HAKEMLİ Denetişim
Ortak Aklın Harmanı
Kamu İç Denetçileri Derneği Meşrutiyet Caddesi Konur Sokak No: 36/6 Kızılay - ANKARA
www.kidder.org.tr/denetisim/ • denetisim@kidder.org.tr
ISSN 1308-8335
Yıl: 13, Sayı: 26, 1-12, 2022

Araştırma Makalesi

ULUSAL MEVZUAT PERSPEKTİFİNDE BİLGİ İŞLEM BİRİMLERİNİN İÇ DENETİMİNDE BİR MODEL ÖNERİSİ

(INTERNAL AUDIT OF IT UNITS IN THE PERSPECTIVE OF NATIONAL LEGISLATION A MODEL SUGGESTION)

Dr. Öğr. Üyesi Yenal ARSLAN[1], Halil İbrahim Özbilger[2]

ÖZ

İç denetçiler, yaptıkları denetimleri belirlenmiş standart ve regülasyonlara dayandırmaktadır. Literatürde, bilişim sistemleri denetiminde kullanılan uluslararası standartlar ve siber güvenlik konusunda birçok çalışma olmasına rağmen ülke regülasyonları hakkında fazlaca çalışma bulunmamaktadır. Yapılan bu çalışmada, Türkiye kamu bilişim yöneticileri ve iç denetçilerine fayda sağlamak ve literatüre katkı sunmak amacıyla kamu kurumlarının uyması gereken mevzuatın derlemesi yapılarak kamu iç denetçileri açısından bir denetim kontrol listesi ortaya konulmuştur.

Anahtar Kelimeler: İç Denetim, Bilgi Teknolojileri, Bilişim Yönetişimi, Uyumluluk

JEL Kodları: M48

ABSTRACT

Internal auditors base their audits on standards and regulations. Although there are many studies on international standards and cyber security used in information systems auditing in the literature, there are not many studies on country regulations. In this study, an audit checklist has been put forward for public internal auditors by compiling the legislation that public institutions must comply with in order to benefit the public information managers and internal auditors of Turkey and contribute to the literature.

Keywords: *Internal Audit, Information Technologies, Information Governance, Compliance.*

JEL Classification: *M48*

1. GİRİŞ

Bilgi ve iletişim teknolojilerindeki gelişmeler; büyük miktarda bilgiyi kullanıma sunmuş, kurumların işlerini yürütme şeklini değiştirmiş, faaliyetlerin daha verimli, etkili, hızlı, anlaşılır bir şekilde yürütülmesini sağlamasının yanında maliyet tasarrufu ve insan hatalarını azaltmıştır. Ancak bu olumlu gelişmeler aynı zamanda kritik operasyonlar ve altyapılar için de önemli riskleri beraberinde getirmiş, veri yönetimi ve kaybı riski, teknolojik operasyonel riskler, veri manipülasyonu riski, bilgi güvenliği riskine de neden olmuştur.

Bilgi güvenliği alanındaki önemli ilerlemelere rağmen yaşanan gelişmeler göstermektedir ki birçok bilgi sistemi hala iç ve/veya dış saldırılara karşı savunmasızdır. Bu durum, yeterli güvenlik önlemlerinin alınmasını, bu saldırıların önlenmesini ve olumsuz sonuçların azaltılmasını gerektirmektedir. Bir kurumun bilgi teknolojisi uygulamalarının,

- Dr. Öğr. Üyesi, Ankara Yıldırım Beyazıt Üniversitesi Mühendislik ve Doğa Bilimleri Fakültesi, Yazılım Mühendisliği Bölümü, Ankara, Orcid Id: 0000-0002-1776-6091, yenalarslan@aybu.edu.tr, Sorumlu Yazar
- İç Denetçi, T.C. Ticaret Bakanlığı İç Denetim Birim Başkanlığı - Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Yönetim Bilimleri Anabilim Dalı Doktora Öğrencisi, Orcid Id: 0000-0002-9137-8855, hiozbilger@hotmail.com

altyapısının, veri kullanımının, politikalarının, prosedürlerinin, yönetiminin, operasyonel süreçlerinin kabul edilmiş standartlara göre incelenmesi ve değerlendirilmesi şeklinde ifade edilen bilgi teknolojisi (BT) denetimi onu yoğun şekilde kullanan çoğu kurum için kritik bir başarı faktörü durumuna gelmiştir.

BT'deki mevcut ve potansiyel riskler dikkate alındığında bilgi güvenliği kontrolü ve süreçlerinin etkinliğini düzenli olarak izlemek ve değerlendirmek gittikçe önemli bir konu haline gelmiştir (NIST, 2013, s. 7). Kurumlar, temel faaliyetler için BT sistemlerine dayanıyorsa, bu sistemlere yönelik risklerin kapsamı ve doğasının farkında da olması gereklidir. Bu nedenle, BT alanında güvenliği sağlamanın ilk adımı, riskleri ve bu risklerle ilgili uygun (örneğin güvenlik riskleri, kullanılabilirlik riskleri, performans riskleri ve uyumluluk riskleri ile ilgili) denetim yöntemlerinin belirlenmesidir.

Öte yandan BT'nin iç denetim faaliyetlerinin etkinliğini artırdığı, iç denetim mesleği üzerinde teknolojik gelişmelerin büyük bir etkiye sahip olduğu kabul edilmesi gereken bir durumdur (Harrison & Datta, 2007). Bu durum; kurumun etkin ve verimli faaliyetlerde bulunmasına yardımcı olması, hem yasal hem de idari düzenlemelere uygunluğunu kanıtlaması, potansiyel zorlukları karşılamaya hazır olup olmadığını teyit etmesi ve belki de en önemlisi, paydaşlara kurumun finansal, operasyonel ve birçok konuda güvence vermesi nedeniyle kurumsal risklere karşı bir tampon görevi gören geleneksel iç denetimin ciddi olarak sorgulanmasını gerektirmiştir (Özbilger, 2021, s. 49).

Araştırmalar, sürekli büyüyen bilgi teknolojilerinin gelişmesi nedeniyle iç denetçilerin geleneksel rolünün değiştiğini de ortaya koymuştur (George, Theofanis & Konstantinos, 2015). Uluslararası İç Denetçiler Örgütü (IIA)'ne göre; önlem alınmazsa ilerleyen dönemlerde en önemli risk faktörü durumuna gelecek BT risklerinin tespiti ve yönetimi hakkında anahtar pozisyonunda olacak iç denetim, risklerin tespiti konusundaki başarısı ve alanda yetişmiş tecrübeli denetçilerin varlığı sayesinde elektronik süreçlerin güvenliği açısından kritik öneme sahip olacaktır (IAA, 2020). Söz konusu analizin en önemli bileşenlerinden biri elbette iç kontrol çerçevesi bağlamında iç denetim fonksiyonunun yeterliliği ve etkinliğidir. BT alanında yaşanan önemli iş dönüşümü kurumların stratejisi ve operasyonlarını fazlasıyla etkilemesi nedeniyle yeni riskleri değerlendirme ve bu risklere maruz kalmayı etkin bir şekilde azaltmak için iç denetim kontrollerini değiştirme ihtiyacını doğurmuş ve iç denetçilerin rolü eskiye nazaran BT bilgisini daha fazla içerecek şekilde genişlemiştir (Stoel, Havelka, & Merhout, 2012, s.68).

