BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ (BTK DERGİ)
CİLT: 1 SAYI: 1 TARİH: TEMMUZ - EYLÜL 2023 ISSN: 2980-1311

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİNİN UYGULANMASI VE DENETİMLERİNE YÖNELİK İYİLEŞTİRME ÖNERİLERİ

Halil İbrahim ÖZBİLGER[1]

Birsen SARIYAR[2]

Ahmet ERTÜRK[3]

Özet

Teknolojik gelişmelerin etkisiyle giderek artan dijitalleşme, hayatı hızla değiştirmektedir. Bu dönüşüm, fırsatlarıyla beraber riskleri de getirmektedir. Bunun doğal sonucu olarak günümüzde, siber tehditlerin kurumların riskleri arasında en üst sıralarda yerini aldığı gözlemlenmektedir. Örneğin; veri sızıntısı, dağıtılmış hizmet reddi (DDoS), kimlik avı, yapılandırılmış sorgu dili (SQL) enjeksiyon, zararlı yazılım ve oltalama (Phishing), casus, reklam ve fidye yazılımları ile truva atları (Trojan), solucanlar (Worm), tuş kaydediciler, botlar olarak nitelendirilen kötü amaçlı zararlı yazılımlar (Malware), kurumların karşılaşabildiği bu tür siber tehditlerden bazılarıdır. Bu nedenle, tüm kurum ve kuruluşlarda olduğu gibi kamu idarelerinde de yürütülen iş ve işleyişin planlanması ile yeniden tasarımında gerek mevcut ve(ya) doğabilecek siber güvenlik risklerine karşı önlem alınması gerekse de bu risklerin gerçekleşmesi durumunda doğacak etkinin azaltılması amacıyla proaktif şekilde harekete geçmek, içinde bulunulan dönemde anahtar aksiyon haline gelmiştir. Bu çalışmada, öncelikle konu hakkında teorik çerçeve çizilmiş olup sonrasında 2022 yılında gerçekleştirilen Rehber denetiminde sahada karşılaşılan zorluklar ve uygulama sonuçlarının değerlendirilmesinden yola çıkarak T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO) tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi (BİGR)'ni uygulayacak idarelerde birincil denetim sorumlusu konumundaki iç denetçilerin BİGR'yi ve Bilgi ve İletişim Güvenliği Denetim Rehberi (BİGDR)'ni esas alarak gerçekleştirecekleri denetim faaliyetlerinde ihtiyaç duyulan iyileştirme önerileri sunulmuştur. Çalışma sonucunda ulaşılan ve sekiz başlıkta sayılan iyileştirilmesi gereken alanlarla ilgili getirilen çözüm önerilerinin, yapılacak denetimlerin etkililiğini ve etkinliğini artıracağı değerlendirilmektedir.

Anahtar Kelimeler: *Bilgi Güvenliği, Siber Güvenlik, Dijital Dönüşüm, İç Denetim, Bilgi ve İletişim Güvenliği Denetimi.*

Jel Kodlar: *K24, M42, M48*

[1] Dr., İç Denetçi, T.C. Ticaret Bakanlığı, hiozbilger@hotmail.com, ORCID: 0000-0002-9137-8855
[2] CIA, İç Denetçi, T.C. Ticaret Bakanlığı, bsariyar@hotmail.com, ORCID: 0000-0001-9656-1491
[3] CISA, İç Denetçi, T.C. Ticaret Bakanlığı, aerturk77@hotmail.com, ORCID: 0009-0009-2556-9360

IMPROVEMENT RECOMMENDATIONS FOR IMPLEMENTATION AND AUDITS OF THE INFORMATION AND COMMUNICATION SECURITY GUIDE

Abstract

Increasing digitalization with the effect of technological developments is rapidly changing life. This transformation brings risks along with opportunities. As a natural consequence of this, it is observed that cyber threats take their place among the top risks of institutions today. For example; data leakage, distributed denial of service (DDoS), phishing, structured query language (SQL) injection, malware and phishing (Phishing), spyware, adware and ransomware, as well as trojans (Trojans), worms (Worm), keyloggers, Malicious malware (Malware), which is described as boots, are some of these types of cyber threats that institutions may encounter. For this reason, as in all institutions and organizations, in the planning and redesign of the work and operation carried out in public administrations, it is necessary to take proactive action in order to take precautions against the existing or cyber security risks that may arise, and to reduce the impact that will arise in the event of the realization of these risks. became the key action in the period. In this study, firstly the theoretical framework was drawn on the subject, and then the based on the evaluation of the difficulties encountered in the field and the results of the implementation during the Guideline inspection carried out in 2022, The improvement needed in the audit activities to be carried out by the internal auditors, who are the primary auditors in the administrations that will implement the Information and Communication Security Guide (ICSG) published by the the Republic of Turkey Presidency Digital Transformation Office (DTO), based on the ICSG and the Information and Communication Security Audit Guide (ICSAG). recommendations are presented. In the study, it is evaluated that the solution proposals regarding the areas that need improvement listed in the eight titles will increase the effectiveness and efficiency of the audits to be made.

Keywords: *Information Security, Cyber Security, Digital Transformation Internal Audit, Information and Communication Security Audit.*

Jel Codes: *K24, M42, M48*

GİRİŞ

Günümüzde dijitalleşmenin etkisiyle iş ve işlemlerin planlanmasında, iş yapma şeklinde ve süreçlerin bilgi teknolojileri (BT) kullanımı ile yeniden tasarımında yaşanan dönüşüm; çalışma hayatında birçok kolaylık ve faydayı beraberinde getirse de kurum ve kuruluşların maruz kaldıkları risklerde de farklılaşmalara sebep olmaktadır. Bu değişim, risk haritalarında önlem alınması gereken BT ve(-ya) siber güvenlik risklerinin ilk sıralara yerleşmesi ile sonuçlanmaktadır. Bu durum yalnızca elektronik haberleşmede faaliyet gösteren kurum ve kuruluşlarda değil enerji, bankacılık vb. kritik hizmetleri sunan işletmelerde de görülmektedir. Nitekim risklerin gerçekleşmesi durumunda kurumların karşılaştıkları sonuçlar olarak tanımlanabilen kriz kavramı, geçmiş dönemlerde akla ilk gelen mali durumlarda yaşanılan çöküntü ya da bozukluklukların karşılığı iken bugün mali durumların yanında ve hatta öncesinde siber saldırılar, veri sızıntıları, iş sürekliliğinin temin edilememesi gibi bilgi güvenliğinin sağlanamamasıyla sonuçlanan BT kaynaklı krizlerin ifadesi olarak önemli konuma gelmiştir.

Etkileri tam olarak ölçülemediği ve anlaşılamadığı düşünülen, sosyo-ekonomik alandaki değişimleri de beraberinde getiren dijitalleşme ile birlikte yaşanan teknolojik gelişmeler, zamanda ve mekânda esneklik sağladığı gibi diğer taraftan yeni riskleri ve saldırı arayüzlerini de ortaya çıkarmıştır.

2025 yılına kadar dünya çapında yüz milyardan fazla bağlantı olacağı; yüzde 55'inin akıllı üretim ve akıllı şehirler gibi iş dünyasında, yüzde 45'inin nesnelerin interneti (IoT) ile araçların interneti (IoV) şeklinde gerçekleşeceği tahmin edilmektedir. Bağlantıların toplamda sadece yüzde 10'unun insanlar arasında, yüzde 90'ının ise eşya\şeyler *(things)* arasında gerçekleşeceği tahmin edilmektedir (Ping, 2016).

Bilgi sistemlerindeki muhtemel güvenlik durumlarının yeterince anlaşılamaması ve(ya) sağlanamaması sonucunda kötü niyetli kişilerce güvenlik önlemlerinin bertaraf edilmesiyle bilgi sistemlerinin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sekteye uğraması, özellikle kamu güvenliği açısından 21.yy'ın petrolü olarak nitelendirilen (Schwab vd., 2011; Taffel, 2021) verilerin korunmasını, kritik önemi haiz bir durum haline getirmiştir.

Kamu idarelerinde ortaya çıkabilecek veri sızıntısı, dağıtılmış hizmet reddi (*DDoS*), kimlik avı, yapılandırılmış sorgu dili (*SQL*) enjeksiyon, zararlı yazılım ve

oltalama (*Phishing*) olarak adlandırılan, her on bir saniyede bir gerçekleştiği tahmin edilen siber saldırılar (Morgan, 2019) ile kurumların bilişim sistemlerine zarar vermek amacıyla tasarlanmış casus, reklam ve fidye yazılımları ile truva atları (*Trojan*), solucanlar (*Worm*), tuş kaydediciler, botlar olarak nitelendirilen kötü amaçlı zararlı yazılımlar (*Malware*), kurumsal imajı derinden etkileyebileceği gibi ciddi veri kaybı ve mali kayıplara da neden olacaktır (Chu ve Holt, 2012, s. 33-34). Ülkelerin maruz kaldıkları zararlı yazılım saldırıları çeşitlilik göstermektedir. 2023 yılının ilk iki ayı ile ilgili istatistiklere göre dünya genelindeki kullanıcılar ortalama en çok (yüzde 9,2) fidye virüsüne (*Ransomware*), en az ise (yüzde 0,01) şifre kırıcı (*password hacking*) virüslere maruz kalırken, Türkiye'de ise en çok (yüzde 12) trojanlere, en az ise (yüzde 0,2) arka kapı (*backdoor*) virüslere maruz kalınmıştır. Öyle ki; her bir dakikada dünya çapında ekonomik etkisi 1.141.553 ($) olan 34.740 şifre, 1.902 IoT tabanlı, 1.095 DDoS, 7 oltalama, 18.295 zararlı yazılım saldırıları gerçekleşmektedir (Özkaya, 2023). Bu durum her ne kadar ülkelerin sosyo-ekonomik durumlarıyla açıklansa da söz konusu kötü amaçlı yazılım ve saldırılara maruz kalmamak için BT risklerini azaltmak amacıyla uluslararası bilgi güvenliği standartları ve ulusal yasal düzenlemelere uygun olarak gerekli önlemlerin alınması ve sistematik şekilde bağımsız denetim birimleri tarafından denetimlerin gerçekleştirilmesi siber güvenliğin en önemli gereksinimi haline gelmiştir.

Bu çalışmada, dijital dönüşümün doğal sonucu olarak bilginin ve bilgi güvenliğinin artan öneminden bahisle BT risklerini azaltabilmek amacıyla Türkiye örneğinde kamu kurum ve kuruluşları ile önemli altyapı hizmeti sağlayan işletmelerde uygulanmak amacıyla ulusal düzeyde usul ve esasların belirlendiği T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO) tarafından yayımlanan "*Bilgi ve İletişim Güvenliği Rehberi (BİGR)" ve* Rehberin uygulama süreci ile tedbirlerin etkinlik durumunun değerlendirilmesi amacıyla gerçekleştirilecek denetim faaliyetlerinde kullanılacak "*Bilgi ve İletişim Güvenliği Denetim Rehberi (BİGDR)*"nin genel içeriği hakkında bilgi verilerek denetimlerin icra edileceği idarelerin kurum içi kaynaklarından olan İç Denetçi (*Internal Auditor*) perspektifiyle süreçte iyileştirilmesine ihtiyaç duyulan alanlar akademik bakış açısıyla ele alınmıştır.

Çalışmanın amacı, Bilgi ve İletişim Güvenliği Denetimi kapsamında kamu idarelerince gerçekleştirilen denetimlerde karşılaşılan sorunları tespit etmek ve bu sorunlarla ilgili iyileştirme önerileri sunmak olarak belirlenmiştir. Bu kap-

samda çalışmanın birinci bölümünde öncelikle dijital döşümde iç denetime ilişkin çalışmalar yer almaktadır. İkinci bölümde günümüz dünyasında etki ve sonuçları açısından oldukça önemli olan dijital dönüşüm ve bilginin artan önemi ele alınmıştır. Çalışmanın üçüncü ve dördüncü bölümlerinde birbirleriyle bağlantılı olarak sırasıyla bilgi ve iletişim güvenliği ve denetimi rehberleri ile rehber denetiminde iyileştirilmesi gereken alanlar ve çözüm önerileri çalışmanın dördüncü bölümünde açıklanan araştırma yöntemi çerçevesinde farklı açılardan değerlendirilmektedir.

1. DİJİTAL DÖNÜŞÜMDE İÇ DENETİME İLİŞKİN ÇALIŞMALAR

Uluslararası meslek standartları ile etik kuralları ve metodolojisi olan İç Denetimin, AB uyum yasaları çerçevesinde, Türk kamu yönetiminde ilk defa Türkiye Cumhuriyet Merkez Bankası'nda, 2002 yılında uygulamaya geçmesinden itibaren, gerek akademinin gerekse de konunun uygulayıcısı ve uzmanları tarafından sıklıkla ele alınan konulardan biri olduğu görülmektedir.

