için tercih edilir.
- **İç Denetim Senaryosu:**
  - **Senaryo:** Bir kurum, kullanım ömrünü tamamlamış 100 adet bilgisayarın sabit disklerini imha etmeye karar vermiştir. Denetim ekibi olarak bu sürecin güvenli ve politika uyumlu bir şekilde ilerlediğini doğrulamamız gerekmektedir.
  - **Denetim Adımları:**
    1. **Politika ve Prosedür İncelemesi:** Kurumun "Veri İmha Politikası" ve "Varlık Yönetimi Prosedürü"nün güncel ve uluslararası standartlara (örn. NIST SP 800-88) uygun olup olmadığını değerlendirin. Politikada hangi veri silme yöntemlerinin tercih edildiği, hangi varlıklar için hangi seviyede silme gerektiği, sorumluluklar ve belgeleme gereksinimleri kontrol edilmelidir.
    2. **Süreç Denetimi:** İmha edilecek cihazların envanter kayıtlarının doğru ve eksiksiz tutulduğunu doğrulayın. İmha sürecini gerçekleştiren personelin yetkinliğini ve eğitimlerini kontrol edin.
    3. **Yöntem Doğrulaması:** Kullanılan veri silme yöntemlerinin (yazılımsal, manyetik, fiziksel) politika ile uyumlu olduğunu gözlemleyin. Eğer yazılımsal silme kullanılıyorsa, kullanılan yazılımın veya komutların doğru paternleri uyguladığından emin olun.
    4. **Kayıt ve Belgeleme:** Her bir cihaz için veri silme/imha işleminin başarılı olduğuna dair oluşturulan log kayıtlarının, sertifikaların veya imha raporlarının eksiksiz ve doğrulanabilir olduğunu kontrol edin. Bu belgelerin yasal ve kurumsal gereksinimleri karşıladığından emin olun. Özellikle ticari araçlar kullanılıyorsa, bunların sunduğu sertifikaların güvenilirliği incelenmelidir.
    5. **Rastgele Kontrol (Spot-Check):** İmha edilen disklerden rastgele örnekler seçilerek, üzerinde herhangi bir veri kalıntısının olup olmadığını kontrol etmek için adli bilişim teknikleri (veri kurtarma yazılımları, hex editörler) ile analizler yapılması önerilir. Bu, uygulanan yöntemin etkinliğini doğrular.
    6. **Fiziksel Güvenlik:** İmha öncesi ve sonrası depolama birimlerinin fiziksel güvenliğinin (depolama alanı, taşıma, imha tesisinin güvenliği) sağlanıp sağlanmadığını denetleyin.

4. **Risk ve Zafiyet Analizi:**
   - **Yetersiz Silme Yöntemleri:** Sadece "sil" tuşuna basmak veya disk formatlamak, veriyi kalıcı olarak silmez. Veriler kolayca kurtarılabilir.
   - **SSD'lerdeki Zorluklar:** Aşınma dengeleme (Wear Leveling) ve gizli alanlar (Over-Provisioning) nedeniyle yazılımsal üzerine yazma yöntemleri SSD'lerin tüm alanına ulaşamayabilir, bu da veri kalıntılarına yol açabilir. Bu nedenle SSD'ler için ATA Secure Erase veya Crypto Erase gibi spesifik yöntemler kullanılmalıdır.
   - **Manyetik İmha (Degaussing) Sonrası Kalıntılar:** Yetersiz güçlü bir degausser kullanılması veya degaussing işleminin doğru yapılmaması durumunda, disk üzerinde okunabilir manyetik izler kalabilir. Degaussing sonrası diskin çalışıp çalışmadığı kontrol edilmeli ve çalışmaması, işlemin başarılı olduğuna dair bir gösterge olarak kabul edilmelidir.
   - **Fiziksel İmha Eksiklikleri:** Disklerin yeterince küçük parçalara ayrılmaması veya anahtar veri depolama yongalarının (örn: NAND çiplerinin) tamamen imha edilmemesi durumunda veri kurtarma riski devam eder.
   - **Belgeleme ve İzlenebilirlik Eksikliği:** Hangi cihazın ne zaman, kim tarafından, hangi yöntemle silindiğinin kaydının tutulmaması, denetim izi bırakmaz ve olası bir veri ihlali durumunda sorumluluğun belirlenmesini zorlaştırır.
   - **Üçüncü Taraf Riskleri:** Veri imha işlemi bir üçüncü tarafa yaptırılıyorsa, bu hizmet sağlayıcının güvenlik protokolleri, yetkinlikleri ve sertifikasyonları denetlenmelidir. Sözleşmelerde veri imha yükümlülükleri açıkça belirtilmelidir.