Son yıllarda, artan farkındalığa ve çok sayıda ileri teknolojik ve süreç savunma mekanizmasına rağmen BT suçlarının artması sonucu veri bütünlüğü, veri gizliliği ve veri kullanılabilirliği hakkındaki kurumsal siber güvenlik politikaları, risk yönetimi süreçleri ve iç kontrollere uygunluk ve bunların korunmadaki etkinliği ile ilgili bağımsız kanıtlar elde etmek amacıyla gerçekleştirilen (IIA, 2016; FERMA, 2019; IIA, 2020) denetimler kurumun faaliyetlerini geliştirmek için tasarlanan bağımsız, nesnel güvence sağlayan iç denetim uygulamasını hızla gelişen bir alan haline getirmiştir (IIA, 2020). Sağlam iç kontrol ilkeleri, BT ile ilgili risklerin yönetimi ve denetimini üçlü hat modelinde düzenlenmesini önermektedir (COSO, 2019; IIA,2020). Eski haliyle "Üçlü Savunma Hattı" şeklinde isimlendirilen, 2020 yılı içerisinde güncellenerek BT ile ilgili her birinin önemli rollere sahip olduğu "Üçlü Hat Modeli" olarak adlandırılan yeni modele göre; ilk hatta, faaliyetleri yürütürken riske maruz kalan ve bu yönüyle riskleri üstlenerek kabul eden ve yöneten ilgili uygulayıcı birimler yer alırken birinci hattan bağımsız olarak ikinci hatta yer alan kurum çapında riskin daha fazla tanımlanmasından, ölçülmesinden, izlenmesinden ve raporlanmasından sorumlu BT ile ilgili birimler yer almaktadır. İç denetim işlevi ise, üçüncü hattan sorumludur: risk yönetişimi ve iç kontrol çerçevesi dâhil olmak üzere genel BT çerçevesinin etkin olduğuna dair kuruma güvence sağlamak için BT ile ilgili riske dayalı denetimler ve incelemeler gerçekleştirir. Bu nedenle, ilk iki hattın bağımsız bir şekilde gözden geçirilmesinden ve iş alanlarındaki mevcut ana zayıflıkları ele alarak kurum içinde proaktif olarak en iyi uygulamaları teşvik etmekten sorumlu olan iç denetim fonksiyonunun diğer denetim türlerinde olduğu gibi bilgi teknolojileri denetiminde de hayati ve önemli bir role sahip olduğunu söylemeye gerek yoktur (Deloitte, 2017).

Avrupa İç Denetçiler Enstitüsü Konfederasyonu (ECIIA) tarafından yürütülen çalışma sonuçlarına göre, BT alanındaki riskler gelecek ilk beş iş riskinden biri olarak kabul edilmiştir (ECIIA, 2020). Ancak, BT denetiminin pratikte nasıl yürütüldüğüne dair tanımlamalar hala büyük ölçüde eksiktir. Bu nedenle özellikle Türkiye gibi iç denetimin olgunlaşamadığı ülkelerde özellikle BT denetiminin etkinliğini ölçmek oldukça zordur. İç denetim fonksiyonunun amacı, kabul edilebilir bir risk düzeyine ulaşmak ve kayıpları en aza indirmek olmasına rağmen bu alandaki faaliyetler genellikle ya BT konusundaki eksiklik ya da ülke genelindeki yeterli teknik bilgiye sahip deneyimli iç denetçilerin eksikliği nedeniyle istenilen seviyeye ulaşamamıştır. Literatüre baktığımızda konu ile ilgili az sayıda çalışma yapılmıştır. Köse ve Polat yaptıkları çalışmada dijitalleşmenin denetim yöntem ve yaklaşımlarına, denetimin planlanmasına, kanıt toplamaya, uygunluk değerlendirmesine, işlem mutabakatına, bulgu ve önerilere, raporlamaya ve denetim verilerine etkisini değerlendirmişlerdir (Köse & Polat, 2021). Ağdeniz yaptığı çalışmada Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO) tarafından çıkarılan bilgi ve iletişim güvenliği rehberi uyum denetiminde kamu iç denetçilerinin rolü ve yetkinliklerini sertifika ve denetim sayıları temelinde değerlendirmeye çalışmıştır (Ağdeniz, 2021). Akmeşe yaptığı çalışmada karmaşıklaşan teknoloji uygulamaları ile siber saldırıların yöntemlerinin gelişmesi, dağınık bilgi teknolojileri mimarisi, üçüncü taraf hizmet sağlayıcılar ile genişleyen saldırı yüzeyi, siber güvenliğe ilişkin kontrol faaliyetlerinin uçtan uca tüm sistemler ile entegre edilememesi, insan kaynağı yetersizlikleri gibi durumların organizasyonların başarılı bir siber

güvenlik stratejisi uygulamalarını zorlaştırdığını ifade etmiştir. Sürekli gelişen ve değişen teknolojinin getirdiği riskleri yönetmek için iç denetim fonksiyonunun da kendini güncellemesi gerektiği aşikârdır (Akmeşe, 2020). Koç ve arkadaşları BT denetiminde bilgi güvenliği ile ilgili uluslararası standartlardan ve Türkiye'de bilgi güvenliği ile ilgili regülasyonlardan bahsetmişlerdir (Koç v.dğr., 2019). Dutta ve arkadaşları yaptıkları çalışmada organizasyonların fonksiyonlarını yerine getirmesi için çalışanlarına, iş süreçlerine ve teknoloji kullanımına ihtiyaç duyduğunu ve teknoloji kullanımının günümüzde şirket değerini belirlemede önemli bir parametre olduğundan bahsederek BT mimarisini ve süreçlerini, iş süreçlerini ve kullanıcıları göz önünde bulunduran bir BT olgunluk modeli önermiştir (Dutta v.dğr., 2022).

1.1. Problem

BT yönetişimi (Information Technology Governance) organizasyonlara iş hedeflerine ulaşmaları adına BT'de doğru kararların verilmesi ve risklerin yönetilmesi için uygun mekanizmalar sunar (Dutta ve diğerleri., 2022). BT yönetişiminin temelinde ise ulusal/uluslararası standartlar ve ulusal regülasyonlar bulunmaktadır. Denetim elemanları yaptıkları denetimleri bu standartlar ve regülasyonlara dayandırmaktadırlar. Yapılan literatür incelemelerinde uluslararası standartlar ve siber güvenlik konusunda çokça çalışma olmakla beraber ülke regülasyonları hakkında fazlaca çalışma olmadığı görülmüştür. Gerek bu nedenden gerekse Türkiye'de bilişim politikalarına yön veren tekil bir otorite bulunmadığından mütevellit mevzuatın derli toplu olmamasından dolayı zaman zaman kamu zararları da oluşmaktadır. Gerçekleştirilen çalışmada, aşağıdaki sorulara cevap aranmaya çalışılmıştır.

- Kamu idarelerindeki bilgi işlem daire başkanlıkları ya da ilgili genel müdürlüklerde idari açıdan bilişim mevzuatı nelerdir?
- Türkiye'de kamu iç denetimi açısından bakıldığında bilişim mevzuatı nelerdir?
- Türkiye'de kolluk kuvvetleri ve yargı açısından bilişim mevzuatı nelerdir?

