ISSN 1308-8335

Yıl: 9 • **Sayı:** 19
Ocak / Nisan 2019

HAKEMLİ Denetişim

Ortak Aklın Harmanı

SİBER GÜVENLİK RİSKLERİ VE BİLGİ TEKNOLOJİLERİ DENETİMİ

kidder 2007
Kamu İç Denetçileri Derneği

Kamu İç Denetçileri Derneği (KİDDER) Yayınıdır

HAKEMLİ
Denetişim
Ortak Aklın Harmanı

Kamu İç Denetçileri Derneği (KİDDER) Yayınıdır

Sahibi
Kamu İç Denetçileri Derneği Adına
Bahadır TOPAL

Sorumlu Yazı İşleri Müdürü
Ahmet KEBELİ

Abone İşleri
Ömer GEÇGİL

Yönetim Merkezi
Meşrutiyet Caddesi Konur Sokak
No: 36/6 Kızılay - ANKARA
Tel: 0.312 424 06 20

Yazışma Adresi
Kamu İç Denetçileri Derneği
Meşrutiyet Caddesi Konur Sokak
No: 36/6 Kızılay - ANKARA
www.kidder.org.tr
denetisim@kidder.org.tr

Grafik Tasarım & Baskı
İsmail Aygül Ofset Matbaacılık San. Tic. Ltd. Şti.
Büyük Sanayi 1. Cadde No: 95/6
İskitler - ANKARA
Tel: 0.312 310 59 95

Basım Tarihi / Yeri
08 Haziran 2019 / ANKARA

Abonelik Şartları
Yıllık KDV dahil 100 TL, iki yıllık KDV dahil 180 TL olan abonelik bedelinin,
Ziraat Bankası Başkent Şubesi nezdindeki
TR 82 0001 0016 8358 7849 3750 01 No'lu
IBAN'a yatırıldığını gösterir dekontun ve derginin gönderilmesi istenen posta adresinin iletilmesi yeterlidir.
Perakende satış fiyatı 35 TL'dir.

ISSN 1308-8335

Dört ayda bir yayımlanan hakemli dergidir.
Kaynak gösterilerek alıntı yapılabilir.
Yazıların sorumluluğu yazarlarına,
reklamların sorumluluğu ilan sahiplerine aittir.
Yazım dili Türkçe'dir.
Yazıların Araştırma ve Yayın Etiğine uygunluğunda COPE *(Committee on Publication Ethics)* standartları gözetilir.

Yerel Süreli Yayın • 2019/19

kidder 2007
Kamu İç Denetçileri Derneği

Danışma ve Hakem Kurulu

Yayın Kurulu

Yayın Kurulundan

Değerli Okurlarımız,

"Derdiniz varsa derginiz olur!" düşüncesiyle sizi yeni bir sayıyla buluşturmanın tarifsiz mutluluğunu yaşıyoruz.

"Muhteşem bir maziyi daha muhteşem bir istikbale bağlama" heyecanı ile sürekli okuyan, düşünen ve yazan ünlü mütefekkir Cemil Meriç'in ***"Kitap fazla ciddi, gazete fazla sorumsuz. Dergi, hür tefekkürün kalesi. Belki serseri ama taze ve sıcak bir tefekkür. Kitap, çok defa tek insanın eseri, tek düşüncenin yankısı; dergi bir zekalar topluluğunun. Bir neslin vasiyetnamesidir dergi; vasiyetnamesi, daha doğrusu mesajı. Kapanan her dergi, kaybedilen bir savaş, hezimet veya intihar…"*** sözleri, belki de dergicilik üzerine söylenmiş en güzel sözlerdir.

Bu güzel sözlerden esinlenerek kamu iç denetçileri olarak bizim de derdimiz/mesajımız; kamu kaynaklarının ekonomik, etkili ve verimli kullanılmasını sağlayan bir güvence mekanizması olmak.

"Siber Güvenlik Riskleri ve Bilgi Teknolojileri Denetimi" temalı bu sayıdaki;

Birinci yazımızda; siber güvenliğin sağlamasındaki barikatlar ve iç denetimin rolü irdelenmiştir. İkinci yazımızda; siber güvenlik ve siber hijyen bağlamında iç denetçilerin ve iç denetimin siber rolü değerlendirilmiştir. Üçüncü yazımızda; veri tabanı yönetim sürecine ilişkin denetim fonksiyonu, kamu kurumları özelinde ele alınarak idari ve teknik alanda belirlenen risk ve bulgu örnekleri için öneriler geliştirilmiş ve bu önerilerin nasıl izlenmesi gerektiği hakkında görüşler sunulmuştur. Dördüncü yazımızda; blokzincir teknolojisinin temel özelliklerinden bahsedilerek denetim mesleğine potansiyel etkileri incelenmiştir. Beşinci yazımızda; nesnelerin internetinin denetiminde değerlendirilebilecek kontroller üzerinde durulmuştur. Altıncı yazımızda; ilk bölümü 18. sayımızda yayımlanan "COSO 2017 Kurumsal Risk Yönetimi Çerçevesine Kontrol Öz Değerlendirme Yaklaşımıyla Bakış ve Bir Kurum Uygulaması" başlıklı çalışmanın ikinci bölümüne yer verilmiştir. Yedinci yazımızda; iç denetim faaliyetlerinin ülkemiz sigortacılık mevzuatındaki yeri, önemi ve mevcut durumu incelenmiş ve iç denetim sisteminin daha etkili ve verimli şekilde oluşturularak, denetim faaliyetlerinin de daha etkin şekilde yürütülebilmesi amacına yönelik olarak, yasal mevzuattaki gelişim alanları araştırılmış ve yapılan tespitlere bağlı olarak çözüm önerileri sunulmuştur.

20. sayımızın temasını "Performans Yönetimi (Kurumsal-Takım-Bireysel) ve Denetimi" olarak belirledik. Bu temanın alt açılımı olan; stratejik yönetimde performans yönetimi, performans yönetiminde bilgi teknolojileri, performans denetimi, performans odaklı insan kaynakları stratejileri, performans esaslı bütçe, performansa dayalı ücret sistemi ile ilgili çalışmalarınızı bekliyoruz.

Gelecek sayıda buluşmak ümidiyle esen kalınız…

İÇİNDEKİLER

SİBER GÜVENLİK RİSKLERİNDEN KORUNMADA KÖPRÜ VE KATALİZÖR OLARAK İÇ DENETİM

(INTERNAL AUDIT AS A BRIDGE AND CATALYST IN THE PROTECTION OF CYBER SECURITY RISKS)

Seval SELİMOĞLU* / Mehtap ALTUNEL**

ÖZ

Günümüz iş ortamına bakıldığında hem kamu hem de özel sektörde işlemlerin gerçekleştirilmesi için dijital alt yapıya sahip oldukları ve bu kapsamda bilginin depolanması, işlemlerin yapılması ve raporlamanın elektronik ortamda gerçekleştiği görülmektedir. Bu dijital alt yapı internet, bilgisayar sistemi, yazılım, donanım ve hizmetler yani dijital ortamın tamamı siber alan olarak ifade edilmektedir. Bu alt yapının faaliyetlerin gerçekleştirilmesinde fırsatlar sağlamanın yanında büyük tehdit ve riskleri de beraberinde getirmektedir. Yakın zamanda yaşanan önemli siber saldırılar (WannaCry, BadRabbit, NotPetra vb.) göz önünde bulundurulduğunda ciddi zararlara ve maliyetlere sebep olmuştur. Bu kapsamda hem özel sektörde hem de kamu sektöründe siber saldırılara karşı önlemlerin alınması ve etkilerinin azaltılması önemlidir. Bu kapsamda üçlü savunma hattının siber riskleri kapsayacak şekilde tasarlanması ve iç denetim biriminin siber güvenlik risklerine yönelik çalışmalar yürütmesi, siber güvenlik risklerinin azaltılmasında etkili olacaktır. Bu çalışmada siber riskler ve siber risklerin yönetilmesine ilişkin bilgi verilmekle birlikte, siber güvenliğin sağlamasında iç denetimin rolü ortaya konulmaya çalışılmıştır.

Anahtar Kelimeler: Siber Risk, Siber Güvenlik, Üçlü Savunma Hattı, İç Denetim

JEL Kodlaması: M40, M42, O30

ABSTRACT

When we look at today's business environment, it is seen that they have digital infrastructure for the realization of transactions in both public and private sectors and in this context, information storage, transactions and reporting are realized in electronic environment. This digital infrastructure is expressed as the internet, computer system, software, hardware and services. In addition to providing opportunities for the realization of these activities, this infrastructure brings with it great threats and risks. Considering the recent cyber attacks (WannaCry, BadRabbit, NotPetra, etc.), it has caused serious damages and costs. In this context, it is important to take measures against cyber attacks in both the private and public sectors and to reduce their impact. Therefore, the design of the three lines of defense covering cyber risks and the internal audit unit's work on cyber security risks will be effective in reducing cyber security risks. In this study, information is given on the management of cyber risks and cyber risks, but the role of internal audit in providing cyber security is tried to be explained.

Keywords: *Cyber Risks, Cyber Security, The Three Lines of Defense Model, Internal Audit.*

JEL Classification: *M40, M42, O30*

* Prof. Dr., Anadolu Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Eskişehir, Orcid:0000-0003-1185-9980, sselimoglu@anadolu.edu.tr
** Doktora Öğrencisi, Anadolu Üniversitesi, İşletme Anabilim Dalı, Muhasebe Bilim Dalı, Eskişehir, Orcid: 0000-0003-3149-7753 altunelmehtap@hotmail.com, Yazı Gönderim Tarihi: 19.03.2019, Yazı Kabul Tarihi: 26.03.2019

1. GİRİŞ

Bilgi teknolojisindeki gelişmeler, işletmeleride bu gelişmeler ile paralel yönde hareket etmeleri yönünde gerekli kılmıştır. Böylece artık bütün dünya bilginin herkes tarafından hızlı şekilde erişildiği küresel bir oluşum içinde yer almaktadır. Bu oluşum birçok fırsatı beraberinde getirmekle birlikte kötü amaçlı kullanımlara da ortam hazırlamaktadır. Bu kötü amaçlı kullanımlar siber suçlar olarak nitelendirilmektedir. Siber suçlar sadece birebir kişilere karşı yapılan bir eylem olmanın dışında işletmelere hatta ülkelere karşı eylemleri içermektedir. Dolayısıyla siber suçların etkileri hem mikro hem de makro seviyede kişilere ve kurumlara zarar verdiği söylenebilir.

Bilgi teknolojilerinde yaşanan gelişmelerin sunduğu fırsatlar ve beraberinde gelen siber suçlar ile mücadeleye ilişkin veri tabanlarının, bilgi sistemi ve uygulamaların güvenliğinin sağlanmasının önemi artmıştır (Öztürk, 2018: 209).

Siber güvenliğin sağlanması adına yapılan denetimler, ülkemizde finansal tabloların güvenirliliğini sağlamak adına yapılan denetimler kadar önemli bir yere sahip olduğunu söyleyebiliriz. Çünkü siber güvenlik risklerine ilişkin önlem alınmaması ile birlikte işletme hem büyük maliyet kayıpları ile karşı karşıya kalacaktır hem de itibari zedelenecektir. Bu anlamda siber güvenlik risklerine karşı farkındalık oluşturmak ve mücadele etmek adına yurtiçinde ve yurtdışında düzenlemeler ve akademik çalışmalar yapılmaya başlanmıştır. Siber güvenliğe ilişkin yapılan en önemli düzenlemelerden biri 2015 yılında COSO, Deloitte ile birlikte *Siber Çağda COSO* (COSO in theCyber Age) isimli rapor yayınlamıştır. Bu rapor kapsamında siber riskin işletmedeki değerlendirilmesi süreçleri üzerine bir çerçeve sunulmaktır (COSO, 2015). Diğer bir çalışmada Uluslararası İç Denetçiler Enstitüsü tarafından *Küresel Teknoloji Denetim Rehberi: Siber Risklerin Değerlendirilmesi: Üçlü Savunma Hattının Rolü* (Global Technology Audit Guide (GTAG): AssesingCybersecurity Risk: Roles Of The Three Lines Of Defense) yayınlanmıştır. Bu rehber iç denetçilerin siber güvenlik riskleri konusunda güvence sağlamaları adına yetkinliklerini geliştirmelerine yardımcı olması için tasarlanmıştır. Ayrıca bu rehber iç denetimin siber güvenlikteki rolünü ele almıştır (IIA, 2016). Bu düzenlemelerin yanında ISACA (Information SystemAnd Control Association) tarafından *Denetim: Siber Güvenlik* (Auditing: Cyber Security- Evaluating Risk and Auditing Controls) raporu yayınlanmıştır. Bu rapor siber güvenlik kontrollerini, risk değerlendirme ve yönetim incelemelerini içerir(ISACA, 2017). Bunların yanında siber risklerin yönetilmesinde kullanılan COBIT (Control Objectivesfor Information andRelatedTechnology), ISO 27000, NIST (NationalInstitute of StandardsandTechnology) diğer düzenlemelerdir (COSO, 2015).

Diğer taraftan ülkemizde yapılan çalışmalara bakıldığında Sermaye Piyasası Kurulu tarafından Ocak 2018 tarihinde *Bilgi Sistemleri Yönetim Tebliği* ve *Bilgi Sistemleri Bağımsız Denetim Tebliği* yayınlanmıştır. Bu tebliğler kapsamında bilgi sitemi yönetimi ve denetimine ilişkin açıklamalar sunulmuştur (SPK, 2018).

Akademik çalışmalara incelendiğinde, çalışmamızın kapsamı itibariyle denetim ve siber güvenlik ile ilgili çalışmalara yeni başlandığı görülmektedir. Fakat bilgi teknolojilerindeki gelişmeler ile birlikte, siber riskleri azaltmak ve önlemek adına denetime olan ihtiyacın artmasından kaynaklı bu yönde çalışmaların artacağı düşünülmektedir.

Türkiye'de siber risk ve siber güvenliğe ilişkin birçok çalışma bulunmakla birlikte, denetim kapsamında siber güvenlik risk değerlendirmesi adına çok çalışma bulunmamaktadır. Yayınlanan çalışmalara bakıldığında; Öztürk(2018) tarafından yapılan çalışmada siber güvenlik denetiminde sürecin bütüncül bir biçimde ele alınması suretiyle bir model gösterilmiştir. Bu kapsamda çalışmada siber güvenlik denetim sürecine ilişkin açıklamalar akış şeması ile açıklanmıştır. Kurt ve Uysal (2015) tarafından yapılan çalışmada güncellenen COSO ve yeni yayınlanan Siber Çağda COSO raporu doğrultusunda siber risklere yönelik nasıl bir iç kontrol sistemi geliştirilmesi gerektiği ele alınmıştır.

Yurtdışında yapılan akademik çalışmaların bir kısmına bakıldığında; Kahyaoğlu ve Çalıyurt (2018) tarafından yapılan çalışma kapsamında, iç denetim ve risk yönetimi perspektifinde anahtar konuları ve zayıflıkları belirlemek amacıyla siber güvenlik güvence yaklaşımı analiz edilmiştir. Mukhopadhyay ve diğerleri (2013) tarafından yapılan çalışmada siber riske karşı alınacak önlemler incelenmiştir. Shackelford (2012) tarafından yapılan çalışmada ise işletmelerin

siber saldırıları önlemede daha çok siber risk sigortasına yöneldiklerine ulaşılmıştır. Ayrıca bu çalışmada siber saldırıların firmalar üzerindeki etkisi, veri ihlallerine yönelik ABD'deki yasalar ve siber risk sigortalarının siber tehditleri azaltmaya yardımcı olmadaki boyutu ele alınmıştır. Nijerya'da banka sektöründe Ojeka ve diğerleri (2017) tarafından yürütülen çalışmada denetim komitesi etkinliği ve siber güvenlik arasındaki ilişki değerlendirilmiştir. Değerlendirme sonucunda denetim komitesinin denetim ve gözetim konusunda yetersiz olduğuna ulaşılmıştır. Sabillon ve diğerleri (2017) yürüttükleri çalışmada siber güvenlik güvencesi ve denetim alanında küresel liderlerin en iyi uygulamaları ve metodolojileri incelenmiştir. American Accounting Association tarafından 2017 yılında yapılan çalışmada, siber güvenliğin en baskın konuları ve siber güvenlik güvencesi için yeni yaklaşımların gerekliliği açıklanmıştır (American Accounting Association, 2017:1).

Bu çalışmada, siber güvenlik riskinin engellenmesinde bir barikat olan iç denetimin rolü ortaya koymak amaçlanmıştır. Bu amaçla çalışmanın ikinci bölümünde siber risk kavramının ciddiyetini ortaya koymak için yakın zamanda yaşanmış siber saldırılardan bahsedilmiş ve siber riske ilişkin genel açıklamalar yapılmıştır. Üçüncü bölümde siber risklerin belirlenmesi ve yönetilmesi konuları ele alınmıştır. Dördüncü bölümde siber güvenlikte üçlü savunma hattına ilişkin Uluslararası İç Denetim Enstitüsü'nün yayınladığı rehber çerçevesinde açıklama yapılmıştır. Son bölümde ise siber güvenlikte iç denetimin rolü ortaya konulmaya çalışılmıştır.

2. SİBER RİSK KAVRAMINA GENEL BAKIŞ

Artan rekabet koşulları ile küresel ortama ayak uydurmak için hem özel sektör hem de kamu sektöründe bilgi teknolojileri yaygın şekilde kullanılmakta, işlemler elektronik ortamda gerçekleştirilmekte ve raporlama yapılmaktadır. Bilgi teknolojileri hem kamu hem özel sektörde birçok kolaylık sağlayarak fırsat yaratmanın yanında riskleri de beraberinde getirmektedir(Öztürk, 2018: 208). Günümüzde teknolojinin gelişmesi ile birlikte bu riskler arasında ön plana çıkanı siber risklerdir. Siber riskin artışı ve buna bağlı olarak siber güvenliğin önemini vurgulamak adına PWC tarafından yürütülen 2018 yılına ait "Küresel Ekonomide Suçlar ve Hile Araştırmaları" başlıklı çalışma incelendiğinde hile beş kategoride ele alınmıştır. Bu çalışmada en sık yapılan hilelerden biri de "siber suçlar" olarak ifade edilmektedir (PWC, 2018:8). Dolayısıyla işletmenin karşılaştığı hileler arasında sıralanan siber suçların ifade edilmesi, siber risklerin işletmeler açısından önemini ve bu risklere yönelik işletmelerin önlemler alması gerektiğini göstermektedir.

Siber risk kavramını anlamak adına en bilindik siber saldırılardan bahsederek konunun önemliliğini ortaya koyduktan sonra siber, siber risk ve siber güvenlik kavramını tanımlamanın yararlı olacağı düşüncesindeyiz.

Yapılan araştırma sonucunda en ses getiren siber saldırının 12 Mayıs 2017 tarihinde ağırlıklı olarak Avrupa ülkelerinde etkisinin görüldüğü "WannaCry" adlı siber saldırıdır. Uzmanlara göre bu tarihe kadar gerçekleştirilmiş en yaygın ve en büyük saldırı olarak görülmektedir. Hastaneler başta olmak üzere birçok kuruluş bu siber saldırıdan etkilenmiştir. WannaCry siber saldırıların en yaygın şekli olan fidye yazılım saldırısıdır. Sisteme kullanıcı erişimi engellenerek karşılığında, 300 dolar değerinde Bitcoin fidye istenmiştir. Bu fidyenin üç gün içinde ödenmemesi halinde iki katına çıkacağı; bir hafta içinde ödenmediği takdirde ise sistemdeki tüm bilgilerin silineceği yönündedir (Burca, 2017). Diğer bir siber saldırı da Ekim 2017'de gerçekleşen "BadRabbit" dir. Bu siber saldırıdan en çok etkilenen ülkeler arasında Türkiye, dördüncü sırada yer almaktadır. BadRabbit zararlı yazılım olarak bilgisayara bulaşarak WannaCry'da olduğu gibi fidye istenmektedir (Burca, 2017). Bunun gibi diğer siber saldırılar Burca tarafından şöyle özetlenmiştir (Burca, 2017):

- Amerika'nın en büyük kredi bürosu "Equfax"ın kayıtlarına sızılarak 145.5 milyon Amerikalı'nın kişisel bilgileri çalınmıştır (Temmuz, 2017).
- "Yahoo"nun ana şirketi olan Verizon, Yahoo'nun 3 milyar kullanıcısının hesabının saldırıya uğradığını açıklamıştır (Ekim, 2017).
- ShadowBrokers adlı anonim grup, Amerikan Ulusal Güvenlik Merkezi'nin "hacking" araçlarını sızdırmıştır (Nisan 2017).

- 64 ülkede, Petya (NotPetya) fidye siber saldırısı gerçekleştirilmiştir (Haziran 2017).
- Amazon'un bulut hizmetinin güvenlik ayarındaki bir açık nedeniyle, 200 milyon Amerikan seçmeninin kimlik bilgileri açık hale getirilmiştir (Haziran 2017).
- 57 milyon Uber müşterisinin verilerinin 2016 yılında çalındığı açıklanmıştır (Kasım 2017).

Siber risk kavramına bakacak olursak öncelikle siber kavramını açıklamanın konunun anlaşılması açısından yararlı olacaktır. Siber kavramı, hayatımızın birçok noktasında karşımıza çıkmasına karşın TDK (Türk Dil Kurumu) tarafından nasıl bir açıklama yapıldığı incelendiğinde kurum tarafından herhangi bir açıklamanın mevcut olmadığı tespit edilmiştir. Oxford sözlüğünde ise siber, "bilgisayar, bilgi teknolojisi ve sanal gerçeklik ile ilişkili veya özelliği" şeklinde tanımlanmıştır (Oxford Dictionaries, 1857). Sağıroğlu (2018: 23-24) tarafından siber, tanım itibarıyla "elektronik ortamları" ifade etse de içerisinde çok farklı unsurları barındırdığı ifade edilmiştir. Bu unsurların bulunduğu, işletildiği, yönetildiği ve geliştirildiği ortamlarda bulunan veriler; "bilgisayar, sunucu, cihaz, donanım, yazılım, protokol, algoritma, işlem, politika, süreç, laboratuvar ve sistem" gibi unsurları içermektedir. Ayrıca insan, siber dünyanın önemli unsurlarından birisi olduğuna vurgu yapılmıştır.

Siber risk ise, bir kuruluşun bilgi teknolojisi sisteminin bir tür başarısızlık nedeniyle finansal kayıp, işleyişini durdurma veya itibar kaybına sebep olan tüm riskleri kastetmektedir. Böyle riskler aşağıdaki sınıflandırılmış eylemler sonucu ortaya çıkmaktadır (The Institute of Risk Management, 2014: 8):

- Casusluk, dolandırıcılık veya para sıkıntısı sebebiyle bilgi sistemlerine erişmek için kasıtlı veya yetkisiz güvenlik ihlalleri,
- Kasıtsız veya kazara güvenlik ihlali,
- Zayıf sistem bütünlüğü ve diğer faktörlerden dolayı operasyonel BT riskleri.

Siber güvenlik "siber ortamlarda karşılaşılabilecek tehdit ve tehlikeler ile oluşabilecek riskleri önceden öngörüp bunlara karşı önceden önlem alma girişimi" veya "siber varlıkların tehdit ve tehlikelerden korunması için doğru teknolojiler, yöntemler, çözümler, önlemler, politikalar, standartlar, testler gibi girişimlerin doğru amaç, hedef veya şekilde kullanılarak siber varlıkların veya sistemlerin istenilmeyen kişiler/sistemler tarafından elde edilmesini önleme girişimi" olarak ifade edilmektedir (Sağıroğlu, 2018: 26).

Geçmişte yaşanan siber saldırılar ve tanımsal ifadelerin ardından bilgi sistemlerine yönelik gerçekleştirilen yaygın siber tehditler aşağıdaki şekildedir (Kumar, Srivastava, & Lazarevic, 2005: 5-6):

Kimlik Doğrulama Suçları (AuthenticationViolations): Şifreler çalındığında kimlik doğrulama suçları ile sonuçlanır. Bu sorunun çözümü için birçok şifre ve ek bilgiye sahip olmak gereklidir.

İnkar Edememe (Nonrepudiation): Mesaj gönderen kişi çok iyi bir biçimde mesaj gönderdiğini inkar edebilir. İnkar edememe teknikleri ile göndericinin mesajları takip edilerek inkar edilmesi engellenebilmektedir. Ancak web sayfasına erişen kullanıcının yerini belirlemek zordur.

Truva Atları ve Virüsler (Trojan Horses and Viruses): Truva atı ve virüsler, birçok etkiye neden olan kasıtlı programlardır. Virüsler makineden makineye yayılır ve çeşitli bilgisayarlardaki dosyaları silebilir. Truva atları, yüksek seviyeden düşük seviyeye bilgi sızdırabilir. Bunlar için çeşitli virüs paketleri geliştirilmiştir.

Sabotaj (Sabotage): Bilgisayar korsanları sistemleri kırarak uygun olmayan mesajlar gönderebilir.

Hile (Fraud): Ticaret ve işlerin çoğu, uygun kontroller olmadan internet üzerinden yürütülmektedir ve internet hileleri işletmelere milyon dolar kayıplara neden olmaktadır. Suçlular yasal kullanıcıların kimlik bilgilerinin elde edebilir ve banka hesaplarını boşaltabilir.

Hizmet ve Altyapısal Engellemelere Yönelik Saldırılar (Denial of Service and InfrastructureAttacks): Korsanlar tarafından alt yapılar kırılarak zarar görmektedir. Altyapılar, telekomünikasyon sistemleri, güç sistemleri ve sıcaklık sistemlerinden oluşur. Böyle saldırılar hizmet engellemelerine neden olacaktır.

Doğal Afetler (Natural Disasters): Siber terörizme ek olarak kasırga,deprem, yangın gibi doğal felaket-

lerde bilgisayarların ve ağların zarar görmesine neden olabilmektedir. Bu durumlara yönelik önlemler, verilerin korunması ve veri tabanlarının iyileştirilmesidir.

Yukarıdaki sıralanan tehditlerin yanında Aslay (2017: 25-26) tarafından; sosyal mühendislik, web sayfası hırsızlığı ve yönlendirme, hukuka aykırı içerik sunulması, sistem güvenliliğinin kırılarak içeri sızılması, yerine geçme, çöpe dalma, istem dışı alınan elektronik postalar, bukalemun, oltalama, mantık bombaları, zararlı yazılımlar, bilgi ve veri aldatmacası, salam tekniği ve süper darbe gibi siber saldırı türleri sıralanmıştır.

Davenport ve Amjad tarafından 2016 yılında yayınlanmış olan "Siber Güvenliğin geleceği adlı çalışmada bir istatistik sitesinin 2016 yılında 22.9 milyar cihazın birbirine bağlı olduğunu ve 2020'de bu rakamın 50 milyara çıkacağı tahmin edilmektedir. Milyarca cihazın çevrim içi olmasıyla birlikte siber riskler artacaktır ve siber güvenliği karmaşık ve zorlu hale getirecektir(Davenport & Amjad, 2016). Davenport ve Amjad'ın yapmış olduğu çalışmadan da görüldüğü üzere siber riskler her geçen gün artmaktadır. Bu nedenle siber risklerin belirlenmesi ve yönetilmesi önemli hale gelmektedir.

3. SİBER RİSKLERİN BELİRLENMESİ VE YÖNETİLMESİ

İşletmelerin siber risklerini belirlenmesi ve siber riskleri yönetmesi işletme hedeflerine ulaşılması, zarara uğramama ve itibar kaybının yaşanmaması adına önemlidir. Hem özel sektörde hem de kamu sektöründe bilginin korunması önemlidir. Bu noktada öncelikle farkındalık düzeyinin artırılması öncelikli adımdır. Türkiye'de farkındalık düzeyini değerlendirmek adına yapılan bir çalışmada 501 kullanıcının %96.3'ü bilgi güvenliğinin önemini farkında olmasına rağmen aynı kullanıcıların %51.5'lik kısmı kullandıkları teknolojik cihazlara ilişkin tehditleri farkında değillerdir. Dolayısıyla bireysel, kamu kurumu ve özel sektör olarak öncelikle siber tehditlerin konusunda farkındalığın olması gereklidir. Bu nokta işletmeler tarafından çalışanlarına siber risklere ilişkin farkındalık eğitimi verilmesi önemli ölçüde etkili olmanın yanında hızlı değişim nedeniyle farkındalığın etkin yönetim ile süreklilik sağlanacağı göz ardı edilmemelidir (Erol & Sağıroğlu, 2018:107-109). IIA (The Institute Of Internal Auditing- İç Denetim Enstitüsü) tarafından yapılan çalışma incelendiğinde, siber ile ilişkili riskleri aşmak ve çözümlemek için, liderlik ekibinin önleyici tedbirler geliştirmesi, bu tedbirleri eğitim ve bilinçlendirme programlarıyla birlikte uygulamaya konmasının öneminden bahsedilmiştir. Dolayısıyla farkındalığı artırmak adına çalışanlar, tedarikçiler, ortaklar ve yükleniciler de aynı şekilde eğitilmeli ve siber güvenlik tedbirleri ve protokolleri konusunda onlardan neyin beklendiğini tam olarak anlamaları sağlanmalıdır (IIA, 2018:7).

Siber güvenlikte temel hedef; güvenliğin makul seviyede sağlanmasıdır. Burada yüzde yüz bir güvenliğin hiçbir zaman sağlanamayacağı yaklaşımı göz önünde bulundurulmalıdır. Bu noktada siber güvenliğin sağlanması için siber risklerin belirlenmesi ve doğru yönetilmesi önemli bir faktördür. Dolayısıyla risklerin iyi belirlenmesi, giderilmeye çalışılması için iyi bir risk yönetimi yapılmalı, mevcut teknikler, teknolojiler, politikalar, standartlar ve çözümler uygulanarak siber güvenlik kapsamında çalışmalar yürütülmelidir. Siber güvenlikte aşağıdaki unsurlar yer almaktadır:

- Bir güvenlik politikası oluşturulmalı ve uygulanmalıdır.
- Gereği kadar koruma prensibi uygulanmalıdır.
- İyi bir risk analizi ve yönetimi yapılmalıdır.
- Sistemlere belirli periyotlarla hataları, eksiklikleri, açıklıkları ve zafiyetleri gidermek amacıyla testler (sızma testleri) yapılmalıdır.
- Sistemleri kullanan her kullanıcıya en az hak verme yaklaşımı benimsenmelidir.
- Siber güvenliğin sağlaması adına düzenleme ve standartlar (Siber Çağda COSO, ISO 27000 vb.) takip edilmeli ve uygulanmalıdır.
- Elektronik ortamlarda her zaman güvensiz bir ortam olduğu göz önünde bulundurulmalıdır. Bu bağlamda bilgi varlığının yedeklenmesi ve kurtarılmasına yönelik sistemler kurulmalı ve işletilmelidir.
- Güncel tehdit ve tehlikeler takip edilerek giderilmelidir.
- Olası tehdit ve tehlikeler öngörülmeli ve önlem alınmalıdır bu amaç doğrultusunda mekanizma ve yapılar kurularak işletilmelidir.