Tarihsel kökeni her ne kadar 13. yüzyıla kadar dayandırılsa da modern anlamda 1900'lü yılların başlarında Kıta Avrupası ülkelerinde ilk olarak uygulanan iç denetim (Kızılboğa, 2013, s. 108), 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunun'da; kamu idarelerinin çalışmalarını geliştirmek ve onlara değer katmak için etkililik, ekonomiklik ve verimlilik esaslarına göre kaynakların yönetilip yönetilmediğini belirlemek ve idari kademelere rehberlik yapmak amacıyla gerçekleştirilen nesnel güvence sağlama ve danışmanlık faaliyeti şeklinde ifade edilmektedir. Klasik denetim yöntemlerini kapsamakla birlikte rehberlik fonksiyonu kapsamında ileriye dönük faaliyetlerle ilgili alınması gereken iyileştirici aksiyonları da belirleyen, dinamik bir denetim sistemi olarak nitelendirilen (Bilge ve Kiracı, 2010; Stewart ve Subramaniam, 2010, s. 334) iç denetim sistemi, çalışmanın konusu çerçevesinde literatürde farklı yönleriyle ele alınmıştır.

Appelbaum ve Nehmer (2017) tarafından gerçekleştirilen çalışmada dijital dönüşüm çağında kurumların iç ve dış denetimlerinin tasarlanması ve uygulanması için bir çerçeve ortaya konulmaktadır. Çalışma, dijital dönüşüm araçlarının kanıt toplama yetenekleri aracılığıyla bazı işlevlerde denetim sırasında denetçiler tarafından değerlendirilen belirli iddiaları desteklemek için denetimlerde nasıl yararlanılacağını göstermektedir. Dijital dönüşüm araçlarının bazı durumlarda

varlık ve değerleme iddiaları hakkında kanıt sağlayabileceklerine vurgu yapılarak, dijital dönüşüm ve güvenliğinde denetim elemanlarının önemine vurgu yapılmıştır.

Barrigon'a göre (2020), teknolojik gelişmelere ayak uydurma ihtiyacının, iç denetim mesleğinin bir gereği olduğu, dijital dönüşümde sadece karşı karşıya kalınan risklerin değil aynı zamanda bunları azaltmak için uygulanan kontrollerin de daha iyi değerlendirilmesi gerektiği, siber güvenliğin test edilmesinde iç denetçilerin veri analitiği, yapay zeka ve blockchain (blok zincir) teknolojilerindeki riskli alanlara eğilirken hangi tür eylemleri gerçekleştirmesi gerektiği tablo halinde sunulmuştur.

Lois vd.'nin (2020), dijital çağda iç denetimi etkileyen çağdaş faktörleri ve bunun uygulanması için kullanılabilecek teknikleri araştırdığı ve 105 çalışan ile gerçekleştirdiği çalışmada elde ettikleri bulgulara göre; etkin bir dijital denetim sisteminin kurulması için teknolojik gelişmelerin vazgeçilmez olduğu, siber saldırılara karşı veri koruma önlemlerinin yanı sıra çalışanların becerileri ve eğitimlerinin etkisinin önemli bulunduğu, siber güvenliğin sağlanıp sağlanmadığının test edilmesi için sanal iç denetim ekiplerinin hazırlanmasına ve oluşturulmasına özel önem verilmesi gerektiği sonucuna varılmıştır.

Gupta ise (2020), iç denetçilerin dijital dönüşüm sürecindeki önemi ve karşılaştıkları zorlukları ortaya koymuştur. Bu kapsamda iç denetçilerin siber ortamdaki muhtemel riskleri belirlemede ve değişen çevrede denetim faliyetlerinin nasıl gerçekleştirileceği değerlendirilmiştir. Bu çalışmada denetçinin teknoloji odaklı süreçlere daha fazla ilgi göstermesi gerektiği önerilmiş, denetimin dijitalleşme süreci yani BT denetimi, dijital denetim ve siber denetim için BT desteği söz konusu çalışmada; grafik halinde sunulmuştur.

Pizzi vd.'nin çalışmasında (2021), "Endüstri 4.0" ile hızlanan dijital dönüşümün çalışma hayatındaki ve iç denetim mesleğiyle ilgili dört farklı araştırma alanındaki (teknolojik yenilik, sürekli denetim, veri analitiği ve suistimal tespiti) etkisi sorgulanarak araştırma sonuçları değerlendirilmiştir.

Otia ve Bracci (2022), yaşanılan dijital dönüşümün kurumların paydaşları ile ilgili talep ve beklentilerinde ne yönde değişikliklere neden olduğunu incelemiştir. Üç yüzden fazla katılımcı ile gerçekleştirilen araştırma sonuçları tablo halinde sunulmuştur. Elde edilen bulgularda teknolojik gelişmelerin tetiklediği hesap ve-

rebilirlik ve şeffaflık için artan denetim talebinin denetimin yapılma biçiminde bir etkiye sahip olduğu tespit edilmiştir.

BİGR'nin gündeme gelmesi ve gerekli denetimlerin başlamasıyla bahse konu uygulayıcıların olduğu kadar akademinin de ilgisini çekmeye başlamış, Rehber hakkındaki ulusal literatürdeki çalışmalar da aynı ölçüde hız kazanmıştır.

Ağdeniz (2021), yaptığı çalışmada DDO tarafından çıkarılan BİGR denetiminde kamu iç denetçilerinin rolü ve yetkinliklerini sertifika ve denetim sayıları temelinde değerlendirmeye çalışarak yılda en az bir kez kamu iç denetçilerinin söz konusu Rehber kapsamında denetim yapma zorunluluğunu belirtmiş, Kamu İç Denetim Genel Raporlarının içerik analizini de yaparak iç denetimin mevcut durumunu *açıklamıştır.*

Meral ve Bülbül (2022), örneklem yöntemiyle belirlenen kamu kurumlarında farklı alanlarda görev yapan çalışanlara yönelik gerçekleştirdikleri araştırmayla kurumların sahip olduğu verilerin önem düzeyi yükseldikçe buna benzer şekilde bilgi güvenliği politikalarının da arttığını; ancak kamu kurumlarının bilgi güvenliği politikalarının etkinliği konusunda genel olarak yetersiz olduğunu ortaya koymuştur.

Özen ve Gürel (2022), fiziksel varlıkların programlama dilleri yoluyla yansımalarının oluşturulması şeklinde ifade edilebilen "*Dijital İkiz Yöntemi*"ne açıklık getirerek bu yöntemin modern kamu denetimlerinde yararlanılmasını ve denetim kalitesine katkısını ortaya koymuştur.

Karagöz (2022), BİGR'nin uygulanması yöntemini ve uygulamayla ilgili oluşturulması gereken denetim mekanizmalarını belirterek, denetimde bağlı kalınması gereken etik ilkelere vurgu yapmıştır.

Çalışma konusu hakkında yapılan başka bir akademik çalışma da Tulgar vd. (2022) tarafından yapılmıştır. Çalışmayla uluslararası bilgi güvenliği standartları izah edilerek, Rehber uygulama süreçlerindeki her bir adım ile ilgili açıklamalarda bulunulmuş ve Rehber'deki temel başlıklardan birisi olan Nesnelerin İnterneti (IoT) Güvenliği ile ilgili örnek bir uygulama örneği ortaya konulmuştur.

Arslan ve Özbilger (2022), ulusal mevzuat altyapısı ve düzenlemelerine göre kamu yönetimindeki bilgi işlem birimlerinin iç denetiminde örnek bir kontrol modeli açıklamıştır.

Selimoğlu ve Saldı (2022) tarafından yapılan çalışmada, Bilgi ve İletişim Güvenliği Rehberi ve Rehber denetimini doğrudan ele almasa da esas olarak siber güvenlikle ilgili olaylarda blok zincir teknolojisinden nasıl yararlanılacağı ve iç denetçilerin bu teknolojiye uyum sağlamaları için ne yapmaları gerektiği hakkında bir takım öneriler ortaya konulmuştur.

Çalışma konusuna ilişkin ulusal ve uluslararası literatürde daha önce yapılan akademik çalışmaların değerlendirilmesi sonucunda, dijitalleşmenin ve bilgi güvenliğinin sağlanması ve denetlenmesindeki önemin fark edilmesiyle uluslararası literatürdeki çalışmaların özellikle son yıllarda önemli ölçüde arttığı ve konunun yoğun olarak işlendiği; ancak Türkiye'deki literatürün sınırlı olduğu anlaşılmaktadır. Konunun güncel olması ve literatür çalışmalarının sınırlı olması nedenleriyle bu çalışmayla BİGR ve denetimi hakkında literatürde uygulamaya yönelik önemli bir açığın giderilmesine katkıda bulunulacağı ve yapılacak yeni teknik çalışmalar için yol göstermesi hedeflenmiştir.

2. DİJİTAL DÖNÜŞÜM VE BİLGİNİN ARTAN ÖNEMİ

Günlük hayatı kolaylaştıran, yapılacak işler için harcanması gereken zamanı önemli ölçüde azaltan, iş modellerini değiştirmek için teknolojiden faydalanılması süreci olarak nitelendirilen (Otia ve Bracci, 2022, s. 255) dijitalleşme ile birlikte, yeni riskler ve saldırı arayüzleri ortaya çıkmıştır. Örneğin günümüzde bir bankayı soymak için fiziksel olarak bankada bulunma gereksinimi ortadan kalkmış, internet üzerinden online olarak bankaların bilişim sistemlerine uzaktan erişip hedeflenen kötücül/zararlı işlemler yapılabilmektedir (Özkaya, 2018, s. 114). Bankacılık sektöründe dijitalleşmenin etkisiyle karşımıza çıkan risklerdeki değişikliğin yanısıra pandemi sürecinin de etkisiyle ivmelenen dijital dönüşüm ile birlikte uzaktan çalışma kamu kurumlarının dahi olağan işleyişi haline gelmiş, diğer taraftan büyük veri ve yapay zeka uygulamaları gibi yeni teknolojilerin kullanımı da artmıştır. Dijital dönüşüm ile birlikte eksponansiyel olarak artan hacimdeki bilgiye erişim kolaylaşırken, bilginin diğer iki unsuru olan gizlilik ve bütünlüğünün korunması giderek güçleşmeye başladığından, günümüzün en değerli madeni olarak nitelenebilecek bilginin güvenliği, dijital çağın en önemli gereksinim olgusu olarak literatüre girmiştir.

Bilginin depolanması ve korunması mevcut durumdaki en büyük zorluklar-

dan biri haline gelmiştir. Dijital dönüşüm ile ilgili olarak iş yaşamında sıklıkla karşılaşılan, bilgi güvenliği disiplininde oldukça önemli bir rol oynayan, çeşitli disiplinler aracılığıyla ifade edilen ve gelinen noktada ulusal güvenlik ile yakinen ilişkilendirilen siber güvenlik; elektronik ortamda gerçekleştirilen işlemler esnasında varlıkların, kullanıcıların bilgi güvenliği farkındalık eksikliğinden kaynaklanan kusurlardan, kötü niyetli kişilerin veya organizasyonların illegal eylemlerinden kaynaklanan saldırılar sonucunda zarar görmesinin önüne geçmek amacıyla alınan önlemler/tedbirler olarak tanımlanabilmektedir (Kavitha ve Preetha, 2019, s. 4).

Günümüzde kurumlar, her türlü bilgi varlıklarına siber ortamda bulunan güvenlik risklerine karşı önlem almayı ve bu durumun sürdürülmesini amaçlamaktadır. Gelişmiş güvenlik teknolojisi kullanımlarının artması sonucu, olası teknik siber saldırıların gerçekleşmesine ilişkin risk azalabilmektedir (Aloul, 2012, s. 181). Siber güvenlik risklerinin azaltılması ihtiyacı, ülkelerin uluslararası standartlar ve iyi uygulamalardan faydalanarak bilgi güvenliği alanında uygun yasal mevzuat hazırlanmasını ve uygulanması gereken tedbirlerin belirlenmesini tetiklemiştir (Sağıroğlu ve Şenol, 2018). Bu gelişmeler, dijital dönüşümü yalnızca yeni teknolojileri devreye almak olarak algılamaktan ziyade bu dönüşümün, kurumsal yeniden yapılanma modeli olarak, yeni yönetim ve denetim yapısının tasarlaması şeklinde düşünülmesi ihtiyacını zorunlu kılmıştır.

Ülkeleri dijital dönüşüme yönlendiren ve e-Devlet uygulamalarının artmasının ana nedenlerinin başında, vatandaşların bulundukları lokasyonları değiştirmeden hizmetlere ulaşmalarına imkân sağlaması ve dezavantajlı grupların kamu hizmetlerinden faydalanmaları konusunda önemli faydalar içermesi yer almaktadır. Ayrıca sosyoekonomik yapıya etki eden COVID-19 gibi krizler de özel sektör kuruluşlarında olduğu kadar devletleri de hizmet sunumunda dijital dönüşüme zorlamıştır. Diğer taraftan internet ara bağlantılarının çoğalması genellikle kamu kurumları ve vatandaşlar için en tehlikeli bir savaş uçağından, tanktan, toptan daha tehlikeli, yıkıcı ve ciddi sonuçlar doğuran siber saldırı olaylarında da önemli bir artışa yol açmıştır. Öyle ki, OECD'nin "21. yy'da Ortaya Çıkan Sistematik Riskler (Emerging Systemic Risks in the 21st Century)" başlıklı yayımladığı rapora göre; siber riskler doğal afetler, bulaşıcı hastalıklar, gıda güvenliğiyle birlikte geleceğin en yüksek riskli alanları arasında sayılmıştır (OECD, 2003).