1.2. Amaç

Kurumlar dijital dünyada rekabet etmek, müşteri ve vatandaş memnuniyetini sağlayabilmek için yeni dijital iş modellerini ortaya koymakta ve bu dijital teknolojileri organizasyon kültürüne entegre etmeye gayret sarf etmektedirler. İç Denetimin de bu eş güdümde hareket etmesi gereklidir (Görmen ve Korkmaz, 2022). Ancak yukarıdaki varsayımları kanıtlar nitelikte 2008-2019 Kamu İç Denetim Genel Raporları incelendiğinde diğer denetim türlerine kıyasla BT denetimi oransal olarak oldukça azdır. Diğer taraftan, Sertifikalı Bilgi Sistemleri Denetçisi (CISA - Certified Information Systems Auditor) sertifikasına sahip kamu iç denetçisinin sayısı yalnızca 5 (beş) dir (Arkın, 2022). Gerçekleştirilen çalışmada BT denetim sayılarını artırmak adına kamu sektöründe görev yapan BT yöneticileri ile iç denetçilere fayda sağlamak ve literatüre katkı sunmak amacıyla bilgi teknolojilerinin denetimi ile ilgili kamu kurumlarının uyması gereken mevzuatın derlemesi yapılarak kamu iç denetçileri açısından bir denetim kontrol listesi ortaya konulmaktadır.

1.3 Araştırmanın Temel Varsayımları, Sınırlılıkları ve Yöntemi

Çalışma, idari ve yargısal bilişim mevzuatının uygulanmasına dair birkaç varsayım yapılmıştır. Bunlar;

- İç denetim birimlerinde BT konusunda yetkin yeteri kadar iç denetçi bulunmaması.
- İç denetim birimlerinde BT konusunda mevzuatın yeteri kadar bilinmemesi.
- BT birimlerinde BT konusunda yasal ve idari mevzuatın yeteri kadar bilinmediği.

Araştırmada aşağıda belirtilen sınırlıkların mevcudiyeti kabul edilmiştir. Bu kapsamda;

- Çalışmanın yapıldığı tarih itibari ile güncel olan mevzuat değerlendirilmiş olup, mevzuatın daha önceki sürümlerine bakılmamıştır.
- Çalışmada tüm idari ve yargı mevzuatını değil konusu itibari ile BT ile ilişkilendirilebilen kısımlar incelenmiştir.
- Çalışmada ilgili mevzuat BT birim yöneticileri ve iç denetim bakış açısı ile incelenmiştir.
- Çalışmada incelenen mevzuatın dışında her kurumun ve organizasyonun kendi iç yönergeleri, uluslararası mevzuat ve standartlar değerlendirilmemiştir.

Araştırmada nicel olarak yapılmış ve temel olarak tarama yöntemi kullanılmıştır. Çalışmada, evrenin tümü ele alınmış herhangi örneklem alma yoluna gidilmemiştir.

2. YASAL ALTYAPI

Türkiye'ye ilk bilgisayarlar 1960'lardan sonra gelse de yaygın olarak kullanımı 1980'lerden sonra kişisel bilgisayarların ve x86 mimarisine sahip sunucu bilgisayarlarının ortaya çıkması ile olmuştur. Kamu kurumlarında 1990'lı yılların başından itibaren o güne kadar kurum içi uygulamalar amacı ile kullanılan ana bilgisayar sistemleri açık sistem denilen x86 mimariye sahip sunuculara taşınmıştır.

2000'li yılların başında e-Türkiye ve e-dönüşüm projeleri ile beraber iş süreçlerinin sayısallaştırılması hızlanmış ve o zamana kadar yalnızca kurum personeline ve üniversite araştırmacılarına sunulan kurumsal hizmetler internet ortamından vatandaşlara ve diğer paydaşlara sunulmaya başlanmıştır.

Aşağıda bu dönemde dijital dönüşümün yaygınlaştırılması amacı ile gerçekleştirilen bazı çalışmalar sunulmaktadır.

- Dünya Bankası İş Birliği ile Hazırlanan Bilişim ve Ekonomik Modernizasyon Raporu (1993)
- TUBİTAK Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) 'nin Kurulması (1996)
- Dış Ticaret Müsteşarlığı Bünyesinde Elektronik Ticaret Koordinasyon Kurulu (ETKK) 'nun kurulması (1997)
- Başbakanlığı 1998/13 Sayılı Genelgesi ile Kurulan Kamu-Net Kurulu (1998)
- Ulaştırma Bakanlığı ve TUBİTAK Tarafından Hazırlanan Türkiye Ulusal Enformasyon Altyapısı ve Ana Plan Çalışması (TUEANA) (1999)
- 2002 / 20, 2002 / 55, 2003 / 12, 2003 / 48 Sayılı Başbakanlık Genelgeleri ile Şekillendirilen e-Dönüşüm Türkiye Projesi
- 2018 / 1 Sayılı Cumhurbaşkanlığı Kararnamesi ile Dijital Dönüşüm Ofisi (DDO)'nin Kurulması

Öte yandan; e-dönüşümün hızlanması ile beraber artan uygulama ve sunucu enflasyonunu yönetmek, verilerin bütünlüğünü, güvenliğini ve erişilebilirliğini sağlamak, kişisel verileri korumak, internetin kötüye kullanımını önlemek amacı ile çeşitli standart ve yasalar 1980'li yıllardan itibaren tüm dünyada uygulanmaya başlamıştır.

Son dönemde bilgi teknolojileri, siber güvenlik ulusal bir alan haline gelmiş ve mevcut kanunlara ek olarak bu konuda çok sayıda tebliğ, plan ve rehber yayınlanmıştır. Aşağıda ayrı alt başlıklarda BT ile ilgili mevcut düzenlemeler hakkında kısaca bilgi verilerek değerlendirilmektedir.

2.1. 5237 Sayılı Türk Ceza Kanunu

Bilişim suçları açısından baktığımızda Türkiye'deki ilk yasal mevzuat Türk Ceza Kanunu (TCK)'na 1991 yılında eklenen bilişim sistemine girme, sitemi engelleme ve sistemi bozma suçlarıdır (Kızıltan, 2007). Bu mevzuata ek olarak özel hayata ve gizliliğine karsı suçlar kısmında kişisel verilerin kaydedilmesi, ele geçirilmesi, verilerin yok edilmemesi suçları da bilişim yoluyla işlendiğinden bilişim suçu olarak değerlendirilebilir. TCK'da bilişim ile alakalandırılabilecek diğer suçlar ise hâlihazırda uygulandığı şekliyle organ ticareti, tehdit, taciz, hırsızlık, hakaret, uyuşturucu madde kullanılmasını özendirme, Cumhurbaşkanına hakaret ile devletin egemenlik alametlerini, kurum ve organlarını, cumhuriyeti ve Türklüğü aşağılama olarak sıralanabilir (Akaslan, 2021).

Her ne kadar kamu idareleri açısından yürürlükte olan mevzuatın bir kısmında doğrudan idari ve mali yaptırımlar belirtilmese de bu mevzuatlarda belirtilen tedbirlerin ve faaliyetlerin yerine getirilmediğinde kurum zarara uğruyorsa veya vatandaş ve paydaş zarara uğruyorsa, kasıt ve ihmal yönünden TCK'nın 256. Maddesine göre görevi kötüye kullanma suçu kapsamına girmektedir. Ancak kurumların görevleri net ve açık bir şekilde belirlemesi ve personele doğru şekilde tebliğ etmesi gerekmektedir.