- Güvenli bileşenleri tanımlama ve güvenlik gerektiren bileşenlerin sayıları en aza indirme temel amaç olmalıdır.
- Siber güvenlik sistemleri ile ilgilenen uzmanların kendilerini geliştirmeleri konusunda fırsat verilmelidir (Sağıroğlu, 2018: 44).

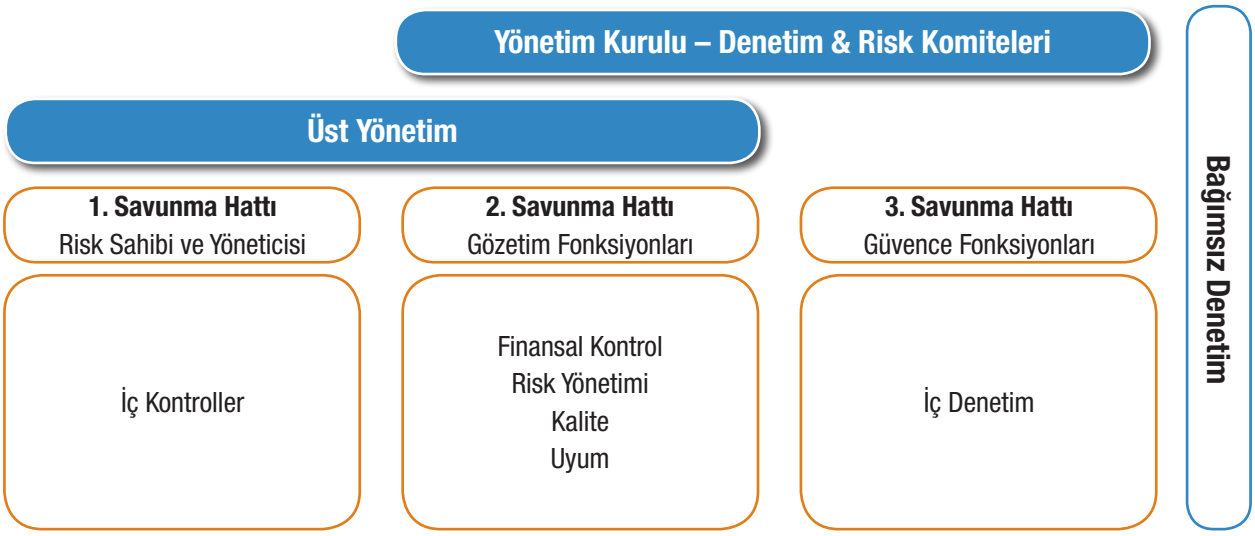
Son olarak KPMG tarafından siber güvenliğin sağlanması dolayısıyla siber risklerin belirlenmesi ve yönetilmesi şöyle özetlenmiştir (KPMG, 2016: 7):

- İşletmelerin sahip olduğu ağları korumak amacıyla gerekli anti-virüs yazılımlarını kurmak, güvenlik duvarı oluşturmak, siber olay yönetimi politikası oluşturmak ve kullanıcı eğitimine ve farkındalığa önem vermek gibi temel konuları ele almak,
- Siber güvenlik önlemlerinin merkezinde, yönetim kurulunun sorumluluğunda olan bilgi riski yönetimi yatmaktadır. Bu nedenle şirketin en önemli bilgi varlıklarının neler olduğunu anlamak ve bu varlıklara yönelik riskleri yönetmek,
- Siber güvenliği artırma projelerinde, insan faktörünü, kültürü, iş süreçlerini ve teknik güvenlik tedbirlerini birlikte ele alacak bütüncül bir yaklaşım benimsenmesi,
- Siber güvenlik sadece teknik bir konu olmadığı; siber güvenliğin sağlanması için siber olaylara karşı hazırlıklı olmayı, korunmayı, böyle olayları tespit etmeyi ve gerektiğinde tepki vermeyi içeren entegre bir yaklaşımın benimsenmesi,
- Çalışanlar kasıtsız şekilde en büyük güvenlik açığını oluşturuyor olabilirler, bu yüzden doğru davranışlara teşvik etmek için teknik eğitim ve farkındalık eğitimi verilmesi,
- Siber güvenlik sisteminin etkinliğini takip edecek bir yönetim yapısının oluşturulması ile siber tehditleri takip ederek daha iyi risk kararlarının alınmasını sağlayacak bir araştırma sisteminin kurulması.

4. SİBER GÜVENLİKTE ÜÇLÜ SAVUNMA HATTI

Geçmişte yaşanan muhasebe skandalları, başarısızlıklar, bilgi hırsızlığı, ve doğal afetler gibi küresel olaylar risk yönetimini yatırımcılar, ortaklar, yönetim kurulları, paydaşlar ve müşteriler açısından yeniden önemli hale getirmiştir (KPMG, 2016: 7). Bu kapsamda işletmelerin risk yönetimi görevlerini sistematik bir yaklaşımla atamaları ve koordine olmalarına yardımcı olacak en iyi uygulama üçlü savunma hattı modelidir. Dolayısıyla işletmelerin siber güvenliği sağlamada organizasyondaki tüm taraflara önemli görevler düşmektedir. Bu kapsamda işletmenin tüm süreçlerine atamalar yapılması, rol ve sorumlulukların net şekilde belirlenmesi, sahiplenilmesi ve zamanında, eksiksiz

Şekil 1. Üçlü Savunma Hattı



(Erdemir Grubu, 2015: 2)

şekilde yerine getirilmesi tüm risklerde olduğu gibi siber güvenlik yönünden de kritik öneme sahiptir.

Üçlü savunma hattı, Uluslararası İç Denetçiler Enstitüsü tarafından işletmelerin karşılaşabileceği birçok riske yönelik bir model olmakla birlikte çalışmamızın konusu itibariyle Enstitünün yayınladığı rehber (Global Technology Audit Guide (GTAG): Assessing Cybersecurity Risk: Roles of the Three Lines of Defense) kapsamında siber risklerin değerlendirilmesinde üçlü savunma hattının rolü ortaya konulmaya çalışılmıştır.

Rehber çerçevesinde üçlü savunma hattına ilişkin açıklamalar aşağıdaki başlıklarda sırasıyla özetlenmiştir (IIA, 2016: 6-15).

4.1. Birinci Savunma Hattı

Birinci savunma hattı, yönetim kontrollerinden oluşmaktadır. Bu savunma hattı Kaya (2017) tarafından *"riske karşı çarpışmanın en şiddetli yaşandığı cephe"* olarak ifade edilmiştir. Diğer bir ifadeyle şirketlerin tüm süreçlerine yönelik risklerin ilk kontrol altına alındığı hattır. Birinci savunma hattında yönetim, otomasyon, süreç, manuel vb. kontrollerin tasarlandığı kısımdır. Siber güvenlik açısından bakıldığında GTAG rehberinde ilk savunma hattı,riskleri kontrol eden ve yöneten ve süreçleri ve kontrol eksikliklerini gidermek için düzeltici eylemler uygulayan operasyonel yöneticilerden meydana geldiği ifade edilmiştir. Bu bağlamda işletmelerde teknolojiden sorumlu genel müdür (CTO, Chief Technology Officer), bilgi güvenlik yöneticileri (CISO, Chief Information Security Officer), bilgi yöneticisi (CIO, Chief Information Officer) veya BT (Bilgi Teknolojisi)'den sorumlu başka bir sorumluyu işe alabilir. Teknolojiden sorumlu genel müdür genellikle kuruluşun misyonunu yürütmek için mevcut teknolojiler hakkında bilgi ve yön sağlamaktan sorumludur ayrıca kuruluşun fikri mülkiyetini korumaktan sorumludur. Diğer sorumlu kişiler ise kuruluşun varlıklarının ve paydaş verilerinin uygun şekilde korunduğunu doğrulamak için sık sık gözetim programları geliştirmede liderlik ederler. Rehberde birinci savunma hattına ilişkin faaliyetler aşağıdaki şekilde sıralanmıştır:

- Güvenlik prosedürlerinin yönetimi, eğitimi, testi.
- Düzenlemelerin/konfigürasyonların güvenli araçlarla sürdürülmesi, uygulamaların güncellenmesi, yamaların yapılması,
- Saldırı tespit sistemini etkin kullanmak ve penetrasyon (sızma) testlerinin yürütülmesi,
- Network trafik akışını yeterli seviyede yönetmek ve korumak için güvenli şekilde network yapılandırılması,
- Bilgi varlıklarının, teknolojik araçların ve ilgili yazılımların envanteri,
- İzleme/gözetim ile ilgili veri koruma ve kayıp önleme programlarının etkin kullanımı,
- Erişim kısıtlaması,
- Gerekli yerlerde verilerin şifrelenmesi,
- İç ve dış taramalar ile zafiyet yönetimi uygulamaları,
- Sertifikalı IT, IT riski ve bilgi güvenlik personelinin işe alımı ve devamlılığı.

4.2. İkinci Savunma Hattı

İkinci savunma hattına baktığımızda finansal kontrol, kalite yönetimi, risk yönetimi, uyum gibi güvence fonksiyonlarından oluşmaktadır. Birinci savunma hattını aşarak yakalanan ve ciddi boyuttaki risklerin takip edildiği savunma hattıdır. İkinci savunma hattında oluşacak bir hata işletmeyi ciddi zararlara uğratabilir (Kaya, 2017). İkinci savunma hattının, siber güvenliğe ilişkin bir takım sorumlulukları vardır. Bunlar:

- Siber güvenlikle ilgili risklerin değerlendirilmesi ve risklerin kuruluşun risk iştahına uygun olup olmadığını belirlemek,
- Mevcut ve ortaya çıkan riskleri izleme, yasalarda ve düzenlemelerdeki değişiklikleri izlemek,
- Uygun kontrol tasarımı sağlamak için birinci savunma hattı fonksiyonları ile işbirliği yapmak.

Uluslararası İç Denetçiler Enstitüsünün yayınlamış olduğu rehberde ikinci savunma hattında siber güvenlikle ilgili yaygın faaliyetler şöyle sıralanmıştır:

- Siber güvenlik politikaları, eğitimi ve testlerinin tasarlanması,
- Siber risk değerlendirmelerinin yapılması,
- Siber tehdit bilgilerinin toplanması,
- Verilerin sınıflandırılması ve kısıtlı erişim rollerinin tasarlanması,

- Olayların anahtar risk göstergelerinin izlenmesi ve iyileştirilmesi,
- Sertifikalı IT risk personelinin işe alınması ve devamlılığı,
- Üçüncü taraflarla, tedarikçilerle ve hizmet sağlayıcılar ile ilişkilerin değerlendirilmesi,
- İş sürekliliği planlarının yapılması/test edilmesi ve olağanüstü durumları iyileştirme uygulamaları ve testlerine katılım.

Savunma hattının son aşamasında iç denetim yer almaktadır. İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. İç denetim, kurumun risk yönetim, kontrol ve yönetişim süreçlerinin etkililiğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur (Türkiye İç Denetim Enstitüsü, 1994). Üçlü savunma hattının en önemli kısmıdır. Çünkü üçüncü savunma hattını geçen riskler organizasyonlar için yıkıcı sonuçlara neden olabilir. Bu nedenle iç denetim üçlü savunma hattında önemli sorumluluğa sahiptir (Kaya, 2017). Bu kapsamda üçüncü savunma hattına ilişkin açıklamalar aşağıda kısaca yapılmıştır.

4.3. Üçüncü Savunma Hattı

Üçüncü savunma hattı olarak iç denetim faaliyeti üst yönetime ve yönetim kuruluna yönetişim, risk yönetimi ve kontroller konusunda bağımsız ve objektif bir güvence sağlar. Bu, siber güvenlik risklerini ve tehditlerini yönetme ve azaltmada birinci ve ikinci savunma hattının gerçekleştirdiği faaliyetlerin genel etkinliğinin değerlendirilmesini içerir. İç denetim faaliyeti aşağıdaki konularla ilgili danışmanlık yapabilir:

- Siber güvenlik ve organizasyonun riskleri arasındaki ilişki,
- Tepkilere ve kontrol faaliyetlerine öncelik vermek,
- Organizasyonun tüm ilgili yönlerinde siber güvenlik riskinin azaltılması için denetim. Örneğin, ayrıcalıklı erişim, ağ tasarımı, satıcı yönetimi, izleme ve daha fazlası.
- İyileştirme faaliyetlerinde güvence,
- Risk farkındalığını artırmak ve özellikle ikinci savunma hattı olmayan veya yeterince olgun olmayan işletmelerde risk yönetimi aktivitelerinin koordinasyonuna yardımcı olur,
- Siber risklerle ilgili konuların iş sürekliliği planları ve olağanüstü olayların iyileştirilme testleri kapsamına dahil edilip edilmediğini doğrular.

Üçüncü savunma hattı yani iç denetim tarafından gerçekleştirilen ortak faaliyetler şöyledir:

- Siber güvenlikle ilgili önleyici ve tespit edici önlemlerin sürekli bağımsız değerlendirilmelerini sağlamak,
- Standart güvenlik yapılandırmaları, sorunlu web siteleri, kötü amaçlı yazılımlar ve veri sızıntıları için kısıtlı erişime sahip kullanıcıların BT varlıklarını değerlendirmek,
- İyileştirme tedbirlerini takip etmek,
- Hizmet kuruluşları, üçüncü şahıslar ve tedarikçilerin siber risk değerlendirmelerini yapmak.

5. İÇ DENETİMİN SİBER GÜVENLİK AÇISINDAN ÖNEMİ

5.1. Siber Güvenlik Gereksinimi

Siber güvenlik, her yıl şirketler, organizasyonlar ve hükümetler için daha önemli bir konu haline gelmeye başlamıştır. Siber saldırılar nedeniyle, birçok şirket hem bilgi hem de maddi kayıplarla da karşılaşabilmektedir. Bunların en büyük sebepleri arasında, birçok şirketin halen eski teknolojiler kullanıyor olmaları ve yeni teknolojilerini, eski ve kalabalıklaşmış olan güvenlik sistemlerinin üzerine kuruyor olmalarıdır. Güvenlik sistemlerinin güncellenmemesi ve eski teknolojilerin kullanılıyor olması, internet korsanlarının işini biraz daha kolaylaştırmaktadır.

Dijital dünyada iş yapan firmaların siber güvenlik konusuna özellikle önem vermeleri ve güvenlik sistemlerini geliştirmeleri, bu saldırılardan korunmalarını sağlayacak çalışmaların başında gelmektedir. Her geçen gün büyümekte olan saldırı hacimleriyle aynı olmadığı için de, bu saldırıları önlemek için siber güvenlik harcamalarına yapılan yatırımlar her yıl biraz daha artma eğilimindedir.

Siber güvenlik süreçleri hem iç hem de dış denetçiler tarafından denetimin amacı ve kapsamı çerçevesinde ele alınmalıdır. Çünkü işletmelerde artık siber riske

maruz kalmayan hiçbir süreç bulunmamaktadır. Endüstri 4.0, akıllı şehirler, yapay zeka ve büyük verinin (big data) alanının etkileri göz önüne alındığında, finansal, operasyonel veya sistematik tüm süreçler siber riske maruz kalmaktadır.

Her denetimde olduğu gibi siber güvenliğe yönelik yapılan denetiminde bir amaç bulunmaktadır. Bu amaç şöyle ifade edilmiştir: *Yönetimin siber güvenlik süreçlerini, politikalarını, prosedürlerini, yönetişim ve diğer kontrollerin değerlendirilmesini saptayarak yönetime sistematik ve bilimsel güvence ve danışmanlık hizmeti sunmaktır.* Denetimde siber güvenlik standartlarına, iç kontrollere uygunluğun değerlendirilmesine odaklanılmaktadır (Efe, 2018: 351).

5.2. Siber Güvenlik ve İç Denetimin İlişkisi

Yapay zekanın benimsenmesi ve gelişimi kamu kuruluşları ve özel sektörün kendi siber kapasitelerine yeniden daha dikkatli şekilde önem vermeye zorlamıştır. Yapay zekanın güçlenmesi ve büyük veri sistemlerini kullanmak ve bu sistemleri kurum dışı ve kötü niyetli güçlerden korumak başarı açısından kritik bir önem kazanmıştır (IIA, 2017: 10). Her ne kadar siber güvenlik gibi karmaşık ve hızlı değişen bir konu hakkında mutlak bilgi sahibi olunması mümkün olmamakla birlikte bir iç denetçi yöneticisi (İDY) veya iç denetim birimi başkanının siber güvenlik konusunu yakından takip etmesi ve konu hakkında bilgi sahibi olmasının önemi artmaktadır. Ayrıca yukarıda belirtildiği üzere siber riskler sadece bir teknoloji riski olmanın ötesinde bir iş riskidir. Dolayısıyla iç denetçiler bu konuda kritik rol oynamaktadır. Bu noktadaki başarı, yönetim ve denetim komitesinin bu konuya ne kadar önem verdiğine ve İDY'nin benimsediği yaklaşımla ilişkilidir. İDY, yalnızca siber güvenlik denetimlerinin yürütülmesi ile ilgili sorumluluklara değil aynı zamanda kuruma, ileriye dönük ve stratejik düşünce liderliği sunmak suretiyle kurum için güvenilir danışmanlık hizmeti sunmaya da fırsat vermektedir (IIA, 2016: 4).

Siber güvenlik konusunu oluşturan karmaşıklık arasında iç denetimin doğrudan etki edebileceği dört önemli alan bulunmaktadır. Bunlar:

- Siber tehditlere karşı hazırlık ve müdahale hakkında güvence vermek,
- İcrai yönetime ve kurula kurumun karşı karşıya olduğu risk seviyesini ve bu risk seviyelerine cevap vermek için sarf ettiği çabanın düzeyini bildirmek,
- Etkili savunma ve müdahale mekanizmalarını temin etmek için BT ve diğer taraflarla birlikte çalışmak,
- Risklerle ilgili olarak organizasyonlarda bulunan taraflar arasında iletişimi ve koordinasyonu sağlamak ve kolaylaştırmak (IIA, 2017: 10).

Uluslararası İç Denetçiler Enstitüsü'nün 2016 yılında "Global Perspektif ve Anlayışlar: Güvenilir Siber Danışmanlık İçin İç Denetim" kitapçığında belirtildiği üzere siber güvenlik bütüncül bir bakış açısıyla ve sistemli bir şekilde ele alınması gereklidir. Aksi durumda, siber güvenliğin sağlanamaması halinde, işletmenin en temel faaliyetlerinin bile yürütülemeyeceği, fikri mülkiyet haklarının kaybedilmesine ve hatta itibar kaybına uğrayacağı belirtilmiştir. Bu sebeple siber güvenlikte iç denetimin sorumluluğu yüksektir. İç denetim bu kadar önemli bir noktada kilit taşı olmasına karşın E&Y (Ernst&Young) tarafından 2016 yılında "Dijital Dünyada Güven Yaratmak" başlıklı rapor incelendiğinde birçok işletmenin siber güvenliği önemsemediği tespit edilmiştir. Ayrıca pek çok işlemenin bu sorunu ciddiye almayan bir yaklaşım sergilediği, mevcut zafiyetin etkisini daha da artırdığı konusunda raporda uyarıda bulunulmaktadır.

Yukarıdaki açıklamalar neticesinde siber risklere karşı bilinçli ve hazırlıklı olmanın gerekli olduğu söylenebilir. Bu noktada birçok kuruluş bilinçli olmasına karşın hazırlıklı değildir. Hazırlıklı olmak için işletmelerin bir siber saldırıları önleme, siber saldırılara direnme veya en az zararla kurtulma yeteneğine sahip olmaları gereklidir. Tüm bunların sağlanmasında iç denetimin etkisinin önemli olduğunu, işletmelerdeki iç denetim birimlerinin kendilerini siber güvenlik alanında geliştirmesi gerektiğini tekrar ifade edebiliriz.

Siber risklere (bilgisayar korsanlığı/izinsiz girişler, şifre avcılığı, ekonomik casusluk vb.) ilişkin endişeler artıkça paydaşlar siber güvenlik risk programlarını takip etmektedir ve yönetim kurulu iç denetim biriminden siber güvenlik konusunda güvence talep etmektedir. Bu sebeple iç denetim birimi siber riskler konusunda bilgi sahibi olmalı ve siber risklere karşı dirençli olmada rol üstlenmeli ve oynamalıdır.

İç denetim biriminin risk değerlendirme stratejileri, siber güvenliğe özgü tüm riskleri içerecek şekilde geliştirilmeli, politika ve iç kontrollere uyulması konusunda güvence vermelidir. Dolayısıyla iç denetim birimi paydaşlara gerekli güvenceyi vermek adına siber sorunlarla ilgili denetim programı geliştirmesi gereklidir. Bu denetim programının etkinliği için kontrol ortamı, kontrol faaliyetleri, risk değerlendirme, iletişim ve izleme süreçlerinin kurulması ve siber güvenlik tedbirlerinin değerlendirilmesi için bir çerçevenin kurulması gereklidir.

Üçüncü savunma hattı olarak iç denetim, kuruluşun siber risklerini tespit etme ve azaltma yeteneğini geliştirmek için siber güvenlik stratejileri ve politika geliştirme çalışmalarını yönetim ve yönetim kurulu ile iş birliği içinde gerçekleştirmelidir. İç denetim birimi gelişmekte olan teknoloji ve trendler kuruluşun siber güvenlik risk profilini etkileyeceğinden sürekli teknolojiden haberdar olmalıdır. Ayrıca kuruluşun kırılganlık seviyesini değerlendirmeli ve işletmenin risk faaliyetlerini tercih edilen siber güvenlik planına kıyasla gözden geçirmelidir (IIA, 2018: 6-9).

Son olarak iç denetim faaliyetleri ilk savunma hattındaki kontrollerin etkinliğini değerlendirir. BT genel kontrollerinin temel olduğunu ancak siber güvenlik riskini azaltmak için tam bir çözüm sunmadığını göz önünde bulundurmak önemlidir. Siber güvenliğin karmaşıklığı dolayısıyla risklerin izlenmesi, suiistimallerin ortaya çıkartılması ve düzeltici faaliyetlerin başlatılması gibi ilave kontrol katmanlarına ihtiyacı olduğu unutulmamalıdır (IIA, 2016).

6. SONUÇ VE ÖNERİLER

Endüstri 4.0, yapay zeka, bigdata, nesnelerin interneti gibi kavramların hayatımıza girmesi birçok bilgiye kolaylıkla ulaşmamızı ve işlememizi sağlarken, diğer taraftan birçok bilgisayarın birbirine bağlı olduğu bir dünyada tehlikelere açık bir ortamın olması kaçınılmaz hale gelmektedir.

Kuruluşlar birçok riskle karşı karşıya olmakla birlikte bilgi teknolojisindeki yaşanan gelişmeler kuruluşları yeni bir risk ile mücadele etmek zorunda bırakmaktadır. Bahsedilen bu yeni risk siber güvenlik riski olarak adlandırılmaktadır. Siber güvenlik riski, kuruluşların dijital ortamda işlemlerini gerçekleşmesi sonucu bir takım tehditlerle karşılaşma riski olarak kısaca ifade edilebilir.

Siber saldırıların artışıyla birlikte birçok düzenleyici kurumun bu konu üzerine yoğunlaşmasına neden olmuştur. Çünkü siber saldırılar ile kuruluşların değerli varlıkları ve verilerine tehdit altındadır. Kuruluşların karşılaştıkları siber tehditler müşteri bilgilerinin açıklanması, fikri mülkiyetlerin çalınması, işletmeye ait verilerin çalınması ya da işletmelerin sahip olduğu uygulamaların veya tedarik zincirlerinin zarar görmesi şeklinde özetlenebilir. Tüm bu tehditlerin etkileri finansal kayıp ve itibar kaybı şeklinde yansımaktadır. Dolayısıyla kuruluşların siber güvenlik risklerine odaklanmaları, bu riskleri tespit etmek, azaltmak veya en az zararla kurtulmak için özel çalışmalar gerekmektedir. Siber güvenlik riskleri ile mücadelede öncelikle kuruluşta farkındalık düzeyinin artırılması önemlidir. Bu yönde hem işletme içinde hem de işletme dışındaki tarafların siber güvenlik riski konusunda bilinç seviyelerini artırmaya yönelik eğitimler, programlar düzenlenmelidir.

Kuruluşların siber güvenlik riskine ilişkin farkındalığın oluşmasının ardından risklerin yönetilmesinde kullanılan, önemli bir model olan, üçlü savunma hattı modeli oluşturulmalıdır. Bu kapsamda kuruluşların birinci savunma hattında siber güvenlikten sorumlu kişilerin tanımlandığı ve kontrol faaliyetleri ele alınmaktadır. İkinci savunma hattı, risklerin değerlendirilmesi, risklerin kuruluşun risk iştahına uygun olup olmadığının izlenmesi, risklerin ve risk değerlendirmeleri kapsamında düzenlemelerin izlenmesi, risklerin azaltılmasında birinci savunma hattıyla işbirliği yapılması sorumluluğuna sahiptir. Üçüncü savunma hattı yani iç denetim, yönetişim, risk yönetimi ve kontroller konusunda bağımsız ve objektif güvence sağlar. Dolayısıyla siber güvenlik konusunda önleyici ve tespit edici kontrollerin bağımsız ve objektif şekilde iç denetiminin yapılması, işletmenin sahip olduğu BT varlıklarının saldırılara karşı etkinliğinin değerlendirilmesi, iyileştirme çalışmalarının takibi ve üçüncü tarafların siber değerlendirilmelerinin yapılması gibi sorumluluklara sahiptir.

Son olarak, siber güvenlik risklerinin engellenmesinde önemli role sahip olan iç denetimin değişen dünya karşısında geri kalmaması gerektiğini vurgulamak faydalı olacaktır. Bu değişen dünya karşısında hazırlıklı olmak adına yapay zeka, big data, siber saldırılar vb. konularda iç denetçilerin bilgi sahibi olması bir zorunluluktur. Ayrıca iç denetçiler, gelişen dünya karşısında rollerinin ne olacağının, kurum ve işletmelere ne gibi katma değerler sağlayacaklarının farkında olarak kendilerini geliştirmeli ve çalışmalarını yürütmelidirler.

Kaynakça

American Accounting Association. (2017). Cybersecurity and Continuous Assurance. *Journal Of Emergıng Technologıes In Accountıng* , 1-12.

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies* , 24-28.

Burca, N. (2017, Aralık 29). *2017 Siber Saldırıları 2018 Beklentileri ve İç Kontroller*. Mart 5, 2019 tarihinde https://nazifburca.com adresinden alındı

Burca, N. (2017, Haziran 3). *İç Kontrolleriniz Etkin Mi? «WannaCry» Siber Saldırısında Sorumluluk Kime Ait?* Mart 5, 2019 tarihinde https://nazifburca.com adresinden alındı

Burca, N. (2017, Ekim 25). *Yeni Bir Siber Saldırı: BadRabbit*. Mart 2019 tarihinde https://nazifburca.com adresinden alındı.

COSO. (2015). *COSO in the Cyber Age: Report Offers Guidance on Using Frameworks to Assess Cyber Risks.*

Davenport, T., & Amjad, A. (2016). *The Future Of Cybersecurity.* Mart 8, 2019 tarihinde Deloitte Insight: ttps://www2.deloitte.com adresinden alındı.

Efe, A. (2018). Siber Güvenlik Denetimi. Ş. Sağıroğlu, & M. Alkan içinde, *SiBer Güvenlik ve Savunma-Farkındalık ve Caydırma* (s. 349-370). Ankara: Grafiker Yayıncılık.

Erdemir Grubu. (2015, Mayıs 9). *İç Denetim Sistemi*. Mart 7, 2019 tarihinde https://slideplayer.biz.tr/slide/4870511/ adresinden alındı.

Erol, S. E., & Sağıroğlu, Ş. (2018). Siber Güvenlik Farkındalığı, Önemi Ve Yapılması Gerekenler. Ş. Sağıroğlu, & M. Alkan içinde, *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık* (s. 105-134). Ankara: Grafiker Yayınları.

IIA. (2016). *Assessing Cybersecurity Risk Roles of the Three Lines of Defense.* The Institute of Internal Auditors. https://www.aicpa.org.

IIA. (2018). *Global Bakış AÇıları ve Anlayışlar: 2018 Global Risk Raporu-İç Denetim Yöneticilerinin Karşılaştığı En Büyük Riskler.* The Institute Of Internal Auditing.

IIA. (2016). *Global Perspektifler ve Anlayışlar: Güvenilir Bir Siber Danışman Olarak İç Denetim.* The Institute of Internal Auditors.

IIA. (2017). *Küresel Bakış Açıları ve Anlayışlar Yapay Zeka - İç Denetim Mesleğine İlişkin Dikkate Alınması Gerkenler.* The Institute of Internal Auditors.

ISACA. (2017). *Auditing: Cyber Security Evaluating Risk and Auditing Controls.*

Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, 360-376.

Kaya, B. (2017, 4 9). 3 10, 2019 tarihinde Şirketlerin Güvencesi Üçlü Savunma Hattı: http://bertankaya.net adresinden alındı.

KPMG. (2016). *Denetim Komiteleri İçin Siber Güvenlik.*

KPMG. (2016). GRC Gündemi: Yönetişim, Risk ve Uyumluluğu Anlamak.

Kumar, V., Srivastava, J., & Lazarevic, A. (2005). *Manager CyberThreats Issues, Approaches and Challenges.* U.S.A.: Springer.

Kurt, G., & UysaL, U. T. (2015). Siber Riskler ve COSO İç Kontrol Bütünleşik Çerçevesi. *Muhasebe ve Denetime Bakış dergisi* , 1-10.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems* , 11-26.