Dijitalleşmenin getirdiği avantajlardan faydalanabilmek adına 2000'li yılların başında e-Devlet dönüşümünü hızlı bir şekilde hayata geçiren Estonya, vatandaşlarına sunduğu hizmetlerinin büyük bir kısmını online platformlara taşımıştır. İlk başta oldukça güzel ve beklenildiği gibi hizmet veren bu sistem, gerekli siber güvenlik önlemlerinin alınmaması sonucunda bilişim altyapısına yapılan hizmet dışı bırakma (DoS) saldırılarıyla hizmet veremez hale gelmiştir (Bıçakçı, 2013, s. 29). E-devlet uygulamalarına yapılan bu saldırı ile Estonya'da kamuya sunulan hizmetlere erişilememiş, hizmetlerin büyük kısmının online platformlara taşınması nedeniyle de kamu hizmetleri durma noktasına gelmiştir. Estonya özelinde yaşanan bu e-dönüşüm sürecinden elde edilen deneyimlerle tüm dünyada dijital dönüşüme yönelik yapılan çalışmalar sonucunda gerekli stratejik yol haritaları belirlenmiştir (Darıcılı, 2014, s. 7). Aynı dönemde, "*Endüstri 4.0*" ve son gelinen nokta da dijitalleşmenin en üst seviyede olduğu "*Süper Akıllı Toplum*" ya da başka bir deyişle "*Toplum 5.0*" kavramları ile birlikte görünülürlüğü ve bilinirliği artan, etkileşim içindeki bireyleri ve kurumları etkileyen, entegre bir oluşum olan (Potii, 2018) siber güvenlikle ilgili ulusal yazılım ve bilişim altyapı yatırımlara öncelik veren Estonya bugün gelinen noktada Global Siber Güvenlik Endeksi (The *Global Cybersecurity Index*-ITU)'ne göre, dünyada birinci Amerika Birleşik Devleti, ikinci İngiltere ve Suudi Arabistan'dan sonra üçüncü, Avrupa'da ise ikinci sırada yer almaktadır (ITU, 2021).

Kurumların dijital altyapıya daha fazla bağımlı olması onları siber suçlara karşı daha savunmasız hale getirmiştir (Verma ve Charu, 2022). Bu nedenle, siber uzay ülkelerin fiziksel sınırları kadar korunmaya muhtaç bir alana evrilmiştir. Bu konuda İran, Çin, ABD gibi bir çok ülke tarafından gayriresmi bilgisayar korsanı (*hacker*) ekipleri oluşturulmaktadır. Bu ekipler hem kendi siber sınırlarını korumayı hem de düşman olarak belirledikleri ülkelere siber zarar verme, gizli bilgileri çalma gibi faaliyetler göstermektedir. Bu konuda Kuzey Kore'deki Lazarus (APT38) olarak adlandırılan hacker grubunun gerçekleştirdiği faaliyetler, konu hakkında örnek olarak gösterilebilmektedir (Page, 2012).

Yakın geçmişte farklı ülkelerde bilgisayar korsanlarının gerçekleştirdiği çok sayıda siber saldırı yaşanmıştır. Son yıllarda, görülen belki de en büyük, en karmaşık ve de en şiddetli olduğu düşünülen siber saldırılardan yüze yakın ülkedeki kamu ve özel kuruluşlardaki Microsoft Windows kullanıcılarını hedef alan WannaCry virüs olayı (Savita ve Patil, 2017, s. 1939), ABD'deki en büyük finansal ku-

rumlardan biri olan Capital One'da 2019 yılında yaşanan, yüz milyondan fazla kişiyi etkileyen veri ihlali (Nelson vd., 2020), yaklaşık yüz elli milyon kişinin sağlık ve sosyal güvenlik ile ilgili kişisel verilerinin ifşa edildiği Equifax veri ihlali (Lambet, 2017, s. 33) ve 87 milyon Facebook kullanıcısının kişisel bilgilerinin ABD'deki seçim kampanyalarında izinsiz şekilde kullanıldığı "Facebook-Cambridge Analytica Scandal" olarak da bilinen veri skandalı olayında kullanıcıların kişisel facebook sayfalarında yer alan bilgiler izinli ve/veya izinsiz elde edilerek ilgili kişilerin profillerini çıkarmada ve konum bilgilerini elde etmede kullanılmış, bu bilgilerden faydalanılarak belirli bir kişinin siyasi olaylar karşısında verecekleri tepkileri değiştirmek amacıyla ne tür reklamların kullanılabileceğini öneren profiller oluşturmada kullanılması amacıyla üçüncü kişilere satılmıştır (BBC, 2018).

Ülkeler yukarıda birkaç örneği verilen veri ihlallerinin bir daha yaşanmaması için sadece bilgi güvenliği önlemleri almamakta ayrıca vatandaşlarının kullandıkları uygulamalar üzerinden verilerinin izinli veya izinsiz olarak başka ülkelerin istihbarat teşkilatları tarafından kullanılmalarını önlemek amacıyla da çeşitli düzenlemeler yapmaktadır. Bunun son örneği, ABD'nin Pekin merkezli ByteDance Ltd. tarafından geliştirilen Tik-Tok uygulamasındaki kişisel verilerin, Çin hükümetinin kullanımı amacıyla toplandığı gerekçesi ve ulusal güvenlik endişeleri nedeniyle merkezi hükümet çalışanlarının kuruma ait cihazlarına TikTok indirmesini yasaklayan tasarıyı kabul etmesidir (Shepardson, 2023). Yine benzer şekilde vatandaşlarının veri güvenliğini sağlamak amacıyla Çin menşeili bilgi ve iletişim güvenliği cihazları üreten Huawei firmasının ürünlerinin ABD ve Kanada hükümetleri tarafından ithaline ve satışına yasak getirilmesi (Bartz ve Alper, 2022), bu kapsamda yapılmış başka bir düzenleme olarak görülmektedir.

"Her Tehdit Olası Riskleri Belirlemekle Başlar" anlayışı doğrultusunda BT alanındaki risklerin ve olası etkilerinin detaylı bir çalışmayla belirlenmesi ve buna uygun tedbirlerin uygulamaya konulması gerektiği dersinden hareketle siber güvenlik risklerine yönelik aksiyonların alınması için bilimsel temelli yaklaşımların geliştirilmeye başlandığı görülmektedir. Dünyada bu konuda çalışan ulusal ve uluslararası kuruluşlardan bazıları aşağıda sıralanmıştır.

- Kanada için siber güvenlik konusunda uzman tavsiyesi, rehberlik, hizmet ve destek sağlayan Kanada Siber Güvenlik Merkezi (*The Canadian Centre for Cyber Security - CCCS*)

- Avrupa Birliği bünyesinde siber güvenlik alanında BT ürünlerinin, hizmetlerinin ve süreçlerinin güvenilirliğini artıran üye devletler ve kurumlarıyla işbirliği yapan Avrupa Birliği Siber Güvenlik Ajansı (*The European Union Agency for Cybersecurity - ENISA*)
- Amerika Birleşik Devletleri'nde siber güvenlik konusunda Siber Güvenlik ve Altyapı Güvenliği Ajansı (*Cybersecurity and Infrastructure Security Agency - CISA*)
- NATO bünyesinde kurulan NATO İletişim ve Bilgi Ajansı (*NATO Communications and Information Agency - NCIA*) buna yönelik çalışan dünya çapındaki örnekler olarak karşımıza çıkmaktadır.

Genel olarak bu organizasyonlar tarafından BT ve siber güvenlik alanında rehber, denetim programları, iyi uygulama örnekleri, araçlar, kontrol listeleri hazırlanmıştır. Örneğin Kanada Siber Güvenlik Merkezi'nin hazırladığı *Siber Güvenlik Denetim Programı*[1], AB üye ülkelerin bilgi güvenliğinden sorumlu *Avrupa Ağ ve Bilgi Güvenliği Ajansı*'nın hazırladığı araçların[2], ABD Savunma Bakanlığı tarafından hazırlanan *teknik uygulama klavuzları*[3]nın çeşitli kurum ve kuruluşların kullanımına sunulduğu görülmektedir.

Siber güvenlik ekosistemi hakkında son yıllarda birçok ülke örneklerinde olduğu gibi Türkiye'de de gerek mevzuat altyapının düzenlenmesi gerekse de teorik ve uygulama çerçevesinde önemli adımlar atılmıştır (Sağıroğlu ve Şenol, 2018). Bu konudaki ilk önemli ve somut adım, 2003 yılından itibaren *e-D*önüşüm Türkiye Projesi kapsamında gerçekleşmiş, iki kısa vadeli eylem planı hazırlanmıştır. İhtiyaç duyulan altyapının oluşturulması amacıyla Devlet Planlama Teşkilatı (mülga) tarafından hazırlanan *Uzun Vadeli Gelişmenin Temel Amaçları ve Stratejisi (2001-2023)*'yle Türkiye'de bilgi toplumu ile ilgili hedeflenen dönüşüme ulaşılması planlanmıştır. (DPT, 2000: 21) Kalkınma Planlarında da göze çarpan bu dönüşüm vizyonu ile DPT tarafından *Bilgi Toplumu Stratejisi (2006-2010)* ve Kalkınma Bakanlığı (mülga) tarafından *2015-2018 Bilgi Toplumu Stratejisi ve Eylem Plan*ı ve *Ulusal Siber Güvenlik Stratejisi ve Eylem Planları* hazırlanmıştır.

Yapılan çalışmalar, sadece mevzuat ve düzenlemelerin hazırlanmasıyla kalmamış gerekli kurumsal organizasyonel oluşumların kurulmasını da sağ-

1 Siber güvenlik denetim programı için bkz: https://www.cyber.gc.ca/en/government-institutions
2 Hazırlanan denetim araçları için bkz: https://www.enisa.europa.eu/tools
3 Teknik uygulama klavuzları için bkz: https://public.cyber.mil/stigs

lamıştır. 2000'li yılların başından itibaren Türkiye'de siber güvenlik hakkında çalışmalar yapmak ve bu kapsamda ihtiyaç duyulan eğitim ve insan kaynağı ihtiyacını karşılamak amacıyla *KamuNet Teknik Kurulu*, 2002 yılında yeniden organizasyonu ve göreve başlamasından itibaren ilgili kamu kurumları siber suçlarla mücadeleye ilişkin bilgi toplumuyla ilgili hedef, politika ve stratejiler çerçevesinde, *Siber Güvenlik Enstitüsü (SGE)*, Türk Silahlı Kuvvetleri (TSK) Siber Savunma Merkezi Başkanlığı, siber güvenlik alanında dünya genelinde yapılan kurumsal yapılar örnek alınarak, *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı* uyarınca Bilgi Teknolojileri ve İletişim Kurumu bünyesinde *Ulusal Siber Olaylara Müdahale Merkezi (USOM)* ve müstakil bir bilgi işlem alt yapısına sahip kurumlarda yer alan *Siber Olaylara Müdahale Ekipleri (SOME)* kurulmuştur. Tüm bunların kurulması organizasyonel gelişmelerdendir.

Yaşanan teknolojik gelişmeler, yapılan kamusal reformlar çerçevesinde farklı kamu kurumlarınca geçmiş dönemlerde Başbakanlık, Kalkınma Bakanlığı ile Ulaştırma ve Altyapı Bakanlığı ve ilgili diğer kamu kurum ve kuruluşlarınca ayrı ayrı sürdürülen siber güvenlik, dijital dönüşüm (e-Devlet) vb. çalışmalarının tek çatı altında yürütülmesi amacıyla, 24 Ekim 2019 tarihli ve 30928 sayılı Resmi Gazete'de yayımlanan 48 sayılı Cumhurbaşkanlığı Kararnamesi kapsamında, T.C. Cumhurbaşkanlığı DDO kurulmuştur. Ofisin ulusal siber güvenliğin temin edilmesi amacıyla hazırladığı ve kamu kurum, kuruluş ile kritik altyapı[4] özelliğinde hizmet sağlayan işletmelerde uygulanması zorunlu olan, ilgili tarafların görüşleri alınarak oluşturulan 27 Temmuz 2020 tarihinde yayımlanan "*Bilgi ve İletişim Güvenliği Rehberi*" ve 10 Ekim 2021 tarihinde yayımlanan "*Bilgi ve İletişim Güvenliği Denetim Rehberi*" Türkiye'de siber güvenlik hakkında atılan önemli adımlar olmuştur.

DDO'nun kurulmasının, siber güvenlik alanında yapılacak çalışmaların üst düzeyde tek elden koordineyi sağlamasının yanı sıra bilgi ve siber güvenlik hakkında atılacak adımların kuvvetli şekilde en üst düzeyde desteklendiğinin göstergesi olarak da kıymetli olduğu değerlendirilmektedir. E-Devlet dönüşümü kapsamında yapılan çalışmalarda Estonya'nın yaşadığı saldırılardan dersler çıkarılmış, kamu kurum ve kuruluşlarının birbirleri ile yapacakları

4 Kritik altyapılar; enerji üretim ve dağıtım, su ve kanalizasyon sistemleri, telekomünikasyon altyapısı ile sağlık, finansal, güvenlik ve ulaştırma servisleri (Ak, 2019, s. 42).

bağlantılarda/veri transferinde internete açık olmayan kapalı bir ağ sistemi üzerinden haberleşmelerini zorunlu tutan, ilk olarak 2000'li yılların başlarında başlatılan "*KamuNet Projesi*[5]*"*nin hayata geçirilmesini sağlamıştır. Öte yandan kamu kurum ve kuruluşlarının KamuNet'i kullanmalarının teşvik edilmesi ve hangi düzeyde/oranda KamuNet'i kullandıklarının belirlenmesi amacıyla BİGR tedbir maddeleri içerisinde bu durumun ölçülebilmesi amacına yönelik düzenlemelere yer verilmesinin sürece katkı sağlayacağı değerlendirilmektedir.