2.2. 5846 Sayılı Fikir ve Sanat Eserleri Kanunu

Ülke mevzuatı tarandığında TCK'dan farklı olarak bilişim suçları ile alakalı karşımıza çıkan bir diğer kanun 5846 sayılı Fikir ve Sanat Eserleri Kanunudur. Kanunda fikri ve sınai bir hak olarak değerlendirilen bilgisayar yazılımlarına ilişkin izinsiz kopyalamalar ve kullanımlara karşı telif hakkı suçları düzenlenmiştir. Buna göre, web sayfaları ve bilgisayar programları dâhil olmak üzere her türlü fikir ve sanat eserini izinsiz olarak kullanan, işleyen, çoğaltan, bilgisayar programlarını koruyan aygıtları geçersiz kılan teknik araçları (keygen ..vb) bulunduran, dağıtan ve izinsiz olarak yayınlayanlar siber suçlu olarak kabul edilmektedir. Buradan hareketle denetim açısından bakıldığında kamu ya da özel

sektör bilgi işlem departmanlarında veya iş birimlerinde kaçak lisanslı ürün kullanılması veya eksik lisans kullanması (örneğin kurumda 2000 personelin kullandığı bir ürünün 250 lisansla satın alınıp geri kalanınca lisanssız kullanımı) kanuna göre suçtur (Arslan, 2022a).

2.3. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" 23.05.2007 tarihinde resmî gazetede yayımlanarak yürürlüğe girmiştir. Kanunla internet ortamındaki içerik üreticileri, yer sağlayıcılar (sunucu ve web sayfası gibi), erişim sağlayıcılar (internet servis sağlayıcılar ya da kurumsal internete çıkış hizmeti veren organizasyonlar) ve toplu kullanım sağlayıcıların sorumluluk ve yükümlülükleriyle internette gerçekleşen suçlarla mücadeleye ilişkin usul ve esaslar düzenlenmiştir. Kanun içerik, yer, erişim ve toplu kullanım sağlayıcılarına çeşitli sorumluluklar yüklemektedir. Buna ek olarak 1 Ekim 2020'de söz konusu kanunda değişiklik yapılarak Türkiye'de yoğun kullanılan sosyal medya devlerinin de suçla mücadeleyi kolaylaştırmak ve hızlandırmak açısından Türkiye de ofis açması istenmiştir.

Erişim sağlayıcı olarak değerlendirildiğinde kamu kurumları ve işletmeler çalışanların ve misafirlerin adli ve idari merciler tarafından istenmesi durumunda herhangi bir kullanıcısının yayınladığı mevzuata aykırı içeriğe erişimi teknik olarak engelleme imkânı bulunduğu ölçüde engellemeli, personelin ve misafirlerin internet trafik bilgisini en az 6 ay en fazla 2 yıl saklamalı ve bu bilgilerin doğruluğunu, bütünlüğünü, gizliliğini sağlamalıdır. Kanunda belirtilen süreler içerisinde mahkemelerden ve savcılıklardan gelen talepleri cevaplamalıdır.

2.4. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Avrupa Birliği Veri Koruma Tüzüğü (GDPR) ile uyumlu bir şekilde 2016 yılında Türkiye Büyük Millet Meclisinde kabul edilen kanunun temel amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen kişilerin sorumlulukları ve uyacakları esas ve usulleri düzenlemektir. Kanun ile beraber mevzuatı uygulamak amacı ile kurulan Kişisel Verileri Koruma Kurumu özel sektörde olduğu gibi kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının da aydınlatma, veri güvenliği sağlama, kişisel veri işleme envanteri hazırlama, kişisel veri saklama ve imha politikası hazırlama ve Veri Sorumluları Sicil Bilgi Sistemi (VERBİS)'ne kaydolmalarını yani mevzuata tam anlamıyla 31.12.2021'e kadar uyum sağlamasını istemiştir. Ancak bir istisna olarak kamu kurumlarına Kişisel Verileri Koruma Kurumu (KVKK) tarafından idari para cezası uygulanmamaktadır. Bunun yerine kurum aykırılık tespit ettiğinde disiplin hükümlerine göre sorumlulara gerekli yaptırımların uygulanmasını ilgili kurumlardan istemektedir.

2.5. On Birinci Kalkınma Planı

Kalkınma planları Cumhurbaşkanlığı, bakanlıklar, kamu kurum ve kuruluşları ve çeşitli sivil toplum örgütlerinin katkılarıyla hazırlanmaktadır. Bu planlar devletin temel dokümanlarından biri olarak stratejik planların hazırlanmasında tüm kurumlara önceliklerini belirlemede yön vermektedir. 1963'ten bu yana her 5 yılda bir yayınlanan kalkınma planlarının 2019-2023 yıllarını kapsayan 11.'sinde bilgi ve iletişim teknolojilerinin geliştirilmesi ile kullanımı yoluyla ekonomide rekabet gücünün ve verimliliğin artırılması ve bu suretle iş süreçlerinin dönüştürülmesi temel amacıyla 20 temel tedbir ve politika belirlenmiştir. Bu itibarla kamu kurumlarının hazırladıkları stratejik planlarda ve eylem planlarında kalkınma planı ile eşgüdüm halinde olması gerekmektedir.

2.6. Bilgi ve İletişim Güvenliği Rehberi

Dijital Dönüşüm Ofisi (DDO) 10 Temmuz 2018 tarih ve 30474 sayı ile Resmî Gazete'de duyurulan Cumhurbaşkanlığı Kararnamesi ile kurulmuştur. Söz konusu Kararname ile DDO'ya aşağıdaki görevler verilmiştir;

- Kamu için e-dönüşüm yol haritasını belirlemek,
- Ekosistem oluşturmak için üniversite, kamu ve özel sektör ile sivil toplum kuruluşları arasındaki iş birliğini geliştirerek dijital kamu katılımlarını teşvik etmek,

- Görev alanına giren hususlarda kamu kurumları tarafından hazırlanan yatırım projesi tekliflerine ilişkin Strateji ve Bütçe Başkanlığı'na (Mülga Kalkınma Bakanlığı) görüş vermek ve projelerle ilgili gelişmeleri takip edip gerektiğinde yönlendirmek,
- Bilgi güvenliğini ve siber güvenliği artırıcı çalışmalar yapmak,
- Kamuda büyük veri kullanımına yönelik stratejiler geliştirmek ve eş güdümü sağlamak,
- Kamuda yapay zekâ uygulamalarına yönelik stratejiler geliştirmek ve eş güdümü sağlamak,
- Yerli ve milli dijital teknolojilerin kamuda kullanımının artırılmasını sağlamak,
- Kamu kurum ve kuruluşlarının bilişim ürün ve hizmetlerini maliyet etkin şekilde tedarik etmesine yönelik stratejiler geliştirmek,

Görevleri verilmiştir. Bu çerçevede, 2019/12 sayılı bilgi ve iletişim güvenliği tedbirleri konulu Cumhurbaşkanlığı Genelgesi yayımlanmıştır. Genelge ile kamu kurumları ve kritik altyapı hizmeti veren işletmeler veri güvenliğinin sağlanması amacıyla belirli güvenlik önlemlerini almakla yükümlü kılınmıştır. Genelge 'den sonra 10 Temmuz 2020 tarihinde büyük ölçüde ISO 27001 standardını referans alan Bilgi ve İletişim Güvenliği Rehberi ve bu rehbere göre yapılacak denetimler için de 27 Ekim 2021 tarihinde Bilgi ve İletişim Güvenliği Denetim Rehberi yayınlanmıştır. Rehbere göre kamu kurumları ve kritik altyapı hizmeti veren işletmeler 27.07.2022 tarihine kadar rehbere uyum sağlamalıdır. Rehberin güncel haline göre her yıl yapılması gereken denetimlerin ilkinin 31.12.2022 tarihine kadar tamamlanması gerekmektedir. Rehberde yapılacak denetimlerin öncelikle ilgili kurumun iç denetim birimleri vasıtası ile yapılması, kurumda bilişim teknolojileri (BT) konusunda yetkin denetim elemanı olmaması durumunda ise Türk Standartları Enstitüsü (TSE)'nün "Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Sağlayan Personel ve Firma Belgelendirmesi" programı kapsamında belgelendirilmiş denetmen ve firmalardan hizmet alınması regüle edilmiştir. Ancak rehberde tamamlanmayan denetimler ve karşılaşılan uyum eksiklikleri konusunda kurumlara herhangi bir yaptırım öngörülmemiştir.