Ojeka, S. A., Ben-Caleb, E., & Ekpe, E.-O. I. (2017). Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. *International Review of Management and Marketing* , 340-346.

Öztürk, M. S. (2018). Siber Saldırılar, Siber Güvenlik Denetimleri Ve Bütüncül Bir Denetim Modeli Önerisi. *Muhasebe ve Vergi Uygulamaları Dergisi*, 208-232.

PWC. (2018). Global Economic Crime and Fraud Survey 2018.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A Comprehensive Cybersecurity Audit Model to Improve

Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). *International Conference on Information Systems and Computer Science*, 253-259.

Sağıroğlu, Ş. (2018). Siber Güvenlik Ve Savunma: Önem, Tanımlar, Unsurlar Ve Önlemler. Ş. Sağıroğlu, & M. Alkan içinde, *Siber Güvenlik ve Savunma-Farkındalık ve Caydırıcılık* (s. 21-45). Ankara: Grafiker Yayınları.

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizon*, 349-356.

SPK. (2018). Bilgi Sistemleri Bağımsız Denetim Tebliği. Sermaye Piyasası Kurulu.

SPK. (2018). Bilgi Sistemleri Yönetimi Tebliği. Sermaye Piyasası Kurulu.

The Institute of Risk Management. (2014). *Cyber Risk Executive Summary.*

İnternet kaynakları

Oxford Dictionaries. (1857). Mart 2019, 8 tarihinde https://en.oxforddictionaries.com adresinden alındı.

Türkiye İç Denetim Enstitüsü. (1994). Mart 2019, 10 tarihinde https://www.tide.org.tr adresinden alındı.

SİBER HİJYENİN SAĞLANMASINDA İÇ DENETİMİN ROLÜ[1]

(THE ROLE OF INTERNAL AUDITING IN PROVIDING CYBER HYGIENE)

Alptuğ GÜLER* / Ali Kasım ARKIN**

ÖZ

Dünya tarihinde en yıkıcı savaşlar olarak 1. ve 2. Dünya Savaşları kabul edilmektedir. Ancak bu durum artık değişmektedir. Siber dünyadaki siber savaşların siber saldırganları, kendilerini 7 gün / 24 saat hazırlamakta ve çok uzun olmayan bir gelecekte bir ameliyathanenin enerji sistemlerini kesintiye uğratma, metro hattındaki trenleri çarpıştırma, fabrikaların üretim hatlarını durdurma gibi teknolojik saldırı potansiyeline sahip olma yolunda ilerlemektedirler. Ülke, kurum ve kişisel kullanıcı olarak, teknolojik araçların sahip olduğu siber riskler göz önünde bulundurulduğunda bu risklerin kontrolü için siber güvenlik ve siber güvenlik risk yönetimi temelli yaklaşım önem kazanmaktadır. Siber hijyen, siber bilgi güvenliği ile ilgili temel bir ilkedir ve kişisel hijyenle benzerlik gösterdiği gibi, siber tehditlerden kaynaklanan riskleri en aza indirgemek için basit rutin önlemler almanın eşdeğeridir. Bu bağlamda, bir olgunluk modeli olarak siber hijyen, kişisel hijyen ile aynı önemde görülmeli ve bir kuruma düzgün şekilde entegre edildiğinde, kurumsal siber bağışıklık sistemleri ve sağlıklarının en iyi durumda olacağı göz önünde bulundurulmalıdır. Günümüz kurumları için bu denli kritik olan risk yönetimi ve siber güvenlik sitemleri için gerekli bağımsız güvence, iç denetim tarafından benzersiz bir şekilde sağlanabilir. İç denetçiler bu süreçte önemli danışmanlar olabilir. Bu bakımdan, siber güvenliğin oluşturulması sürecinde siber hijyenden başlayarak üçüncü savunma hattına kadar iç denetim faaliyetinin siber rolü her geçen gün artmaktadır.

Bu makalede, siber güvenlik ve siber hijyen bağlamında iç denetçilerin ve iç denetimin siber rolü değerlendirilmektedir.

Anahtar Kelimeler: Siber Güvenlik, Siber Hijyen, İç Denetim, Siber Güvenlik Yönetişimi, Siber Güvenlik Olgunluk Modeli

JEL Kodlaması: G32, M42

ABSTRACT

The most destructive wars in the history of the world are accepted as the first and second world wars. However, this situation is changing now. The cyber attackers of cyber wars in the cyber world prepare themselves for 7 days / 24 hours, and in the not too long future, they are on the way to interrupt the energy systems of an operating room, collide the trains in the subway line, and have the potential of technological attacks such as stopping the production lines of the factories. As a country, organization and personal user, the cyber security and cyber security risk management based approach is important for controlling these risks when the cyber risks of technological tools are taken into consideration. Cyber hygiene is a fundamental principle of cyber information security and is equivalent to personal hygiene and is equivalent to taking simple routine measures to minimize the risks associated with cyber threats. In this context, cyber hygiene as a model of maturity should be seen as of the same importance as personal hygiene, and when integrated properly into an organization, it should be considered that organizational cyber immune systems and health are in the best condition. The independent assurance for risk management and cyber security systems that are so critical for today's organizations can be uniquely provided by internal audit. Internal auditors may be important consultants in this process. In this respect, starting from cyber hygiene in the process of cyber security creation the cyber role of internal audit activity is increasing day by day until the third line of defense.

In this article, the cyber role of internal auditors and internal audit is evaluated in the context of cyber security and cyber hygiene

Keywords: *Cyber Security, Cyber Hygiene, Internal Auditing, Cyber Security Governance, Cyber Security Maturity Model*

JEL Classification: *G32, M42*

---

*) İç Denetçi (CGAP), Düzce Üniversitesi, Orcid: 0000-0001-8439-9511, alptugguler@duzce.edu.tr

**) İç Denetçi (CGAP,CCSA), Düzce Üniversitesi, Orcid: 0000-0002-6826-0998, aliarkin@duzce.edu.tr

Yazı Gönderim Tarihi: 21.03.2019, Yazı Kabul Tarihi: 11.04.2019

1) Bu çalışmaya görüş ve önerileriyle katkıda bulunan Gençlik ve Spor Bakanlığı İç Denetçisi Sayın Ahmet Kebeli'ye teşekkür ederiz.

1. GİRİŞ

Günümüzde dijital teknolojilere bağımlılığın artması ve dijital araçların hayatımızın her anını kapsaması, ülkeleri, kurumları, sıradan insanları siber dünyaya ve buna bağlı olarak siber güvenlik risklerine karşı daha duyarlı hale getirmiş durumdadır. Siber kavramı, toplumun tamamında üretkenlik gelişimini ve bilgileri tam zamanında dağıtımını sağlaması yönüyle vazgeçil(e)mez bir olgu haline gelmiştir. Siber kavramı ile hangi endüstrinin veya uygulamanın tanıtıldığı önemli değildir, odak noktasında verimlilik artışı yer almaktadır. Bununla birlikte, bilginin siber alana hızlı bir şekilde iletilmesi genellikle genel sistem güvenliğini azaltmaktadır. Siber dünya hayatımıza birçok kolaylıklar getirirken, yanında belirsizlikleri ve kırılganlıkları da getirmektedir. Bu belirsizlikler ve kırılganlıkların önemli kısmı, bilgisayar korsanları ve siber saldırganların yaşam alanı buldukları ülkeleri, kurumları, kurum çalışanlarını, sıradan insanları tehdit ederek adeta siber terör estirmelerinden kaynaklanmaktadır.

Teknolojik gelişmeler, son on yılda altyapı gelişimi ile ilgili riskleri kökten değiştirmiştir. Bir ülkenin elektrik sistemine yapılacak başarılı bir siber saldırı yıkıcı etkileri tetikleyebilir (WEF, 2019: 83). Hizmet sektörünün enerji sistemlerini siber saldırılara karşı korumak için 2017 yılında 1,7 milyar ABD doları harcadığı tahmin edilmektedir (Nhede, 2017). Modern, birbirine bağlı olan küresel ekonomide, siber sistemler sürekli saldırı altındadır. Bugün milyarlarca kullanıcı ve internet cihazının (nesnelerin interneti) beslediği çok boyutlu bir bağlanabilirlik ortamı, saldırganların artık daha fazla kişiyi daha fazla cihaz üzerinden rahatsız edebilecekleri ve her yıl daha fazla ihlal, daha fazla etkilenen kurum ve kullanıcı ve daha fazla hasar olduğu anlamına gelmektedir[2] (GAC 16, 2016: 4).

Siber saldırganlar her gün daha sofistike ve daha yıkıcı olmaktadırlar. Bu durum karşısında kurumlar kendilerine "asla başımıza gelmez" demeye devam edemezler. Artık tüm kurumların bilgi güvenliği operasyonlarını modernize etmeleri ve daha da gelişmiş tehditlerle dolu bir geleceğe hazırlanma zamanı gelmiştir (Ling, 2017: 286). Hiç kimsenin siber saldırılara karşı kesin bir bağışıklık kazanmadığı açıkça anlaşılmaktadır. Artan sayıda bilgisayar ve ağ güvenliği ihlali rapor edildiğinden, genellikle binlerce hatta milyonlarca vatandaşı etkileyen, siber güvenliğe olan ilgi artmıştır. Aynı zamanda, tüm sektörler, güvendikleri kritik siber altyapılara bağımlılıklarını anlamaya çalışmaktadırlar. Dolayısıyla, her geçen gün daha fazla kurum, artan tehdidi ele almak için siber güvenlik programları geliştirmeye çalışmaktadır. Devletler ve topluluklar, uygulanabilir ve sürdürülebilir siber güvenlik programları oluşturmaya çalışan kurumlar arasındadır. Ancak devletler ve topluluklar, hem kamu hem de özel kurumlara dayanan ve hizmet veren karmaşık organizasyonlar olarak, siber riskleri güvence altına alma yönünde nasıl ve nereden başlayacakları konusunda kafa karışıklığı içerisindedirler. Kurumlardaki kafa karışıklığının giderilmesi için ele almaları gereken öncelikli soru(n)lardan biri, tam olarak ne tür bir siber olaya hazırlıklı olmaları gerektiğidir (Whit, 2011: 173).

İşlerinin kesintiye uğramasını istemeyen hemen hemen her ölçekteki kurum için bütünsel bir siber güvenlik sistemi kaçınılmaz bir gerçeklik haline gelmiş durumdadır. Kurumların kuracağı herhangi bir siber güvenlik programının temel hedeflerinden biri, olası saldırıların çekiciliğini sınırlandırmak olmalıdır. Zira bir saldırganın bir sisteme girmesi ne kadar uzun sürerse hedef o kadar az arzu edilir hale gelir. Bahsedilen siber tehditlere dur demek için; ister ülke çapında olsun, ister bir kurum çapında olsun, isterse de sıradan bir bilgi teknolojisi kullanıcı olsun bir siber güvenlik kalkanına ihtiyaç vardır. Bu kalkanı bir siber mücadele aracı yapacak olan kavram ise etkin bir siber hijyen anlayışıdır.

Çalışmanın konusunu siber güvenlik çalışmalarında kurum bazında önem kazanması beklenen siber hijyen kavramı ve iç denetim faaliyetinin siber rolü oluşturmaktadır. Çalışmanın ana amacı; odağına siber güvenliği alarak iç denetimim siber dünyada üstlenmesi gereken rolü ile siber hijyenin kurumlara sağlayacağı katkının çerçevesini çizmek ve bunun temelini oluşturmaktır. Çalışmada yöntem olarak,

2) 2016 itibariyle, 1.789.393 maruz kalma kaydında 1.093 veri ihlali açığa çıkarılmıştır (ITRC, 2017: 4). 2017 yılında 197.612.748 maruz kalma kaydında 1.632 veri ihlali açığa çıkarılmış ve buna karşılık 2018 yılında 446.515.334 maruz kalma kaydında 1.244 veri ihlali açığa çıkarılmıştır (ITRC, 2019: 2).

siber uzayın artık yadsınamaz bir gerçekliği olan siber güvenlik temelinde siber hijyen olgusu literatür üzerinden irdelenmekte, iç denetçilerin ve iç denetimin siber rolüne ilişkin çıkarımlar yapılmaktadır. Çalışma üç bölümden oluşmaktadır. İlk bölümde siber güvenliğin tanımı ve içeriği açıklanmıştır. İkinci bölümde, kurumların sürdürülebilir bir siber hijyen için siber olgunluk modelleri işlenmiş ve atılması gereken adımlar açıklanmıştır. Son olarak üçüncü bölümde iç denetim faaliyetinin siber güvenlik ve siber hijyende rolü ile siber güvenlik denetiminin kavramsal içeriği paylaşılmıştır.

2. SİBER GÜVENLİK

Siber güvenlik son birkaç yıldır ön plana çıkmıştır. Siber olayların artan sayısı ve ciddiyeti ile medyanın bu tür olaylara odaklanması her yerde kurum yöneticilerinin dikkatini çekmektedir (Hermans ve Diemont, 2017: 109). Son yıllarda siber teknolojinin hızla gelişmesi nedeniyle; kurumlarda, kuruluşlarda ve cihazlarda bilgisayar sistemlerinin korunması sağlanmış, tehditlere ve saldırılara güçlendirme sağlanmıştır. Veri sızmasından ağ çöküşüne kadar değişen siber güvenlik ve gizlilik olayları geçmiş yıllara göre daha sık yaşanmakta ve bunlar günümüz toplumunda en büyük tehditler haline gelmektedir (Li, Chen ve Susilo, 2019a: ix). Günümüzün bilgi teknolojisi, hızlı değişen, artan bağlantı (örneğin, nesnelerin interneti, bulut bilişim, mobil ağ) ve sürekli artan veri hacmi ile karakterize edilmektedir. Birbirine daha bağlı ve birbirine bağımlı bir bilgi teknolojisi ortamı, siber güvenlik olaylarından kaynaklanan ticari etkilerin artmasına neden olmaktadır. Böyle dinamik bir ortamda riski azaltmak için, güçlü bir yapılanma yoluyla siber güvenlik, bilgi sistemleri geliştirme yaşam döngüsünde olmazsa olmaz bir unsur haline gelmiştir (Wyatt, 2017: 336).

Siber güvenlik, Information Systems Audit and Control Association (ISACA) tarafından; bilgi işlemlerinin işlenen, depolanan ve internet üzerinden çalışan bilgi sistemleri tarafından taşınan bilgilere yönelik tehditleri (ve riskleri) ele alarak koruma olarak tanımlanmaktadır. Siber riskler, bilgi ve iletişim teknolojisi (BİT) sistemlerinin birbirine bağlanmasından kaynaklanan risklerdir. Modern kurumlar için bu bağlantılar kurum içinde, tedarikçileri ve müşterileri arasında ve çalışanlarıyla veya çalışanın kendi cihazlarında mevcuttur (Sunde, 2017: 271). Siber güvenlik, bir kurumun operasyonlarının etkinliği ve etkililiği, iç ve dış raporlamanın güvenilirliği ve geçerli yasal ve düzenlemelere uygunluğu ile ilgili hedeflerini destekleyen sistemlerle ilgilidir (GTAG, 2016: 5). Diğer bir tanım olarak siber güvenlik, kurumların bilgi varlıklarını iç ve dış tehditlere karşı korumak için kullanılabilecekleri araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, kurallar, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojilerin toplanması olarak tanımlanmaktadır (SAMA, 2017: 5). Siber güvenlik, kurumun ve kullanıcı varlıklarının siber ortamdaki ilgili güvenlik risklerine karşı güvenlik özelliklerinin elde edilmesini ve bakımını sağlamayı amaçlar. Genel güvenlik hedefleri aşağıdakileri içerir (ITU-T X.1208, 2014: 2):

1- Erişilebilirlik (Kullanılabilirlik)
2- Bütünlük (doğruluğu ve reddedilmemeyi içerebilecek)
3- Gizlilik

Siber güvenlik, büyüklüklerinden veya faaliyet gösterdikleri sektörden bağımsız olarak, birçok kurumun yönetimi ve üst düzey yöneticileri için büyük bir endişe haline gelmiştir. Çoğu kurum için, siber güvenlik, kurumun karşı karşıya olduğu diğer ticari risklerle birlikte tanımlanması, değerlendirilmesi ve yönetilmesi gereken önemli bir iş riskidir ve kurum içindeki yalnızca bilgi teknolojisinde olanların değil tüm çalışanların ve yönetimin sorumluluğundadır. Bu iş sorununu yönetmek özellikle zordur, çünkü oldukça karmaşık bir siber güvenlik risk yönetimi programına sahip bir kurum bile maddi bir siber güvenlik ihlalinin ortaya çıkması ve zamanında tespit edilememesi riskini taşımaktadır (AICPA, 2017: 1). Siber suçun görülme sıklığı, kapsamı ve etkisi, bu konuyu Bilgi Teknolojisi (BT) departmanının sınırlarından üst düzey yöneticilerin ve kurumların, hükümetlerin ve diğer işletmelerin ofislerine kadar yükseltmiş durumdadır. Bir siber saldırının ciddi finansal, operasyonel ve kurumsal itibara zarar verme potansiyeli ortaya çıktıkça, siber güvenlik bir kurumun en üst düzeyde yönetilmesi gereken kritik bir risk olarak kabul edilmektedir (IIAC, 2015: 4).

Veri olaylarının büyüklüğü artmaya devam ederken, en dikkat çekici gelişme bu olayların arkasındakilerin

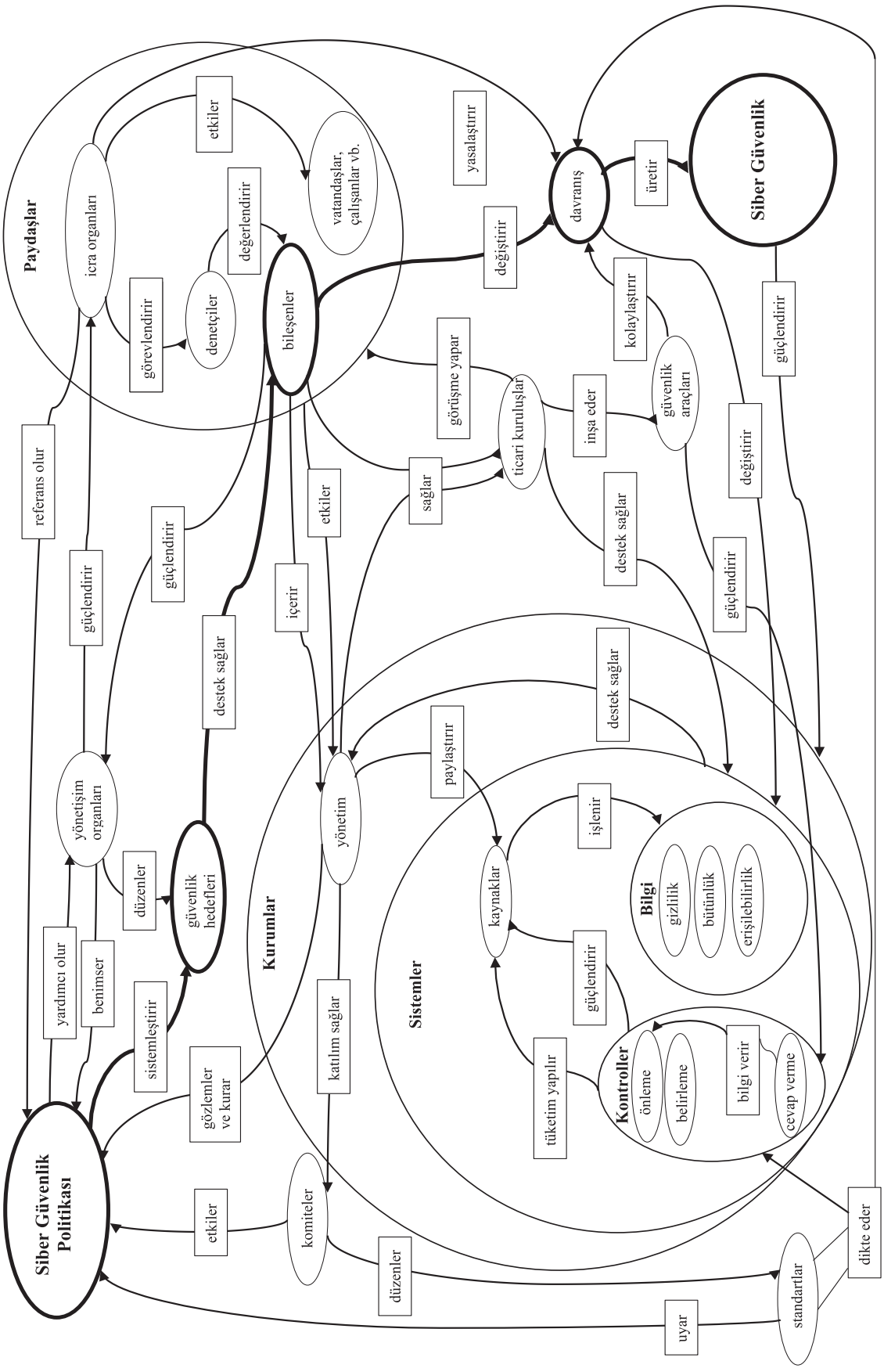
artan karmaşıklığıdır. Siber saldırganların iş modelleri gelişmiş ve daha karmaşık yöntemler kullanmanın yanı sıra, hedefleri de değişmiştir (McCarthy Tétrault, 2017: 4). Kurumlara yönelik saldırıları planlarken ve uygularken bilgisayar korsanları ve siber saldırganlar genellikle bütünsel bir yaklaşım sergilemektedirler. Bilgisayar korsanları ve siber saldırganlar, kurumların hassas işlerini, kurumsal bilgilerini ve kritik kaynaklarını korumak için inşa ettikleri önemli savunmaların üstesinden nasıl gelinebileceğini en iyi şekilde düşünmektedirler. (Hale, 2017: xxviii). Saldırganlar yaklaşımlarında yenilikçidir ve hedefleri genellikle savunma duruşunu bozmaya yöneliktir. Bu sebeple kurumlar için belki de siber güvenlikten daha önemli olan siber esnekliktir. Esneklik, "bilinmeyen ve bilinen tehditlere karşı hızlı bir şekilde dayanma ve kurtarma yeteneği" ile ilgilidir (Linkov vd., 2013: 471). Siber esnekliğe sahip olmak, saldırıları önlemek ve gerekli kurumsal işlevleri sürdürmek veya hızla eski duruma gelmek anlamına gelmektedir. Siber tehditler giderek daha karmaşık hale geldikçe, kurumlar sadece siber güvenliği ele almaya değil, aynı zamanda aşırı bağlantılı dünyamızda başarılı olmak için siber esnekliğe odaklanmalıdır (Keys ve Shapiro, 2019: 69). Siber esnekliğin arttırılması, kamu ve özel sektörlerin yeni ve yenilikçi yollarla işbirliği yapmalarını gerektirmektedir (WEF, 2018: 5).

Siber güvenlikte temel zorluk, sistemlerinizin bütünlüğünü ve gizliliğini korurken dijital hizmet kullanılabilirliğini sağlamaktır. Siber risklerin temel özelliği, risk azaltıcı kontrollerin etkinliğinin devamlı ve sürekli izlenmesini gerektirmeleridir. Sistemler çevrimiçi ve birbirine bağlı olmak üzere 7 gün / 24 saat olarak çalışmaktadır. Bu durum daha organize ve yüksek vasıflı siber saldırganların artan tehditleriyle bir araya geldiğinde, sistemleri korumak için gereken çabayı çok zorlaştırmaktadır. Bu nedenle koruma, herhangi bir kurumun farklı tarafları veya farklı savunma hatları tarafından birleştirilmiş bir çaba olmalıdır (Sunde, 2017: 272).

Verimlilik geliştirmeleri yapan teknoloji uzmanları için, güvenlik önlemleri, kullanıcının erişimini azaltan, engelleyen veya geciktiren önleme önlemleri, hayati önem taşıyan sistem kaynaklarını tüketen tespit önlemleri ve yönetim dikkatini sağlayan sistem özelliklerinden yönlendiren yanıt gereksinimleri nedeniyle, ilerlemeye doğrudan karşı çıkıyor gibi görünmektedir. Siber işlevsellik talebi ile güvenlik gereksinimleri arasındaki mevcut bu gerilim, "siber güvenlik politikası" ile ele alınmaktadır (Bayuk vd., 2012: 3). Yöneticiler, yönetimin siber güvenliğe yönelik kurumsal çapında uygun bir yaklaşım benimsendiğine dair güvence sağlamalıdır (NACD, 2017: 16). Bu güvence bir siber güvenlik politika belgesine bağlanmalıdır. Siber güvenlik politikasının tek bir tanım yoktur, ancak siber güvenlik terimi bir politika açıklamasına sıfat olarak uygulandığında ortak bir tema vardır. Genel olarak, "siber güvenlik politikası" terimi, siber güvenliği korumak için tasarlanmış yönergeleri ifade etmektedir (Bayuk vd., 2012: 4).

Şekil 1'de gösterildiği gibi, politikanın rolünün, siber güvenliğe ulaşması beklenen davranış kuralları için kuralların belirleneceği bir temel sağlamak olduğu unutulmamalıdır. Çok farklı politika bildirimlerine ve ilgili kurallara sahip olan çok çeşitli siber alanlar vardır. Siber güvenlik hedefleri doğrudan davranışa dönüşmemektedir, ancak siber güvenlik hedeflerine dayanan bir siber güvenlik stratejisinin daha iyi bir siber güvenlik politikası ile sonuçlanması beklenmektedir. Kurumlar, teknoloji kontrolleri ve ilgili operasyonel süreçleri uygulamak için standartlar oluşturmakta ve kurucular bu standartları politikaya uymak için kullanmaktadırlar. Standartların kendileri politika değildir. Aksine, politika hedeflerinden bir dizi teknolojiye ve operasyonel sürece yapılan çevirilerdir (Bayuk vd., 2012: 6).

Herhangi bir siber güvenli politikasının başarısında özellikle yönetimin, genel kurumsal bilgi güvenliği stratejisini desteklemek için yeterli kaynakları tahsis etmesi önemlidir (ITGI, 2006: 17). Ancak toplam siber güvenlik gerçekçi olmayan bir amaçtır. Siber güvenlik (genel olarak güvenlikte olduğu gibi) bir son durum değil bir sürekliliktir ve güvenlik de uyumun bir eşdeğeri değildir (NACD, 2017: 18). Bu sürekliliği sağlayacak ana kavram ise siber hijyen olacaktır. Bir kurum için siber güvenlik politikasının siber hijyen odağıyla bağlantılı olarak donanım ve yazılımların düzenli olarak doğrulanması, güvenlik sisteminin yapılandırılması, kurum içerisindeki kullanıcı ayrıcalıklarının kontrol edilmesi, denetlenmesi, kullanıcıların eğitilmesi vb. unsurlar siber başarının temel adımları olmalıdır.



Şekil 1. Siber Güvenlik Politikasına Bakış

(Bayuk vd., 2012: 5)

3. SİBER HİJYEN

Siber saldırıların hem sıklığı ve hem de etkisi her geçen gün artmaktadır. En başarılı saldırılar bilinen güvenlik sorunlarından yararlanmaktadır. Siber saldırıların yaklaşık % 80'inin kurban kurumlarında zayıf siber alışkanlıkların olduğu görülmektedir. Bu durumu ele almak için, düzenli, etkili güvenlik önlemleri almanın önemini vurgulayan bir siber hijyen stratejisi uygulanmalıdır. Bu, bir siber saldırının kurbanı olma veya bir siber saldırının etkisini diğer kurumlara yayma risklerini en aza indirecektir. Bu bağlamda siber hijyen bir kuruma düzgün şekilde entegre edildiğinde, kurumların çevrimiçi sağlık durumunun en iyi durumda olduğundan emin olmak için günlük rutinler, iyi davranışlar ve düzenli yapılan kontrollerin uygulanması yeterli olacaktır (ENISA, 2016: 6). Siber hijyen, bilgi güvenliği ile ilgili temel bir ilkedir ve kişisel hijyenle benzerlik gösterdiği gibi, siber tehditlerden kaynaklanan riskleri en aza indirgemek için basit rutin önlemler almanın eşdeğeridir. Altta yatan varsayım iyi siber hijyen uygulamalarının, savunmasız bir kurumun saldırılara maruz kalma riskini azaltarak, kurumlar arasında artan bağışıklık kazanabileceği yönündedir (ENISA, 2016: 14).

Geleneksel bilgi güvenliği modelleri bugünün gerçeklerine hitap edememektedir. Bu modeller, ofisin arkasını emniyet altına almayı hedeflerken, hala büyük ölçüde teknoloji odaklı, uyum temelli ve çevre odaklı bir yaklaşıma ihtiyaç vardır. BT siber güvenlik hijyeni genellikle eksiktir ve etkin olmayan erişim kontrolleri, 2015 yılında kaybedilen veya çalınan yarım milyar kişisel kayıtlara doğrudan katkıda bulunmuştur (Villiers, 2017: 321). Siber hijyen, birçok siber güvenlik olayından sorumlu olan az sayıdaki kök nedeni için önerilen önlem alma uygulamalarını açıklamaktadır. Birkaç basit uygulama bu yaygın kök nedenleri ele alabilir. Örneğin bir yama, siber hijyenin özellikle önemli bir bileşenidir, ancak mevcut araçlar ve işlemler çoğu zaman bu ortamlarda ve durumlarda bu riski hızla azaltmak için yetersizdir (Souppaya vd., 2018: 2). Bu nedenle sağlam bir siber güvenlik "Çin Seddi" kurulmalıdır, ancak özellikle insan faktörlerinden kaynaklanan güvenlik açıkları nedeniyle güvenlik cihazlarının ve sistemlerinin en iyileri tehlikeye girebilir. Bilgi sistemleri kurumdaki herkes tarafından kullanıldığından, bilgi güvenliği hijyenine uyma sıkıntısı da beraberinde gelir. İyi tasarlanmış güvenlik sistemleri, uygun kurum kültürü, eğitim, farkındalık, uyum ve denetim, güvenli davranış sergileyen kullanıcılarda çok önemli bir rol oynamaktadır (Totade ve Godbole, 2017: 243). Siber hijyen uygulamaları saldırganların başarılı olmalarını zorlaştırmakta ve saldırıların sebep olabileceği hasarı azaltabilmektedir (Souppaya vd., 2018: 4).