DDO tarafından daha önce Türkiye'de bu konuda yürütülen strateji ve eylem planı çalışmalarının devamı niteliğindeki dijitalleşme yol haritasını belirlemek amacıyla Dijital Devlet Stratejisinin hazırlık çalışmaları kapsamında *OECD* ile ortak çalışma halinde çeşitli faaliyetler yürütülmektedir (DDO, 2023). Ayrıca 20 Ağustos 2021 tarihinde DDO ile Sanayi ve Teknoloji Bakanlığı işbirliği sonucunda yayımlanan *Ulusal Yapay Zeka Stratejisi (2021-2025)* doğrultusunda Kamu Bulut Bilişim Stratejisi'nin hazırlık faaliyetleri sürdürülmektedir. Bu çalışmalar kapsamında DDO tarafından *Kamu Bulut Bilişim Stratejileri Ülke İncelemeleri Raporu* ve *Mevcut Durum Analiz Raporları* tamamlanmış ve kamuoyu ile paylaşılmıştır.

Türkiye'de dijitalleşme yönünde son dönemde atılan adımlar ve gerçekleştirilen çalışmaların bir sonucu olarak *On İkinci Kalkınma Planı (2024-2028)* Özel İhtisas Komisyonları *ve Çalışma Grupları El Kitabı*'nda "*Bilgi ve İletişim Teknoloji*"leri ayrı bir özel ihtisas komisyonu kurulmuş ve dijitalleşme ile ilgili olduğu değerlendirilen "*e-Devlet Hizmetlerinin Geliştirilmesi*", "*Dijitalleşme ve Vergileme*", "*Dijital Gelişmelerin Sosyoekonomik Etkileri*" adlarında üç ayrı çalışma grubu oluşturulmuştur. 2023 Yılı Cumhurbaşkanlığı Yıllık Programı'nda "*Dijital Türkiye*" vizyonu ve "*Milli Teknoloji Hamlesi*"ne yönelik hedeflerin belirlenmesi de dijitalleşmenin ülke içerisinde dikkate alındığını ve bu konuda çeşitli önlemlerin belirlendiğini gösteren diğer düzenlemelerdendir.

ITU'ya göre dünyada on birinci, Avrupa'da altıncı sırada yer alan Türkiye'nin geldiği noktayı geliştirip en üst sıraları hedeflemesi gerekmektedir. Bu amaçla, Estonya örneğinde olduğu gibi yerli, milli ve hatta global siber yazılımlarla ilgili AR-GE çalışmalarının desteklenmesinin yanında ulusal mevzuat ve denetim

5 KamuNet Projesi için bkz: https://cbddo.gov.tr/projeler/kamu-net/

süreçleri ile ilgili altyapıların da hazır olması gereklidir. Bu süreçte devlet, özel sektör ve sivil toplum kuruluşlarıyla beraber uygun yapının oluşturulması önemlidir.

3. BİLGİ VE İLETİŞİM GÜVENLİĞİ VE DENETİMİ REHBERLERİ

2019/12 sayılı "*Bilgi ve İletişim Güvenliği Tedbirleri*" konulu Cumhurbaşkanlığı Genelgesi ile bilgi ve iletişim güvenliğine ilişkin temel prensipler ve yol haritası belirlenmiştir. Bahse konu Genelge ve Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ile uyumlu biçimde kamu kurum ve kuruluşları ile kritik altyapı hizmeti sağlayan kurumların uyması zorunlu kılınan, bilgi ve iletişim güvenliğinin sağlanması amacıyla DDO koordinesinde bilişim alanında tüm dünyada geçerli standartlar, iyi uygulamalar, rehberler incelenerek hazırlananan "*Bilgi ve İletişim Güvenliği Rehberi*", 27 Temmuz 2020 tarihinde yayımlanarak yürürlüğe girmiştir.

Bilişim alanında belirlenen tüm tedbirlerin nihai hedefi bilgi güvenliğinin sağlanmasıdır. Bilgi güvenliğinden bahsedebilmek için bilginin üç temel unsuru olan gizliliğin (bilgiye sadece yetkili kişilerin erişimi), bütünlüğün (bilginin sadece yetkili kişiler tarafından değiştirilmesi) ve erişilebilirliğin (bilginin yetkili kişilerin talebi halinde kullanılabilir olması) sağlanması gerekmektedir. Rehbere uyum ile bilginin bu üç unsurunun korunması hedeflenmektedir. Rehberin hazırlanmasında temel amaç, rehbere uymakla zorunlu tüm kurumlarda siber güvenlik ve bilgi güvenliği alanında yapılacak çalışmaların belirli bir çerçeve dâhilinde yürütülmesine ve bu tedbirlere uyum konusunda yapılacak denetimlerin aynı bakış açısıyla yapılmasına olanak sağlanmasıdır.

Bilgi güvenliğinde Türkiye nezdinde hazırlanmış, içerisinde teknik tedbirleri bulunduran referans doküman niteliğindeki BİGR'nin, ihtiyaç halinde yaşayan bir doküman olarak değişiklik yönetimi kurgusu içerisinde güncellenmesi ve geliştirilmesi ile sürekliliğinin sağlanması önemlidir.

Bilgi ve iletişim güvenliğine yönelik belirlenen tedbirlerin uygulamaya geçirilmesi ile ülke nezdinde siber güvenlik alanında dayanıklılığın ve iş sürekliliğinin artırılması hedeflenen BİGR ile 24 aylık uyum ve(ya) geçiş süreci ve alınacak tedbirlere yönelik aksiyonlar oluşturulmuştur. Rehbere uyum sağlamakla sorumlu tutulan kurum ve kuruluşların; bilgi varlıklarını gruplandırmaları, bu grupların kritiklik seviyelerini ve bu seviyelere yönelik BİGR tablolar bölümünde belirle-

nen tedbirlere ilişkin uygulanma durumlarını veya eksikliklerini ve yapılacak çalışmaları belirleyerek dokümante etmelerinin yanısıra, belirlenen takvimin 6-24 aylık bölümünde mevcut bilgi sistemlerini kritiklik derecelerine uygun tedbirler ile uyumlu hale getirmesi, yeni kurulacak bilgi sistemlerinde ise BİGR'de yer verilen tedbirlere uyulması gerekmektedir.

Rehberin ilgili bölümlerinde uyum süreci aşağıdaki şekilde tanımlanmaktadır;

- Bilgi sistemleri, personel ve fiziksel mekanlar dâhil kurumun tüm bilgi varlıklarının gruplandırılması diğer bir deyişle varlık gruplarının tanımlanması.
- Bu grupların her birine ilişkin olarak varlık sahipleri ve ilgili bilgi işlem personeline (sistem yöneticisi, yazılım personeli vb.) uygulanacak anket ile belirlenecek puanların karşılığı olacak biçimde varlık grubu kritiklik seviyelerinin belirlenmesi.
- Rehberde belirlenen kritiklik seviyelerine uygun Rehber ekinde yer alan toplam 661 adet tedbirlere yönelik varlık grupları bazında mevcut durum ve boşluk analiz çalışmalarının yapılarak ihtiyaçların ve gerçekleştirilecek faaliyetlerin belirlenmesi.
- Uyum sürecine ilişkin gerçekleştirilecek faaliyetlerin belirlenerek yol haritasının oluşturulması.
- Kritiklik derecesine (1., 2. ve 3. seviye) uygun olarak tedbirlerin gerçekleştirilmesi.
- Çalışmaların BİGR eklerinde belirlenen formatlarda dokümante edilmesi.

Yılda en az bir kez denetlenmesi ve sonuçların DDO'ya bildirilmesi gereken BİGR, bilişim sistemlerinde kullanılan güvenlik yazılımlarında olması gereken veya parametrelerde ayarlanması gereken değerleri vurgulaması açısından (örneğin bilişim sistemlerinde kullanılan antivirüs yazılımlarında otomatik kod çalıştırma (autorun) korumasının açılmasının zorunlu tutulması), diğer Bilgi Güvenliği Yönetim Sistemlerinden (BGYS) ayrılmaktadır. Ayrıca Rehber, varlıkların gruplandırılması ve kritiklik derecelerine göre uygulanacak tedbirlerin belirlenmesi ile de BGYS risk değerlendirme sürecinden farklılaşmaktadır.

Rehbere uyum sürecinde, tüm kurumu ilgilendiren bilgi varlıklarının gruplan-

dırılması ve kritiklik derecelendirme çalışmalarının koordinesi ile sonuçlandırılması ve dokümantasyonun oluşturulmasında zorluk yaşanabildiği görülmüştür. İlaveten tüm dünyada etkileri hissedilen COVID-19 krizi, Rehbere uyum sürecini olumsuz yönde etkilemiş ve kurumlarda yapılması gereken faaliyetlerin zamanında gerçekleştirilememesine neden olmuştur.

Uyum sürecinin tamamlanmasını müteakip 2022 yılının ikinci yarısında ilk denetimler gerçekleştirilmeye başlanmıştır. Bahse konu denetimlere ilişkin usul ve esaslar ile denetim metodolojisi Ekim 2021' de DDO tarafından yayımlanan "*Bilgi ve İletişim Güvenliği Denetim Rehberi*" ile belirlenmiştir.

Bahse konu Rehberde; en az iki kişiden oluşacak denetim ekibinin sahip olması gereken yetkinlikler kapsamında ISO/IEC 27001 Baş Denetçi Sertifikası, CISA (Certified Information Systems Auditor/Sertifikalı Bilgi Sistemleri Denetçisi) Sertifikası veya TSE tarafından verilen D1 tipi Ağ ve Sistem Denetçisi veya D2 tipi Uygulama Denetçisi sertifikaları şart koşulmuş olmakla birlikte kamu kaynaklarının etkin, ekonomik ve verimli kullanımı amacıyla kamu kurum ve kuruluşlarında bu denetimleri gerçekleştirecek iç denetçiler için istisna getirilerek bu sayılanlar veya bu sertifikalar yoksa bilgi güvenliği eğitimi almış ve iç tetkikçi ve(ya) iç denetçi olarak görev yapmış olmak şeklinde esnetilmiştir.

Ayrıca kamu kurumlarından görevlendirmeler yoluyla da denetim ekiplerinin oluşturulması hususuna yer verilmiştir. Bununla birlikte Rehber denetimlerinde özellikle tedbirlerin etkinliğinin değerlendirilebilmesi için ağ ve sistem, veri tabanı, yazılım gibi farklı uzmanlık alanlarında teknik yeterlilik gerektiği de aşikârdır.

Rehber denetimlerinin öncelikli ve esas olarak kurum iç denetçileri tarafından gerçekleştirilmesi gerekli olmakla birlikte denetimleri gerçekleştirecek yetkin personelin bulunmaması halinde ise dış kaynak kullanımı da (başka kurumlardan geçici personel görevlendirme veya hizmet alımı) diğer yöntemler olarak belirlenmiştir. BİGR'de yer alan tedbirlerin denetlenmesi için denetimi gerçekleştirecek personelde ileri düzeyde BT denetim yetkinliğine gereksinim duyulmaktadır. İç Denetim Koordinasyon Kurulu (İDKK) tarafından hazırlanan 2021 yılı *Kamu İç Denetim Genel Raporu*'nda[6], kamu kurumlarındaki iç denetim birim-

6 2021 yılı Kamu İç Denetim Genel Raporu için bkz: https://ms.hmb.gov.tr/uploads/2022/08/2021-Kamu-Ic-Denetim-Genel-Raporu-Son-Hali.pdf

lerinde görev yapan iç denetçilerin sadece yedisinin CISA sertifikasına sahip olduğu görülmektedir (İDKK, 2022a). Rehber denetimlerinden gereken faydanın sağlanması için bu sayının artırılmasına yönelik projelerin hızlıca hayata geçirilmesi oldukça önemlidir.

Rehber denetimlerinin sonucunda uygulama sürecinin etkinliği ve tedbir etkinlik durumunun belirlenmesi şeklinde iki temel hedef bulunmaktadır. Bu süreçte denetim ekibince oluşturulacak dokümanların formatına BİGDR eklerinde ulaşılabilmekte olup formata uyulması ihtiyacı özel olarak belirtilmektedir.