2.7. 2020-2023 Ulusal Siber Güvenlik Strateji Belgesi

20/10/2012 tarih, 28447 sayılı Resmi Gazetede yayınlanan Bakanlar Kurulu Kararı ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince ulusal siber güvenliğin sağlanmasına ilişkin strateji, politika ve eylem planlarını hazırlamak ve gerekli eş güdümü sağlama görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na (sonrasında ismi Ulaştırma ve Altyapı Bakanlığı olarak değişti) verilmiştir.

Türkiye'de siber güvenlik alanında ilk temel mevzuat olan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", 20 Haziran 2013 tarih ve 28683 sayılı Resmî Gazete' de yayımlanarak yürürlüğe girmiştir. Devamında 2016-2019, 2020-2023 olarak iki kez güncellenmiştir. Bununla beraber 27 Ocak 2000 tarih ve 4502 sayılı Kanun ile "Telekomünikasyon Kurumu" adıyla kurulan ve daha sonra 809 sayılı ve 10 Kasım 2008 tarihli Elektronik Haberleşme Kanunu ile adı Bilgi Teknolojileri ve İletişim Kurumu olarak değiştirilen BTK'ya 15 Ağustos 2016 tarihinde 5809 sayılı Elektronik Haberleşme Kanunu'na eklenen hükümler ile siber saldırıların engellenmesi ve caydırıcılığın sağlanması görevleri verilmiştir. Yine aynı kanunla yükümlülüklerini yerine getirmeyen taraflara yaptırım uygulama yetkisi de BTK'ya verilmiştir. Ancak Cumhurbaşkanlığı hükümet sistemine geçilmesi ve DDO'nun kurulması ile beraber Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, BTK ve DDO arasında siber güvenlik otoritesi olma noktasında bir görev çakışması bulunmaktadır.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, Türkiye'nin siber güvenlik alanındaki vizyon ve misyonu doğrultusunda 4'er yıllık dönemlere ilişkin politikalarını konu almaktadır. Bu çerçevede, son yayınlanan planda belirlenen stratejik amaçlar aşağıda sıralanmıştır;

- Kritik Altyapıların Korunması ve Dayanıklılığının Artırılması
- Ulusal Siber Güvenlik Kapasitesinin Artırılması
- Organik Siber Güvenlik Ağı
- Yeni Nesil Teknolojilerin Güvenliğinin Sağlanması
- Siber Suçlarla Mücadelenin Etin Bir Şekilde Sağlanması
- Siber Güvenlik Alanında Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi
- Siber Güvenliğin Milli Güvenliğe Entegrasyonunun Sağlanması
- Siber Güvenlik Alanında Uluslararası İş Birliğinin Geliştirilmesi

Plana göre gerçekleştirilmesi hedeflenen toplam 8 adet stratejik amaçla ilişkilendirilen 40 adet eylem ve bunlarla ilişkili 75 adet uygulama adımı vardır.

2.8. KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Tebliğ

Kamu kurum ve kuruluşları arasında ihtiyaç duyulan veri iletişiminin, güvenli ağ üzerinden yapılarak siber güvenlik risklerinin azaltılması amacıyla oluşturulmuş KamuNet tebliği 21 Haziran 2017 Tarih ve 30103 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Tebliğ KamuNet'e dâhil edilecek ve dâhil olan kamu kurumlarının veri merkezlerinde karşılaması gereken asgari gereklilikler ile bu kurumların denetlenmesine ilişkin usul ve esasları belirlemektedir. Söz konusu mevzuata uyum sağlanması için kamu kurumlarının bir Bilgi Güvenliği Yönetim Sistemi (BGYS) sistemi kurması gerekmektedir. Tebliğde ISO 27001 sertifikası alımını dahil olmak üzere bir dizi siber güvenlik tedbiri alınmasını zorunlu kılınmıştır. Denetimlerin ise periyodik sürelerde Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yapılacağı ifade edilmiştir. Ancak mevzuatta periyodik denetimlerde tespit edilen eksiklikleri gidermeyen kamu kurumlarının KamuNet erişimini askıya alınır veya çıkarılır denmesine rağmen şu ana kadar söz konusu denetimlerin yapılıp yapılmadığına ya da denetimlerin sonuçlarına dair bakanlık tarafından herhangi bir geri bildirim kamuoyu ile paylaşılmamıştır.

2.9. Lisanslı Yazılım Kullanımına Dair Başbakanlık Genelgesi

16 Temmuz 2008 Tarih ve 26938 sayılı Başbakanlık Genelgesinde 5856 Sayılı Fikir ve Sanat Eserleri Kanuna atıf yapılarak, fikri hakların korunması açısından, kamu kurum ve kuruluşlarında, bilgisayar programlarının edinilmesi, kullanılması, yönetimi ve alınacak tedbirlere yönelik esasların tespiti ile ilgili düzenlemeler yapılmıştır. Buna göre; lisans hakları kamu kurum ve kuruluşuna ait olmayan tüm programların medya ve bilgisayarlardan silinmesi ve lisanslı olanların alınması istenilmiştir. Yine aynı tebliğde bu konunun denetiminin kamu kurum ve kuruluşunda bilgi işlem ünitesi veya bu işten sorumlu birimin eş güdümünde hukuk müşavirliğiyle teftiş veya denetiminden sorumlu kurul veya birimlerin ortak veya ayrı ayrı çalışması sonucu tamamlanması istenmiştir. Ancak yapılan mevzuat ve olay taramasında kamu kurumlarında bu konuya ilişkin örnek bir karara veya disiplin soruşturmasına rastlanmamıştır.

2.10. Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Sektörel SOME'ler

Bölüm 2.7'de de bahsedildiği gibi BTK siber saldırıların engellenmesi ve caydırıcılığın sağlanması amacı ile gerekli önlemleri almak, mevzuata uymayan, belirtilen tedbirleri yerine getirmeyen taraflara yaptırım uygulamakla sorumludur. Öte yandan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu'nun 10. maddesi ile 5809 sayılı Elektronik Haberleşme Kanunu'na benzer şekilde BTK'ya siber saldırıların tespiti ve önlenmesi konusunda yer, içerik, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlama, ihtiyaç duyulan önlemlerin alınması ve aldırılması konusunda çalışmaları yürütme yetkisi verilmiştir.

2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında da öngörüldüğü şekilde 11 Kasım 2013 tarih ve 28818 Sayılı "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Kanunun yürürlüğe girmesinden sonra Ulusal Siber Olaylara Müdahale Merkezi (USOM) siber güvenlik ile ilgili tehditler ve alınacak önlemlere ilişkin ulusal ve uluslararası çalışmalar yapmak için BTK bünyesinde kurulmuştur. Kanunla beraber Siber Olaylara Müdahale Ekiplerinin (SOME) kamuda, kritik sektörler ile bu sektörleri düzenlemek ve denetlemekten sorumlu kurumlar bünyesinde kurulması istenmiştir. Kurumsal SOME'ler, siber olayların engellenmesi ve(ya) zararlarının azaltılmasına yönelik olarak kurumların bilişim sistemlerinin kurulması, geliştirilmesi işletilmesi ve siber güvenlik farkındalığının oluşması ile ilgili çalışmalar yapmak varsa birlikte çalıştığı sektörel SOME ile eş güdüm içerisinde siber olayları USOM'a bildirmekle sorumludurlar.