Önümüzdeki yıllarda ulusal düzeydeki tüm savunma paydaşları arasında, en karmaşık ve en güçlü siber savunma sistemleri kadar temel siber hijyen becerilerini ve farkındalığını arttırmak öncelik olacaktır. Çeşitli ülkelerde siber temelli güvenlik programları; özellikle küçük kurumlara yönelik olarak en temel kontrol ve güvenlik uygulamalarını benimsemelerini teşvik etmek amacıyla oluşturulmuştur ve iyi siber hijyenin işletmelerin karşılaştığı tehditlerin yüzde 80›ini karşılayacağı prensibi üzerine çalışmaktadır (Caravelli ve Jones, 2019). Bununla beraber kurumsal risk yönetimi sistemi yetenekleri de yıllar geçtikçe olgunlaşmaktadır. Aynı durum siber risk yönetim sistemi için de geçerlidir (Antonucci ve Verstichel, 2017: 375-376). Etkin bir siber risk yönetimi kurum bünyesinde içselleştirilmiş bir modele dayanmalıdır. Bu model siber hijyeni kurum bünyesinde hem yatay ve hem de dikey olarak yayabilmeli ve çalıştırabilmelidir.

3.1. Siber Hijyen İçin Siber Güvenlik Olgunluk Modeli

Olgunluk modeli, belirli bir disiplinde yetenek ve ilerlemeyi temsil eden bir dizi özellik, gösterge veya yapıdır. Model içeriği tipik olarak en iyi uygulamaları örneklendirir ve standartları veya disiplinin diğer uygulama kurallarını içerebilir. Dolayısıyla bir olgunluk modeli, bir kurumun uygulamalarının, süreçlerinin ve yöntemlerinin mevcut yetenek seviyesini değerlendirebileceği ve iyileştirme için hedef ve öncelikleri belirleyebildiğine dair bir kıyaslama sağlamaktadır (ONG-C2M2, 2014: 5).

Mevcut durumu analiz etmek için, diğer siber güvenlik kontrolleri değerlendirilirken ve yeni teknoloji, insanlar veya süreç kontrolleri uygulanırken istenen duruma yönelik bir siber güvenlik programı olgunluk modeli de uygulanabilir. Farklı kurum ve çerçevelerin artan olgunluk seviyeleri için çeşitli isimleri var-

dır; bununla birlikte çoğu, olgunluğu göstermek için bir olgunluk modeline bağlı kalır (ISACA, 2017: 12). Siber (güvenlik) hijyen seviyesi, önceden tanımlanmış bir siber güvenlik olgunluk modeli ile ölçülebilir. Siber güvenlik olgunluk modeli aşağıdaki Tablo 1'de özetlenen 6 olgunluk seviyesi ile (0, 1, 2, 3, 4 ve 5) belirlenmektedir. Seviye 3, 4 ya da 5'e ulaşmak için, bir kurumun öncelikle önceki olgunluk seviyelerinin (ölçütlerinin) tüm kriterlerini karşılaması gerekmektedir (SAMA, 2017: 10).

Tablo 1. Siber Güvenlik Olgunluk Modeli-1

Olgunluk Seviyesi	Tanım ve Kriterler	Açıklama
0 (Mevcut Değil)	• Herhangi bir dokümantasyon yoktur. • Bazı siber güvenlik kontrolleri için farkındalık veya dikkat yoktur.	• Siber güvenlik kontrolleri yerinde değildir. Belirli bir risk alanı hakkında herhangi bir farkındalık olmayabilir veya bu siber güvenlik kontrollerini uygulamak için mevcut planlar olmayabilir.
1 (Geçici)	• Siber güvenlik kontrolleri tanımlanmamış veya kısmen tanımlanmıştır. • Siber güvenlik kontrolleri tutarsız bir şekilde gerçekleştirilmektedir. • Siber güvenlik kontrolleri tam olarak tanımlanmamıştır.	• Siber güvenlik kontrol tasarımı ve uygulaması ilgili bölüme veya kuruma göre değişir. • Siber güvenlik kontrol tasarımı, tespit edilen riski sadece kısmen azaltabilir ve uygulama tutarsız olabilir.
2 (Tekrarlanabilir ancak gayri resmi)	• Siber güvenlik kontrolünün yürütülmesi, standartlaştırılmış olsa da, gayri resmi ve yazılı olmayan bir uygulamaya dayanmaktadır.	• Tekrarlanabilir siber güvenlik kontrolleri yerindedir. Bununla birlikte, kontrol hedefleri ve tasarımı resmi olarak tanımlanmamış veya onaylanmamıştır. • Yapılandırılmış bir gözden geçirme veya kontrolün test edilmesi konusunda sınırlı bir değerlendirme vardır.
3 (Yapısal ve resmileştirilmiş)	• Siber güvenlik kontrolleri, yapılandırılmış ve resmileştirilmiş bir şekilde tanımlanır, onaylanır ve uygulanır. • Siber güvenlik kontrollerinin uygulanması gösterilebilir.	• Siber güvenlik politikaları, standartları ve prosedürleri oluşturulmuştur. • Siber güvenlik belgelerine uyum, yani politikalar, standartlar ve prosedürler, tercihen bir yönetişim, risk ve uyum (GRC)[3] aracı kullanılarak izlenir. • Uygulamanın değerlendirilmesi için kilit performans göstergeleri tanımlanır, izlenir ve raporlanır.
4 (Yönetilebilir ve ölçülebilir)	• Siber güvenlik kontrollerinin etkinliği periyodik olarak değerlendirilir ve gerektiğinde geliştirilir (iyileştirilir). • Bu periyodik ölçüm, değerlendirmeler ve iyileştirme fırsatları belgelenmiştir.	• Siber güvenlik kontrollerinin etkinliği ölçülmekte ve periyodik olarak değerlendirilmektedir. • Siber güvenlik kontrollerinin etkinliğini belirlemek için temel risk göstergeleri ve trend raporlaması kullanılmaktadır. • Ölçme ve değerlendirme sonuçları, siber güvenlik kontrollerinin iyileştirilmesine yönelik fırsatları belirlemek için kullanılır.
5 (Uyarlanabilir)	• Siber güvenlik kontrolleri sürekli bir iyileştirme planına tabidir.	• Kurumsal çapta siber güvenlik programı, siber güvenlik kontrollerinin sürekli uyumu, etkinliği ve iyileştirilmesine odaklanmaktadır. • Siber güvenlik kontrolleri, kurumsal risk yönetimi çerçevesi ve uygulamaları ile entegredir. • Siber güvenlik kontrollerinin performansı, emsal ve sektör verileri kullanılarak değerlendirilir.

(SAMA, 2017: 10)

3) GRC- Governance, Risk and Compliance

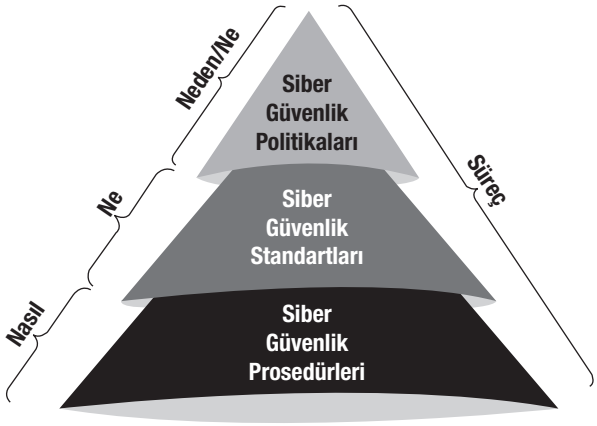
Modelin amacı, siber güvenliği ele almak ve siber güvenlik risklerini yönetmek için etkili bir yaklaşım oluşturmaktır. Uygun bir siber güvenlik olgunluk seviyesine ulaşmak için, kurumlar en azından aşağıda açıklanan 3 veya daha yüksek olgunluk seviyelerinde çalışmalıdır (SAMA, 2017: 10). Bu seviyeler aşağıda kısaca açıklanmıştır.

3.1.1. Olgunluk Seviyesi-3 (Yapısal ve Resmileştirilmiş)

BT faaliyetlerinin gözetimi ve yönetimi için bir kurum / süreç çerçevesi tanımlanmış ve kuruma BT yönetişiminin temeli olarak tanıtılmıştır. Yönetim birimleri, temel yönetişim faaliyetlerini kapsayan özel prosedürler geliştirerek rehberlik yapmıştır. Bunlar arasında düzenli hedef belirleme, performansın gözden geçirilmesi, planlanan ihtiyaçlara karşı yetenek değerlendirmesi, gerekli BT iyileştirmeleri için proje planlama ve fonlama yer almaktadır (ITGI, 2003: 48-49). Orta vadede detaylı, resmi işlemler tanımlanır. Kontroller onaylanmış ve tutarlıdır. Risk yönetimi uygulamaları ve analizleri işletme stratejilerine entegre edilmiştir (FFIEC, 2015: 7).

Seviye 3 olgunluğa ulaşmak için bir kurum, siber güvenlik kontrollerini tanımlamalı, onaylamalı ve uygulamalıdır. Ek olarak, siber güvenlik dokümantasyonuna uyumu da izlemelidir. Siber güvenlik dokümantasyonu "neden", "ne" ve "nasıl" siber güvenlik kontrollerinin uygulanması gerektiğini açıkça göstermelidir. Siber güvenlik dokümantasyonu Şekil 2'de gösterildiği gibi siber güvenlik politikaları, siber güvenlik standartları ve siber güvenlik prosedürlerinden oluşmaktadır (SAMA, 2017: 10).

Şekil 2. Siber Güvenlik Dokümantasyon Piramidi



(SAMA, 2017: 11)

Siber güvenlik politikası, kurumun yönetimi tarafından onaylanmalı ve siber güvenliğin kurum için neden önemli olduğunu belirtmelidir. Politika hangi bilgi varlıklarının korunması gerektiğini ve siber güvenlik ilke ve hedeflerinin belirlenmesi gerektiğini vurgulamalıdır. Siber güvenlik politikasına dayanarak, siber güvenlik standartları geliştirilmelidir. Bu standartlar, güvenlik ve sistem parametreleri, görevlerin ayrılması, şifre kuralları, olayların izlenmesi ve yedekleme kuralları gibi uygulanması gereken siber güvenlik kontrollerini tanımlamalıdır. Standartlar; siber güvenlik politikasını destekler ve güçlendirir. Siber güvenlik prosedürlerinde personel veya kurumun paydaşları tarafından yapılması gereken görevler detaylandırılmıştır. Bu prosedürler siber güvenlik kontrollerinin, görevlerinin ve faaliyetlerinin kurum ortamında nasıl yürütülmesi gerektiğini ve kurumun bilgi varlıklarının siber güvenlik politikası ve standartlarına göre korunmasını, desteklemesini öngörmektedir. Uygulamadaki gerçek ilerleme, siber güvenlik kontrollerinin performansı ve uyumu, anahtar performans göstergeleri (KPIs)[4] kullanılarak periyodik olarak izlenmeli ve değerlendirilmelidir (SAMA, 2017: 11). Anahtar performans göstergesi, bir kurumun hedeflere karşı nasıl performans gösterdiğini değerlendiren bir ölçümdür. Tanımlanmış bir hedef (tipik olarak) bir KPI metriğinin değerlendirilmesinde bir ölçüt sağlar (Rodriguez, 2017: 160).

3.1.2. Olgunluk Seviyesi-4 (Yönetilebilir ve Ölçülebilir)

Hedef belirlemede, iş açısından sonuçlar ile hedefler arasındaki ilişkilerde oldukça karmaşık bir aşamaya gelinmiş ve BT süreç iyileştirme önlemleri şimdi daha iyi anlaşılmaktadır. Gerçek sonuçlar, yönetime bir karne kartı şeklinde iletilmektedir. Kurumun yönetimi bu seviyede BT değer sunumunu en üst düzeye çıkarmak ve BT ile ilgili riskleri yönetmek için ortak bir amaç için birlikte çalışmaktadır. BT yeteneklerinin düzenli olarak değerlendirmeleri yapıl-

4) KPIs-Key Performance Indicators

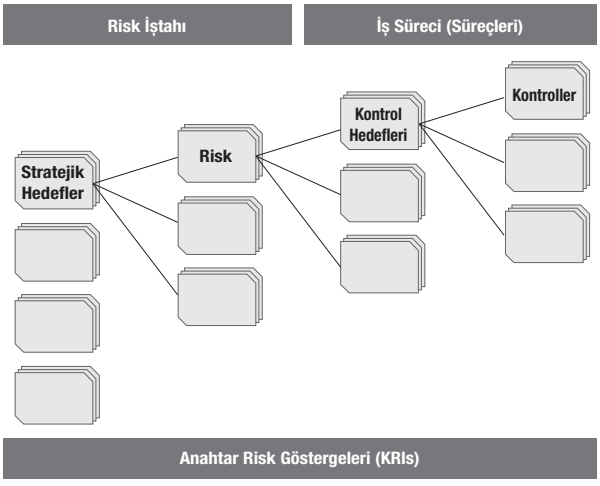
makta ve BT'nin performansında gerçek gelişmeler sağlayan projeler tamamlanmaktadır (ITGI, 2003: 49). Olgunluk, iş kolları arasında entegre olan siber güvenlik uygulamaları ve analitiklerle karakterize edilmektedir. Risk yönetimi süreçlerinin çoğunluğu otomatiktir ve sürekli süreç iyileştirmeyi içermektedir (FFIEC, 2015: 7).

Kurum, 4. olgunluk seviyesine ulaşmak için uygulanan siber güvenlik kontrollerinin etkinliğini periyodik olarak ölçmeli ve değerlendirmelidir. Siber güvenlik kontrollerinin etkili olup olmadığını ölçmek ve değerlendirmek için, anahtar risk göstergeleri (KRIs)[5] tanımlanmalıdır. Bir KRI, etkinlik ölçümü için normu gösterir ve gerçek ölçüm sonucunun hedeflenen normun altında mı yoksa üstünde mi olduğunu belirlemek için eşikleri tanımlamalıdır. KRI'ler eğilim raporlaması ve potansiyel iyileştirmelerin tanımlanması için kullanılır (SAMA, 2017: 11-12).

Her kurumun kendine özgü bir iş stratejisi, risk iştahı ve kurum kültürü vardır. Dijital çağda faaliyet gösteren bu faktörlerden bağımsız bir dizi siber risk de bulunmaktadır. Bunlar, web sitelerinin, e-postaların ve dijital cihazların neden olduğu ve bunlara zarar verebilecek riskleri içerir. Bu nedenle bir kurumun karşılaştığı belirli siber riskler, program ve ilgili KRI'ler gibi değişecektir. Tüm KRI'lerde olduğu gibi, daha geniş faaliyet risklerine bağlantı sağlayan KRI'lerin tasarlanması önemlidir (Rodriguez, 2017: 160-161).

Bir KRI programı oluştururken risk taksonomisine sahip olmak çok önemlidir. Kontrol düzeyindeki ölçüm ölçütler ile düşürülen riskler, sonuçta Şekil 3'de görüldüğü gibi stratejik hedeflerle olan ilişkisini destekler. Taksonomi aynı zamanda KRI'leri kullanan bir paydaş aralığında bir kuruluş içinde hesap verilebilirlik, cevap verme ve karar verme tutarlılığı konusunda netlik sağlar (Rodriguez, 2017: 161). KRI tasarımı kurumun karşılaştığı risklerin net bir görüntüsü ile başlar ve bu risklerin kontrol amaçlarına ve kilit kontrollere daha fazla sentezlenmesiyle devam eder (Şekil 3'deki gibi). Risk taksonomisinin bu unsurları, kurumun, endüstrinin en iyi uygulamalarının yanı sıra geçerli yasalar ve düzenlemeler tarafından yönlendirilen politika ve programlarla başlayan kapsamlı siber güvenlik programında daha belirgindir (Rodriguez, 2017: 162-163).

Şekil 3. Anahtar Risk Göstergeleri (KRIs) İçin Risk Taksonomisi



(Rodriguez, 2017: 162)

3.1.3. Olgunluk Seviyesi-5 (Uyarlanabilir)

BT yönetişim uygulamaları, etkili ve verimli teknikler kullanılarak karmaşık bir yaklaşım haline gelmiştir. Bu seviyede, BT faaliyetlerinde şeffaflık söz konusudur ve yönetim BT stratejisinin kontrolünü ele geçirmektedir. BT faaliyetleri en iyi şekilde gerçek iş öncelikleri için yönlendirilmekte ve önemli sapmaların veya problemlerin düzeltilmesi için zamanında önlem alınabilmektedir. Risk yönetimi (ve genel olarak BT yönetimi faaliyetleri) için harcanan çaba, standart ve mümkünse otomatikleştirilmiş süreçlerin benimsenmesi ile kolaylaştırılmıştır. BT yetkinliğinin sürekli iyileştirilmesi uygulaması kurum kültürüne dahil edilmiştir (ITGI, 2003: 49). Bu olgunluk seviyesindeki siber güvenlik kapasitesinin Şekil 4'te gösterildiği gibi beş boyuttan oluştuğu düşünülebilir (CMM, 2016: 5):

1- Siber güvenlik politikası ve stratejisinin geliştirilmesi,
2- Kurum içinde sorumlu siber güvenlik kültürünün teşvik edilmesi,
3- Siber güvenlik bilgisinin geliştirilmesi,
4- Etkili yasal ve düzenleyici çerçeveler oluşturulması ve
5- Standartlar, kurumlar ve teknolojiler aracılığıyla risklerin kontrol altına alınması.

5) KRIs-Key Risk Indicators

Şekil 4. Siber Güvenlik Kapasite Boyutları

(CMM, 2016: 5)

Bu beş boyutta, siber güvenlik kapasitesini arttırmaya çalışırken göz önünde bulundurulması gereken alanlar bir ülke kapsamında ele alınmıştır. Bu boyutların belirli konularda birbirleriyle örtüşebileceği kabul edilir ve aslında siber güvenlik kapasiteleri arasındaki karşılıklı bağımlılık mevcuttur. Her boyutta, her biri aşağıdaki gibi tanımlanmış çeşitli faktörler, yönler, olgunluk aşamaları ve siber güvenlik kapasitesi göstergeleri vardır (CMM, 2016: 5):

1. Boyut: Siber Güvenlik Politikası ve Stratejisi

Bu boyut ülkenin, siber güvenlik stratejisini geliştirme ve sağlama kapasitesini ve olay tepkisini, kriz yönetimini ve kritik altyapı koruma kapasitelerini geliştirerek siber güvenlik direncini arttırıyor. Siber güvenliğin sağlanması, erken uyarı, caydırıcılık, direnç ve toparlanma kabiliyetini içermektedir. Bu boyut, ulusal savunma ve esneklik kabiliyetini sağlamada etkili güvenlik politikasını göz önünde bulundurarken, genel olarak devlet, uluslararası ticaret ve toplum için hayati bir siber ortamın faydalarını korur (CMM, 2016: 14).

2. Boyut: Siber Kültür ve Toplum

Bu boyut, toplumdaki siber risklerin anlaşılması, internet servislerine güven düzeyi, e-devlet ve e-ticaret hizmetleri ve kullanıcıların kişisel bilgilerin korunmasını çevrimiçi olarak anlama gibi sorumlu bir siber güvenlik kültürünün önemli öğelerini incelemektedir. Ayrıca, bu faktör, kullanıcıların siber suçları rapor etmeleri için kanal olarak işlev gören raporlama mekanizmalarının varlığını araştırmaktadır. Ayrıca, bu faktör medya ve sosyal medyanın siber güvenlik değerlerini, tutumlarını ve davranışlarını şekillendirmedeki rolünü gözden geçirir (CMM, 2016: 25).

3. Boyut: Siber Güvenlik Eğitimi, Eğitimi ve Becerileri

Bu boyut, hem kamuoyu hem de yöneticiler için siber güvenlik bilinci artırma programlarının mevcudiyetini gözden geçirmektedir. Ayrıca, çeşitli hükümet paydaş grupları, özel sektör ve bir bütün olarak nüfus için eğitim ve öğretim tekliflerinin mevcudiyetini, kalitesini ve alımını değerlendirir (CMM, 2016: 32).

4. Boyut: Yasal ve Düzenleyici Çerçeveler

Bu boyut, hükümetin, BİT güvenliği, gizlilik ve veri koruma konularında ve diğer siber suçlarla ilgili konular üzerinde özellikle durularak doğrudan ve dolaylı olarak siber güvenlikle ilgili ulusal mevzuatı tasarlama ve çıkarma kapasitesini incelemektedir. Bu tür yasaları uygulama kapasitesi kanun uygulama, kovuşturma ve mahkeme kapasiteleriyle incelenir. Ayrıca, bu boyut, siber suçla mücadeleye yönelik resmi ve gayri resmi işbirliği çerçeveleri gibi konuları da gözlemlemektedir (CMM, 2016: 39).

5. Boyut: Standartlar, Kuruluşlar ve Teknolojiler

Bu boyut, bireyleri, kuruluşları ve ulusal altyapıyı korumak için siber güvenlik teknolojisinin etkin ve yaygın bir şekilde kullanılmasına yöneliktir. Boyut, siber güvenlik standartlarının ve iyi uygulamaların uygulanmasını, süreçlerin ve kontrollerin yayılmasını ve siber güvenlik risklerini azaltmak için teknolojilerin ve ürünlerin geliştirilmesini özel olarak incelemektedir (CMM, 2016: 49).

Olgunluk seviyesi 5, siber güvenlik kontrollerinin sürekli iyileştirilmesine odaklanmaktadır. Şekil 5'teki modelde gibi sürekli iyileştirme, siber güvenliğin amaç ve kazanımlarının sürekli analiz edilmesi ve yapısal iyileştirmelerin belirlenmesi ile sağlanır. Siber güvenlik kontrolleri, kurumsal risk yönetimi uygula-

Şekil 5. Siber Güvenlik Olgunluk Modeli-2

(KPMG, 2018: 2)

malarına entegre edilmeli ve otomatik gerçek zamanlı izleme ile desteklenmelidir. İş süreci sahipleri, siber güvenlik kontrollerinin uygunluğunu izlemek, siber güvenlik kontrollerinin etkinliğini ölçmek ve siber güvenlik kontrollerini kurumsal risk yönetimi çerçevesine dahil etmekten sorumlu olmalıdır. Ek olarak, siber güvenlik kontrollerinin performansı, emsal ve sektör verileri kullanılarak değerlendirilmelidir (SAMA, 2017: 12).

5. olgunluk seviyesi, kurumun ve endüstrinin siber riskleri yönetmesi için insanlarda, süreçlerde ve teknolojide yeniliğe yol açmasıyla karakterize edilmektedir. Bu durum yeni kontroller, yeni araçlar geliştirmek veya yeni bilgi paylaşım grupları oluşturmak anlamına gelebilir (FFIEC, 2015: 7). Siber hijyen için ulaşılması hedeflenen bu son seviye siber güvenlik anlayışın kurum kültürüne eklenmekten ziyade içselleştirme anlamına gelmektedir. Bu seviyede artık kurum her türlü siber saldırıya karşı hazırdır ve siber bağışıklık kazanılmıştır. Kurumun bu bağışıklığı kazanmasında kullanabileceği kurumsal araçlar çok çeşitlidir. Bu çeşitlilik içerisinde kurumun siber güvenlik politikalarına net bir bakış açısı sunabilecek en etkin araçlardan biri olarak iç denetim faaliyeti görünmektedir.

4. İÇ DENETÇİNİN VE İÇ DENETİMİN SİBER ROLÜ

Büyük veri, akıllı cihazlar, nesnelerin interneti, robotik proses otomasyonu, davranışsal analitik, üç boyutlu baskı gibi kavramlar kurumların artan dijitalleşmesine paralel olarak verimlilik ve maliyet etkinliği açısından önem kazanmaktadır. Ancak bu gelişmelerin kurumların operasyonlarına getirdiği artan riskler ve bunların kurumlara zarar vermesinin nasıl önleneceği iyice anlaşılmadır. Yalnızca BT sistemlerinin güvenlik açıklarına değil, kurum ortamına derinlemesine bakarak bu sistemlerin ürettiği verilere de ilişkin fikir edinilmesi gerekir. Mevcut portföydeki risklerin nasıl tespit edildikleri ve onları iyileştirmek için kurumun hangi stratejileri izlemesi gerektiği anlaşılır ve akıcı hale getirilmedir. Kurumlar bu konuda bilgi güvenliği uzmanlarına ve ekiplerine bu çabanın sorumluluğunu üstlenmesini isteyebilir. Siber risklere karşı güvenlik duvarları ve virüs koruma yazılımları yeterli çözüm değil midir? Keşke bu kadar basit olsaydı. Siber güvenlik, görünürlükle başlayan ve iç görü sağlayan, kapsamlı bir kurumsal çapta organizasyon çözümü gerektiren bir kurum sorunudur. Tehditleri ortaya çıkarmak, çözümün sadece bir parçasıdır. Kurumların BT uzmanları, tehditlerin nasıl ortaya çıka-

cağını tahmin etmesi ve bunlara yönelik stratejileri bildirmesi gerekir (Holmes ve Phillippe, 2017: 309-310). Teknolojinin hızla ilerlediği zamanımızda, BT uzmanları bile teknolojik değişimin nabzını tutmakta zorlanmaktadır. Öyleyse, iç denetçilerin bu siber çağda ortaya çıkan çeşitli riskleri yeterince değerlendirmeleri ve incelemeleri ve etkileriniz azaltmaları nasıl mümkün olabilir? Bu sorunun cevabı kısaca "bütüncül bir bakış açısıyla siber güvenlik sisteminin güçlendirilmesine yardımcı olmak" şeklinde verilebilir.

Bir kurumun iç denetim birimi, kurumun yönetişiminin, risk yönetiminin ve iç kontrol süreçlerinin etkinliğini değerlendirmek ve iyileştirmek için tasarlanan güvence ve danışmanlık faaliyetlerini yerine getirir. Bir iç denetim işlevi tarafından gerçekleştirilenlere benzer faaliyetler, bir kurum içindeki diğer unvanlar ile gerçekleştirilebilir. Bir iç denetim biriminin faaliyetlerinin bir kısmı veya tamamı bir üçüncü taraf servis sağlayıcıya dış kaynaklı olabilir. Örneğin, bir işletme (a) penetrasyon testini gerçekleştirmek için bir servis sağlayıcıyı çalıştırabilir; (b) İç denetim biriminin, işlevin yerine getirebilecek yetkinlik veya niteliklere sahip olmadığına dair sorumlulukları (örneğin, BT iç denetim işlevini yerine getirme) veya (c) yönetimin talebi üzerine tek seferlik özel bir değerlendirme yapabilir (AICPA, 2017: 46).

Kurumların bilgi sistemlerine ve yeni teknolojilerin geliştirilmesine dayanması, BT genelinin ve uygulama kontrollerinin geleneksel değerlendirmelerini siber güvenlik konusunda güvence sağlamak için yetersiz kılmaktadır. Siber güvenlik, bir kuruluşun bilgi varlıklarını (bilgisayarları, ağları, programları ve verileri) yetkisiz erişime karşı korumak için tasarlanmış teknolojiler, işlemler ve uygulamalar anlamına gelir. İç denetim faaliyeti, aşağıdakileri dikkate alarak bir kuruluşun siber güvenlik risklerini değerlendirmede çok önemli bir rol oynar (GTAG, 2016: 3):

1- Kuruluşun en değerli bilgilerine kim erişebilir?
2- Hangi varlıklar siber saldırılar için en olası hedefler?
3- Hangi sistemler tehlikeye girerse en önemli bozulmaya neden olur?
4- Yetkisiz kişilerce elde edilmesi durumunda hangi veriler finansal veya rekabetçi zararlara, yasal sonuçlara veya kurumun itibarına zarar verir?
5- Bir siber güvenlik olayı meydana gelirse, yönetim zamanında tepki vermeye hazır mıdır?

Kurumlar ve devlet kurumları için bilgilerin, iş süreçlerinin, uygulamaların ve sistemlerin mevcudiyeti, gizliliği ve bütünlüğüne yönelik artan tehditleri önlemek için uygulamaya konulan bilgi güvenliği yönetiminin önemli bir parçası iç denetim tarafından yerine getirilen **Siber Güvenlik Denetimi**dir. Uygulanan güvencelerin ve bilgi güvenliği sürecinin düzenli aralıklarla gözden geçirilmesiyle, bunların etkinliği, güncelliği, eksiksizliği ve uygunluğu ve dolayısıyla bilgi güvenliğinin mevcut durumu hakkında fikir vermek mümkündür. Bu nedenle, iç denetim, bir kurumda uygun bir güvenlik düzeyi belirlemek, elde etmek ve sürdürmek için bir araçtır. İç denetiminin temel görevi, bilgi güvenliğini uygularken ve optimize ederken yönetime, kurum yöneticilerine ve özellikle de BT'den sorumlu üst yöneticiye destek sağlamaktır. Denetimler bilgi güvenliği seviyesini iyileştirmek, yanlış bilgi güvenliği tasarımlarından kaçınmak ve güvenlik önlemlerinin ve güvenlik işlemlerinin verimliliğini optimize etmek için tasarlanmıştır. Bilgi güvenliği denetiminin bir sonucu olan denetim raporu, kurumun güvenlik durumunu, mevcut güvenlik eksikliklerine dayanarak yapılması gerekenler ile birlikte gösterir ve sonraki siber güvenlik optimizasyon sürecinde yardımcı olarak kullanılır. Denetim raporu, yönetim için bir bilgi kaynağı ve güvenlikten sorumlu herhangi biri tarafından kullanılabilecek bir araçtır (BSI, 2008: 5).

Teknoloji gelişmeye devam ettikçe, iç denetim de gelişmek zorundadır. Uzun yıllar boyunca, iç denetim birimleri, entegre denetimlerde ortak olarak BT denetim uzmanlarına güvenmiştir (Fountain, 2019: 19). Siber güvenlik için bağımsız güvence rolü, iç denetim tarafından benzersiz bir şekilde oynanabilir (Antonucci, 2017: 215). Dolasıyla günümüzde iç denetimin güncel çalışma portföyüne bir de siber rol eklenmektedir. İç denetçilerin siber güvenlik riskleri konusunda güvence sağlamak için güncellenmiş bir yaklaşıma ihtiyaçları vardır. BT genel kontrol değerlendirmeleri yararlı olsa da, siber güvenlik güvencesini sağlamada yetersizdirler, çünkü bunlar ne zamanında gerçekleştirilebilmektedir ne de tam değildirler. Bütünlük, doğruluk ve yetkilendirme gibi temel denetim hedefleri hala geçerlidir. Bununla birlikte, ortaya çıkan birçok faktör, siber güvenlik iddiaları hakkında değerli

sonuçlar sağlayan güncellenmiş bir iç denetim yaklaşımına ihtiyaç duymaktadır (GTAG, 2016: 4).