BİGDR'de tanımlı denetim metodolojisi; halihâzırdaki kamu iç denetim uygulamalarına benzer uygulamalar taşımakla birlikte farklılıklar da içermektedir. İç denetim jargonunda ön çalışma olarak isimlendirilen süreç, Rehber'de denetimin planlanması; saha çalışması süreci, denetim prosedürlerin uygulanması; raporlama, aşaması ise denetim sonuçlarının raporlanması olarak isimlendirilmektedir. Üç aşamanın her bir aşamasında gerçekleştirilecek çalışmalar, çalışma kâğıtlarıyla kayıt altına alınması ve belirlenen hususların Rehber ekinde verilen formatlar kullanılarak oluşturulacak dokümanlar aracılığıyla, 04 Ocak 2023 tarihinde DDO tarafından devreye alınan *Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemi (BİGDES)* sistemine işlenmesi öngörülmüştür.

4. REHBER DENETİMİNDE İYİLEŞTİRİLMESİ GEREKEN ALANLAR VE ÇÖZÜM ÖNERİLERİ

Rehber denetimi uygulayıcılarına fayda sağlaması açısından iyileştirilmesi gereken alanlar ve bunlarla ilgili çözüm önerilerini ele alan, akademik değerlere uygun olarak yürütülen araştırmanın çalışma kümesi, süre kısıtı olması nedeniyle 5018 Sayılı Kanunun 3/b maddesinde tanımlanan merkezi yönetim kapsamındaki kamu idarelerinde görev yapan rehber denetimini yürüten kamu iç denetçileridir. Rehber denetimi hakkındaki görüşlerini ve tutumlarını ortaya çıkarmak amacıyla hazırlanan soruların doğru analizi, çözüm önerilerinin belirlenmesi ve araştırma odağının kaymaması için uzun ve karmaşık ifadelerin yer almadığı yapılandırılmamış beş sorudan oluşan anket yöntemi çalışmada uygulanmıştır. Rehber denetimi gerçekleştiren kamu iç denetçi sayısının oldukça sınırlı olması ve söz konusu denetim türünün sınırlı sayıdaki kamu idaresinde 2022 yılında ilk kez uygulanması, araştırmanın sınırlılığını oluşturmaktadır. Hazırlanan anket çalışması gönüllülük esasına göre örneklem olarak belirlenen dokuz kamu

idaresinde görev yapan yirmi bir kamu iç denetçisiyle gerçekleştirilmiştir. Tüm katılımcılar anket sorularını eksiksiz cevaplandırarak sorulara yönelik herhangi bir kaçınma eğilimi sergilememiştir. Araştırma yönteminde insan-hayvan üzerinde deneysel çalışma uygulaması bulunmadığından etik kurul iznine ihtiyaç duyulmamıştır.

Rehber denetimi faaliyetlerinde; kamu kurum ve kuruluşlarında kurum içinden görevlendirilen iç denetçilerin bilgi ve tecrübe paylaşımları, denetimlerde sahada karşılaşılan zorluklar ve uygulama sonuçlarının anonimleştirilerek değerlendirilmesi neticesinde iyileştirilmesi gereken alanlar ve çözüm önerileri şu başlıklar altında ele alınmıştır.

- Varlık grubu kritiklik derecelendirme puanlamaların güncellenmesi,
- Bulgu tablosuna bulgu tanımı ifadesinin eklenmesi,
- Bulgu izleme sürecinin iyileştirilmesi,
- Denetim raporunun her sayfasının e-imza ile imzalanması,
- BİGDES denetim görüşü bölümü uygulanması gereken toplam tedbir sayısı algoritmasının güncellenmesi,
- Tedbir maddelerine KamuNet'in teşvik edilmesine yönelik ilave yapılması,
- İç denetçilerin sertifika süreçlerinin desteklenmesi,
- Rehber denetimi yapabilecek iç denetçi havuzunun oluşturulması.

4.1. Varlık Grubu Kritiklik Derecelendirme Puanlamaların Güncellenmesi

Kamu idarelerinin varlık grup derecelendirmelerinin güvenilir olması oldukça önemlidir. Dolayısıyla hem ilgili kamu kurumunun BT güvenliğinin sağlanması hem ilgili kurumunun daha etkin çalışabilmesi hem de vatandaşın doğru bilgiye ulaşabilmesi için varlık kriterlerinin doğru şekilde sınıflandırılması gereklidir (Özçayan ve Aslan, 2021, s. 32).

BİGR kapsamında varlık gruplarına uygulanacak tedbirler, varlık grupları bazında gerçekleştirilen anket sonucuna göre tespit edilen kritiklik dereceleri baz

alınarak belirlendiğinden, anket puanlamasına göre üçlü ölçekte seviyelendirme işleminin Rehber uyum sürecinde kilit kontrollerden biri olduğu aşikârdır. Anketlerin; her bir varlık grubu için varlık sahibi, yazılım geliştiricisi ve sistem yöneticisi gibi ilgili kişilerce doldurularak farklı farklı alanlarda görev yapan ve süreçte yer alan uzman personelin veri toplama aşamasında yer aldığı Delphi metodunun (Bahar ve Somuncu Demir, 2021, s.37) uygulanması ve puanlama yapılarak sonuçlara göre varlık grubu seviyelerinin belirlenmesi gerekmektedir.

Güvenlik perspektifinde hazırlanan BİGR'nin tedbir maddeleri incelendiğinde, kritiklik derecelerine göre uygulanması öngörülen üçüncü seviye bazı tedbirlerin oldukça ileri seviyede belki de sadece milli güvenliği tehdit edebilecek ve(ya) askeri sistemlerde uygulanması gerekecek önlemler içerebildiği değerlendirilmektedir. Denetim uygulamalarındaki tecrübe edilen sonuçlar da kurum kültürü, bütçe kısıtlamaları, personel yetersizliği veya birebir vatandaşa yönelik özellikle kamuya açık gizlilikten daha yüksek oranda erişilebilirlik unsurunun ön planda olduğu iş ve işlemlerde üçüncü seviyedeki tedbirlerin uygulanması veya sonuçlarından bazı hizmet süreçlerinin olumsuz etkilenebildiği ya da buna yönelik ciddi kaynak planlamalarına ihtiyaç olabileceği görülmüştür.

Bu nedenlerle, anket sonuçlarına göre tedbirlerin uygulanması için kritiklik dereceleri belirlenirken uygulanmakta olan anket puan aralıklarının yukarı yönde revize edilmesi veya kritiklik derecelendirmelerinde beşli ölçeğe geçilmesinin daha fazla fayda sağlayabileceği düşünülmektedir. Yapılan değerlendirmede mevcut her iki Rehberin kurgusu ve ekli tablolarda yer alan tedbirlerin yeniden beşli ölçeğe göre kritiklik seviyelerinin belirlenmesi süreçte radikal bir değişiklik ve çalışma gerektireceğinden ilk aşamada üçlü ölçekle devam edilmesi ve kritiklik derecelendirme sürecinde kullanılan sınır değerlerin yukarı yönlü revize edilmesinin bu aşamada hızlıca uygulanabilir etkin bir öneri olduğu sonucuna varılmıştır.

Örnek olarak bir kurumda fiziksel ve sanal sunuculardan oluşan 'Sunucu Sistemleri' varlık grubu tanımlandığını ve bu varlık grubuna yönelik kritiklik derecelendirme anket sonuçlarının, aşağıda yer alan örnek olarak oluşturulan Tablo 1'de verildiği gibi olduğunu varsayalım.

Tablo 1: Sunucu Sistemleri Varlık Grubu Anket Sonuçları Örnek Tablosu

Boyut	Soru No	Şıkların Puanları					Soru Puanı
		a	b	c	d	e	
İşlenen Veri Açısından							
Gizlilik	1	1 puan	2 puan	3 puan	5 puan		3
Bütünlük	2	1 puan	2 puan	3 puan	5 puan		3
Erişilebilirlik	3	1 puan	2 puan	3 puan	5 puan		5
Etki Alanı Açısından							
Etkilenen Kişi Sayısı	4	1 puan	2 puan	3 puan	4 puan	5 puan	5
Toplumsal Sonuçlar	5	1 puan	2 puan	3 puan	5 puan	6 puan	3
Kurumsal Sonuçlar	6	1 puan	2 puan	3 puan			3
Sektörel Etki	7	1 puan	2 puan	3 puan	5 puan		5
Bağımlı Varlıklar	8	1 puan	2 puan	3 puan	5 puan	6 puan	5
Anket Puanı (Tüm soruların puanlarının toplamı)							32

Kaynak: Yazarlar tarafından oluşturulmuştur.

Bu senaryoda; yürütülen iş ve işlemlerin doğası gereği ikinci seviye tedbir uygulanmasının daha uygun olacağı değerlendirilmekle birlikte kritiklik derecesinin 3. seviye belirlenmesi nedeniyle uygulanması gerekecek ilave tedbirlere ilişkin donanım, yazılım, personel, eğitim ve lisans ihtiyaçlarına yönelik beş örneğe aşağıda yer verilmiştir.

- 3.1.6.33 "*Kripto Ağ Cihazlarının Kullanım*" tedbiri kapsamında kripto ağ cihazı kullanımı,
- 3.1.6.36 "*Veri Transferi*" tedbiri kapsamında veri diyotu kullanımı,
- 3.1.11.9 "*Düzenli Kırmızı Takım Tatbikatlarının Yapılması*" tedbiri kapsamında kırmızı takım tatbikatları yapılması,
- 5.1.2.8 "*Zorunlu Erişim Kontrolünün (MAC) Aktif Edilmesi*" tedbiri kapsamında işletim sistemindeki erişim kontrolü, ilgili servisler (SELinux, AppArmor vb.) aracılığıyla zorunlu erişim kontrolü (MAC) modeline göre yapılması,

- 5.3.2.15 "*Disk ve İmajların Şifreli Olarak Saklanması*"na ilişkin ilave sıkılaştırma tedbiri.

Bahse konu BİGR EK.C1'de verilen anket sorularının puan değerleri kullanılarak herhangi bir varlık grubunun alabileceği minimum ve maksimum puanlara ilişkin sınır değerler aşağıdaki Tablo 2'de gösterildiği gibi 8 (sekiz) ile 40 (kırk) puan olarak belirlenebilmektedir.

Tablo 2: BİGR'nin Anket Sonuçlarına Göre Varlık Grubu Alabileceği Sınır Değerler

Soru No	Minimum Puan	Maksimum Puan
1	1	5
2	1	5
3	1	5
4	1	5
5	1	6
6	1	3
7	1	5
8	1	6
Toplam	**8**	**40**

Kaynak: Yazarlar tarafından oluşturulmuştur.

Hâlihazırda BİGR'de mevcut uygulamada anket puanı 18'den küçük ise 1. derece, 18 (dâhil) – 28 puan aralığı 2. derece ve 28 ve daha yüksek olanlar ise 3. derece (en kritik ve en fazla tedbir) şeklinde belirlenmektedir.

Yukarıda açıklanan hususlar ve edinilen tecrübelerden hareketle BİGR'de yer alan "*Anket Puanına Karşılık Gelen Kritiklik Derecesi*" tablosundaki değerlerin gözden geçirilmesi, 3.Derece kritiklik seviyesinin sadece milli güvenliği doğrudan etkileyen sistemlere yönelik olacak biçimde iyileştirilmesine ihtiyaç bulunduğu değerlendirilmektedir. Konuya ilişkin mevcut durum ve yapılabilecek iyileştirmeye yönelik karşılaştırmalı öneri tablosu aşağıda verilmiştir.

Tablo 3: Anket Puanına Karşılık Gelen Kritiklik Derecesi Değişiklik Önerisi

Kritiklik Derecesi	Anket Puanı	
	BİGR Mevcut Durum	**Önerilen**
1. Derece	**18**'den küçük ise	**23**'den küçük ise
2. Derece	**18** (dâhil) ile **28** arasında ise	**23** (dâhil) ile **33** arasında ise
3. Derece	**28** ve daha yüksek ise	**33** ve daha yüksek ise

Kaynak: Yazarlar tarafından oluşturulmuştur.

4.2. Bulgu Tablosuna Bulgu Tanımı İfadesinin Eklenmesi

Denetim sonuçları doğrultusunda ilgili birimlerin ihtiyaç duyulan, gerekli aksiyonları alabilmesi ve denetim standartları gereği denetim raporlarının açık ve anlaşılabilir olması oldukça önemlidir (Yanık ve Karataş, 2017). BİGDR'nin "*Bulguların Tespiti, Değerlendirilmesi ve İzlenmesi*" başlıklı maddesinde belirlendiği biçimde "*EK-G Bulgu Tablosu*"na işlenerek denetlenen birime iletilen bulguların (özellikle kısmen etkin olarak belirlenen tedbirler için) denetlenen birim tarafından anlaşılması, denetim kapsamına alınan varlık grubu içindeki hangi bilgi varlığında eksiklik olduğunu ifade edecek ve ilgili tedbir maddesinin etkin olarak uygulanması için ne yapması gerektiğini bildirecek bir yapının bulunmaması nedeniyle gerçekleştirilecek düzeltici faaliyetin belirlenmesi ve buna yönelik doğru aksiyonların alınması hususunda güçlük yaşanmaktadır.