2.11. Türkiye'nin Taraf Olduğu Uluslararası Sözleşmeler

Türkiye, Avrupa Konseyi'nin 23.11.2001'de imzaya açtığı Siber Suçlar Sözleşmesini (Budapeşte Sözleşmesi de denir) 10.11.2010'da imzalamış ve devamında 02.05.2014 tarihinde yürürlüğe koymuştur. Aliusta ve Benzer yaptıkları çalışmada sözleşmeyi ve Türkiye'nin dahil olma sürecini detaylı olarak ele almışlardır (Aliusta & Benzer, 2018).

Sözleşmede özetle bilişim suçlarıyla ilgili taraf devletlerin mevzuatlarını uyumlu hale getirerek uluslararası adli yardım ve iş birliği konusunda etkili ve hızlı bir sistem oluşturmak amaçlanmıştır.

Türkiye'nin bilişim alanında taraf olduğu bir diğer uluslararası sözleşme, fikri hakların dünya çapında korunmasını sağlamayı amaçlayan Dünya Fikri Mülkiyet Örgütü (WIPO-World Intellectual Property Organization)' dür. Türkiye 12 Mayıs 1976 tarihinde imzaladığı kuruluş sözleşmesi ile beraber toplamda imzaladığı 15 sözleşme ile örgüte taraftır.

2.12. Başsavcılıklar Bünyesinde Kurulan Bilişim Suçları Soruşturma Büroları ve Bilişim İhtisas Mahkemeleri

Bugüne kadar Adalet Bakanlığına bağlı 145 Ağır Ceza Mahkemesi ve Cumhuriyet Başsavcılığında Bilişim suçları büroları kurulmuştur (Bilişim Suçları Değerlendirme Toplantısı, 2022). Mevcut işleyişe göre Hakimler ve Savcılar Kurulu (HSK) tarafından Bilişim Suçları Soruşturma Bürolarına Bilişim Suçları Savcıları atanmakta ve bilişim sistemleri yoluyla işlenen suçlar değerlendirilmektedir. Öte yandan Türkiye'de bilişim ihtisas mahkemeleri 15.12.2021 tarihinden itibaren hizmet vermeye başlamıştır. HSK'nın 25 Kasım 2021 tarih ve 1229 numaralı kararına göre bu mahkemeler Türk Ceza Kanunu'nun bilişim suçları kapsamına giren konuları ile 29.04.1959 tarih ve 7258 sayılı "Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun" kapsamındaki davalara bakmaktadırlar.

2.13. Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Dairesi

2011/2025 sayılı Bakanlar Kurulu Kararı ile Emniyet Genel Müdürlüğü bünyesinde Siber Suçlarla Mücadele Daire Başkanlığı kurulmuştur. Daire, Elektronik Haberleşme Kanunu, Türk Ceza Kanunu'nun bilişimle ilgili maddeleri, Fikir ve Sanat Eserleri Kanunu ile Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına yönelik ilgili yönetmelikler gereğince işlem tesis etmektedir.

Dairenin genel olarak görev alanında bilişim ve internet alanını içerisinde gerçekleştirilen e-mail ve sosyal medya adreslerinin çalınması, kredi kartı bilgilerinin ele geçirilmesi vasıtası ile hırsızlık, sahte evraklar düzeyerek dolandırıcılık, kişisel ve kurumsal verilere yetkisiz erişim ve iletişimin yetkisiz dinlemesi, yazılımların izinsiz ve lisanssız kullanımı, çocuk pornografisi ve istismarı, hakaret ve tehdit, uyuşturucu kaçakçılığı, siber terör gibi konular bulunmaktadır.

2.14. Adli Tıp Bünyesinde Kurulan Adli Bilişim İhtisas Dairesi

01.09.2016 tarih ve 674 sayılı Kanun Hükmünde Kararname (KHK) ile 14.4.1982 tarih ve 2659 sayılı Adlî Tıp Kurumu Kanununa ek yapılmış ve kurum bünyesinde Adli Bilişim İhtisas Dairesi kurulmuştur. Dairenin görevleri ise mahkemeler ile hâkim ve savcılıklar tarafından istenilen bilişimle ilgili konularda her türlü sayısal ve elektronik materyal üzerinde analiz ve incelemeleri yapmak olarak belirlenmiştir.

2.15. Adalet Bakanlığı Bilirkişilik Daire Başkanlığı

03.11.2016 tarih ve 6754 sayılı Bilirkişilik Kanunu, 24.11.2016 tarih ve 29898 sayılı Resmî Gazetede yayımlanmıştır. Bu Kanun kapsamında bilirkişilik hizmetlerinin etkin, etkili ve verimli şekilde gerçekleşmesini sağlamak için Adalet Bakanlığı Hukuk İşleri Genel Müdürlüğü bünyesinde "Bilirkişilik Daire Başkanlığı" kurulmuştur.

Mahkemeler, bilişim davaları ile ilgili konularda Türkiye'de 15 adet bulunan bilirkişilik bölge kurullarından hangisinin bölgesine giriyor ise o bölgenin bilirkişi listesinden uzman görevlendirmesi yapabilirler.

3. DENETİM KONTROL LİSTESİ

Yukarıda bahsedilen yasal mevzuat ve düzenlemelerin değerlendirilmesi sonucunda bilgi işlem birimlerinde BT denetimi yapacak olan iç denetim birimleri ve iç denetçilere izleyebilecekleri yol haritası örneği olması amacıyla toplam yedi kategoride hazırlanan soru seti aşağıda Tablo-1' de sunulmuştur.

Tablo 1. İç Denetçiler İçin Soru Seti

6698 Sayılı Kanununa Uyum	Veri Sorumluları belirlenmiş midir?
	Kurum içerisindeki veri tabanlarında ve dokümanlarda bulunan kişisel veriler tespit edilmiş midir?
	Veriyi işleyen personeller belirlenmiş midir?
	VERBİS'e kaydedilmiş ve güncel midir?
	Sürdürülebilir güncel bir sistem kurulmuş mudur?
	Kurumda zorunlu olmayan ya da kanuni tutma süresi biten kişisel verilerin silinmesine yönelik bir sistem var mıdır?