4.1. İç Denetim İçin Siber Güvenlik Risklerini ve Kontrollerini Değerlendirmeye Yönelik Bir Yaklaşım

Siber güvenlik yönetişimi, stratejik yönlendirme sağlayan, hedeflere ulaşılmasını sağlayan, riskleri uygun şekilde yöneten, kurumsal kaynakları sorumlu bir şekilde kullanan ve kurumsal güvenlik programının başarısını veya başarısızlığını izleyen bir kurumsal yönetim alt kümesidir (ITGI, 2006: 17). Şekil 6'da gösterilen çerçevenin birbirine bağlı altı bileşeni, yönetim siber güvenlik kontrollerinin ve yönetişiminin tasarım ve işletme etkinliğini değerlendirmek için kullanılabilir. Herhangi bir bileşendeki eksiklikler, siber güvenliğin genel etkinliğini etkileyeceğinden, her birinin diğerleriyle nasıl tasarlanıp işletildiğini değerlendirmek, iç denetime (iç denetim yöneticisine) kurumun siber güvenlik risklerini ele almak için ne kadar iyi hazırlandığını belirlemek için bir temel oluşturur. Bileşenler birlikte tasarlanmadığında veya iyi çalışmadığında, kurum siber tehditleri ve ortaya çıkan riskleri ele almak için hazır değildir demektir (GTAG, 2016: 17). Bu çerçevede, iç denetimin değerlendirmek durumunda olduğu bileşenler aşağıda açıklanmaktadır.

4.1.1. Siber Güvenlik Yönetişimi Bileşeni

Siber güvenlik yalnızca bir bilgi teknolojisi riski değildir. Kurum genelinde bir risktir ve bir yönetimin kurumsal risk yönetimi yetkisinin parçası olmalıdır (McCarthy Tétrault, 2017: 8). Siber güvenlik yönetişimi, güvenlik çabalarını tanımlayarak, yöneterek ve destekleyerek siber güvenlik yönetimi ve kontrolleri için gündem ve sınırları belirler (CBN, 2018: 3). İç denetim faaliyeti kurumun siber güvenlik yönetişimini anlamalıdır. 2100 numaralı IIA Standardı: yönetişim, risk yönetimi ve kontrol süreçlerinin iyileştirilmesine yönelik değerlendirme ve katkı sağlayan bir iç denetim faaliyetini gerektirmektedir.

Güçlü bir siber güvenlik yönetişimi şunlara bağlıdır (ITGI, 2006: 18; GTAG, 2016: 18):

Şekil 6. Siber Güvenlik Risk Değerlendirme Çerçevesi

(GTAG, 2016: 17)

1- Risk iştahı ve toleransı belirleme

2- Bir kesinti durumunda iş sürekliliği ve afet kurtarma için planlama

3- Güvenlik ihlallerine derhal yanıt verme

4- Bilgi güvenliği risk yönetimi metodolojisi

5- İş ve BT hedefleriyle açıkça bağlantılı kapsamlı bir güvenlik stratejisi

6- Etkili bir güvenlik organizasyon yapısı

7- Korunan ve sunulan bilgilerin değeri hakkında konuşan bir güvenlik stratejisi

8- Strateji, kontrol ve düzenlemenin her yönünü ele alan güvenlik politikaları

9- Her politika için eksiksiz bir güvenlik standardı seti

10- Siber güvenlik politikası ve politikalara uygun prosedürler

11- Uyumluluk sağlamak ve riskin etkililiği ve azaltılması konusunda geri bildirim sağlamak için kurumsallaşmış izleme süreçleri

12- Güvenlik politikalarının, standartlarının, prosedürlerinin ve risklerinin sürekli değerlendirilmesini ve güncellenmesini sağlayan bir süreç

13- Siber güvenlik riskleri ve tehditleri konusunda farkındalık kültürü

Güçlü bir siber güvenlik programı uygulamak, en son siber güvenlik araçlarını kullanmaktan daha fazlasını içerir. Önde gelen güvenlik araçlarının bile kısıtlamaları vardır ve eski sistemlerle entegrasyon zor olabilir. Siber güvenlik meselesi, son kullanıcıları ve BT uzmanlarını içeren bir olgudur. Ek olarak, güçlü siber güvenlik kurum kültürü, üst yöneticinin yanı sıra üst düzey risk yöneticisi, üst düzey işletme görevlisi, üst düzey bilgi yöneticisi ve diğer üst düzey liderlerin katılımını gerektiren kurumun başında başlayan bir kavramdır. Güçlü yönetici desteği olmadan, siber güvenlik, bir uyumluluk egzersizidir veya daha da kötüsü, kurumsal risk yönetimi meselesinden ziyade, sadece bir BT problemidir (Wyatt, 2017: 336-337).

Etkili bir yönetişim açıkça tanımlanmış politikalarda, ilgili araçlarda, yeterli personel ve konuya uygun eğitimle kanıtlanır. Farklı bakış açıları olan çok sayıda paydaş, yönetişimin kalitesini güçlendirmektedir. Bir siber güvenlik yönetişim komitesi, genellikle birinci, ikinci ve üçüncü savunma hattından üst yönetim ve temsilciliği içerir; teknoloji ve süreç sahipleri, müşteriler, servis sağlayıcılar ve tedarikçiler gibi potansiyel olarak kilit dış paydaşlardır. Olay müdahale ekipleri düzenli olarak yönetime rapor eder ve daha önce bilinmeyen boşluklara ek iç görü sağlamak için karşılaşılan ihlal türlerini bildirir. Yönetim daha sonra tespit edilen sorunları iyileştirme yoluyla izleyebilir (GTAG, 2016: 18).

4.1.2. Bilgi Varlıkları Envanteri Bileşeni

BT departmanı tüm bilgi varlıklarının güncel bir envanterini tutmalı ve kurumun amaçlarını ve sürdürme operasyonlarını ilerletmek için en gerekli olanları önceliklendirmelidir. Stratejik kurumsal hedef ve girişimleri karşılamak için, bu varlıklar geleneksel BT genel kontrollerinden ve periyodik değerlendirmelerden daha fazlasını gerektirir. En değerli varlıkları korumak için tasarlanmış önleyici ve izleyici kontrollerin devamlı bir etkinliğini sağlamak için sürekli izlenmesi gerekir (GTAG, 2016: 18).

Kuruluşun bilgi varlıkları değerlendirilirken aşağıdakiler göz önünde bulundurulmalıdır (GTAG, 2016: 18-19):

1-Veri

Türler (örneğin, işlemsel, BT yapılandırması, yapılandırılmamış)

Sınıflandırma (standardizasyon ve önceliklendirme sağlar)

Ortamlar (örneğin, veri ambarları, temel veri tabanları)

2-Teknoloji varlıklarının altyapı deposu

Sunucular

Ağ cihazları

Depolama

Son kullanıcı cihazları (örneğin dizüstü bilgisayarlar, mobil cihazlar)

3-Uygulamalar

4-Dış ilişkiler

Üçüncü tarafça barındırılan ortamlar

Veri dosyalarının dış kuruluşlarla paylaşılması (örneğin, satıcılar, düzenleyici kurumlar, hükümetler)

Hangi yazılım ve cihazların ağ üzerinde etkileşime girdiğini belirleme yeteneği siber tehditlere karşı savunma yapabilmek için esastır. Kurum bilinmeyen aygıtlara ve yazılımlara yapılan ağ saldırılarına karşı savunma yapamaz. Çalışanların kendi cihazlarını getirmelerine izin veren kurumlar, kurumsal ağ üzerinden verilere erişen daha büyük bir hacim ve çeşitli cihaz ve yazılımlar deneyimlemektedir. Çalışanların sahip olduğu cihazları kontrol etmek ve ağa olan bağlantı, yönetimin kilit odağını oluşturmalıdır. Giderek artan bir şekilde, daha fazla sayıda çalışanın kurumsal bilgilere rutin bir 8 saatlik çalışma süresini aşan belki de 24 saat süreyle erişebilmeleri gerektirmektedir. Bilinmeyen aygıtları algılama, doğrulama ve envanter oluşturma, kurumun, genel siber güvenlik stratejisinin etkili olmasını sağlamak için bu aygıtlardaki değişiklikleri izlemesine ve ölçmesine olanak sağlamaktadır (GTAG, 2016: 19).

4.1.3. Standart Güvenlik Yapılandırmaları Bileşeni

Birçok kurum, yüksek riskli sistemlerin daha sık test edildiği bir risk değerlendirmesine dayanarak test

Şekil 7. Fiziksel Güvenlik Risk Yönetim Sistemi

(Vandijck ve Lerberghe, 2018: 290)

edilecek sistemleri ve bunların test edilme sıklığını belirler. Yüksek riskli sistemlerin belirlenmesinde göz önünde bulundurulan faktörler, bu sistem tarafından içerilen veya erişilen verilerin hassasiyetini, sistemin operasyonel önemini ve bilinen tüm güvenlik açıklarının varlığını içerir (FINRA, 2018: 13).

Yönetim yazılımı kullanmak, sistemleri manuel olarak veya standart olmayan bir şekilde yönetmekten daha etkilidir. Bilgi güvenliği ve iç denetim faaliyeti, riske dayalı ortamların doğru bir şekilde değerlendirilebilmesini sağlamak için temel yapıları gözden geçirmelidir (GTAG, 2016: 19). Tipik bir siber rol olarak kurumun fiziksel güvenlik risk yönetim sistemi gözden geçirilebilir. Bunun için bir fiziksel güvenlik yönetim sisteminin nasıl planlanacağı uygulanacağı, izleneceği ve gözden geçirileceği Şekil 7'deki gibi belirlenmelidir. Bir **iç denetçinin yönetime raporlama yaparken izlemesi gereken adımlar** (Vandijck ve Lerberghe, 2017: 290-291):

1- Fiziksel güvenlik tehdidi alanı hakkında siber güvenlik ile ilgili net bir görüş edinin.
2- Fiziksel güvenlik sisteminin kurumun özellikle siber güvenlik ile nasıl ilişkili olduğunu anlayın: Kim ne yapar? Kaynaklar ve yeterlilikler nelerdir?
3- Siber güvenlikle ilgili olan güvenlik kontrollerini tanımlayın.
4- Bir kesinti olasılığını hesaplayarak kontrollerin etkinliğini değerlendirin.
5- Kontrollerin maliyet etkinliğini, toplam güvenlik maliyetlerine dayanarak haritalayın ve değerlendirin.
6- Fiziksel güvenlik risk yönetim sisteminin ne kadar olgun olduğu, siber güvenliği nasıl desteklediği, artırdığı ve uygulanabilir yasal ve düzenlemelere (örneğin veri odaları için katman gereksinimleri) ne kadar olgun olduğu konusunda net bir görüş edinin.

4.1.4. Bilgi Erişim Yönetimi Bileşeni

Yönetim, kullanıcılara iş rollerini temel alarak onaylama ve erişim sağlama süreci gibi önleyici kontroller

uygulamayı düşünmelidir. Ek olarak, çalışanların kurum içinde ne zaman hareket ettiğini tespit etmek için bir işlem, kullanıcı erişiminin ayarlanması ve yeni rolle ilgili olmasını sağlamak için yardımcı olacaktır. İç denetim faaliyeti, erişim seviyelerinin mevcut roller için haklı olduğunu doğrulamak için kilit verilere ve sistemlere kullanıcı erişimini gözden geçirebilir (GTAG, 2016: 19).

Ayrıcalıklı idari erişim özellikle önemlidir. Bilgiye erişme ve bilgileri salıverme özelliğine sahip kullanıcılar, siber güvenlik riskine karşı en hassastır. Yanlışlıkla kimlik avı denemelerinin bir sonucu olarak parolalarını yanlışlıkla bildirerek veya kötü amaçlı yazılım yükleyerek, kullanıcılar yetkisiz erişimi engellemek için tasarlanmış sistematik kontrol katmanlarını aşabilirler. Erişimi olan kişiler kuruluşun içinde ve dışında bulunur, bu nedenle verilerin içeride mi yoksa dışarıda mı barındırıldığına bakılmaksızın, anahtar verilere erişimi olan çalışanlara, danışmanlara ve satıcılara dikkat edilmelidir. Ayrıcalıklı erişime sahip kullanıcıların duyarlılık ve davranışlarını değerlendirmek ve erişimi sağlamak ve iptal etmek için önleyici kontrol faaliyetlerini onaylamak, kuruluşun siber güvenlik programının etkinliğinin öncü bir ölçüsüdür (GTAG, 2016: 20).

4.1.5. Ani Cevap ve İyileştirme Bileşeni

Uygulanan risk değerlendirmesi ve politika reçetelerinin sonucuna dayanarak, kurum uygun güvenlik özelliklerini ve kontrollerini tanımlayabilir veya tasarlayabilir. Güçlü bir siber güvenlik, derinlemesine savunma ilkesine dayanır. Beklenen koruma seviyesine ulaşıldığı ilgili kontroller katmanı (örneğin, erişim kontrolü, şifreleme ve izleme) eklenerek gerçekleştirilir. Böylece güvenlik tasarımı daha geniş güvenlik mimarisi ve sistem bağlantısı dikkate alınarak yapılır. Ek teknik olarak odaklanmış risk değerlendirmeleri (örneğin, teknik mimari, sistem ara yüzleri ve programlama dili) ilk uygulanan risk değerlendirmesini destekleyebilir (Wyatt, 2017: 338).

Kurumun riskleri hızla iletebilmesi ve düzeltebilmesi, programın etkinliğini ve olgunluk seviyesini gösterir. Olgun programlar, yönetim yanıtına verilen zamanı sürekli olarak kısaltabilir. Bu savunma hattının yansımaları şunlar olacaktır (GTAG, 2016: 20):

1- Önemli riskleri iletimi,

2- İyileştirmenin kabulü,

3- Çözüm için belirlenen sorunların takibi,

4- Kurum genelinde çözüme dair eğilim ve rapor.

4.1.6. Devam Eden İzleme Bileşeni

Bu çerçevenin son bir bileşeni olarak, yukarıda açıklanan beş bileşenin her birinin sürekli denetlenmesi, riskin nasıl yönetildiğini ve düzeltici faaliyetin ne kadar iyi çalıştığını belirlemeye yardımcı olacaktır. Etkili bir değerlendirme yaklaşımı rutin bir kontrol listesinden daha fazlasını gerektirir. İkinci savunma hattının, aşağıdakileri içeren davranışsal değişiklik üretmek için tasarlanmış bir izleme stratejisi uygulaması beklenir (GTAG, 2016: 20-21):

1- İlgili siber güvenlik riskini ölçmek için hassas bilgilere erişimi olan kişilerin izlenmesini içeren erişim seviyesi değerlendirmesi ve taraması: Kritik işlemler gerçekleştiren bir kullanıcı grubu için, ilgili BT varlıkları, güvenlik yapılandırmaları, sorunlu web siteleri, kötü amaçlı yazılım olayları ve veri sızma durumları arasındaki açıkları bulmak için sistematik bir yol geliştirmek yararlı olacaktır.

2- Güvenlik açığı değerlendirmesi yapılması: Düzenli olarak tarama sistemleri, ortamdaki güvenlik açıklarını tespit etmek için kritik öneme sahiptir. Güvenlik açıkları tanımlandıktan sonra, kategorize (örneğin kritik, büyük, orta) ve ele alındıktan sonra (örneğin, 30 gün içinde yüksek riskli sistemlerdeki tüm kritik güvenlik açıklarını ele alın), tespit edilen güvenlik açıkları için düzeltme etkinlikleri başlatılmalıdır.

3- Dış kaynak kullanımı genellikle kurumlar için en yüksek riskleri oluşturur ve öncelik almalıdır**:** Bununla birlikte, iyileştirme faaliyetleri sadece dışarıya bakan ortamlarla sınırlı değildir. Birinci ve ikinci hat kaynakları, Hizmet Seviyesi Anlaşmaları (SLAs)[6] tanımlamak ve üzerinde anlaşmak için

6) SLAs-Service Level Agreements

kurum genelinde çalışabilir ve iç denetim, yönetimin tanımlanmış SLA'lara uygun olup olmadığını değerlendirerek yardımcı olabilir.

4- Üçüncü taraf risk değerlendirmeleri ve izleme: Programlar, üçüncü taraf satıcıların risklerini ve verilen hizmetlere dayanarak kuruma verilen güvenlik risk düzeyini değerlendirmede yardımcı olabilir.

5- Olay izleme ve müdahale: Bu süreçlerin birleşimi bir kuruluşun ihlal durumunda tespit etmesine, yanıt vermesine, düzeltmesine, kurtarmasına ve yönetime rapor vermesine olanak tanır. Bu kontrollerin karşılanma hedeflerinde başarılı olmasını sağlamak için kayıt ve izleme teknolojilerinin yanı sıra yüksek eğitimli bir yanıt ekibi de gereklidir.

4.2. Siber Güvenlik Denetimi

Kurumlar birçok nedenden dolayı denetimler yaparlar. Denetim kurumun etkin operasyonlar gerçekleştirmesine, idari ve yasal düzenlemelere uygunluğunun kanıtlanmasına yardımcı olabilir. Yönetim için kurumun iyi çalıştığını ve olası zorlukları karşılamak için hazır olduğunu doğrulayabilir. Belki de en önemlisi, kuruluşun mali, operasyonel ve etik refahını paydaşlarına garanti edebilir. Siber güvenlik denetimleri, tüm kurumların ve kamu kurumlarının rekabet avantajı için dayandığı bilgi ve ilgili sistemlere özel olarak odaklanarak, tüm bu sonuçları desteklemektedir. Etkili bir denetim ile birçok faydanın başarılması, denetim faaliyetinin doğru ve tam olarak planlanmasına bağlıdır. Denetimin kapsamı ve amacı hem denetçi hem de denetlenen alan tarafından anlaşılmalı ve kabul edilmelidir. Denetimin amacı açıkça tanımlandıktan sonra, denetim sonuçlarını almak ve desteklemek için ilgili prosedürleri kapsayacak olan denetim planı oluşturulmalıdır. Denetim planının önemli bir bileşeni, çalışma programı olarak da bilinen denetim programıdır. Denetim programı, kontrol etkinliğini test etmek ve doğrulamak için kullanılacak özel prosedürleri ve adımları belgelemek için yaygın olarak kullanılır. Denetim programının kalitesi, denetim sonuçlarının tutarlılığı ve kalitesi üzerinde önemli bir etkiye sahiptir. Bu nedenle iç denetçilerin kapsamlı denetim programlarının nasıl geliştirileceğini anlamaları zorunludur (ISACA, 2016: 3). Plan ve program temelinde bir siber güvenlik denetimi için iç denetçinin / iç denetimin yapabilecekleri şu şekilde sıralanabilir (Frazıer & Deeter, 2015: 17-18; ISPG-SM01, 2017: 34):

1- Mevcut güvenlik politikasına, standartlarına, yönergelerine ve prosedürlerine uyumu kontrol edin.

2- Yetersizlikleri belirleyin ve mevcut politika, standartlar, kılavuzlar ve prosedürlerin etkinliğini inceleyin.

3- İlgili yasal, düzenleyici ve sözleşmeye bağlı gerekliliklerı belirleyin ve gözden geçirin.

4- Mevcut güvenlik açıklarını tanımlayın ve anlayın.

5- Risk ve azaltma stratejisi konusunda tartışmayı yönlendirin

6- Siber riskleri diğer kritik kurumsal risklere karşı bağımsız olarak değerlendirin ve önceliklendirin

7- Siber sorunları önlemek veya tespit etmek için kontrollerin optimize edilmesine yardımcı olun

8- Değişen siber riskin devamlı izlenmesini sağlayın

9- Operasyonel, idari ve yönetsel konulardaki mevcut güvenlik kontrollerini gözden geçirin, güvenlik önlemlerinin etkin bir şekilde uygulanmasını ve asgari güvenlik standartlarına uygunluğunu sağlayın.

10- İyileştirmeler için öneriler ve düzeltici eylemler sağlayın.

Dijital dönüşüm, iç denetim faaliyetine hem zorluklar hem de fırsatlar sunmaktadır. Verilerin hacmi, çeşitliliği ve kırılganlığı arttıkça, iç denetimin izlemesi gereken risklerin kapsamı da artmaktadır. Aynı zamanda, iç denetim birimlerinin performans ve farkındalığını arttırması için "son sınır"ın ne olabileceği konusunda çeşitli fırsatlar vardır. Teknoloji etkin denetim araçları, süreçleri ve uygulamaları, iç denetçilerin örnekleme ve varsayımlar yapmak yerine tüm verileri ve süreçleri sürekli olarak izlemelerini ve anormallikleri tespit edebilmelerini mümkün kılmıştır. Veri analizi ve bilgisayar destekli denetim araçları, iç denetçiler için yeni ufuklar açmaktadır (Ahıa ve Protıvıtı, 2016: 11).

Birçok iç denetim faaliyeti, kurumun siber güvenlik hazırlığına ilişkin bileşenleri değerlendirerek ilgili prosedürleri gerçekleştirmiştir. Saldırı ve sızma pro-

sedürleri gibi hedefli denetimler değerlidir, ancak siber güvenlik riskleri yelpazesinde yeterli güvenceyi sağlamazlar. İç denetimin siber güvenliğin kapsamlı bir görünümünü sağlaması ve yalnızca hedeflenen denetimleri yaparak yanlış bir güvenlik duygusu sağlamasından kaçınmak için geniş bir yaklaşım kullanılmalıdır (Deloitte, 2017: 2). Siber güvenlik amaçları ve denetim hedefleri kurumun siber güvenlik ihtiyacını göz önünde bulundurmalıdır. Siber güvenlik amaçları ve ilgili denetim hedefleri için Tablo 2'de gerekli açıklamalar yapılmıştır.

Tablo 2. Siber Güvenlik Amaçları ve İlgili Denetim Hedefleri

Siber Güvenlik Amacı	Denetim Hedefleri
Siber güvenlik politikaları, standartları ve prosedürleri yeterli ve etkilidir.	❏ Belgelerin eksiksiz ve güncel olduğunu doğrulayın. ❏ Resmi onay, onay ve uygulamanın yerinde olduğunu onaylayın. ❏ Belgelerin tüm siber güvenlik gereksinimlerini karşıladığını doğrulayın. ❏ Yan denetimlerin politikalarda, standartlarda ve prosedürlerde yapılan tüm hükümleri kapsadığını doğrulayın.
Ortaya çıkan risk güvenilir bir şekilde tanımlanır, uygun bir şekilde değerlendirilir ve uygun şekilde iyileştirilir.	❏ Risk tanımlama işleminin güvenilirliğini onaylayın. ❏ Kullanılan araçları, yöntemleri ve teknikleri içeren risk değerlendirme sürecini değerlendirin. ❏ Tüm risklerin sonuçların değerlendirilmesine göre ele alındığını onaylayın. ❏ İyileştirmenin yeterli olduğunu veya iyileştirilmemiş riske karşı resmi risk kabullerinin bulunduğunu doğrulayın.
Siber güvenlik dönüşüm işlemleri tanımlandı, konumlandırıldı ve ölçüldü.	❏ Dönüşüm sürecinin ve ilgili rehberliğin varlığını ve eksiksizliğini doğrulayın. ❏ Dönüşüm sürecinin, işletmenin tüm bölümleri tarafından uygulandığını ve takip edildiğini doğrulayın. ❏ Dönüşüm hedefleri, risk ve performans ile ilgili kontrolleri, metrikleri ve ölçümleri onaylayın.
Ataklar ve ihlaller zamanında ve uygun bir şekilde tespit edilir ve iyileştirilir.	❏ İzlemeyi ve belirli teknik saldırı tanıma çözümlerini onaylayın. ❏ Güvenlik olayı yönetimi ve kriz yönetimi süreçleri ve planları ile ilgili ara yüzleri değerlendirin. ❏ (Geçmiş saldırılara dayanarak) saldırı müdahalesinin zamanlamasını ve yeterliliğini değerlendirin.

(ISACA, 2017: 11)

Güvenlik yeteneklerini korumak ve geliştirmek, siber tehditleri azaltmaya yardımcı olabilir ve kurumu istenen siber güvenlik olgunluk seviyesine taşıyabilir. İç denetim kapsamlı bir siber risk değerlendirmesi yaparak, denetim komitesi ve yönetime objektif bakış açıları ve bulgular sunabilir. Bu bulgular, Kurumun siber risk alanlarını göz önüne alan geniş bir iç denetim planı geliştirmek için kullanabilir (Deloitte, 2017: 4). Bunun dışında siber güvenliğin iç denetim değerlendirmesi Tablo 3'de gösterildiği gibi tüm alanları, ilgili yetenekleri kapsamalı ve uygun olduğunda konu uzmanlarını içermelidir (Deloitte, 2015: 8).

Tablo 3. Siber Güvenliğin İç Denetim Değerlendirmesi

Aşama	I. Aşama: Planlama ve Kapsam Belirleme	II. Aşama: Mevcut Durumu Anlama	III. Aşama: Risk Değerlendirmesi	IV. Aşama: Boşluk Değerlendirmesi ve Öneriler
Anahtar Faaliyetler	**Faaliyetler:** • Özel iç ve dış paydaşları tanımlayın: BT, UYgunluk, Yasal Risk vb. • Örgütün görev ve hedeflerini anlayın • Endüstri gereksinimlerini ve yasal düzenlemeleri belirleyin • Endürstri ve sektör riski profili oluşturma (endüstri raporlarını haberlerini, trendlerini, risk vektörlerini gözden geçirme) • Kapsam içi sistemleri ve varlıkları tanımlayın • Satıcıları ve üçüncü tarafların katılımını tanımlayın	**Faaliyetler:** • Mevcut profili anlamak için görüşmeler ve atölye çalışmaları yapın • Mevcut kontrolleri anlamak için kapsam içi sistem ve süreçlerin adım adım gerçekleştirilmesi • Uygulanabilir raporların incelemeleri de dahil olmak üzere üçüncü tarafların kullanımını anlayın • Hem iç hem dış paydaşlar için güvenlik ortamı, stratejik planlar ve yönetişim dahil olmak üzere ilgili politika ve prosedürleri gözden geçirin • Öz değerlendirmeleri inceleyin • ÖNceki denetimleri inceleyin	**Faaliyetler:** • Kapsam dahilindeki tüm yetenekler arasındaki potansiyel risk listesini belgeleyin • Ortaya çıkan riskleri katmanlaştırmak ve potansiyel etkiyi belgelemek için konunun uzmanları ve yönetim ile işbirliği yapın • Risklerin olasılığını ve etkisini değerlendirin • Örgütün hedeflerine, yeteneklerine ve risk iştahına göre riskleri önceliklerindirin • Risk değerlendirme sonuçlarını yönetimle gözden geçirin ve doğrulayın, ayrıca kritikliği belirleyin	**Faaliyetler:** • Yetenek değerlendirme sonuçlarını belgeleyin ve değerlendirme puan kartı geliştirin • Belirli paydaşlarla değerlendirme sonuçlarını inceleyin • Boşlukları tanımlayın ve potansiyel şiddeti değerlendirin • Olgunluk analizine haritalama yapın • Önerileri belgelendirin • Çok yıllı siber güvenlik / BT denetim planı geliştirin
Dağıtımlar	**Dağıtım:** • Değerlendirme hedefleri ve kapsamı • Yetenek değerlendirme puan kartı çerçevesi	**Dağıtım:** • Çevre ve mevcut durumun anlaşılması	**Dağıtım:** • Öncelikli risk sıralaması • Yetenek değerlendirme bulguları	**Dağıtım:** • Olgunluk analizi • Değerlendirme puan kartı • İyileştirme önerileri • Siber güvenlik denetim planı

(Deloitte, 2015: 8)

4.3. Üçüncü Savunma Hattı Olarak İç Denetim Faaliyetinin Siber Hijyen Rolü

Üçüncü savunma hattı olarak iç denetim, siber güvenlik çabalarının, riskleri doğru bir şekilde tanımlayan ve önceleyen, doğru bilgileri toplayan ve uygun yanıtlar veren bir risk temelli yaklaşım olduğunu doğrulamaktan sorumludur. Gerçekte, iç denetim mevcut programın değerlendirilmesinde kaynak ve altyapıdan yoksundur. Bunun yerine birçok iç denetim birimi, siber güvenlik programlarını değerlendirmek için siber güvenlik uzmanlarına ve dış paydaşlara yönelir (Jamison, Morris ve Wilkinson, 2018: 11). İç denetim BT risk evreninin en kritik bileşenlerine odaklanarak kurumun siber hassasiyetini değerlendirmelidir. BT risk evreninin BT ile ilgili en kritik kavramları; (1) güvenlik ve mahremiyet, (2) altyapı ve (3) veri kategorisinde olduğunu görünmektedir (EY, 2011: 10). Aşağıdaki şekil risk evrenini değerlendirmede; iç denetime risk odaklı bir ileri görüş sağlamada yardımcı olacaktır (Sadek ve Close, 2015: 6).

Siber risklerin sıklığı ve çeşitliliği artarken, kurumlara verebilecekleri potansiyel zararları da devamlı artmaktadır. Çoğu kurum bu riskleri ciddiye almaktadır, ancak hem tehlikelerle mücadele etmek hem de kurum yöneticilerinin siber güvenlik hazırlıklarından haberdar olmasını sağlamak için daha fazlası yapılabilir. İç denetimin mevcut ve ihtiyaç duyulan kontrollere bağımsız bir değerlendirme sağlayarak; siber tehditleri yönetme mücadelesinde kurumlara yardım etmesinde, yönetimin birbirinden farklı siber riskleri anlamalarına ve ele almalarına yardımcı olma konusundaki kritik rolleri Tablo 4'te listelenmiştir (Deloitte, 2017: 6). Teknoloji geliştikçe, iç denetçilerin de görevleri gelişmektedir. İç denetçiler mesleğin, mevcut bölgesinden çıkmalı ve uzmanlığını siber riskleri ele almak için kullanması gerekmektedir (Fountain, 2019: 21). İç denetçilerin ve iç denetim yöneticilerinin öncelikleri ve sahip olması gereken siber dünyaya özgü iç denetim yetenekleri ve bilgisi Tablo 5'te görülmektedir.