Ayrıca denetim sonucunda elde edilen bulguların, denetlenen birimle paylaşımı sırasında farklı varlık gruplarına yönelik aynı tedbirle ilişkili bulguların bulunması durumunda konunun anlaşılmasının daha da güçleşebildiğinden denetim ekibi ile denetlenen birimler arasında iletişim problemleri ile karşılaşılabilmektedir. Bulguların anlaşılabilirliği bakımından EK-G Bulgu Tablosuna ilave bir sütun ile "İlgili *Olduğu Tedbir Maddesi*"nden sonra "*Bulgu Tanımı*" ifadesinin aşağıdaki tablodakine benzer biçimde eklenmesinin sürece önemli katkı sağlayacağı değerlendirilmektedir.

Tablo 4: Önerilen Bulgu Tablosu Örnek Gösterimi

Sıra No	Bulgu Kodu	İlgili Olduğu Tedbir Maddeleri	Bulgu Tanımı
1	2022.1.1.U02.Y	U02 Kurumsal bilgi varlıklarının varlık grubu altında belirtilmesi	Yazıcıların ve kartlı geçiş sisteminin varlık grubunda yer almadığı belirlenmiştir.
2	2022.1.2.T01.Y	FELAKET KURTARMA VE İŞ SÜREKLİLİĞİ YÖNETİMİ 3.1.13.1. Yedekleme Planının Oluşturulması	Yedekleme planın mevcut değildir.
3	2022.1.3.T02.Ç	DOSYALARIN VE KAYNAKLARIN GÜVENLİĞİ 3.2.4.1. Denetim Kayıtları, Yapılandırma Dosyaları, İz Kayıtları vb. Bilgilerin Kullanıcı Verisiyle Aynı Ortamda Saklanmaması	İz kayıtlarının merkezi iz kayıt sistemine gönderilmediği belirlenmiştir.

Kaynak: Yazarlar tarafından oluşturulmuştur.

4.3. Bulgu İzleme Sürecinin İyileştirilmesi

Denetim sonuçlarının değerlendirilmesi ve izlenmesi süreci kamu kurumlarının hesap verilebilirliğinin ve uygulama sonuçlarının görülebilmesinde, kurumlarda sağlam bir bilgi tabanı oluşturulmasında kulanılabilecek en güçlü kamu yönetimi araçları arasında yer almaktadır (Kusek ve Rist, 2004, s. 170). Dolayısıyla BİGDR "*Bulguların Tespiti, Değerlendirilmesi ve İzlenmesi*" başlıklı maddesi bulguların değerlendirilmesi ve izlenmesi kısmında kurum kaynakları ile gerçekleştirilen denetimlerde oluşturulacak izleme sisteminde tanımlanan süreçte tespit edilen bulguların izleme sürecinin beklenen faydayı sağlayabilmesi amacıyla süreçteki adımların, rol ve sorumlulukların netleştirilmesi ihtiyacı bulunduğu düşünülmektedir. Bu amaçla aşağıdaki tabloda verilen Bulgu Tablosu Eylem Planının BİGDR'ye ilave edilmesinin izleme sürecine katkısı olabileceği değerlendirilmektedir.

Tablo 5: Bulgu Tablosu Örnek Eylem Planı

Sıra No	Bulgu Kodu	Tedbir Alt Başlığı	İlgili Olduğu Tedbir Maddeleri	İlgili Birim	İlgili Personel	Tamamlanma Tarihi
1	2022.1.1.U02.Y	-	U02 Kurum bilgi varlıklarının mutlaka bir varlık grubu altında tanımlanması	Bilgi Güvenliği Dairesi Başkanlığı	Ali BİLGER (Uzman)	26.05.2023
2	2022.1.2.T01.Y	FELAKET KURTARMA VE İŞ SÜREKLİLİĞİ YÖNETİMİ	3.1.13.1. Yedekleme Planının Oluşturulması	Sistem ve Sunucu Yönetimi Dairesi Başkanlığı	Zeynep BERBER (Mühendis)	26.10.2023
3	2022.1.3.T02.Ç	DOSYALARIN VE KAYNAKLARIN GÜVENLİĞİ	3.2.4.1. Yapılandırma Dosyaları, Denetim Kayıtları, İz Kayıtları vb. Bilgilerin Kullanıcı Verisiyle Aynı Konumda Depolanmaması	Yazılım Geliştirme Dairesi Başkanlığı	Emin ER (Bilişim Uzmanı)	12.07.2023

Kaynak: Yazarlar tarafından oluşturulmuştur.

Esasen iç denetim faaliyetlerinde önemli bir yeri olan, yönetim ve karar alma süreçlerini desteklemek amacıyla özel amaçlı bir yönetim fonksiyonu olarak da görülen (Kusek ve Rist, 2004, s. 12) izleme faaliyetinden istenilen faydaya ulaşabilmek için bilgi güvenliği yönetim sisteminde yürütülmekte olan "*Düzeltici Faaliyet*" tanımlanması ve sürekli iyileştirmeyi tanımladığı değerlendirilen izleme sistemine ilişkin bölümün netleştirilmesi veya en azından varsa BGYS içinde veya buna benzer biçimde bulgu tanımlamalarının "*Bulgu Tablosu*"na ilavesine ilişkin önceki maddede açıklanan önerilerin hayata geçirilmesi ile denetim eki-

bince kısaca tanımlanacak olan bulgu tanımlarına yönelik Düzeltici Faaliyetler ile alınacak ve(ya) alınmış aksiyonların kayıt altına alınmasının sağlanmasının izleme sürecinin etkinliğine ve uygulanabilirliğine katkı sağlayacağı değerlendirilmektedir.

Diğer taraftan; varlık gruplarının yapısının dinamik olmasından dolayı bulgu yazılan bir varlık bileşeninin izlemenin yapıldığı dönem süresince farklı bir varlık grubuna taşınması, kurumlarda denetimi gerçekleştiren denetim ekiplerinin her sene bu denetimi en az bir defa yapmaları ve sonuç odaklı izleme ve değerlendirme sürecinin de en az bir denetim kadar uzun sürebileceği gibi nedenlerle sınırlı denetim kaynağı ile izleme sürecinin zorlukları da dikkate alınmalı, her bir izleme için kurum içinde "İzleme Raporu" oluşturularak yeknesaklığın sağlanması gereklidir.

4.4. Denetim Raporunun Her Sayfasının e-imza ile İmzalanması

Son yıllarda yaşanan dijital dönüşüm süreci kamu yönetimini ciddi oranda etkilemiştir. Bürokratik işlem fazlalığı ve gereksiz prosedürler e-devlet uygulamalarıyla birlikte azaltılarak zaman ve maliyet açısından önemli ölçüde kazanç elde edilmesine rağmen iş yapış tarzındaki bürokratik işlemlerin büsbütün ortadan kaldırıldığı da söylenemez (Taş vd., 2017, s. 2317). Örneğin denetim raporunun her sayfasının imzalanması gibi.

BİGDR "*3.3.1. Denetim Raporunun Hazırlanması ve Kuruma Sunumu*" başlıklı bendi hükümleri kapsamında denetim raporunun her sayfasının e-imza ile imzalanması süreci denetim ekibindeki denetçi sayısı ve raporun sayfa sayısına bağlı, oldukça zaman almaktadır. Oysa ki kamu kurum ve kuruluşlarının birçoğunda e-imza kullanılan *Elektronik Belge Sistemleri (EBYS)* üzerinden yazışmalar yürütülmektedir. Bu nedenle söz konusu sistemlerin kullanıldığı kurumlarda, kurum iç denetçileri tarafından hazırlanan raporların, ayrıca her sayfasının e-imza ile imzalanması ihtiyacı bulunmadığına dair bir kolaylık getirilmesinin, sürece ciddi katkı sağlayacağı değerlendirilmektedir.

4.5. BİGDES Denetim Görüşü Bölümü Uygulanması Gereken Toplam Tedbir Sayısı Algoritmasının Güncellenmesi

Denetim Rehberi ekindeki örnek formata göre denetim görüşü (*EK-H*) içinde yer verilen tedbirlerin etkinlik durumlarına ilişkin özet tabloda; her bir varlık grubuna uygulanması gereken toplam tedbir sayısı, bu tedbirlerin etkinlik durumları sayısı "*Etkin*", "*Etkin Değil*", "*Kısmen Etkin*" şeklinde belirlenmiştir. Bu bakımdan; aşağıdaki tabloda sunulduğu biçimde seçilen varlık grubunda uygulanan tedbirlerin elli adedi etkin, otuz adedi etkin değil ve yirmi adedi kısmen etkin ise uygulanması gereken toplam tedbir sayısının bu üç durumun toplamı olacak biçimde yüz adet olması ve doğal olarak bu toplamda tedbir uygulanma durumu "*Uygulanabilir Değil*" olan tedbirlerin yer almaması beklenir.

Hal böyle iken BİGDES sisteminde gerçekleştirilen otomatik hesaplamalarda, varlık gruplarına uygulanması gereken tedbir sayısı; EK-B'de belirlenen üst tedbir grupların esas alınması nedeniyle EK-F "*Tedbir Etkinlik Durumu*" tablosunda yer alan tedbirlerin uygunmasına ilişkin durumları gösteren sütunda "*Uygulanabilir Değil*" olarak belirlenen tedbirler dahil olarak hesaplanmaktadır.

Bu nedenle, aşağıdaki tabloda gösterildiği gibi uygulanabilir olmayan tedbir bulunması durumunda tedbir etkinlik durumlarına ilişkin toplam sayı ile BİGDES hesaplama sonuçlarında bulunan uygulanması gereken tedbirlerin toplamı örtüşmeyecektir.

Tablo 6: Uygulanması Gereken Toplam Tedbir Sayısı Hesaplama Örneği

Mevcut Durum	Uygulanması Gereken Toplam Tedbir Sayısı	Etkin Tedbir Sayısı	Etkin Olmayan Tedbir Sayısı	Kısmen Etkin Tedbir Sayısı	Uygulanabilir Değil Tedbir Sayısı
Denetim Rehberi	100	50	30	20	Tabloda yer verilmemiştir.
BİGDES Hesaplama Sonuçları	100	50	30	20	0
	130	50	30	20	30

Kaynak: Yazarlar tarafından oluşturulmuştur.

Tedbir etkinlik durumlarının toplamının, uygulanması gereken toplam tedbir sayısını göstermesi üst yöneticinin de imzaladığı anılan dokümanın tutarlılığı bakımından önemlidir. Bu nedenle; BİGDES hesaplama algoritmasında, üst tedbir grupları bazında uygulanması gereken toplam tedbir sayısından EK-F tabloda tedbir uygulanma durumu "*Uygulanabilir Değil*" olarak belirlenen tedbirlerin çıkarılarak "*Uygulanması Gereken Toplam Tedbir Sayısı*"nın belirlenmesi için gerekli güncellemenin yapılması önerilmektedir.

4.6. Tedbir Maddelerine KamuNet'in Teşvik Edilmesine Yönelik İlave Yapılması

İlgili kurumda gerçekleştirilen rehber denetiminde, kamu kurumları arasında çeşitli amaçlar için gerçekleştirilen veri transferlerinde ve bilgi paylaşımında KamuNet kullanım oranının rehberin mevcut haliyle değerlendirilemediği, bu nedenle de Kamu kurum ve kuruluşlarının KamuNet'i kullanmalarını teşvik ve hangi düzeyde/oranda KamuNet'i kullandıklarının değerlendirilmesi amacıyla BİGR tedbir maddeleri ve benzer biçimde BİGDR eki tablolara aşağıdaki tedbir maddelerinin ilave edilmesiyle KamuNet kullanımının teşvik edilebileceği, bunun da sürece olumlu katkı sağlayacağı değerlendirilmektedir.

Tablo 7: BİGR Eki Tablolar İlave Edilebilecek KamuNet Tedbir Maddeleri

Sıra No	Tedbir No	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3. VARLIK GRUPLARINA YÖNELİK GÜVENLİK TEDBİRLERİ				
3.1. Ağ ve Sistem Güvenliği				
3.1.6. Ağ Güvenliği				
X[7]	3.1.6.X	1	Kamu idareleri arasında gerekli olan veri iletişiminin KamuNet üzerinden yapılması	Kamu idarelerindeki siber güvenlik risklerinin azaltılması amacıyla aralarındaki gerekli veri iletişiminin, genel ağ yerine daha güvenli sanal bir ağ üzerinden sağlanması için KamuNet ağına dâhil olunmalıdır. Kurumun üst yönetimince kabul edilen bilgi güvenliği yönetim sistemi politikasına uygun şekilde KamuNet ile ilgili politika ve prosedürler tanımlanmalıdır.
X	3.1.6.X	1	KamuNet üzerinden sunulan/alınan hizmetlerin envanterinin tutulması	KamuNet üzerinden sunulan/alınan hizmetlerin envanteri tutulmalı ve güncelliği sağlanmalıdır.
X	3.1.6.X	2	Kamu kurum ve kuruluşlarının işletmeci ile arasındaki KamuNet ağı erişiminin yedekliliğinin sağlanması	Kamu idarelerinin işletmeci ile arasındaki KamuNet ağı erişimi farklı güzergâh ve santrallerde yedeklenmelidir.

Kaynak: Yazarlar tarafından oluşturulmuştur.

BİGR eki tablolarda yer alan tedbir maddelerine ilave edilebilecek KamuNet'e ilişkin tedbir önerileri Tablo 7'de, bu önerilere ilişkin BİGDR eki tablolara ilave edilebilecek denetim madde önerileri ise Tablo 8'de sunulmuştur.