	Vatandaştan alınan kişisel verilerin gizlenmesi ya da silinmesine yönelik dilekçelerin işlenmesine ve yerine getirilmesine yönelik tüm uygulamaları içeren bir sistematik kurulmuş mudur?
	Diğer kamu kurumları ile veri paylaşımları yapılıyor mu? Yapılıyor ise bir listesi tutuluyor mudur?
	Veri paylaşımları kurumlar arası yapılan protokollere dayanıyor mu? Protokollerin süresinin kontrolü ile ilgili olarak bir sistematik var mıdır?
5651 Sayılı Kanuna Uyum	Kablolu ağlardan sisteme katılan personelin internete çıkışları zaman damgalı bir şekilde loglanıyor mudur?
	Kablosuz ağlardan sisteme katılan personelin internete çıkışları zaman damgalı loglanıyor mudur?
	Kablosuz ağlardan sisteme katılan misafirlerin internete çıkışları zaman damgalı loglanıyor mudur?
	Kurumun sunduğu portallara, web ve mobil uygulamalara erişenler kayıt altına alınıyor mudur?
	Kayıtlar kanunda belirtilen süreler dâhilinde saklanıyor mudur?
	Savcılık, mahkeme, teftiş kurulları ve iç denetim birimlerinden gelen taleplere kanuna göre uygun cevaplar veriliyor mudur?
USOM ve SOME İlkelerine Uyum	Personelin ve bilişim sistem yöneticilerinin karşılaşacakları siber olayları bildirdikleri bir SOME ekibi oluşturulmuş mudu?
	Resmi olarak ekip üyelerine ve personele bildirilmiş midir?
	SOME ekibi rutin olarak toplanıp siber olayları değerlendiriyor mu? Toplantı tutanakları tutulmuş mudur?
	SOME ekibi tespit edilen zafiyet ve saldırıları USOM'a formal bir şekilde iletiyor mudur?
	USOM'dan gelen bildirimleri SOME ekibi formal bir şekilde ilgililere iletiyor mudur?
5846 Sayılı Kanununa ve 26938 Sayılı Genelgeye Uyum	Kurumda kullanılan tüm yazılım ve donanım ürünlerinin envanteri tutulmuş mu ve güncelliği sistematik olarak sağlanıyor mudur?
	Kurumun kendi geliştirdiği yazılımlar dışında dışarıdan satın aldığı yazılım ve lisans gerektiren donanım (appliance) ürünlerinin lisansı satın alınmış mıdır?
	Kurumun kendi geliştirdiği yazılımlar dışında dışarıdan satın aldığı yazılım ve lisans gerektiren donanım (appliance) ürünlerinin lisansı güncel midir?
	Kurumun kendi geliştirdiği yazılımlar dışında dışarıdan satın aldığı yazılım ve lisans gerektiren donanım (appliance) ürünlerinin lisansı kullanıcı sayısı, kullanılan CPU vb lisans parametreleri ile uyumlu mudur?
Bilgi ve İletişim Güvenliği Rehberine Uyum	Kurumda bir varlık envanteri çıkarılmış mıdır?
	Envanterler için bir risk hesaplaması yapılmış mıdır?
	Boşluk analizi yapılmış mıdır?
	1, 2 ve 3. seviye tedbirlerin yerine getirilmesi için bir eylem planı yapılmış mıdır?
	Her yıl düzenli bir şekilde İç Denetim Birimlerine ya da Dış Denetim birimlerine uyum denetimi yaptırılmış mıdır?
	Denetim bulguları sonucu ortaya çıkan eksikliklerle ilgili sistematik bir eylem planı yönetimi yapılıyor mudur?
KamuNET Genelgesine Uyum	Kurum KamuNET sistemine bağlı mıdır?
	Hangi uygulamalar KamuNET üzerinden hizmet vermekte belirli midir?
	KamuNET Genelgesine uygun şekilde siber güvenlik önlemleri alınmış mıdır?
	İnternet Hizmeti KamuNET genelgesi kapsamında indirimli tarifeden ilgili ISP'ye ödeniyor mudur?
5237 sayılı Kanuna Uyum	Kurumda tüm bilişim organizasyonunun yapısı net ve anlaşılır bir şekilde tanımlanmış mıdır?
	Tüm bilişim ve diğer iş birimi personellerinin görev ve sorumlulukları belli midir?
	Tüm personellerinin görev ve sorumlulukları kendilerine resmi olarak iletilmiş, imzalatılmış ve personel özlük dosyasına konulmuş mudur?
	Görevi kötüye kullanan ve suiistimal eden personellere yönelik yapılacak adli idari soruşturmalar konusunda bir akış çıkarılmış mı? ve tüm personellere duyurulmuş mudur?

(Araştırmacılar Tarafından Geliştirilmiştir)

3.1. Tartışma ve Öneriler

İç denetçilerin bilişim denetimi konusunda yetkinliklerinin artırılması kamu kurumlarının bilişim mevzuatına uyumunu sağlamak açısından önemlidir. Gerçekleştirilen bu çalışmada, 2000'li yılların başından bugüne Türk kamu idarelerinin dijital dönüşümüne öncülük eden dokümanlar ile dağınık vaziyette çeşitli yönetmelik ve yasalar içerisinde bulunan bilişim mevzuatı tespit edilerek değerlendirilmiştir. Yapılan incelemede Cumhurbaşkanlığı hükümet sistemi ve devamında kurulan DDO ile beraber çeşitli görev çakışmalarının ortaya çıktığı gözlemlenmiştir. Özellikle Ulaştırma ve Altyapı Bakanlığı (UAB), BTK ve DDO arasında bulunan bu görev çakışmalarının izleme ve denetim açısından sorunlara yol açabileceği değerlendirilmektedir.

DDO bilgi ve iletişim güvenliği rehberinde mevzuatın herhangi bir yaptırımının olmaması idarelerin uyum motivasyonunu düşürebilir. Ortaya konan mevzuatın (kamu ihale süreçleri de gözetilerek) gerçekleştirilmesinin

izlenmemesi ve yaptırımının olmaması zımni olarak mevzuata uyan idareleri ve idarecileri cezalandırmak anlamına gelebileceği unutulmamalıdır.

Özellikle bilişim ve siber güvenlik yatırımları halihazırda büyük oranda ithalata bağlıdır. Bu nedenle kamu kurumlarına herhangi bir mevzuata uyum için sorumluluk verilirken, kurumların mevzuata uyum için yapacağı yatırımlarla ilgili ödeneklerin de sağlanması gerekmektedir.

5651 ve 6698 sayılı yasalar ile kurumlarla ilgili münhasır yasalar dikkate alınarak toplanan kişisel verilerin en fazla ve en az ne kadar süre tutulabileceği konusu üst yönetim ve ilgili diğer birimler tarafından tartışılarak netleştirilmelidir.

Denetim elemanlarınca gerçekleştirilen denetimlerde WIPO sözleşmelerine ülke olarak taraf olunduğundan, 16 Temmuz 2008 Tarih ve 26938 sayılı "Lisanslı Yazılım Kullanımına Dair Başbakanlık Genelgesi"ni de dikkate alarak lisanssız ve kaçak ürün kullanıp kullanılmadığının denetlenmesi gerekmektedir. Bu konuda farkındalığın artırılması ve Başbakanlık mülga olduğundan ilgili mevzuatın Cumhurbaşkanlığınca güncellenerek yeniden yayınlanmasında fayda bulunmaktadır.

4. SONUÇ

Çalışmada BT yöneticileri, bilişim mevzuatını denetlemekle sorumlu olan iç denetim birimleri ve iç denetçiler için bir denetim kontrol seti hazırlanmıştır. Hazırlanan soru setleri yalnızca mevzuata uyum açısından hazırlanmış olup bununla beraber denetimlerde ISO20000, ISO 27001, ISO 9001, ISO 14001, ISO 22237, BICSI 002, ISO 38500, ISO 22301, ISO 17799, ITIL, TOGAF, CMMI, COBIT gibi uluslararası bilişim standartlarını merkeze alan özel denetimler de yapılması mümkündür. Bununla beraber denetçilerin denetime başlamadan önce kurum faaliyet alanı, vizyon, misyon, kurum stratejik planı, servis kataloğu, performans programı, faaliyet raporu ve eylem planları kurum organizasyon yapısı, bilgi işlem biriminin organizasyondaki yeri ve sorumlulukları, kurum dış paydaşları ve protokollerini de incelemesinde fayda bulunmaktadır (Arslan, 2022b).