Bu yeteneklerin haricinde, iç denetim ve iç denetçiler için göz önünde bulundurulması gereken siber hijyen (güvenlik) eylemleri (Ahıa ve Protıvıtı, 2016: 6; Protıvıtı, 2016: 6) şunlardır:

Şekil 8. BT İç Denetim Evreninin Gelişimi

(Sadek ve Close, 2015: 6)

1- Bir siber güvenlik stratejisi ve politikası geliştirmek için yönetim ile birlikte çalışın.
2- Kurumun siber güvenlik riskini kabul edilebilir bir düzeyde tutması için risk belirleme, değerlendirme ve azaltma yeteneğini geliştirme fırsatlarını belirleyin ve harekete geçirin.
3- Siber güvenlik riskinin yalnızca dış nedenlere bağlı olmadığını bilin (bir çalışanın, satıcının veya iş ortağının davranışlarından kaynaklanabilecek potansiyel tehditleri değerlendirin ve azaltın).
4- Denetim komitesi ve yönetimle olan iç ilişkileri (a) siber tehditlere ilişkin farkındalık ve bilgiyi arttırın ve (b) yönetimin siber güvenlik meseleleriyle yüksek derecede bağlı kalmasını ve siber güvenlik riskinin değişen doğası hakkında güncel kalmasını sağlayın.
5- Siber güvenlik riskinin resmi olarak denetim planına entegre edilmesini sağlayın.
6- Gelişen teknolojilerin ve trendlerin kurumu ve siber güvenlik risk profilini nasıl etkilediğine dair bir anlayış geliştirin ve güncel tutun.
7- Kurumun siber güvenlik programını, NIST Siber Güvenlik Çerçevesi, ISO 27001/27002 veya HITRUST CSF gibi uygun bir çerçeveye göre değerlendirin.
8- Siber güvenlik konusunda en güçlü önleme yeteneğinin insan ve teknoloji güvenliğinin eğitim, farkındalık, dikkat ve teknoloji araçlarının tamamlayıcı bir birleşimini gerektirdiğini yönetime iletme fırsatlarını araştırın.
9- Siber güvenlik izlemenin ve siber olay tepkisinin üst yönetim önceliği olması gerektiğini vurgulayın (net bir yükseltme protokolü, bu önceliğin ortaya çıkmasına (ve sürdürülmesine) yardımcı olabilir).
10- Her ikisi de siber güvenlik riskini etkin bir şekilde yönetme çabalarını engelleyebilecek her türlü IT / denetim personeli ve kaynak sıkıntısı ile destekleyici teknoloji araçlarının bulunmamasına yöneliktir. Bu farkındalığa sahip olun.

İç denetim faaliyetinin kurum süreçlerine olan hakimiyeti nedeniyle siber güvenlik uygulamalarına ve politikalarına artı değer katması beklenmektedir. İç denetim Siber hijyenin olgunluk seviyelerinin yükseltilmesinde danışmanlık ve güvence sağlama; kurumsal yönetim içerisinde siber güvenliğin farkındalığının arttırılması ve buna bağlı olarak kuramsal risk yönetiminde siber risklerin daha görünür şekilde değerlendirerek, etkin kontrolleri sağlamada üçüncü savunma hattının kritik bir öğesi olarak proaktif bir rolü ve potansiyeli vardır. İç denetimin siber güvenliğe bakışı ve alacağı rol ile kurumun siber bağışıklığı sağlamasında önleyici ve özellikle de yönlendirici bir tarafı olacaktır. Bu roller aşağıdaki tabloda gösterilmektedir.

Tablo 4. Öncelikler - İç Denetim Yetenekleri ve Bilgisi

Tüm İç Denetçiler	İç Denetim Yöneticileri (Birim Başkanları)
Veri analizi araçları - istatistiksel analiz	Veri analizi araçları - istatistiksel analiz
Çevik risk ve uyum	Veri analizi araçları - veri manipülasyonu
Sürekli denetim	Çevik risk ve uyum
Büyük veri / iş zekası	Sürekli denetim
Sürekli izleme	Sürekli izleme

(Ahıa ve Protıvıtı, 2017: 7)

Tablo 5. İç Denetim Faaliyeti İçin Siber Hijyen Rol

	İÇ DENETİMİN SORUMLULUK ALANI	İÇ DENETİMİN HESAPVEREBİLİRLİK ALANI	İÇ DENETİMİN DESTEK KAYNAKLARI	İÇ DENETİMDEN DANIŞMANLIK ALANLAR	İÇ DENETİME BİLGİ SAĞLAYAN KAYNAKLAR
Siber krizden önce	• Siber risk yönetim sisteminin etkinliği konusunda yönetim kurulu ve yönetime bağımsız güvence verme • Önemli riskler için siber kontrolleri ve iyileştirme planlarını değerlendirme • Yönetim kurulu düzeyindeki danışman siber komitenin denetimleri ve/veya incelemeleri	• Tavsiyeler yoluyla yüksek düzeyde bağımsız ve objektif güvence	• Yönetim Kurulu ve Denetim komitesi yönetişimi, gözetimi, görevi, tonu • Üst yönetici (CEO) ve yöneticiler • Siber risk yönetim sisteminin arkasındaki ilkeler	• Yönetim kurulu ve üst düzey finansal yönetici (CFO-chief financial officer) • Siber risk yönetimi sisteminin olgunluğunun etkinliği	• Diğer birimlerden birleşik güvence • Tüm üst düzey yöneticilerin ve toplantıların planlama, tartışma ve eylemlerinin kayıtları • Düzenli incelemelerin yönetim kurulu düzeyinde denetim süreci • Siber risk yönetimi iyileştirme planları ve faaliyetleri • Siber güvenlik politikaları ve prosedürleri • Siber strateji ve stratejik performans yönetimi • Siber standartlar ve çerçeveler • Siber güvenlik olay ve kriz yönetimi • İş sürekliliği yönetimi
Siber kriz sırasında / sonrasında	• Siber risk yönetim sistemi ve yönetim kurulu düzeyindeki danışman siber komite sürecindeki değişiklikler konusunda kriz sonrası yeni güvence verme	• Gözden geçirilmiş güvence	• Yönetim Kurulu ve Denetim komitesi • Üst yönetici (CEO) ve yöneticiler	• Yönetim Kurulu ve üst yönetici (CEO)	

(Antonucci, 2017: 222)

5. SONUÇ

İster kişisel olsun isterse bir kurum içeresinde olsun eğer teknolojik bir araç kullanacaksak bunun kolaylıklarının yanında zorluklarını da göz önünde bulundurmalıyız. 21. yüzyılın baş döndürücü değişim hızı siber dünyada çok daha net görülmektedir. Bu hız beraberinde kırılganlıkları, belirsizlikleri, tehditleri ve riskleri de getirmektedir. Özellikle siber riskler yaygın olarak kurumlar için en büyük risk kaynağı olarak kabul edilmektedir. Tüm sektörlerde kurumların güvenlik açığı artmaktadır. Sürekli bir av peşindeki bilgisayar korsanları ve siber saldırganlar için bu av herhangi bir ülkenin elektrik şebekesi, herhangi bir şirketin web sitesi veya sıradan bir kişinin banka hesabı olabilmektedir. Endişe verici bir şekilde siber saldırılar potansiyel zararlarıyla karşılaştırıldığında, orantısız bir şekilde çok ucuzdurlar. Siber saldırıların zaman aralığı 7 gün / 24 saattir. Bir siber saldırının başarılı olması siber saldırganlarının motivasyonuna bağlı olarak sadece bir zaman meselesidir. Bu nedenle sürdürülebilir bir siber hijyen ve siber güvenlik yönetimi anlayışı kurumların kaçınılmaz bir gerçekliğidir. Hiçbir kişi, hiçbir kurum, hiçbir ülke siber uzayda bir ada değildir ve siber saldırı için bir alarm verildiğinde, herkes için bir mücadele alanı vardır, ister siperde olsunlar isterse olmasınlar. 2. Dünya Savaşında öncü bir rol oynayan Winston Churchill'ün bir sözünü ödünç alıp bunu siber mücadeleye aktarırsak *"herhangi bir kurumun siber savunmasında yer alacak olan; en cesur yöneticilerini, en gözü pek bilgi güvenliği uzmanlarını, en donanımlı BT'cilerini, en cüretkar beyaz şapkalı hackerlarını bir masada toplarsanız, ne elde edersiniz? Bütün korkularının toplamını…"* şeklinde durumu özetleyebiliriz.

Küresel ekonominin artan bağlantı ve otomatik sistemlere bağımlılığı göz önüne alındığında, siber güvenlik, herhangi bir kurum veya devlet operasyonunun kritik bir bileşeni haline gelmiştir. Siber güvenliğin ön aşaması olarak siber hijyen, siber bilgi güvenliği ile ilgili temel bir ilkedir. Siber hijyen kişisel hijyenle benzerlik göstermekte ve siber tehditlerden kaynaklanan riskleri en aza indirgemek için basit ve rutin önlemler almayı ifade etmektedir. Ne yazık ki bir siber saldırı, güvenlik hijyeninin sağlanmasından daha kolaydır. Kurumların bir siber saldırının kurbanı olmalarını önleyebilmeleri veya bir siber saldırının risklerini en aza indirebilmeleri için en güçlü silahları, bir siber hijyen stratejisi uygulamalarıdır. Bu bağlamda, bir olgunluk modeli olarak siber hijyen kişisel hijyen ile aynı işlevde görülmeli ve bir kuruma düzgün şekilde entegre edildiğinde, kurumsal siber bağışıklık sisteminin güçlenerek kurumsal sağlığın korunabileceği dikkate alınmalıdır.

İç denetim faaliyeti tüm siber korkularının ötesine geçme potansiyeline sahiptir ve bu potansiyel kullanılmalıdır. İç denetçiler ve iç denetim faaliyeti için bu siber dünyadaki siber savaşın siber cephesinin siperlerinde yadsınamaz bir rol görünmektedir. Risk yönetimi, siber hijyen ve siber güvenlik için bağımsız güvence rolü, kendini buna göre yapılandıran iç denetim fonksiyonu tarafından benzersiz bir şekilde oynanabilir. İç denetçiler bu süreçte önemli danışmanlar olabilir. Siber hijyenin kurumların mevcut savunma hatlarında konumlanmasında kritik görevler üstlenebilirler. Bu yönüyle değerlendirildiğinde, üçlü savunma hattının üçüncü sırasındaki **iç denetim faaliyetinin siber rolünün (ve sorumluluğunun) her geçen gün arttığı sonucuna varılabilir.** Günümüzde -tüm meslekler gibi- iç denetimin de zorluğu, kritik iş bilgilerinin güvenliğini ve kullanılabilirliğini sağlamadaki (güvence sağlama) rolünü eşzamanlı olarak genişletirken, kendi risklerini kontrol ederek siber olaylar karşısında güncel kalabilmekle ilgilidir.

Kaynakça

Ahıa ve Protıvıtı, (2016) *Cybersecurity, IT Transformation and Analytics - Addressing Priorities for Internal Auditors in U.S. Healthcare Provider Organizations*, Ahia and Protiviti.

Ahıa ve Protıvıtı, (2017) *Cybersecurity, Data Analytics and Other Priorities for Internal Auditors in U.S. Healthcare Providers*, Ahia and Protiviti.

AICPA, (2017) *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*, American Institute of Certified Public Accountants Inc.

Antonuccı D,, (2017) "Internal Organization Context", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Antonuccı D. ve Verstıchel D., (2017) "Epilogue", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Bayuk J. L., Healey J., Rohmeyer P., Sachs M. H., Schmıdt J. ve Weıss J., (2012) *Cyber Security Policy Guidebook*, John Wiley & Sons, Inc.: Hoboken, New Jersey.

BSI, (2008) *Information Security Audit (IS audit): - A Guideline for IS Audits Based on IT-Grundschutz*, German Federal Office for Information Security.

Caravellı J. ve JONES N., (2019) *Cyber Security: Threats and Responses for Government and Business*, Praeger Security International.

CBN, (2018) *Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers*, Central Bank of Nigeria.

CMM, (2016) *Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition*, Global Cyber Security Capacity Centre University of Oxford.

DELOITTE, (2015) *Cybersecurity: The Role of Internal Audit*, Deloitte.

DELOITTE, (2017) *Cybersecurity and the Role of Internal Audit: An Urgent Call to Action*, Deloitte.

ENISA, (2016) *Review of Cyber Hygiene practices*, European Union Agency For Network and Information Security.

EY, (2011) *The Evolving IT Risk Landscape: The Why and How of IT Risk Management Today*, Ernst & Young.

FFIEC, (2015) *FFIEC Cybersecurity Assessment Tool*, Federal Financial Institutions Examination Council.

FINRA, (2018) Report on Selected Cybersecurity Practices - 2018, Financial Industry Regulatory Authority https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf Erişim Tarihi: 12.02.2019.

Fountaın L., (2019, February) "Internal Audit's Evolving Cybersecurity Role", *Internal Auditor*, 19-21.

Frazıer & Deeter, (2015) *Cybersecurity: Considerations for Internal Audit*, IIA Atlanta Chapter Meeting, Frazier & Deeter.

GAC 16, (2016) *Global Agenda Council on Cybersecurity*, White Paper, World Economic Forum: Geneva.

GTAG, (2016) *Assessing Cybersecurity Risk: Roles of the Three Lines of Defense,* The Institute of Internal Auditors.

Hale r., (2017) "Foreword The State of Cybersecurity", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Hermans J. ve Dıemont T., (2017) "Treating Cyber Risks", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Holmes C. ve Phıllıppe J., (2017) "Cybersecurity for Operations and Communications", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

IIAC, (2015) *IIAC Cybersecurity Guidebook*, Investment Industry Association of Canada.

ISACA, (2016) *Information Systems Auditing: Tools and Techniques- Creating Audit Programs*, ISACA.

ISACA, (2017) *Auditing Cyber Security: Evaluating Risk and Auditing Controls*, ISACA.

ISPG-SM01, (2017) *Information Security: Practice Guide for Security Risk Assessment & Audit*, Office of the Government Chief Information Officer-The Government of the Hong Kong Special Administrative Region.

ITGI, (2003) Board Briefing on IT Governance, 2nd ed., IT Governance Institute.

ITGI, (2006) Information Security Govenance for Board of Directors and Executive Management, 2nd ed., IT Governance Institute.

ITRC, (2017) *Data Breach Reports: 2016 End of Year Report*, Identity Theft Resource Center.

ITRC, (2019) *Data Breach Report: 2018 End of Year Report*, Identity Theft Resource Center.

ITU-T X.1208, (2014) *Series X: Data Networks, Open System Communıcations and Security: Cyberspace Security – Cybersecurity*, International Telecommunication Union.

Jamıson J., Morrıs L. ve Wılkınson C., (2018) *The Future of Cybersecurıty in Internal Audit*, The Internal Audit Foundation.

KPMG, (2018) *Siber Güvenlik Olgunluk Değerlendirmesi*, KPMG.

Lı K. C., Chen X. ve SusılO W., (2019a) "Foreword I-II", *Advances in Cyber Security: Principles, Techniques, and Applications*, Ed.: Kuan-Ching Li, Xiaofeng Chen, Willy Susilo, Springer Nature Singapore Pte Ltd.: Singapore.

Lıng C., (2017) "Information Asset Management for Cyber", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Lınkov I., Eısenberg D. A., Plourde K., Seager T. P, Allen, J. ve Kott A., (2013) "Resilience Metrics for Cyber Systems", *Environment Systems and Decisions*, 33(4), 471-476.

Keys B. ve Shapıro S., (2019) "Frameworks and Best Practices", *Cyber Resilience of Systems and Networks*, Ed.: Alexander Kott, Igor Linkov, Springer International Publishing AG, part of Springer Nature: Switzerland.

Mccarthy Tétrault, (2017) *Cybersecurity Risk Management: A Practical Guide for Businesses*, McCarthy Tétrault.

NACD, (2017) *Cyber-Risk Oversight*, Director's Handbook, National Association of Corporate Directors.

Nhede N., (2017) "Grid Automation Drives Increase in Utility Cybersecurity Investments: Report". Smart Energy International. 10 August 2017, https://www.smart-energy.com/industry-sectors/smart-grid/cybersecurity-technologies-navigant-research/, Erişim Tarihi: 19.02.2019.

ONG-C2M2, (2014) *Oil and Natural Gas Subsector Cybersecurity Capabılity Maturity Model*, U.S.Department of Homeland Security-Department of Energy.

Protıvıtı, (2016) *Cybersecurity, IT Transformation and Analytics – Addressing Priorities for Internal Auditors in U.S. Healthcare Provider Organizations*, Assoc. of Internal Auditors.

Rodrıguez A,, (2017) "Monitoring and Review Using Key Risk Indicators (KRIs)", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Sadek K. ve CLOSE C., (2015) *The Changing IT Risk Landscape: Understanding and Managing Existing and Emerging Risks*, Deloitte.

SAMA, (2017) *Cyber Security Framework*, Saudi Arabian Monetary Authority.

Souppaya M., Stıne K., Sımos M., Sweeney S. ve Scarfone K., (2018) *Critical Cybersecurity Hygiene: Patching The Enterprise*, National Institute of Standards and Technology.

Sunde S. J., (2017) "Assurance and Cyber Risk Management", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Totade A. ve Godbole S., (2017) "Culture and Human Factors", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

VAndıjck I. ve Lerberghe P. V., (2017) "Physical Security", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Vıllıers S., (2017) "Access Control", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

WEF, (2018) *Cyber Resilience Playbook for Public-Private Collaboration*, World Economic Forum: Geneva.

Whıt G. B., (2011) "The community cyber security maturity model", *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, 173-178.

Wyatt M., (2017) "Cybersecurity Systems: Acquisition, Development, and Maintenance", *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

KAMU KURUMLARINDA VERİ TABANI YÖNETİMİ DENETİMİ

(AUDITING OF DATABASE MANAGEMENT IN PUBLIC SECTOR)

Tolgahan ÖZDEN* / Hüseyin ÇALIŞ**

ÖZ

İnternet kullanımının 90'lı yıllardan sonra artmasıyla birlikte dünya bilgi çağına girmiş ve her alanda olduğu gibi kamu kurumları da bu çağa ayak uydurmak zorunda kalmışlardır. Bilgiyi oluşturan en temel kavram veridir. Günümüzde kamu kurumları fiziki ortamda sahip oldukları verilerin birçoğunu oluşturdukları bilgi sistemleri vasıtasıyla elektronik ortamda işlemekte ve sunmaktadır. Kamu kurumları verdikleri hizmetlerin güvenilirliğini, şeffaflığını, doğruluğunu ve kaynakların etkin kullanımını bilgi teknolojileri sistemleri kullanarak artırmaktadır. Bu durum vatandaş odaklı hizmet anlayışını geliştirmektedir. Bilgi, verilerin işlenmesiyle oluştuğu için verinin yönetimi önem arz etmektedir. Veri, veri tabanı yönetim sistemleri araçlarıyla yönetilmektedir. Veri tabanı yönetim sistemleri büyük çaplı verileri saklama, değiştirme ve koruma gibi süreçleri kolaylaştırmaktadır. Kritik öneme sahip veri tabanı yönetim sistemlerinin denetimi ise bu sistemin etkin, etkili ve verimli çalışmasına makul güvence vermektedir.

Kamu kurumları bilgi çağına ayak uydururken, veri tabanı yönetimindeki eksikliklerini, yeni teknoloji önerilerini, bilgi güvenliği farkındalığını denetim fonksiyonunu etkin kullanarak geliştirebilirler. Bu çalışmada, veri tabanı yönetim sürecine ilişkin denetim fonksiyonu kamu kurumları özelinde ele alınarak, idari ve teknik alanda belirlenen risk ve bulgu örnekleri için öneriler geliştirilmekte ve bu önerilerin nasıl izlenmesi gerektiği hakkında görüşler sunulmaktadır.

Anahtar Kelimeler: Bilgi, veri, veri tabanı, veri tabanı yönetimi, veri tabanı yönetimi denetimi, iç denetim, bilgi teknolojileri denetimi.

JEL Kodlaması: M15, M42

ABSTRACT

With the increase of internet usage after the 90s, the world entered the information age and public institutions has to keep up with this era as in every other fields. The most basic concept of knowledge is data. Today, public institutions operate and present many of the data they have in physical environment via the information systems. Public institutions increase the reliability, transparency and correctness of their services by using information technology systems. This situation improves citizen-oriented service. Since the information is generated by processing the data, the management of the data is important. Data is managed by database management systems. The database management system simplifies processes such as store, update and protection of large data sets. The control of critically important database management systems, gives a reasonable assurance on effective, efficient and productive operation of this system.

While the public institutions keep up with the information age, they can improve their database management deficiencies, new technology suggestions, and information security awareness effectively by using the audit function. In this study, the audit function of the database management process is discussed in the context of public institutions, recommendations for risk and finding examples determined in the administrative and technical fields are developed and opinions are given on how these recommendations should be monitored.

Keywords: *Information, data, database, database management, database management auditing, internal audit, information technology audit.*

JEL Classification: *M15, M42*

---

*) İç Denetçi, Tapu ve Kadastro Genel Müdürlüğü, İç Denetim Birimi Başkanlığı, Ankara, Orcid:0000-0001-6560-3177, tolgahanozden@gmail.com

**) İç Denetçi, Tapu ve Kadastro Genel Müdürlüğü, İç Denetim Birimi Başkanlığı, Ankara, Orcid:0000-0001-8230-5286, huseyincalis@gmail.com

Yazı Gönderim Tarihi: 21.01.2019, Yazı Kabul Tarihi: 14.04.2019

1. GİRİŞ

Bilgi teknolojileri kullanımı tüm dünyada olduğu gibi ülkemizde de artmaktadır. Hızla artan teknolojik gelişmeler sonucunda bireyler bilgi ve iletişim teknolojilerini daha yaygın bir şekilde kullanmaktadır. Elektronik ortama taşınan kamu hizmetleri sayesinde, kaynaklar etkin ve verimli kullanılmakta, rasyonel duruma getirilen işlemler daha hızlı sunulmaktadır (Sevinç, 2007:22).

Devlet kurumları hızla gelişen bilgi teknolojileri konularında birçok politika üretmiş ve Cumhurbaşkanlığı Yönetim Sistemi ile Cumhurbaşkanına bağlı "Bilim, Teknoloji ve Yenilik Politikaları Kurulu" oluşturularak konunun önemi açıkça vurgulanmıştır. Kamu sektöründe, bilgi teknolojileri yönetim süreci, bilgi işlem birimleri tarafından yürütülmektedir. Bilgi işlem birimleri, kurumlarda farklı teşkilatlanma yapıları gösterse de en genel anlamda yazılım geliştirme, veri tabanı yönetimi, bilgi güvenliği ve sistem yönetimi olarak 4 temel konu üzerine kurulmuştur. Üst düzey bir bilgi teknolojileri modeli geliştirmiş olmak, kurumsal bilgi yönetiminin organizasyonda sağlıklı çalıştığını garanti etmez. Kurumsal bilgi yönetimi modelinin tasarlanması ilk adımdır, bunu organizasyona uygulamak bir sonraki zorlu adımdır (De Haes ve Van Grembergen, 2006:2). Tüm bu modelleme ve teşkilatlanma, verinin üretilmesi, saklanması, güvende tutulması ve istenildiğinde ulaşılması için altyapı oluşturmaktadır. Kamu kurumları bilgi teknolojileri yönetim sürecini oluştururken, veri tabanı yönetimindeki eksikliklerini, yeni teknoloji önerilerini, bilgi güvenliği farkındalığını denetim fonksiyonunu etkin kullanarak geliştirebilirler.

Bu çalışmada, veri tabanı yönetim sürecine ilişkin denetim fonksiyonu kamu kurumları özelinde ele alınmaktadır.[1] Kamu kurumlarında idari ve teknik alanda ortaya çıkması muhtemel riskler ve bunlara ilişkin bulgu örnekleri üzerinden öneriler geliştirilmekte ve bu önerilerin nasıl izlenmesi gerektiği hakkında görüşler sunulmaktadır.

2. VERİ TABANI YÖNETİM SİSTEMİ

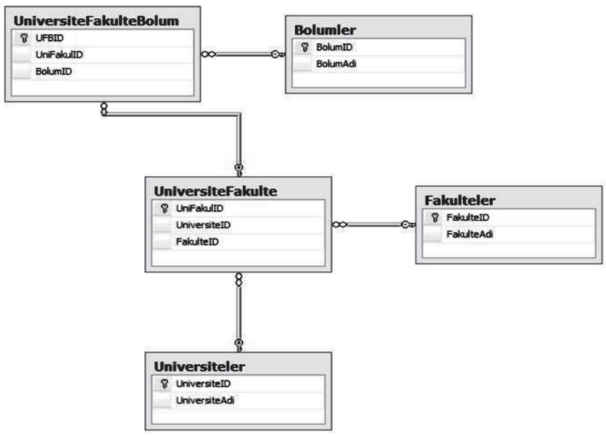
Türk Dil Kurumu güncel sözlüğünde bilgi, "kurallardan yararlanılarak kişinin veriye yönelttiği anlam" olarak tanımlanmaktadır. Tanım içinde geçen "veri" sözcüğü bilginin temel unsurunu temsil etmektedir. Verinin bilgi olabilmesi için tablolama, istatistiksel analiz veya durumun daha iyi anlaşılmasına yol açan başka bir işlemle manipüle edilmesi gerekir (Oz, 2008:9). ISACA terimler sözlüğünde veri tabanı; "işletmelerin ve bireylerin bilgi işleme ve elde etme gereksinimlerini karşılamak için ihtiyaç duydukları ilgili verilerin depolanmış bir koleksiyonudur". Bilgi teknolojilerinin kritik süreçlerinden biri, anlamlandırılarak bilgiyi oluşturacak verinin saklandığı veri tabanlarının yönetimidir. (ISACA, 2018:85)

Veri tabanı yönetim sistemi, büyük veri koleksiyonlarını koruma ve kullanma konusunda yardımcı olmak için tasarlanmış bir yazılımdır. (Ramakrishnan ve Gehrke, 2003:4). Veri tabanı yönetim sistemleri 80'li yıllardan itibaren kullanılmakta ve en genel anlamda dosya tabanlı, ilişkisel (relational) ve ilişkisel olmayan (non-relational) olmak üzere üç ana başlık altında değerlendirilmektedir. Dosya tabanlı veri tabanı yönetim sistemi yönetilmesi en kolay, tek bir dosya içine yazılmış ve sadece gerektiği durumlarda veriye ulaşmak için kullanılan bir sistemdir. Bu yönetim sisteminde ilkel istatistikler dışında herhangi bir bilgi alınamamakta ve günümüzde kullanılmamaktadır ("Types of database", 2014). İlişkisel veri tabanları verilerin satır ve sütunlar içerisinde saklandığı tablolardan meydana gelir. Tablolar belli yapıya uygun verileri saklamak üzere tasarlanır. Bir veri tabanında ilişkiden bahsetmek için en az iki tablo arasında ilişki kurarak, iki tablodaki verileri birbiri ile bağlamamız gerekir. Bu şekilde ilişkisel veri tabanları, veri tabanı olarak adlandırılan büyük dosyalardan oluşur (Sevim, 2005:82). İlişkisel veri tabanı yönetim sistemi ilişkisel veri tabanı oluşturmaya, güncellemeye ve yönetmeye izin veren bir uygulamadır. Veri tabanı yönetim sistemleri kullanıcıların veri tabanından bilgi edinmelerini sağlayacak bir sorgu diline sahiptir. Çoğu ilişkisel

1) Yazarların kamu kurumlarında 10 yılı aşkın süre bilgi işlem departmanındaki ve veri tabanı yöneticiliğindeki görevleri esnasında (hem denetlenen hem de denetim yapan rolleriyle) edindikleri bilgi ve tecrübelerin, ülkemizde mevcut veri tabanı denetimi yazınına aktarımı suretiyle bu denetim türünün geliştirilebilecek yönlerinin ortaya konulmaya çalışılmıştır. Yazıda kaynakçaya atıf yapılmayan bölümler yazarların tecrübe ve görüşlerini yansıtmaktadır.

veri tabanı yönetim sistemleri veri tabanındaki tablolara erişim için SQL (yapılandırılmış sorgu dili) dilini kullanır. SQL, ilişkisel veri tabanı yönetim sisteminde saklanan verilerle iletişim kurmak için kullanılan bir programlama dilidir ("What is a Relational Database", t.y.). SQL ile veri listeleme, kaydetme, güncelleme, silme, veri tabanına yeni bir tablo ekleme, yeni veri tabanı oluşturma veya mevcut veri tabanını değiştirme gibi veri ve veri tabanı yönetimine ilişkin işlemler yapılabilmektedir. Yaygın kullanılan ilişkisel veri tabanları MSSQL, Oracle, MySql, PostgreSql'dir. Şekil 1' de örnek olarak üniversitelerin fakülte ve bölümlerinin kayıtlarını saklayan ilişkisel veri tabanı modeli görülmektedir.

Şekil 1. İlişkisel Veritabanı Örneği



(Unipedi, 2014)

İlişkisel olmayan veri tabanları, verilere erişmek ve verileri yönetmek için belge-tabanlı (Document-Base), grafik tabanlı (Graph-Base), anahtar-değer (Key-Value) ve sütun tabanlı (Column-Base) gibi çeşitli veri modelleri kullanır. Şekil-2'de tiplerine göre ilişkisel olmayan veri tabanları ve örnekleri gösterilmiştir. Anahtar değer veritabanları her veriyi ayrı ayrı anahtarlayarak saklar ve bu anahtar değer ikilisini büyük bir değer tablosu içinde adresler. Belge tabanlı veritabanları, etiketli öğelerden oluşan belgeleri depolar. Sütun tabanlı veri tabanları verileri bir sütundan oluşacak tablolar halinde saklar. Grafik tabanlı veritabanları ise verileri temsil etmek ve saklamak için düğümleri kullanarak bir ağ oluşturur. (Simplilearn, 2019).