7 BİGR'nin ilgili Tablosunda DDO tarafından belirlenecek tedbir sırasına göre numaralandırılacaktır.

Tablo 8: BİGDR Eki Tablolar İlave Edilebilecek KamuNet Tedbir Maddeleri Denetim Yöntemleri Önerisi

Sıra No	Tedbir No	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3. VARLIK GRUPLARINA YÖNELİK GÜVENLİK TEDBİRLERİ				
3.1. Ağ ve Sistem Güvenliği				
3.1.6. Ağ Güvenliği				
X[8]	3.1.6.X	Kamu idareleri arasında gerekli olan veri iletişiminin KamuNet üzerinden yapılması	Mülakat, Güvenlik Denetimi	KamuNet ağına dâhil olundu mu? KamuNet ağı aktif olarak kullanılmakta mıdır? Kamu idareleri arasındaki veri iletişiminin ne kadarı KamuNet üzerinden yapılmaktadır? KamuNet gereksinimleri karşılanmakta mıdır? Kurum üst yönetimince kabul edilen bilgi güvenliği yönetim sistemi düzenlemelerine uygun şekilde KamuNet ile ilgili politika tanımlanmış mıdır?
X	3.1.6.X	KamuNet üzerinden sunulan/alınan hizmetlerin envanterinin tutulması	Mülakat, Güvenlik Denetimi	KamuNet üzerinden sunulan/alınan hizmetlerin envanteri tutulmakta mıdır? Bu envanterin güncelliği nasıl sağlanmaktadır?
X	3.1.6.X	Kamu kurum ve kuruluşlarının işletmeci ile arasındaki KamuNet ağı erişiminin yedekliliğinin sağlanması	Mülakat, Güvenlik Denetimi	Kamu kurum ve kuruluşlarının işletmeci ile arasındaki KamuNet ağı erişiminin yedekliliği sağlanmış mıdır?

Kaynak: Yazarlar tarafından oluşturulmuştur.

8 BİGR'nin ilgili Tablosunda DDO tarafından belirlenecek tedbir sırasına göre numaralandırılacaktır.

4.7. İç Denetçilerin Sertifika Süreçlerinin Desteklenmesi

Tüm kamu kurumları ile kritik altyapı hizmeti sunan işletmelerin uymakla yükümlü olduğu BİGR'e uyum ve tedbirlerin etkinliğinin en az yılda bir defa denetlenerek sürecin etkin bir şekilde izlenmesi planlanmıştır. Farklı kurumlarda yer alan iç denetçiler ile yapılan bilgi alışverişlerinde çeşitli nedenlerle (denetimi gerçekleştirecek yetkinlikte iç denetçi kaynağı olmaması, kurumun rehber uyum sürecini tamamlayamaması nedeniyle tedbir uyum sürecinin değerlendirilememesi gibi) halihazırda rehber denetimi yapılamadığı görülmüştür. Kamu kaynaklarının etkin, ekonomik ve verimli kullanımı amacıyla süreklilik arz eden bu denetimler için ihtiyaç duyulan yetkin denetçi kaynağının oluşturulması, sürecin maliyet etkin bir biçimde sürdürülebilirliği açısından elzemdir. Bu bakımdan kamu kurumlarında Rehber denetimlerini gerçekleştirebilecek sınırlı sayıdaki iç denetçi kaynağının nitelik ve niceliğinin artırılmasına yönelik çalışmalara ihtiyaç duyulmaktadır.

BİGDR ile belirlenen denetim ekibinin sahip olması gereken yetkinlikler "*ISO/IEC 27001 Baş Denetçi Sertifikası*", "*CISA Sertifikası*" veya TSE tarafından verilen D1 tipi "Ağ ve Sistem Denetçisi" veya D2 tipi "*Uygulama Denetçisi*" sertifikalarıdır.

BT alanında denetim yapacak denetçi, veri koruma, kayıt yönetimi süreçleri, güvenlik, kontroller ve teknoloji süreçlerinde uzmanlığa sahip olmalıdır. Denetçi ayrıca iş stratejisiyle uyumu belirlemek için yeterli işlevsel bilgiye ve iş bilgisine sahip olmalıdır. Uluslararası bilgi teknolojileri denetimi standartları arasında kabul edilen ISACA ITAF (IT Audit Framework) 1006 standardı denetçinin değerlendirilen alanlarda teknik beceri, bilgi ve/veya deneyime sahip olmasını gerektirir (ISACA, 2021) .

Bununla birlikte bu duruma bir istisna getirilerek kamu kurum ve kuruluşlarında Rehber denetimlerini gerçekleştirecek iç denetçilerin yukarıda sayılan sertifikalara sahip olmaması durumunda iç denetçinin bilgi güvenliği eğitimi almış olması da yeterlidir. Ancak Rehber denetimlerinde özellikle alınan tedbirlerin etkinliğinin değerlendirilebilmesi için denetimi gerçekleştirecek personelde ileri düzeyde BT denetim yetkinliğine gereksinim duyulmaktadır.

İDKK tarafından hazırlanan 2021 yılı Kamu İç Denetim Genel Raporu'nda[9],

9 2021 yılı Kamu İç Denetim Genel Raporu için bkz: https://ms.hmb.gov.tr/uploads/2022/08/2021-Kamu-Ic-Denetim-Genel-Raporu-Son-Hali.pdf

kamu kurumlarındaki iç denetim birimlerinde görev yapan iç denetçilerin sadece yedisinin CISA sertifikasına sahip olduğu görülmektedir. Rehber denetimlerinden gereken faydanın sağlanması için bu sayının artırılmasına yönelik projelerin hızlıca hayata geçirilmesi oldukça önemlidir.

Kamu kurum ve kuruluşlarında Rehber denetimini gerçekleştirebilecek, BT konusunda yetkin kısıtlı iç denetim kaynağının olgunluk seviyesini artırmak amacıyla BİGDR'de belirlenen temel sertifikalar olarak sayılan CISA, TSE D1 (Ağ ve Sistem Denetçisi) ve D2 (Uygulama Denetçisi) gibi sertifikasyonların teşvik edilmesi, kamu yararı çerçevesinde ihtiyaç duyulan sertifikalarla ilgili eğitim ve sınav ücretlerinin kurumlar tarafından karşılanması amacıyla projelerin hayata geçirilmesi için DDO ile İDKK koordinasyonunda çeşitli fonların (IPA, AB vb.) kullanımının sağlanmasının sürece katkı sağlayacak anahtar çözümlerden biri olduğu görülmüştür.

4.8. Rehber Denetimi Yapabilecek İç Denetçi Havuzunun Oluşturulması

Bir önceki öneride belirtildiği üzere yıllara sari bir yapıda BT konusunda yetkin iç denetçiler tarafından icrası gereken Rehber denetimlerinin maliyet etkin biçimde sürdürülebilirliği; ancak ve ancak kamuda istihdam edilen yetkin iç denetçi kaynağının etkin biçimde kullanımı ile mümkündür. Bu bilinçle BİGDR'de söz konusu denetimlerin farklı kamu kurumlarında görev yapan iç denetçilerin denetimin gerçekleştirileceği idarelerde geçici olarak görevlendirilmesi yoluyla yapılmasına da müsaade edildiği görülmektedir.

Bununla birlikte uygulamada zaten sınırlı sayıdaki BT konusunda yetkin mevcut iç denetçi kaynağının kamuda etkin olarak kullanımının koordinesinde sorunlar yaşanabildiği ve Rehber denetimi gerçekleştiremeyen çok sayıda kurum olduğu görülmüştür. Bu nedenle, kurumunda iç denetçi bulunmayan veya BİGDR'de belirlenen yetkinliklere sahip denetim kaynağı mevcut olmayan ve(ya) rehber denetimlerini hizmet alımı yoluyla gerçekleştiren kamu kurum ve kuruluşlarının denetimlerinin, diğer kamu kurumlarında görev yapan iç denetçiler tarafından kurum dışı görevlendirme yoluyla yapılmasına yönelik kamu personel yönetimine zarar vermeden İDKK ve DDO koordinesinde bu denetimleri yapma yetkinliği bulunan iç denetçilerin olduğu bir denetçi havuzunun oluşturulması için yasal altyapının oluşturulması kaynakların ve denetim faaliyetlerinin etkili, etkin ve ekonomik kullanılmasını sağlayacaktır.

İç denetçilere istekleri dışında farklı bir görev verilemeyeceği, yaptırılamayacağı ve atanamayacağına ilişkin merî mevzuat hükümleri dikkate alınarak denetçi havuzunun gönüllü iç denetçiler tarafından oluşturulması gerektiği aşikardır. Bu nedenle; Rehber denetimlerini gerçekleştirecek gönüllü iç denetçilerden denetçi havuzu oluşturulması, havuzda yer almanın teşviki amacıyla denetimlerin görev kabul onayı ile gerçekleştirilmesi ve havuzun genişletilmesine yönelik BT konusunda yetkin iç denetçi atamalarının teşvik edilmesi amacıyla kurumlara sağlanan kontenjanlardan muaf tutulması, işin niteliği nedeniyle Rehber denetimlerinde görevlendirilecek iç denetçilere ek mali olanakların sağlanması da düşünülmelidir.

SONUÇ

Dijital dönüşüm ve siber güvenlik çalışmalarını yalnızca yeni teknolojileri devreye almak olarak algılamaktan ziyade bu dönüşümün, kurumsal yeniden yapılanma modeli olarak, yeni yönetim ve denetim yapısının tasarlanması şeklinde düşünülmesi gerekmektedir. Siber güvenlik ekosistemini sadece BT olarak değil, bir beka sorunu olarak gören kamu idareleri, BT alanında ortaya çıkabilecek olası krizlerle karşılaşmamak için diğer risklerde olduğu gibi BT risklerini de öngörmek ve bu risklere karşı önlemlerini almak ve ihtiyaç duyulan denetimleri ilgili kurumlarda gerçekleştirmek zorundadır. Dünyada siber güvenliği tek seferde sağlanan ya da alınan bir ürün olarak görmeyerek bunu bir süreç olarak değerlendiren ve bu alanda söz sahibi olacak ülkeler bahsedilen riskleri ön görerek önlem alanlardan olacaktır.

Birçok alanda olduğu gibi dijital dönüşüm ve siber güvenlik alanında da ülkesel gelişmeler oldukça önemli bir durum haline gelmekle birlikte siber dünyada ülkelerin geldiği aşama net olarak bilinememektedir. Sun Tzu'nun "Savaş Sanatı - *The Art of War*" adlı eserindeki "*Kendini ve rakibini biliyorsan korkmana gerek yok, kendini biliyor ancak rakibi bilmiyorsan kazandığın her galibiyet için bir mağlubiyette yaşayacaksın, kendini ve düşmanını da bilmiyorsan her durumda yenilirsin*" (Tzu, 2019) ifadesinden hareketle Türkiye'nin de milli siber ekosistemini geliştirmesi ve açıklarını kapatması gereklidir.

Siber saldırıların artacağı yakın gelecekte kurumlar ikiye ayrılacaktır. Birinci grup, siber saldırıya uğradığını bilenler; ikinci grup ise bu saldırıya maruz kaldığını fark etmeyenler olacaktır. Türkiye'de "Ülke olarak olası bir siber saldırıya ve(ya) savaşa kurum ve kuruluşlar ne kadar hazır?" sorusuna cevap verebilmek için öncelikle denetim faaliyetlerinin yapılabilirliğinin sorgulanması oldukça önemlidir.

İDKK tarafından yayımlanan "*Kamu İdarelerindeki İç Denetim Faaliyetlerine İlişkin Duyuru*"[10] dikkate alındığında kamu kurum ve kuruşlarının tamamında ya iç denetim birimi bulunmamakta ya da iç denetim birimi bulunmasına rağmen kurumlar Rehberde öngörülen denetimi gerçekleştirecek yetkinlik ve yeterlikte iç denetçiye sahip değillerdir (İDKK, 2022b). BİGR'de bu gibi denetim kaynağı

10 Duyuru metni için bkz: https://www.hmb.gov.tr/duyuru/kamu-idarelerindeki-ic-denetim-faaliyetlerine-iliskin-duyuru.

bulunmayan durumlarda denetimin hizmet alımı yoluyla özel sektörden karşılanacağını belirtilse de gerek mesleki gelişimin sürdürülmesi, gerek iç denetim atamalarının sağlanması, gerek siber güvenlik alanında uzman kalifiye personelin yetiştirilmesi gerekse de kamu kaynaklarının verimli, etkili ve ekonomik olarak kullanılması için kamu kurumlarında gerçekleştirilecek denetimlerin kamu iç denetçileri eliyle yürütülmesinin daha faydalı olacağı değerlendirilmektedir.