DDO tarafından ortaya konan Bilgi ve İletişim Güvenliği Rehberi'yle kapsamdaki tüm kurumlarda denetimlerin öncelikli olarak iç denetim birimlerindeki iç denetçiler tarafından gerçekleştirilmesinin esas olduğunun ifade edilmesi iç denetçiler açısından çok faydalı olmuştur. Bu itibarla birçok iç denetçi Kamu İç Denetim Derneği (KİDDER) gibi kuruluşların verdiği BT denetim eğitimlerini alarak denetime hazır hale gelmiştir.

Kamuda BT denetimlerini yapan iç denetçiler açısından konu değerlendirildiğinde kamu idarelerinde büyük oranda boş iç denetim kadrolarının olduğu görülmektedir. Kamu iç denetim kadrolarının daha da artırılarak açık bulunan kadrolara atama yapılması ve iç denetçilerin bilişim denetimi konusunda yetkinliklerinin artırılması kamu kurumlarının bilişim mevzuatına uyumunu sağlamak açısından önemlidir. Denetimler sırasında iç denetçiler; uluslararası metodolojiye uygun şekilde kişilere değil sürece odaklanmalı, hatayı kimin yaptığını değil süreç içerisinde bu hatanın yapılmasına neden olan bilişim süreç eksikliğini sorgulamalı, iyi uygulama örneklerinin altını çizerek idarecileri motive etmeli ve kurumlarda sürdürülebilir bir bilişim yönetim sisteminin kurulumuna öncülük etmelidirler.

Kaynakça

Ağdeniz, Ş. (2021). Bilgi ve iletişim güvenliği denetiminde kamu iç denetçilerinin rolü ve yetkinliklerine ilişkin bir araştırma., *Alanya Akademik Bakış, 5*(2), 525-545.

Akaslan, N. M., (2021). Yeni bir ihtisas mahkemesi olarak bilişim mahkemesi., https://www.hukukihaber.net/yeni-bir-ihtisas-mahkemesi-olarak-bilisim-mahkemesi-makale,8797.html (Erişim Tarihi, 08.03.2022)

Akmeşe, S. (2020). Kamuda dijital dönüşümün siber güvenlik ve dijital güvence boyutları ve iç denetimin rolü. *Denetişim Dergisi*, *0* (20), 108-119.

Aliusta, C. & Benzer, R. (2018). Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dâhil Olma Süreci., *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 4(2), 35-42.

Arkın, A. (2022). Kamu iç denetim genel raporlarının içerik analizi, *Denetişim Dergisi*, 0 (25), 27-57.

Arslan, Y. (2022a). Bilişim suçları ve bilirkişilik mesleği., https://ictmedia.com.tr/Author/Index/55/dr-yenal-arslan/646 (Erişim Tarihi, 15.05.2022).

Arslan, Y. (2022b). Bilgi ve iletişim güvenliği rehberi uyum denetimi., https://ictmedia.com.tr/Author/Index/55/dr-yenal-arslan/646 (Erişim Tarihi, 15.05.2022).

Bilişim Suçları Değerlendirme Toplantısı (2022), https://cigm.adalet.gov.tr/Home/SayfaDetay/Antalya05122022 (Erişim Tarihi, 15.10.2022).

COSO. (2019). *Enterprise Wide Management (ERM) for Cybersecurity*. https:// www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf (Erişim Tarihi, 16.05.2020).

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2019). *Bilgi ve İletişim Güvenliği Denetim Rehberi*. Ankara.

Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. (2019). *On Birinci Kalkınma Planı*. Ankara.

Deloitte. (2017). *Deloitte's Cyber Risk Capabilities, Cyber Strategy, Secure, Vigilant, and Resilient*. https://www2.deloitte.com/content/dam/Deloitte/at/Documents/risk/cyber-risk/Deloitte-Cyber-Risk-Capabilities-Broschuere.pdf (Erişim Tarihi, 15.04.2022).

Dutta, A., Roy, R. & Seetharaman, P. (2022). An assimilation maturity model for IT governance and auditing., *Information & Management*, 59(1), 1-21.

ECIIA. (2020). *Risk in Focus 2021. Hot Topics for Internal Auditors*. https://www.eciia.eu/wp-content/uploads/2020/09/100242-RISK-IN-FOCUS-2021-52PP-ECIIA-Online-V2.pdf (Erişim Tarihi, 20.04.2022).

FERMA. (2019). *At The Junction of Corporate Governance & Cybersecurity*. https://www.eciia.eu/wp-content/uploads/ 2019/02/FERMA-Perspectives-Cyber-risk-governance-09.10.2018_0.pdf (Erişim Tarihi, 16.03.2022).

George, D., Theofanis, K. & Konstantinos, A. (2015). Factors associated with Internal Audit Effectiveness: Evidence from Greece. *Journal of Accounting and Taxation*, 7(7), 113-122.

Görmen, M. & Korkmaz, G. (2022). Kurumsal Sürdürülebilirlik İçin Sürdürülebilir İç Denetim: Geleceğin İç Denetim Fonksiyonu, *Denetişim Dergisi*, 0 (25), 94-115.

IIA. (2013). *The Three Lines of Defence in Effective Risk Management and Control*. https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf (Erişim Tarihi, 20.03.2022).

IIA. (2016). *Assessing Cybersecurity Risk: Roles of the Three Lines of Defense*. https://global.theiia.org/standards-guidance/Member%20Documents/ GTAG-Assessing-Cybersecurity-Risk.pdf (Erişim Tarihi, 05.03.2022).

IIA. (2020). *On Risk2022. A Guide to Understanding, Aligning, and Optimizing Risk*. http://theiia.mkt5790.com/OnRisk2020/webSyncID=9d4b5b56-2d9e-c43b83c5b525&sessionGUID=d03ed4d7-83b6-86b2-406b-326988476708 (Erişim Tarihi, 20.05.2022).

İç Denetim Koordinasyon Kurulu. (2021). *2020 Yılı Kamu İç Denetim Genel Raporu*. Ankara.

Koç, S., Şeker, S. & Şeker, F. (2019). Bilişim teknolojileri (BT) denetiminde bilgi güvenliği ile ilgili uluslararası standartlar ve Türkiye'deki uyum çabalarının incelenmesi., *Muhasebe ve Finans Araştırmaları Dergisi*. 1(2), 121-139.

Köse, H. Ö. & Polat, N. (2022). Dijital dönüşüm ve denetimin geleceğine etkisi., *Sayıştay Dergisi*, 32(123), 9-4.

M., B., Kızıltan. (2007). *5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları*, (Basılmamış yüksek lisans tezi), İstanbul Üniversitesi, İstanbul.

Moore, R. (2005). *Cyber crime: Investigating High-Technology Computer Crime*. Mississippi: Anderson Publishing.

NIST. (2013). "*Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*". USA.

Özbilger, H.İ. (2021). İç denetime yeni bir bakış: Üçlü hat modelinin değerlendirilmesi., *Denetişim Dergisi,* 0 (22), 40-54.

Stoel, D., Havelka, D. & Merhout, J.W. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners., *International Journal of Accounting Information Systems*, 13(1), 60–79.

Turetken, O., Jethefer, S., Ozkan, B., (2020). Internal audit effectiveness: Operationalization and influencing factors. *Managerial Audit*. 35(2), 238–271. https://www.emerald.com/insight/content/doi/10.1108/MAJ-08-2018-1980/full/html (Erişim Tarihi, 19.03.2022).

Ulaştırma ve Altyapı Bakanlığı. (2020). *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023).* Ankara.

Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016*). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2016–2019).* Ankara.