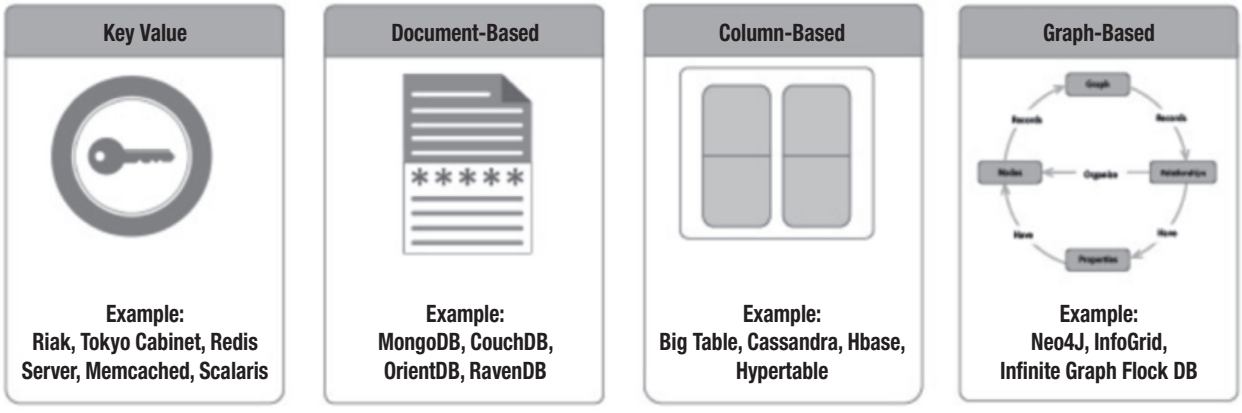
İlişkisel olmayan veritabanları, özellikle büyük veri hacmi, düşük gecikme süresi ve esnek veri modelleri gerektiren uygulamalar için geliştirilmiştir ("NoSQL Nedir", t.y.). Büyük veri (big data) kullanımın artması ve bu büyük veriler üzerinden analiz ve karar destek sistemlerinin geliştirme ihtiyaçlarından dolayı son yıllarda kamu sektöründe ilişkisel olmayan veri tabanlarına ilgi artmaktadır.

Kamu kurumlarında, yaygın bir teknoloji olması ve yönetecek uzman personelin bulunma kolaylığı sebepleriyle, ilişkisel veritabanı kullanımı daha fazla görülmektedir. Veri tabanı yönetimi denetimi incelenirken, kamu kurumlarında daha çok kullanılan ilişkisel veritabanları ön planda tutulmuştur.

3. VERİTABANI YÖNETİMİ DENETİMİ

Günümüzde kamu kurumları hizmetlerini yürütürken yoğun bir şekilde bilgi ve iletişim teknolojileri-

Şekil 2. NoSQL Tipleri



(Simplilearn, 2019)

ni kullanmaktadır. Hizmetlerin etkin ve verimli bir şekilde sunulması adına, veri tabanı yönetim sistemlerinde verilerin güvenli bir şekilde tutulması ve işlenmesi büyük önem arz etmektedir. Veri tabanı yönetim sistemi temel olarak kullanıcılara veri üzerinde düzeltme, ekleme, silme veri tabanı üzerinde ise tasarım, bakım ve erişim gibi işlemleri kolaylaştıran bir yazılımdır (Prabhjot ve Sharma, 2017:362).

Sahip oldukları bilgilerin kritikliği sebebiyle kamu kurumları için veri tabanı yönetimi büyük öneme sahiptir. Risk seviyesi yüksek olan veri tabanı yönetimi belirli periyotlarla denetlenmelidir. Ekip olarak yürütülen bilgi teknolojileri denetimlerinde bütün ekip üyelerinin gerçekleştirecekleri çalışma için uygun seviyelerde yetkinliklere sahip olması, ekip üyeleri arasında görev dağılımı yapılırken her denetim konusu için gerekli profesyonel ve teknik bilgi ve beceriye sahip olan iç denetçinin görevlendirilmesine özen gösterilmelidir (Kamu Bilgi Teknolojileri Denetimi Rehberi, 2014:16). Mevcut denetçiler arasında teknik yönden yeterli olmayan denetçilerin bulunması halinde konunun uzmanından görüş veya destek alınmalıdır.

3.1. Amaç, Kapsam, Yöntem

İlgili yasal düzenlemelere, talimatlara, politika ve prosedürlere uygun hizmet verilmesi, standart veri tabanı yönetiminin hayata geçirilmesi, varsa süreçte aksayan yönlerin geliştirilerek yürütülen çalışmalara değer katma prensibi veri tabanı yönetimi denetiminin amacını oluşturmaktadır. Bu amaç doğrultusunda kurumlarda veri tabanı yönetimi, yazılım geliştirme, sistem ve ağ yönetimi gibi süreçler; yazılım ve donanım envanteri, yedekleme, bakım, her zaman çevrimiçi, kayıt tutma (logging), denetleme (auditing), gerçek zamanlı izleme, kullanıcı yönetimi stratejileri, test ortamları, veri tabanı standartları, kriz yönetimi konuları kapsamında risk bazlı denetlenmelidir. Bilgi, belge ve dokümanların incelenmesi, süreç sahipleri ile görüşmelerin yapılması, sürecin gözlenmesi ve teknik incelemeler başlıca denetim yöntemini oluşturmalıdır.

3.2. Risklerin Belirlenmesi ve Ön Çalışma

Denetlenen kurum için veri tabanı yönetimi sürecindeki muhtemel riskler belirlenmelidir. Ön çalışma sırasında, riskleri belirlemek için, ilgili mevzuatları ve iyi uygulama örnekleri (best-practice) incelenmeli, mevcutta olması gereken durum belirlenmelidir. Bu kapsamda, *Kişisel Verileri Koruma Kanunu, KamuNet Tebliği, E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul Ve Esaslar Hakkında Yönetmelik ve ISO 2700x Bilgi Güvenliği Standartları* gibi bilgi teknolojileri ile ilgili mevzuat, hizmet alım sözleşmeleri ve denetlenecek kurumun teşkilat ve görevleri ile ilgili kanun, yönetmelik, genelgeler ve talimatlar incelenmelidir. Yine ön çalışma sırasında kurumun teşkilat yapısı incelenmeli, veri tabanı yönetim sürecinden sorumlu birim belirlenmeli ve saha çalışması yapılmadan önce birim yöneticisi ve personel ile ilgili bilgi toplanmalıdır. (Kamu Bilgi Teknolojileri Denetimi Rehberi, 2014:27). İlgili birimlerden personel görev dağılımları, sorumlulukları ve eğitim durumları, yazılım ve donanım envanterleri, yedekleme, bakım gibi süreçlere ilişkin yazılı politika, prosedürler ve eylem planları istenmelidir.

Kamuda veri tabanları yönetimi denetimi yapılırken, risklerin belirlenmesi için yapılacak çalışmalar idari ve teknik olarak iki grupta sınıflandırılabilir. Riskler belirlenirken bilgi güvenliği unsurları da göz önünde bulundurulmalıdır. McCumber bilgi güvenliğini "Bilgi ve bilgi sistemlerinin yetkisiz erişimi, kullanımı, ifşa edilmesi, bozulması, değiştirilmesi veya bilginin gizlilik, bütünlük ve kullanılabilirliğine zarar vermek için yapılan kötü niyetli girişimlere karşı sağlanacak koruma" şeklinde tanımlamaktadır (McCumber, 2005:xxiii). McCumber Bilgi Güvenliği Modeli'ne göre bilgi, "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel unsurdan oluşur (McCumber, 2005:136).

- Gizlilik, bir bilgiye erişimi uygun görülen kişilerin bilgiye erişiminin sağlanmasıdır (Henkoğlu ve Yılmaz, 2013:455).
- Bütünlük, verinin yetkisiz kişiler tarafından değiştirilmesi silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır.
- Erişilebilirlik, kullanıcının ihtiyacı olan bilgiye yetkisi dahilinde ve istediği anda ulaşabilmesidir (Henkoğlu ve Yılmaz, 2013:455).

Teknik riskler; süreçte kullanılan bilgi teknolojilerinin yeterli, güncel, güvenli olması, sistem yapılandırması, uygulama erişim, yetki, konfigürasyon kontrolleri olup, bu hususlar bilgi güvenliğine ilişkin McCumber

tarafından belirlenen unsurlarda dikkate alınarak incelenir. İdari riskler ise; süreçlerden sorumlu birimlerin yönetim, mevzuat açısından ve süreç sorumlularının yetkinliği bakımından incelenmesi ile belirlenir.

Saha çalışması sırasında olası risklerin oluşturacağı bulguların tespiti için bu ayrıma dikkat edilmesi gerekir. Veri tabanında çalışan teknik personeli, yönetim veya mevzuatla ilgili konularda teste tabi tutmak zaman kaybına yol açıp doğru bilgiye ulaşmayı engelleyecektir. Aynı şekilde yönetim kadrosunu, teknik konularla değerlendirmek risklerin tespitinde zorluklara yol açacaktır. Bu kapsamda denetim ekibi oluşturulurken, idari ve teknik risk kategorilerinin olacağı göz önünde bulundurulmalıdır.

Kamu kurumlarındaki veri tabanları yönetim süreci için idari riskler;

- Veri tabanı yönetiminden sorumlu birime, görevler ayrılığı ilkesine aykırı verilecek diğer görevler nedeniyle hata ve usulsüzlüklerin tespit edilememesi ve hizmetlerin aksaması,
- Veri tabanlarından sorumlu personelin görev tanımlarının yapılmamış olması nedeniyle mükerrer görevlerin ortaya çıkması veya açıkta görev kalması,
- Mevzuat ile tanımlanmış görevlerin uygulama ile uyuşmaması sebebiyle yetki ve sorumluluk karmaşası yaşanması ve hizmetlerin aksaması,
- Yetkin olmayan teknik personel görevlendirmesi nedeniyle veri kayıplarının yaşanması ve bilgi güvenliği açıklarının oluşması,
- Farklı veri tabanı yönetim sistemlerine ve yeni teknolojik gelişmelere ilişkin personel eğitim ihtiyaçlarının karşılanmaması nedeniyle personelin yönetimde yetersiz kalması ve veri tabanlarının etkin yönetilememesi,
- Kriz anı eylem planlarının oluşturulmaması nedeniyle olaylara zamanında müdahale edilememesi ve hizmetin kesintiye uğraması,
- Güncel yazılım ve donanım envanteri tutulmaması nedeniyle ihtiyaç fazlası alımların yapılması, kullanılmayan yazılım ve donanımların tespit edilememesi ve kaynakların etkin kullanılamaması,
- Veri tabanı yönetiminden sorumlu birim ile diğer birimler arasındaki iletişim problemleri nedeniyle sistem, uygulama ve donanım hatalarının kaynağının tespit edilememesi ve hizmetlerin aksaması,
- Kurumda, veri tabanı yönetiminden sorumlu birimin kontrolü dışında veri tabanı yönetimi yapılması nedeniyle mükerrer yatırımların olması, standart veri tabanı yönetimi sağlanamaması, kaynakların etkin kullanılmaması ve bilgi güvenliği açıklarının oluşması,
- Kurum veri tabanı standartlarının belirlenmemesi nedeniyle anlamsız isimlendirmelerin ve kısaltmaların oluşturulması, veri tabanı kullanıcılarına atanan rol ve sorumlulukların eksik veya fazla olması, veri tabanı yöneticisi ile uygulama geliştiricileri arasında anlaşmazlıkların yaşanması, veri tabanı güvenliğinin yeterli düzeyde sağlanamaması,

şeklinde belirlenebilir. İdari açıdan oluşabilecek muhtemel riskler sorumlu birim yönetimi, mevzuatı ve personeli hakkında bilgi edinildikten sonra güncellenmelidir.

Teknik riskler ise;

- Yedekleme stratejisinin belirlenmemesi nedeniyle eksik yedekleme alınması, yedekten veri kurtarma işleminin yapılamaması ve hizmetin kesintiye uğraması,
- Bakım planlarının (maintenance plan) tanımlanmaması nedeniyle veri tabanı sürekliliğinin sağlanamaması, performansının azalması ve veri kayıplarının yaşanması
- Her zaman çevrimiçi (always on) mimarisinin oluşturulmaması nedeniyle sunulan hizmetlerin kesintiye uğraması sonucunda imaj ve itibar kaybı yaşanması,
- Veri değişim kayıtlarının (log) standartlarının belirlenmemesi nedeniyle anlamlı olmayan kayıtların oluşması ve ihtiyaç duyulan kayıtların bulunmasında zaman kaybı yaşanması,
- Denetim kayıtlarının (audit log) tutulmaması nedeniyle veri tabanı üzerinde değişiklik yapan kullanıcıların tespit edilememesi ve bilgi güvenliği açıklarının oluşması,
- Gerçek zamanlı izlemenin (real-time monitoring) yapılmaması nedeniyle sistem sürekliliğinin ve güvenliğinin sağlanamaması,
- Kullanıcı erişim ve yetkilendirme kontrollerinin belirlenmemesi nedeniyle verilerin yetkisiz kişilerin eline geçmesi ve bilgi güvenliği açıklarının oluşması,

- Canlı (production), test ve geliştirme (development) ortamlarının birbirinden ayrı oluşturulmaması nedeniyle verilerin değiştirilmesi ve sorumlunun tespit edilmemesi,
- Test ve geliştirme ortamlarında gerçek verinin kullanılması nedeniyle veri sızıntılarının olması ve bilgi güvenliği açıklarının oluşması,

şeklinde sıralanabilir.

Belirlenen bu riskler denetim ekibi tarafından test edilerek varlığı, etki ve olasılıkları kontrol edilmelidir.

3.3. Saha Çalışması, Testler, Öneriler

Saha çalışmasında olması gereken durum ile mevcut durum arası farklar test edilmeli ve test sonuçlarından elde edilen bilgiler kayıt altına alınmalıdır. Testlerin uygulanması sonucu elde edilen bilgilerin; yeterli, güvenilir, ilgili, faydalı olması gerekir (Kamu İç Denetim Rehberi, 2013:55). Saha çalışması sonunda denetim ekibi test sonuçlarını incelemeli uygunsuzluk tespit ettiği durumları bulguya çevirerek gerekli önlemler veya düzeltmeler için öneri geliştirmelidir.

Saha çalışması sırasında uygulanacak testler; konusuna göre birebir görüşme, evrak inceleme veya teknik inceleme şeklinde olabilir. Saha çalışması öncesi belirlenmiş olası riskler için yapılacak test konuları dışına çıkılmamaya dikkat edilerek gerçekleştirilmeli ve net bilgiye ulaşılmaya çalışılmalıdır. Yapılan her test bir konuya özel olmalı ve çalışma kağıtlarına test içeriği kayıt edilmelidir. Denetim süresinin verimli kullanılması ve saha çalışmasının etkin planlanması için olası risklerin idari ve teknik olmak üzere iki kategoriye ayrılmasının uygun olacağı düşünülmektedir.

3.3.1. İdari Riskler

İdari risklerin etkisini kontrol için yapılacak testler, genel olarak görüşme ve evrak incelemesi şeklinde olmaktadır. Bu aşamada riskler ve etkileri incelenip olası senaryolar üzerinde durulacaktır.

İdari risklerin tespiti için, saha çalışması başlamadan önce kurumun mevzuatı incelenmeli ve veri tabanı yönetimi ile ilgili görevlerin hangi birime verildiği tespit edilmelidir. Bu birimlerin iş süreçleri incelenmeli ve yeterliliği kontrol edilmelidir. (Kamu Bilgi Teknolojileri Denetimi Rehberi, 2014:27). Kurum mevzuatında veri tabanı yönetimi ile ilgili görevlerin hangi birime verildiğinin belirlenmemiş olduğu tespit edilmişse, sürecin sorumlusunun net olarak belli olmadığı sonucu çıkarılarak bulgu olarak kaydedilmesi gerekir. Bu durum için veri tabanı yönetim süreci sorumluluğunun hangi birime verildiğinin açık şekilde belirlendiği mevzuat çalışması önerilmelidir.

Veri tabanı yönetim sürecinden sorumlu birim tespit edildikten sonra personel bazlı görevlendirmelerin olup olmadığı incelenmelidir. Yedekleme, bakım, gerçek zamanlı izleme gibi kritik işlerden sorumlu personelin tanımlı olması, kişi sayısı fazla olan birimlerde yönetimsel olarak kolaylık sağlayacağı gibi görev karmaşasının da önüne geçecektir. Görev tanımı yapılmış her personelin en az bir yedeğinin belirlenmiş olması iş sürekliliğini sağlama açısından önemlidir. Test esnasında personel görevlendirmelerinin yazılı olarak varlığı incelenmeli, var olduğu görülse dahi görevlendirilmiş personelin görevlerini bilip bilmediği ve görevlendirmesi kapsamında yaptığı çalışmalar sorgulanmalıdır. Görev tanımlarının ve personel yedeklerinin olmadığı tespit edildiğinde, gerekli düzenlemelerin yapılarak personele tebliğ edilmesi önerilmelidir.

Görevler ayrılığı ISO 27001:2013 standardında "*Kuruluşun varlıklarının yetkisiz veya farkında olmadan değiştirilme ya da kötüye kullanılma fırsatlarını azaltmak için, görevler ve sorumluluk alanları ayrılmalıdır.*", Kamu İç Kontrol Standartlarında ise *"Hata, eksiklik, yanlışlık, usulsüzlük ve yolsuzluk risklerini azaltmak için faaliyetler ile mali karar ve işlemlerin onaylanması, uygulanması, kaydedilmesi ve kontrol edilmesi görevleri personel arasında paylaştırılmalıdır.*" şeklinde düzenlenmiştir (Kamu İç Kontrol Standartları, 2007:9). Saha çalışması sırasında düzenlemelerle birimlere ve kişilere tanımlanmış görevlerin uygulamada gerçekleştirilip gerçekleştirilmediği incelenmelidir. Birimlerin tanımlanmış görevlerini yerine getirmediği, sözlü talimatlarla görevi olmadığı halde başka birime tanımlı görevleri ifa ettiği tespit edildiğinde ya görev tanımlarında değişiklik yapılması ya da yerine getirilen görevin ilgili birime devredilmesi önerilmelidir.

Gelişen teknoloji ve hemen her alanda bilgisayar kullanımı, emek yoğun üretimden otomasyona geçişin hızlanması, birçok alanda uzmanlaşmanın öneminin artması ve insan ihtiyaç ve beklentilerindeki değişim,

yeni bazı işlerin ve meslek alanlarının doğmasına yol açmaktadır. (Köklü, 2018:121) Veri tabanı yönetimi de oldukça teknik ve uzmanlık gerektiren bir konudur. Kamu kurumlarının günümüzde özellikle bilişim alanında hizmet alımı veya sözleşmeyle teknik personel çalıştırdığı bilinmektedir. Bu yöntemlerle veri tabanı yöneticisi olarak istihdam edilecek kişilerin yetkinlikleri tam olmalıdır. Kamu kurumlarının veri tabanı yöneticilerini hizmet alımı veya sözleşme yöntemiyle istihdam etmesinin başlıca sebebinin, bu süreci yönetecek kamu personelinin bulunmaması ve uzman personel ihtiyacı olduğu unutulmamalıdır. Test esnasında bu yöntemle istihdam edilmiş personelin işe alım kriterleri, eğitim durumu, uzmanlık alanıyla ilgili sertifikaları, geçmişte çalıştığı projeler, etik sözleşmesi ve kurum tarafından bedeli ödenmiş eğitim alıp almadığı incelenmelidir. Bu yöntemle alınacak veri tabanı yöneticisi alım kriterlerinde eksiklik olması durumunda ulusal mesleki yeterlilik standardında belirtilen veri tabanı yöneticisi kriterlerine uyulması önerilmelidir.

Kamu personeli olup veri tabanı yönetimiyle görevlendirilmiş personelin yetkinliği kritik öneme sahiptir. Her ne kadar günümüzde kamu kurumları bilişim alanında sözleşmeli ve hizmet alımıyla personel çalıştırmayı tercih etseler de bu yöntemin kalıcı çözüm üretmeyeceği aşikârdır. Sözleşmesi sona eren personelin kurumda çalışmaya devam etmesi kesin olmayıp, veri tabanı yönetimi gibi kritik bir görevin sadece hizmet alım yöntemiyle sürdürülmesi bilgi güvenliği açısından düşünülemez.Personel bulma ve seçme sürecinde hangi teknik kullanılırsa kullanılsın, işe tam uyumlu hazır bir çalışan bulmak oldukça güçtür. Bu zorluğun getirdiği eksiklikleri gidermenin en iyi yolu eğitimdir. (Muradova, 2007:77) Kamu kurumlarında çalışan personeller arasında da veri tabanı yöneticisi olarak çalıştırılacak yetkinlikte personel bulmak zordur. Veri tabanı yöneticisi olarak çalışan personel mevcudiyeti ve yetkinliği incelenmeli, mevcut değilse görevlendirilmesi, yetkinliği ile ilgili problem varsa kurumun kullandığı veri tabanı sistemiyle ilgili eğitim aldırılması önerilmelidir.

Günümüzde kamu kurumları bilişim hizmetleri vatandaş odaklı geliştirilmektedir. E-devlet uygulamaları ile vatandaşlara 24 saat kesintisiz hizmet verme politikası yürütülmektedir. Bu politika, veri tabanlarının 24 saat hizmet vermesi zorunluluğunu ortaya çıkarmaktadır. Bu sebeple veri tabanlarında oluşabilecek hatalar vatandaşa ve paydaş kurumlara yapılan paylaşımın aksaması yanında, kurum tarafından verilen hizmetlerde de aksamaya yol açacağından kriz durumunun oluşmasına neden olacaktır. Bilgi teknolojileri hizmetlerinde oluşan beklenmedik kesintiler veya hizmet kalitesinin düşmesine sebep olacak durumlar "olay" olarak değerlendirilmektedir. (Kamu Bilgi Teknolojileri Denetimi Rehberi, 2014:129). Olay anlarında yapılacak işlemlerin önceden planlanması ve görevli personelin belirlenmesi gerekmektedir. Bu durumunun ne zaman olabileceği tahmin edilemeyeceğinden 24 saat esasına göre olay yönetim planı oluşturulmalıdır. Saha çalışması sırasında olay yönetim planının olup olmadığı ve uygulanabilirliği incelenmelidir. Olay yönetimi planı içinde görevlerin net tanımlanması ve müdahale edecek personelin belirlenmesi, mesai saatleri dışında oluşabilecek kriz anları için müdahale edecek personelin nöbet sistemi oluşturularak haftalık veya aylık dönüşümlü görevlendirilmesi önerilmelidir.

Bilgi teknolojileri ürünleri kuruma maddi olarak büyük yük getirmektedir. Kamu kurumları ihtiyaç duydukları kaynakları belirleme konusunda dikkatli davranmalıdır. Kaynak ihtiyaçlarının tespiti mevcut varlıkların iyi yönetilmesi ile mümkün olabilir. Veri tabanı yönetim sürecinde kullanılan sunucular, veri tabanı güvenlik duvarları (database firewall), depolama üniteleri (storage), yedekleme üniteleri (backup device), ağ araçları (network tools), yazılım lisansları ve kullanım durumları kayıt altına alınmalıdır. Bu kontrol sayesinde kaynak ihtiyaçlarının belirlenmesi daha verimli hale getirilmiş olacaktır. Veri tabanı yönetiminden sorumlu birimlerin envanterinin düzenli tutulup tutulmadığı ve güncelliği incelenmelidir. Mevcut veya güncel olmaması halinde kaynakların etkin kullanımı için donanım ve yazılım envanterinin takip edilebileceği *(lisans, versiyon, garanti süresi, teknik özellik, kaynak kodları, sorumlu personel, IP, marka, model vb. kriterleri içeren*) bir uygulama geliştirilmesi veya temin edilmesi ve envantere eklenecek veya envanterden çıkarılacak yazılım ve donanımların anlık olarak güncellemesinin sağlanması önerilmelidir.

Yaptıkları işin mahiyeti itibariyle farklılık gösteren birimler birbirlerinden bağımsız olarak çalışmalı ve yetki ve sorumlulukları net olarak tanımlanmalıdır.

(Koçel , 1982:237).Yazılım geliştirme, veri tabanı yönetimi, bilgi güvenliği ve sistem yönetimi süreçleri görevler ayrılığı ilkesine uyularak farklı birimlerde yönetilmeli ve bu süreçlerin birbirleri ile olan ilişkisinden dolayı birimlerin yatay iletişiminde aksama yaşanmamalıdır. Bilgi işlem hizmeti tüm bu süreçlerin koordineli şekilde çalışmasıyla verimli yönetilebilir. Veri tabanı yönetimi ile ilgili birim denetlenirken diğer birimlerle de görüşülmeli, birimler arası yaşanan problemler tespit edilmelidir. Tespit edilen problemlerin içeriğine göre bağlı oldukları üst yöneticiye bilgi verilip, her birimin görevi dikkate alınarak iletişim yollarını kolaylaştırıcı, resmi yazışmaların en aza indirilip kurumsal eposta yoluyla veya kurulacak bir sistemle isteklerin elektronik ortamda alındığı, cevaplandığı ve kaydedildiği bir sistemin kullanılması önerilmelidir.

Kamu kurumlarında bilgi işlem birimleri yardımcı hizmetler olarak tanımlanmaktadır. Kurumun asli görevlerine yardımcı olacak şekilde bilgi teknolojileri altyapısını oluşturmakla görevlendirilmiştir. Kurumların asli görevlerini yerine getiren birimler günümüz teknolojilerine ayak uydurmak, vatandaşa daha iyi hizmet sunmak amacıyla bilgi teknolojileri projeleri üretebilmektedir. Bazı durumlarda üretilen bu projeler hizmet alımı yöntemleri kullanılarak temin edilmekte, bilgi işlem birimlerinin bilgisi olmadan kurum içinde farklı yerlerde veri tabanı yönetimi yapılabilmektedir. Bu durum kaynakların verimli kullanılmasına engel olmaktadır. Farklı birimlerde bulunan veri tabanları, merkezi veri tabanları için oluşturulan yedekleme, bakım, kriz (olay) yönetimi, kapasite ihtiyaç tespiti gibi stratejilerden faydalanamamaktadır. Kurumda kullanılan tüm uygulamaların tespit edilmesi ve veri tabanlarının yönetiminin veri tabanı yönetim birimine alınmasının sağlanması, bundan sonra geliştirilecek uygulamalarda merkezi veri tabanı altyapısının kullanılmasını zorlayıcı önlemler alınması önerilmelidir.

Kamu kurumlarında süreçlerin standartlarının konulmaması ve dokümantasyonunun yapılmaması, kişi bağımlılığı yaratmakta ve sonucunda yönetim riski oluşmaktadır. Personel bağımlılığı olan işler kişiyle özdeşleşerek başkası tarafından yürütülemeyecek duruma gelebilmektedir. "Standartlar ve prosedürler, süreçler üzerinde daha fazla kontrol sahibi olmanızı sağlar. Tasarım kararları için oluşturulacak yönergeler ile uygulama ve veri tabanı tasarımında verimlilik artar. Açıkça tanımlanmış sorumluluklar sayesinde uygulama geliştiricileri ve veri tabanı yöneticileri arasındaki iletişim gelişir. İşletim prosedürleri ile işlemlerde güvenilirlik artar." ("Standards and procedures", t.y.). Riskin bulguya dönüşmesi halinde veri tabanı yönetim süreci için kurum standartlarının (isimlendirme, kullanıcı, dokümantasyon, teknoloji standartları gibi) oluşturulması önerilmelidir.

3.3.2. Teknik Riskler

Teknik risklerin etkisini kontrol için yapılacak testler, genel olarak görüşme, teknik inceleme ve yerinde izleme şeklinde olmaktadır. Bu yöntemlerin uygulanması aşağıda detaylandırılmaktadır.

Bilgi sistemlerinin erişilebilir olmasını sağlayan profesyoneller tarafından, veri depolama alanlarının her an güncel bilgi ile kullanıcıyı buluşturması noktasında üstlenilen kritik sorumluluk; aktif olarak hizmet veren cihazların altyapı yedekliliği ve yeterliliğinin yanı sıra veri yedekliliğinin de düzenli olarak yapılması ve gerektiğinde en kısa sürede hizmete sunulmasını zorunlu kılmaktadır (Henkoğlu ve Yılmaz, 2013:456). Bu nedenle veri tabanları için yedekleme ve bakım stratejileri kritik öneme sahiptir. İlişkisel veri tabanı yönetiminde yedekleme tam (full backup), fark (differential backup) ve işlem (transactional backup) yedeklemesi olarak üç ana başlık altında toplanmaktadır. Veri tabanı yöneticisi, yönettiği veri tabanının kritikliğine, boyutuna ve sakladığı veriye ilişkin yasal mevzuatına göre yedekleme periyotlarını ve yedeklerin saklanma süresini belirlemelidir. Otomatik yedekleme görevleri günlük olarak kontrol edilmeli, belirli periyotlarla yedekten geri dönüş testleri yapılıp kayıt altına alınmalıdır. Saha çalışması sırasında yedekleme stratejisi incelenmeli, geçmişe dönük yedekleme görevlerinin başarıya ulaşıp ulaşmadığı ve yedekten geri dönüş testlerinin kayıtları kontrol edilmelidir. Yedekleme için kullanılan yedekleme üniteleri belirli periyotlarda kapasite ve hatalara karşı kontrol edilmeli, zamanlanmış yedekleme planlarının doğru çalışıp çalışmadığı günlük olarak izlenmeli ve yedeklerin büyüklüğü ve kritikliği göz önüne alınarak yedekten geri dönüş testleri yapılmalıdır. Yedekleme stratejisinin tüm veri tabanlarını kapsayacak şekilde oluşturulması ve yedekten geri dönüş testlerinin rutin

olarak yapılması ve kayıt altına alınmasının talimatlandırılarak yazılı hale getirilmesi önerilmelidir.