BİGDR denetiminin birincil uygulayıcısı olan iç denetçilerin Rehberde kendilerine tanımlanan uyum sürecinin ve tedbirlerinin etkinliğinin değerlendirilmesi olarak özetlenebilecek Rehber denetimlerinin yanısıra görev yaptıkları kurumlarda tüm birimlerde dijital dönüşüm farkındalığının sağlanmasına ve dijital dönüşüm yol haritasının ilgili üst kademe yönetimince oluşturulmasına katkıda bulunması, faaliyetlerin gerçekleştirilmesi ile ilgili kurumsal kültürün Rehber çerçevesinde iyileştirilmesi oldukça önemlidir. Öte yandan iç denetimin denetim fonksiyonunun yanısıra danışmanlık fonksiyonunun da bulunması nedeniyle iç denetçinin rehberdeki bazı rol ve sorumluklarda danışılan rol olarak da yer alması alanında uzman teknik personel olarak değerlendirilen BT alanında görev yapan iç denetçilerin bilgi ve tecrübelerinden daha fazla faydalanılmasına olanak sağlayacaktır.

Bu çalışmayla, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanan Bilgi ve İletişim Güvenliği Rehberi ile Bilgi ve İletişim Güvenliği Denetim Rehberine dikkat çekmenin yanı sıra çalışmada belirtilen sınırlılıklar çerçevesinde belirlenen kamu iç denetçilerine yapılandırılmamış beş sorudan oluşan anket yönteminin uygulanması sonucunda karşılaşılan ve iyileştirilmesi gereken alanlar belirtilerek atılacak iyileştirici adımlar için aşağıda özetlenen hususlarda çözüm yolları önerilmiştir.

- Varlık grubu kritiklik derecelendirme puanlamaların güncellenmesi,
- Bulgu tablosuna bulgu tanımı ifadesinin eklenmesi,
- Bulgu izleme sürecinin iyileştirilmesi,
- Denetim raporunun her sayfasının e-imza ile imzalanması,
- BİGDES denetim görüşü bölümü uygulanması gereken toplam tedbir sayısı algoritmasının güncellenmesi,
- Tedbir maddelerine KamuNet'in teşvik edilmesine yönelik ilave yapılması,

- İç denetçilerin sertifika süreçlerinin desteklenmesi,
- Rehber denetimi yapabilecek iç denetçi havuzunun oluşturulması.

Yapılan bu ve benzeri akademik çalışmaların literatüre katkı sağlayacağı gibi uygulayıcılara da yol göstereceği temenni edilmektedir.

KAYNAKÇA

Ağdeniz, Ş. (2021). Bilgi ve İletişim Güvenliği Denetiminde Kamu İç Denetçilerinin Rolü ve Yetkinliklerine İlişkin Bir Araştırma. *Alanya Akademik Bakış*, 5(2), 525-545. DOI: 10.29023/alanyaakademik.869215.

Ak, T. (2019). İç Güvenlik Yönetimi Açısından Kritik Altyapılarını Korunması. *Assam Uluslararası Hakemli Dergi 13. Uluslararası Kamu Yönetimi Sempozyumu Bildirileri Özel Sayısı*, 42-51.

Aloul, F.A. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, 3(3), 176-183. DOI:10.4304/jait.3.3

Appelbaum, D., ve Nehmer, R.A. (2017). Using Drones in Internal and External Audits: An Exploratory Framework. *Journal of Emerging Technologies in Accounting*, 14, 99-113.

Arslan, Y ve Özbilger H.İ. (2022). Ulusal Mevzuat Perspektifinde Bilgi İşlem Birimlerinin İç Denetiminde Bir Model Önerisi, *Denetişim*. 13(26), 1-12.

Bahar, M. ve Somuncu Demir, N. (2021). Delphi tekniği uygulama sürecine yönelik örnek bir çalışma: Çok fonksiyonlu tarım okuryazarlığı. *Bolu Abant İzzet Baysal Üniversitesi Eğitim Fakültesi Dergisi*, 21(1), 35-53. https://dx.doi.org/10.17240/aibuefd.2021.21.60703-814729

Barrigon, C.F. (2020). Innovation and Digital Auditing The Journey of The European Commission's IAS Towards State-Of-The-Art Technologies. *ECA Journal*, 97-100.

Bartz, D. ve Alper A. (2023). U.S. Bans New Huawei, ZTE Equipment Sales, Citing National Security Risk, REUTERS, https://www.reuters.com/business/media-telecom/us-fcc-bans-equipment-sales-imports-zte-huawei-over-national-security-risk-2022-11-25. 14.03.2023 tarihinde erişildi.

BBC (2018). Facebook Scandal 'Hit 87 Million Users', https://www.bbc.com/news/technology-43649018. 05.07.2023 tarihinde erişildi.

Bıçakçı, S. (2013). *21. Yüzyılda Siber Güvenlik*. Bilgi Üniversitesi Yayınları.

Bilge, S. ve Kiracı, M. (2010). *Kamu Sektöründe İç Denetim ve İç Denetimin Başarıyla Uygulanmasında Rol Oynayan Faktörler (Kamu İç Denetçileri Üzerine Bir*

Araştırma). Gazi Kitabevi.

Chu, B. ve Holt, T.J. (2012). *Examining the Creation, Distribution, and Function of Malware On-Line*. Bibliogov Publisher.

DDO. (2020). Bilgi ve İletişim Güvenliği Rehberi. Ankara: T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi.

DDO. (2021). Bilgi ve İletişim Güvenliği Denetim Rehberi. Ankara: T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi.

DDO. (2023). Dijital Devlet Stratejisi. https://cbddo.gov.tr/dijital-devlet-stratejisi. 15.01.2023 tarihinde erişildi.

Darıcılı, B. A. (2014). Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırılar, *Uludağ Üniversitesi Sosyal Bilimler Dergisi*, 7(2), 1-16.

DPT (2000). Uzun Vadeli Strateji ve Sekizinci Beş Yıllık (2001-2005) Kalkınma Planı. Ankara: T.C. Başbakanlık Devlet Planlama Teşkilatı.

Gupta, M. (2020). *Asian Journal of Government Audit*. (Ed.) Singh K. ASOSAI.

ISACA. (2021). Blockchain Framework Audit Program. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-25/new-resource-evaluates-blockchain-controls. 03.02.2023 tarihinde erişildi.

ITU. (2021). Global Cybersecurity Index 2020. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf, 15.03.2023 tarihinde erişildi.

İDKK. (2022a). 2021 Yılı Kamu İç Denetim Genel Raporu, chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://ms.hmb.gov.tr/uploads/2022/08/2021-Kamu-Ic-Denetim-Genel-Raporu-Son-Hali.pdf. 05.02.2023 tarihinde erişildi.

İDKK. (2022b). Kamu İdarelerindeki İç Denetim Faaliyetlerine İlişkin Duyuru, https://www.hmb.gov.tr/duyuru/kamu-idarelerindeki-ic-denetim-faaliyetlerine-iliskin-duyuru. 11.02.2023 tarihinde erişildi.

Karagöz, U. (2022). Bilgi ve İletişim Güvenliği/Denetimi Rehberleri ve İç Denetim. İdarecinin Sesi Dergisi, 210.

Kavitha, V. ve Preetha. S. (2019). Cyber Security Issues and Challenges - *A Review. International Journal of Computer Science and Mobile Computing*, 8(11),

1-16.

Kızılboğa, R. (2013). İç Denetim Sisteminde Denetçilerin Bağımsızlık ve Tarafsızlığının Önemi. *Siyasal Bilgiler Dergisi*, 1(1), 107-121.

Kusek J. Z. ve Rist R.C. (2004). *Ten Steps to a Results-Based Monitoring and Evaluation System: A Handbook for Development Practitioners*, World Bank Publications.

Lambet, P. (2017). Equifax Data Breach, 143 Million Only Tip of the Iceberg. *Int'l J. Data Protection Officer, Privacy Officer & Privacy Couns*, 30, 33-34.

Lois, P., Drogalas, G., Karagiorgos, A. ve Tsikalakis, K. (2020). Internal Audits in the Digital Era: Opportunities Risks and Challenges. *EuroMed Journal of Business*, 15(2), 205-217. http://doi.org/10.1108/emjb-07-2019-0097.

Meral, S. ve Bülbül, H.İ. (2022). Kamu Kurumlarının Bilgi Güvenliği Politikalarının Kurumsal Bilgi Güvenliğinin Sağlanması Açısından Etkinliğinin Analiz Edilmesi, *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji*, 10(2), 314-329. DOI: 10.29109/gujsc.1001706.

Morgan, S. (2019). Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021. 12.03.2023 tarihinde erişildi.

Nelson N.N., ve Madnick, S (2020). Case Study of the Capital One Data Breach, Information Institute Conferences, Las Vegas, NV, Mar 30 Apr 01, 2020, https://www.researchgate.net/publication/340012934_A_Case_Study_of_the_Capital_One_Data_Breach. 12.03.2023 tarihinde erişildi.

OECD (2003). Emerging Risks in the 21st Century. Paris: OECD Publications Service.

Otia, J. E. ve Bracci, E. (2022). Digital Transformation and the Public Sector Auditing: The SAI's Perspective. *Financial Accountability & Management*, 38, 252–280. https://doi.org/10.1111/faam.12317.

Özçayan, G. ve Aslan, N. (2021). Standardızatıon of Trıtıum By Cıemat/Nıst Method Wıth Lıquıd Scıntıllatıon Countıng in Turkey and Uncertaınty Budget . *Turkish Journal of Nuclear Sciences*, 33(1), 26-36.

Özen, A. ve Gürel, F.N. (2022). Kamu Denetiminde Dijital Dönüşüm: Dijital İkiz Yöntemi. *İzmir Sosyal Bilimler Dergisi*, 2(1), 16-23.

Özkaya, E. (2018). *The Art of Human Hacking: Learn Social Engineering with Internationally Renowned Expert*. Packt Publishing.

Özkaya, E. (2023). Güncel Küresel Siber Eğilimler ve Alınması Gereken Önlemler. 6. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi, Ankara: 14-15 Mart 2023.

Page, G. (2102). North Korea's Lazarus hackers are exploiting Log4j flaw to hack US energy companies. https://techcrunch.com/2022/09/08/north-korea-lazarus-united-states-energy. 13.03.2023 tarihinde erişildi.

Ping, G. (2016). What should we do before 5G? https://www.huawei.com/us/huaweitech/publication/winwin/25/what-should-we-do-before-5g. 11.03.2023 tarihinde erişildi.

Pizzi, S., Venturelli, A., Variale, M. ve Macario, G.P. (2021). Assessing the Impacts of Digital Transformation on Internal Auditing: A Bibliometric Analysis. *Technology in Society*, 67, 1-11.

Potii, O. (2018). Cybersecurity Ecosystem. https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2018/05_Kiev/ITU%20Seminar%2015.05.18%20-%20Oleksandr%20Potii.pdf. 13.03.2023 tarihinde erişildi.

Sağıroğlu, Ş. ve Şenol M. (Ed.) (2018). *Siber Güvenlik ve Savunma*: *Farkındalık ve Caydırıcılık.* BGD Siber Güvenlik ve Savunma Kitap Serisi 1, Grafiker Yayınları.

Savita, M. ve Patil, M. (2017). A Brief Study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5), 1938-1940.

Schwab, K., Marcus, A., Oyola, J.R., Hoffman, W. ve Luzi, M. (2011). Personal Data: The Emergence of a New Asset Class. An Initiative of the World Economic Forum. https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf. 11.03.2023 tarihinde erişildi.

Selimoğlu, S. ve Saldı, M.H. (2022). İç Denetimin Blok Zincir Yoluyla Siber Güvenlik Yönetimine Adaptasyonu. *Denetim ve Güvence Hizmetleri Dergisi*,

2(2), 121-134.

Shepardson, D. (2023). Exclusive: White House Sets Deadline For Purging Tiktok From Federal Devices, REUTERS, https://www.reuters.com/technology/white-house-gives-agencies-30-days-impose-federal-device-tiktok-ban-2023-02-27. 14.03.2023 tarihinde erişildi.

Stewart, J., ve Subramaniam, N. (2010). Internal Audit İndependence and Objectivity: Emerging Research Opportunities. *Managerial Auditing Journal*, 25(4), 328-360.

Taffel, S. (2021). Data and Oil: Metaphor, Materiality and Metabolic Rifts. *New Media & Society*, 0(0). 140-175.

Taş, İ. , Uçacak, K. ve Çiçek, Y. (2017). Türk Kamu Yönetiminde Yaşanan Dijital Dönüşümün Bürokratik İşlemlerin Azaltılması Üzerindeki Etkileri. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi Kayfor 15 Özel Sayısı*, 2303-2319.

Tzu, S. (2019), *The Art of War.* (Çev.) Giles, L., Karbon Kitaplar.

Tulgar M., Zaim A. ve Aydın M.A. (2022). Ulusal Bilgi ve İletişim Güvenliği Rehberi: IOT Güvenliği İçin Bir Uygulama Örneği. İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 21(42), 353-382.

UDHB (2014). Kurumsal SOME Kurulum ve Yönetim Rehberi. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/kurumsal-some-reh-v1.pdf. 29.02.2023 tarihinde erişildi.

Verma, A. ve Charu, S. (2022). Cyber Security: A Review of Cyber Crimes, Security Challenges and Measures to Control. *Vision: The Journal of Business Perspective*, 09(0), 24-45.

Yanık, S. ve Karataş, M. (2017). Denetim Raporlarının Geleceği: Yeni Düzenlemeler ve Ülke Uygulamaları. *Muhasebe ve Finansman Dergisi*, (73), 1-26. DOI: 10.25095/mufad.396739.