5. **Bağlamsal İlişkiler:**
   - **Veri Yaşam Döngüsü Yönetimi (DLM):** Güvenli veri silme, verinin oluşturulmasından arşivlenmesine ve nihai olarak imha edilmesine kadar olan DLM sürecinin kritik son aşamasıdır. Verinin kullanım süresi dolduğunda, uygun ve güvenli bir şekilde imha edilmesi, tüm yaşam döngüsünün güvenliğini sağlar.
   - **Varlık Yönetimi:** Kurumun sahip olduğu tüm donanım ve depolama birimlerinin envanterinin doğru tutulması, bunların ne zaman ve nasıl elden çıkarıldığının izlenmesi, güvenli veri silme süreçlerinin ayrılmaz bir parçasıdır. Envanterde olmayan bir cihazın güvenli silinmesi gözden kaçabilir.
   - **Olay Müdahale ve Felaket Kurtarma:** Bir siber güvenlik olayı veya felaket durumunda, etkilenen sistemlerdeki verilerin güvenli bir şekilde silinmesi, olayın daha fazla yayılmasını önlemek ve gelecekteki riskleri azaltmak açısından hayati öneme sahiptir.
   - **Bilgi Güvenliği Politikaları:** Güvenli veri silme süreçleri, kurumun genel bilgi güvenliği politikaları, erişim kontrol politikaları ve fiziksel güvenlik politikaları ile uyumlu ve entegre olmalıdır.
   - **Adli Bilişim:** Güvenli veri silme yöntemleri, adli bilişim uzmanlarının veri kurtarma girişimlerine karşı bir önlemdir. Yeterince güvenli silinmemiş veriler, adli soruşturmalarda kritik delil olarak ortaya çıkabilir. Bu durum, "İç Denetim Uzmanı"nın denetim sırasında adli bilişim teknikleri ile olası veri kalıntılarını kontrol etme yetkinliğine sahip olmasını gerektirebilir.
   - **Standartlar ve Sertifikasyonlar:** NIST SP 800-88 Guidelines for Media Sanitization, ISO 27001 (Bilgi Güvenliği Yönetim Sistemi) gibi uluslararası standartlar, güvenli veri silme süreçleri için rehberlik sağlar ve bu süreçlerin belgelenmesi ile ilgili gereksinimleri belirtir. Bir iç denetçi olarak, kurumun bu standartlara uyumunu denetlemek önemlidir.

Bu modül, İç Denetim Uzmanı olarak kurumunuzdaki veri imha süreçlerini etkin bir şekilde denetlemeniz, potansiyel riskleri belirlemeniz ve en iyi uygulamaların benimsenmesini sağlamanız için gerekli bilgi ve araçları sunmaktadır.

Araştırmacıların Katkı Oranı Beyanı

Bu araştırmanın planlanması, yürütülmesi ve yazılı hale getirilmesinde sadece tek bir araştırmacı yer almıştır.

Destek ve Teşekkür Beyanı

Bu araştırmada herhangi bir kurum, kuruluş ya da kişiden destek alınmamıştır.

Çatışma Beyanı

Araştırmacının araştırma ile ilgili diğer kişi ve kurumlarla herhangi bir kişisel ve finansal çıkar çatışması yoktur.

Etik Kurul Beyanı

Bu araştırma, Gazi Üniversitesi Etik Kurulunun 08.07.2025 tarih ve 2025-1244 sayılı onayı ile yürütülmüştür.