Bakım planları (maintenance plan) veri tabanlarının performansı açısından kritik öneme sahiptir.Bakım planları, veri tabanı kritiklik, büyüklük ve kullanım sıklığı gibi kriterler göz önünde bulundurularak yapılmalıdır. Özellikle anlık işlem (transaction) sayısı fazla olan uygulamalarda veya kayıt sayısı fazla olan tablolardan sorgulama yapılırken performans kayıpları, darboğazlar veya sistem çökmeleri yaşanmaması açısından bakım planları önem arz etmektedir.Bakım planları için oluşturulan otomatik görevler, uygulamaların aktif kullanıldığı saatler dışında çalışacak şekilde ayarlanmalıdır. Özellikle ilişkisel veri tabanı kullanan kurumlarda indeks ve istatistiklerin yeniden oluşturulması, bakımları sistemi yormayacak zamanlarda planlanıp uygulanmalıdır. Bakım stratejisinin tüm veri tabanlarını kapsayacak şekilde oluşturulması ve talimatlandırılarak yazılı hale getirilmesi önerilmelidir.

Her zaman çevrimiçi (Always on) mimarisi, aktif çalışan veri tabanlarının plan dışı durması sonucu, kendisiyle eş zamanlı (senkron) çalışan ikinci bir sunucunun devreye girip sistem devamlılığının sağlanması için kullanılmaktadır. İşletim sistemi bazlı olabileceği gibi veri tabanı sunucusu bazlı olarak da kurgulanabilir. Veri tabanını kullanan uygulamaların teknolojik bağımlılıkları da dikkate alınarak otomatik yük devretme (automatic failover) tasarımın içine dahil edilebilir. Her zaman çevrimiçi mimarisi kurumun ihtiyaçları doğrultusunda tasarlanmalı kaynak israfına sebep olmamalı ve belirli periyotlarla birincil sunucu değiştirme testleri yapılmalıdır. Saha çalışmasında her zaman çevrimiçi mimarisinin varlığı sorgulanmalı, yoksa önerilmeli, varsa yük devretme (failover) testlerinin kayıt altına alınması, sistemlerin kritikliğine göre otomatik yük devretme fonksiyonlarının aktifleştirilmesi önerilmelidir.

Günümüz veri tabanı yönetim sistemlerinde bilginin bütünlüğünü korumak ve yetkisiz değişimini tespit etmek için log (kayıt) tutulmaktadır. Veri tabanı içerisinde saklanan verilerin uygulama içinden değiştirilmesi veya silinmesi kayıtlarını uygulamanın kendisi yapması gerekmektedir. Bu kapsamda veri tabanı yönetimine düşen bir görev olmadığı görülse de kurum içinde birçok farklı uygulama olduğu düşünüldüğünde ve bu uygulamaları geliştiren firma veya yazılım geliştiricilerin farklı olmasından dolayı kayıt tutma tasarımları farklı olacaktır. Kamu kurumları bu kayıtlara çoğunlukla adli makamlardan gelen sorular üzerine ulaşmakta ve doğru bilgiyi vermek zorundadır. Bu kapsamda kayıtların (loglar) merkezi bir kayıt sisteminde bulundurulması veya veri tabanı yönetimi tarafından standartlaştırılmış bir formatta tutulması gerekmektedir. Kurumun merkezileştirilmiş veya standartlaştırılmış bir kayıt tutma mekanizması olup olmadığı sorgulanmalı, yok ise kayıtlar için bir standart oluşturulması, kayıt altına alınması gereken asgari verilerin (tarih, ip, sorgu, kullanıcı gibi) belirlenmesi ve yeni geliştirilecek uygulamalarda belirlenen standartlara uyulmasının sağlanması önerilmelidir.

Veri tabanı içinde saklanan verilerin değişimi için tutulan kayıtlardan (log) daha önce bahsedilmişti. Bir diğer değişim izleme mekanizması ise denetim (audit) kayıtlarıdır. Denetim kayıtları (auditing) seçili veri tabanları üzerinde yapılan işlemleri izleme ve kaydetme sistemidir. (Oracle, 2019). Daha önce açıklanan McCumber Bilgi Güvenliği Modeli'ne göre bilginin üç temel unsurundan biri olan bütünlük verinin yetkisiz kişilerce değiştirilmesidir. Veritabanı üzerinde yapılan mimari değişiklikler, tanımlanan veya silinen görevler (job), tanımlanan, silinen veya yetkilendirilen kullanıcılar denetim kayıtlarıyla saklanmalıdır. Bu sayede veri tabanı üzerinde yapılan tüm değişiklik işlemleri kayıt altına alınmış olur. Saha çalışması sırasında denetim kayıtları (audit) saklama stratejileri incelenmelidir. Tüm veri tabanları için sunucu tarafı değişim işlemleri, kullanıcı değişim işlemleri, veri tabanları için oluşturma (CREATE), değiştirme (ALTER), silme (DROP) işlemleri ve başarısız giriş (FAILED_LOGIN) işlemlerinin kayıtlarının açılması önerilmelidir.

Veri tabanlarının güvenliğinin sağlanması ve sistemin sürekliliği açısından gerçek zamanlı izlemenin yapılması büyük öneme sahiptir. Gerçek zamanlı izleme yaparak iç ve dış kullanıcılar tarafından gelebilecek olan saldırılara karşı önlem alınmış olur. Ayrıca veri tabanı yönetim sisteminde gerçekleşebilecek olağandışı durumlar tespit edilerek sistemin devamlılığı sağlanmalı, sistemde meydana gelecek hatalar anlık olarak uyarı sistemi aracılığı ile veri tabanı yöneticilerine sms veya e-posta olarak bildirilmelidir. Veri tabanı sunucularının kullandığı depolama birimi

(disk), işlemci (cpu), bellek (ram) anlık takip edilmeli, eşik değerler belirlenmeli ve bu değerlerin aşılması durumunda alarm üretmelidir. Test esnasında böyle bir izleme ve uyarı sisteminin varlığı kontrol edilmeli varsa geçmişte ürettiği alarmlar incelenerek yeterliliği incelenmelidir. İzleme ve uyarı sistemi bulunmuyorsa kurumun ihtiyaçlarına ve sistemlerin kritiklik durumlarına göre izlenmesi gereken kaynaklar belirlenerek izleme sisteminin geliştirilmesi önerilmelidir.

Veri tabanları kurum içinde kullanılan tüm veriyi saklaması ve veri üzerinde değişiklik yapılabilmesi için tasarlanmıştır. Yetkilendirme, şifre ile erişim ve veri kriptolama işlemleri; bilgi gizliliğinin sağlanması için kullanılan başlıca yöntemlerdir (Henkoğlu ve Yılmaz, 2013:455). Verinin veya verinin içinde bulunduğu tablo (sql tabanlı) ya da dokümanın (no-sql tabanlı) yapısal olarak değiştirilmesi, belirlenmiş bir kimlik doğrulama (authentication) ve yetkilendirme (authorization) prosedürü aracılığı ile yapılmalıdır. Geliştirme, test ve uygulama ortamlarındaki yetkilendirme ve kimlik doğrulama kuralları ayrı ayrı belirlenmeli ve duyurulmalıdır. Geliştirme ortamlarında yazılım geliştiricilere geniş yetkiler verilebilirken test ve uygulama ortamlarında kısıtlı yetkiye izin verilmelidir. Bu kapsamda veri tabanları üzerinde erişim, okuma veya yazma izinleri olan tüm kullanıcılar incelenmeli bu yetkilerin neden verildiği araştırılmalıdır. Sistem yöneticisi yetkisine sahip kullanıcılar ayrıca incelenmeli gereksiz yetkilendirmelerin olup olmadığı kontrol edilmelidir. Varsayılan olarak tanımlanmış sistem yöneticisi kullanıcılarının (MSSQL için sa, PostgreSQL için postgres gibi) pasif hale getirilmesi, tüm kullanıcılar için (uygulama, yönetici, geliştirici vb.) parola politikası belirlenmesi ve sistemsel olarak uymaya zorlanması, tespit edilen gereksiz yetkili kullanıcıların silinmesi önerilmelidir.

Veri tabanı yönetiminde geliştirme, test ve uygulama veri tabanı ortamlarının birbirinden ayrılması ve etkin şekilde kullanılması önem arz etmektedir. Geliştirme ortamı yazılım geliştiricilerin kullandığı veri tabanı üzerinde, uygulamanın geliştirilmesi sırasında gerekli olacak her türlü tasarım ve mimari değişikliklerini yapabileceği fakat içerisinde gerçek verilerin bulunmayacağı ortamdır. Test ortamı, uygulamanın canlı olarak devreye alınmadan önce uygulama ortamıyla hemen hemen aynı özelliklere sahip sunucu içinde test edilmesine olanak sağlayacak, içerisinde gerçek verinin hiç bulunmadığı ya da sadece tanım tablolarının ve kritik olmayan verinin bulunabileceği ortamdır. Verilerin güvenliğini sağlamak üzere test ortamında yazılım geliştirici ve uygulama kullanıcısı kısıtlı yetkiye sahip olmalıdır. Uygulama ortamı ise tüm güvenlik önlemlerinin alındığı, uygulama kullanıcısına sadece gerektiği kadar yetki verilen, yazılım geliştirici kullanıcısına ise yetki verilmemiş canlı ortamı ifade etmektedir. Kaynak planlaması yapılırken geliştirme ortamı için yedekleme ve bakım hizmetleri göz ardı edilebilmektedir. Test ve uygulama ortamları için bakım ve yedekleme hizmetleri verilmelidir. Saha çalışması sırasında bahsedilen bu ortamların varlığı incelenmeli, yok ise nedenleri araştırılmalıdır. Özellikle geliştirme ve test ortamlarında kullanılan test verilerinin gerçek olup olmadığı kontrol edilmelidir. Uygulama ortamı için alınan güvenlik tedbirlerinin test ortamı için alınmaması, test ortamındaki yetkilendirmelerin uygulama ortamındaki yetkilendirmelerden farklı olması gibi nedenlerle test ortamında gerçek verinin bulunması bilginin gizliliği ilkesinin ihlali ile sonuçlanabilir. Ortamların yaratılması için gerekli maliyetlerde göz önünde bulundurularak kurumun ihtiyaçları doğrultusunda geliştirme, test ve canlı ortamların oluşturulması, canlı ortam hariç hiçbir ortamda gerçek verinin bulunmamasının sağlanması, her bir ortam için kullanıcı yetki standartlarının belirlenmesi önerilmelidir.

Yapılan testler sırasında kısa sürede müdahale edilerek düzeltilebilecek tespitler bulunması halinde tespit edilen durumun düzeltilmesi önerilmeli ve bu husus raporda belirtilmelidir.

3.4. İzleme

Denetimin en önemli aşamalarından biri olan izleme faaliyeti etkin bir şekilde uygulanmalıdır. Saha çalışması sırasında riskli alanlar için yapılan testler sonucunda oluşturulan ve denetlenen birim ile hemfikir olunan bulguları önlemek ve düzeltmek için geliştirilen öneriler için makul gerçekleştirme tarihleri belirlenmelidir. Denetlenen birim tarafından belirlenecek bu tarihler bulgunun risk seviyesi, denetlenen birimin kaynak durumu göz önüne alınarak oluşturulmalıdır.

Bulguyu bertaraf etmek için oluşturulmuş öneriler yerine getirilmiş ise bulgu kapatılmalıdır. Öneriler zamanında yerine getirilmemiş ise nedenleri araştırılmalı, yerine getirilmeme sebebinin zorunluluktan mı kaynaklı olduğu belirlenmelidir. Denetlenen birimin bulguyla ilgili yaptığı çalışmalar görülmüş ise süre uzatımı verilmelidir. Eğer denetlenen birimin öneri ile ilgili yaptığı veya devam eden bir çalışması yok ise ve ilave süre istememiş ise riskin denetlenen birim tarafından üstlenildiği ile ilgili bilgilendirme kendilerine ve üst yöneticiye yapılmalıdır. Risklerin belirlenmesi ve saha çalışmasında yapıldığı gibi izleme faaliyetinin de idari ve teknik olarak iki başlıkta yapılması halinde izlemenin daha etkin yürütülebileceği düşünülmektedir.

3.4.1 İdari Risklerin Oluşturduğu Bulguların İzlenmesi

Veri tabanı yönetiminden sorumlu birimin ve personel görevlerinin belirlenmesi konusundaki bulgular için gerekli mevzuat çalışmasının yapılıp yapılmadığı yazılı olarak istenmelidir. Konunun birim tarafından talimatlandırılmış veya bir mevzuata bağlanmış olmasına dikkat edilmesi gerekmektedir. Personel görevlerinin talimatlandırılmasının yanı sıra görevlendirilmiş personel ile konuşulmalı ve görevleri hakkında bilgisi olup olmadığı kontrol edilmelidir.

Mevzuat ile uygulama arasındaki farklardan doğan bulgularda, öncelikle uygulamadaki durumun mevzuata mı dönüştürüldüğü yoksa uygulamanın mevzuat hükümlerince yapılmasına mı karar verildiği bilgisi alınmalıdır. Mevzuat mevcut uygulamaya göre güncellenmiş ise doğruluğu kontrol edilmeli, uygulamanın mevzuata göre yapılacağı bilgisi alınmış ise personel mülakatı ve yerinde incelemeler ile durum kontrol edilmelidir. Veri tabanı yöneticileri ile yazılım geliştirme ekibinin ayrılması gibi görevler ayrılığı ilkesinin gerektirdiği durumlar kontrol edilmelidir. Birimler arası iletişim ile ilgili bulgular da bu kapsamda izlenerek iletişimin sağlıklı olup olmadığı ve hangi yollarla yapılmaya karar verildiği incelenmelidir. Seçilen yöntemlerin birimler arası iletişimde iyileşmeye yol açıp açmadığı belirlenmelidir.

Personel yetkinliği ve eğitimleri ile ilgili bulgularda, personel alım şartlarının değiştirilip değiştirilmediği, denetim sonrası istihdam edilen personelin yerleştirildiği pozisyona uygun olup olmadığı, eğitim ihtiyaçlarının tespit edilip planlamasının yapılıp yapılmadığının kontrol edilmesi gerekmektedir. İzleme sürecinden önce belirlenmiş konularda eğitim alınmışsa, eğitim ile ilgili dokümanlar incelenmeli, eğitim alan personelle görüşülüp eğitimin verimli olup olmadığı belirlenmelidir.

Olay yönetimi ile ilgili bulguların izlenmesinde olay anında yapılacakların yazılı hale getirilip getirilmediği, personelin olay anında yapması gerekenleri bilip bilmediği kontrol edilmelidir. Hazırlanan olay yönetim prosedürünün olası her durumu kapsayacak şekilde tasarlanmış olmasına dikkat edilmelidir. Daha önceki olay anlarının sebeplerinin ve alınan tedbirlerin kayıt altına alınıp alınmadığı, tekrar eden durumlarda yeni oluşturulan olay yönetim sürecinin etkin bir şekilde çözüm üretip üretmediği test edilmelidir.

Güncel envanter bilgisinin olmaması veya eksik olması ile ilgili bulgularda, envanter bilgisini tutmak için hangi yöntemin seçildiği tespit edilmelidir. Test amaçlı yeterli miktarda kayıt incelenmeli ve fiziksel olarak varlıkları tespit edilmelidir. Envanter kayıtlarının ne sıklıkla güncellendiği kontrol edilmelidir. Envanter bilgi sisteminin olmasının birime kattığı faydalar tespit edilmeli ve önemi vurgulanmalıdır.

Veri tabanı yönetimi ile ilgili birim haricinde başka birimlerce yönetilen veri tabanı olup olmadığı ile ilgili birimlerden bilgi istenip istenmediği, tespit edilmiş veri tabanlarının merkezi sisteme alınması ile ilgili çalışma ve ya planlama yapılıp yapılmadığı belirlenmelidir. Taşınamayacak veri tabanlarının neden taşınamayacağı ile ilgili sebepler incelenmelidir.

Veri tabanı standartlarının oluşturulmaması ile ilgili bulgular kritik öneme sahiptir. Standartların veri tabanı yönetiminin verimli ve etkin bir şekilde yürütülmesine zemin hazırlaması beklenir. Bu kapsamda oluşturulan standartlar incelenmeli bu standartların tüm kuruma tebliğ edilip edilmediği kontrol edilmelidir. Kurum içi bilgi teknolojileri projelerinde, veri tabanları için bu standartların kullanılması için yapılmış çalışmalar incelenmelidir.

3.4.2. Teknik Risklerin Oluşturduğu Bulguların İzlenmesi

Yedekleme ve bakım stratejileri ile ilgili bulgular izlenirken öncelikle konularla ilgili yazılı oluşturulmuş prosedürler incelenmelidir. Hangi aralıklarla ne tür yedekleme ve bakım yapılmasına karar verildiği incelenmeli ve mevcut durumla karşılaştırılmalıdır. Yedekleme ve bakım ile ilgili kullanılan veri tabanı yönetim sistemi yazılımında oluşturulmuş görevler incelenmeli, geçmişe yönelik hata kayıtları varsa sebepleri sorgulanmalıdır. Yedekten dönüş testlerinin yapıldığının kayıtları incelenmeli ve başarılı olduğu teyit edilmelidir.

Her zaman çevrim içi mimarisinin varlığı ve hangi veri tabanlarını kapsadığı izleme sırasında tespit edilmelidir. Her zaman çevrim içi mimarisi dışında kalan veri tabanlarının neden dışarıda bırakıldığı ile ilgili inceleme yapılmalıdır. Her zaman çevrim içi mimarisinde yük devretmenin (failover) hangi zamanlarda ve ne sebeple gerçekleştirildiği kayıtlarından incelenmeli ve bununla ilgili alınan önlemler sorgulanmalıdır. Rutin olarak yük devretme testlerinin yapılıp yapılmadığının kayıtları kontrol edilmelidir.

Veri değişim kayıtları (log) standartlarının oluşturulması izlenirken, log kayıtları içerisinde bulunması gereken veri tiplerinin neler olduğunun belirlenmiş olması ve bunun tüm yazılım geliştiricilere bildirilmiş olması kontrol edilmelidir. Standartların belirlenmesinden önce oluşturulmuş log kayıtlarının standart hale dönüştürülüp dönüştürülmediği, yeni veri tabanlarında ise log tablolarının standart halde olup olmadığı kontrol edilmelidir. Log kayıtları içinde arama yapıldığında ne sürede kayıtlara ulaşılabildiği test edilmeli, gerekli optimizasyon ve konsolidasyon işlemlerinin yapılıp yapılmadığı belirlenmelidir.

Denetim kayıtları (audit log) ile ilgili bulgular incelenirken kullanılan veri tabanı yönetim sistemi yazılımına göre sistem üzerinden hangi kayıtların açılmış olduğuna bakılmalıdır. Öneride belirlenen asgari denetim kayıt gruplarının varlığı kontrol edilmelidir. Hangi tarihten itibaren bu kayıtların tutulduğu ve olay görüntüleyicisi (event viewer) yardımıyla denetim kayıtlarının açıldığı tarihten itibaren kayıt almasını engelleyecek bir durum yaşanıp yaşanmadığı belirlemelidir.

Gerçek zamanlı izleme sisteminin incelenmesi iki başlık altında yapılmalıdır. Bunlardan ilki mesai saati içinde izleme, ikincisi ise mesai saati dışında izlemedir. Mesai saatleri içinde hangi yöntemle veri tabanlarını izledikleri belirlenmelidir. İzleme monitörlerinin varlığı, hangi kaynakları izledikleri (bellek, işlemci, depolama) ve olası bir olayı bu izleme sistemiyle tespit edip edemeyecekleri belirlenmelidir. Mesai dışı saatlerde uyarı sisteminin varlığı kontrol edilmelidir. SMS veya e posta gibi teknolojilerle oluşturulan uyarı sistemiyle olay anında müdahale edilip edilmediği ve mesai harici olan olaylara müdahale için personel belirlenip belirlenmediği incelenmelidir.

Kullanıcı erişim ve yetkilendirme ile ilgili bulgularda öncelikle veri tabanı yönetim sistemi uygulamalarında bulunan yönetici (admin) yetkili kullanıcılar tespit edilmelidir. Bu kullanıcıların gerçekten veri tabanı yöneticisi olduğu, kullanıcı adlarının tekil olduğu, ortak bir kullanıcı kullanarak sisteme yönetici olarak bağlanmadıkları belirlenmelidir. Sistem içinde varsayılan olarak tanımlı "sa", "postgres" gibi yönetici yetkili kullanıcıların pasif durumda olup olmadıkları kontrol edilmeli, parola karmaşıklık ve geçerlilik süreleri ile ilgili tanımlı kurallar incelenmeli, istisnai kullanıcı olup olmadığı belirlenmelidir. Uygulama kullanıcılarına ve kişisel kullanıcılara yetki verilmesi ve kullanıcı açılması ile ilgili prosedürlerin varlığı sorgulanmalı ve taleplerin kayıt altında tutulduğu belirlenmelidir.

Canlı, test ve geliştirme ortamları ile ilgili bulguların izlenmesine öncelikle tüm ortamların mevcut olup olmadığının kontrolü ile başlanmalıdır. Kaynak yetersizliği veya risk eşiğinin düşüklüğü gibi sebeplerden bazen geliştirme ve test ortamı birleştirilebilmektedir. Test ve geliştirme ortamındaki veriler incelenmeli, gerçek veri olup olmadığı kontrol edilmelidir. Canlı ve test ortamlarındaki kullanıcı yetkileri ayrı ayrı incelenmelidir. Canlı ortamda uygulama kullanıcısından başka yetkili kullanıcı olmadığı tespiti yapılmalıdır. Canlı ortamda yönetici yetkisine sahip uygulama kullanıcısı olup olmadığının kontrol edilmesi önemli görülmektedir.

4. SONUÇ VE ÖNERİLER

Kamu idarelerinde elektronik ortamdan kesintisiz olarak sunulan hizmetlerin sayısı gün geçtikçe artmakta olup, bu hizmetlerin devamlılığının ve güvenliğinin sağlanması da aynı şekilde önem kazanmaktadır. Bilgilerin elde edildiği veriler, veri tabanı yönetim

sistemleri araçlarıyla yönetilmektedir. Veri tabanı yönetim sistemleri büyük çaplı verileri saklama, değiştirme ve koruma gibi süreçleri kolaylaştırmaktadır. Bilgi teknolojileri denetim süreçlerinden biri olan veri tabanı yönetimi denetimi; standart veri tabanı yönetiminin hayata geçirilmesi, ilgili mevzuatlara, talimatlara, politika ve prosedürlere göre uygun hizmet verilmesinin sağlanması, varsa süreçte aksayan yönlerin geliştirilerek yürütülen çalışmalara değer katma prensibi amacıyla belirli periyotlarla gerçekleştirilmelidir. İç denetçiler veri tabanı yönetimi denetiminde idari riskleri belirlemede zorluk yaşamamasına rağmen teknik riskleri belirlemede zorluklar yaşayabilmektedir. Denetimlerin başarıyla sonuçlandırılabilmesi bakımından, denetim ekibi oluşturulurken bu husus göz önünde bulundurulmalıdır.

Denetim ile birlikte veri tabanları yönetiminin teknik ve idari kontrollerini geliştirmek için önemli öneriler ortaya çıkacaktır. Önerilerin gerçekleştirme tarihleri bulgunun risk seviyesi ve denetlenen birimin kaynak durumuna göre belirlenmelidir. Özellikle risk seviyesi yüksek teknik bulgular ile ilgili önerilerin gerçekleştirilme zamanı mümkün olduğunca kısa tutulmalı ve sonuçları yerinde incelenmelidir.

Denetim sürecinin aktörleri denetçiler, denetlenenler ve üst yönetimdir. Denetiminin istenilen makul güvenceyi sağlayabilmesi için tüm aktörlerin sürece katkı sağlaması gerekmektedir. Veri tabanı yönetimi uzmanlık gerektiren bir iş olduğundan, denetim ekibi içinde mutlaka teknik konudan anlayan bir denetçinin veya destek alınan bir dış uzmanın olması başarıyı artıracaktır. Denetlenen taraf denetimin, süreci iyileştirmek için yapıldığının farkında olmalı, denetim ekibi tarafından oluşturulan bulgular ve bu bulguların önerilerini makul sürede gerçekleştirmelidir. Üst yönetimin desteğini almak hem denetçiler hem de denetlenenler tarafından önemlidir. Denetçiler mevcut durumu, olması gereken durumu, bulguları ve önerileri üst yönetime aktarmalı ve farkındalık yaratmalıdır. Denetlenen taraf ise önerilerin gerçekleştirilmesi için uygulayacakları eylemleri üst yönetime doğru ve eksiksiz anlatmalı ve desteğini almalıdır.

Yönetimin onayı ile önerilerin uygulanması ve sürdürülmesi büyük önem arz etmektedir. Denetim sonucunda yasalara uyum, verinin korunması, standartların oluşturulması, yetkin personel istihdamı, sistem sürekliliği, kesintisiz hizmet sunulması, kaynakların etkin ve verimli kullanılması hususlarına ilişkin makul güvence sağlanmış olacaktır.

Kaynakça

De Haes, S., & Van Grembergen, W. (2006). Information Technology Governance Best Practices in Belgian Organisations. Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06). doi:10.1109/hicss.2006.222.

Henkoğlu T.,Yılmaz, B. (2013). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları. *Türk Kütüphaneciliği 27, 3 (2013)*, 451-471. Erişim adresi: http://www.bby.hacettepe.edu.tr/e-bulten/dosyalar/file/Eylul2013/henkoglu_yilmaz_tk.pdf.

Koçel T., (1982). *İşletme Yöneticiliği,* İstanbul: Beta Yayınları.

Köklü K. (2018). İşAnalizi, İş Analistliği ve İş Zekası. *Lectio Socialis*, *Volume 2, Issue 2*, 121-142 Erişim Adresi: http://dergipark.gov.tr/download/article-file/515874.

McCumber, J. (2005). *Assessing and managing security risk in IT systems.* Washington: CRC.

Muradova T. (2007). İnsan Kaynakları Yönetiminde Eğitim ve Geliştirmenin Önemi, *Khazar Journal Of Azerbaijani Studies, 10*(3-4), 75–84. Erişim Adresi :http://www.jhss-khazar.org/2009-12-2/INSAN%20KAYNAKLARI%20YONETIMINDE%20EGITIM%20VE%20GELISTIRMENIN%20ONEMI.pdf.

Oz E. (2008). *Management Information Systems* (6. bs.). Course Technology.

Prabhjot P., Sharma N. (2017). Overview of the Database Management System. *International Journal of Advanced Research in Computer Science,* Vol 8, No 4. Erişim adresi: http://www.ijarcs.info/index.php/Ijarcs/article/download/3778/3259.

Ramakrishnan R., Gehrke J. (2003). *Database Management Systems* (3. bs.). McGraw-Hill Education.

Sevim, A. (2005). "Veri Tabanı ve Yönetimi". *Muhasebe Bilgi Sistemi.* Ed. F. Sürmeli. Eskişehir: Açık Öğretim Fakültesi Yayınları no.860. 82-83.

Sevinç, İ. (2007). Kamu Kurumlarında Bilgi Teknolojileri Kullanımı Ve Bunların Çalışanların Fiziksel Ve Psikolojik Durumlarına Etkileri. *Journal of Knowledge Economy & Knowledge Management 2007,* (Volume II Spring), 21-31. Erişim Adresi:http://beykon.org/dergi/2007/I.Sevinc.doc.

İç Denetim Koordinasyon Kurulu. (2014). *Kamu Bilgi TeknolojileriDenetimiRehberi* (1. sürüm). Erişim adresi: http://www.idkk.gov.tr/SiteDokumanlari/Mevzuat/Ucuncul%20Duzey%20Mevzuat/KamuBTDenetimiRehberi/KamuBTDenetimiRehberi.pdf.

İç Denetim Koordinasyon Kurulu. (2014). *Kamu* İç *Denetim Rehberi* (1. sürüm). Erişim adresi: http://www.idkk.gov.tr/SiteDokumanlari/Mevzuat/Ucuncul%20Duzey%20Mevzuat/K%C4%B0DR_v1.0.pdf.

Kamu İç Kontrol Standartları Tebliği. (2007, 26 Aralık). *Resmi-Gazete (Sayı:26738).* Erişim adresi: http://www.resmigazete.gov.tr/eskiler/2007/12/20071226-21.htm.

TS ISO/IEC 27001:2013, Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Gereksinimler.

Types of database management system and their evolution. (2014, 24 Kasım). Erişim adresi: https://www.analyticsvidhya.com/blog/2014/11/types-databases-evolution/.

Veritabanı. (2018). ISACA terimler sözlüğünde. Erişim adresi: https://www.isaca.org/About-ISACA/History/Documents/ISACA-Glossary-English-Turkish_mis_Tur_0418.pdf.

İnternet Kaynakları

Bilgi. (t.y.). Türk Dil Kurumu Türkçe Sözlük. Erişim adresi: http://www.tdk.gov.tr/index.php? option=com_gts&view=gts (Erişim Tarihi:20 Aralık 2018).

NoSQL Nedir?. (t.y.). Erişim adresi: https://aws.amazon.com/tr/nosql/ (Erişim Tarihi:09 Ocak 2019).

Oracle (2019), Database Auditing: Security Considerations. Erişim adresi: https://docs.oracle.com/cd/B19306_01/network.102/b14266/auditing.htm#CHDJBDHJ (Erişim Tarihi: 01 Şubat 2019).

SimpliLearn. (2019, Nisan). Introduction to NoSQL databases Tutorial. Erişim adresi: https://www.simplilearn.com/introduction-to-nosql-databases-tutorial-video (Erişim Tarihi:03 Nisan 2019).

Standards and procedures for database systems. (t.y.). Erişim adresi:https://www.ibm.com/support/knowledgecenter/en/SSEPH2_15.1.0/com.ibm.ims15.doc.dag/ims_dbsystemstds.htm (Erişim Tarihi: 02 Nisan 2019).

Unipedi (2014, Ocak).İlişkisel Veritabanı. Erişim adresi:http://www.unipedi.com/teknoloji/tag/iliskisel-veritabani-ozellikleri/ (Erişim Tarihi:04 Ocak 2019).

What is a Relational Database Management System?. (t.y.). Erişim adresi: https://www.codecademy.com/articles/what-is-rdbms-sql (Erişim Tarihi:21 Ocak 2019).

BLOKZİNCİR TEKNOLOJİSİNİN İÇ DENETİM FAALİYETLERİNE ETKİLERİ: FIRSATLAR VE TEHDİTLER

(BLOCKCHAIN TECHNOLOGY AND ITS IMPACTS ON THE INTERNAL AUDIT ACTIVITIES: OPPORTUNITIES AND THREATS)

Çetin KARAHAN* / Aslıhan TÜFEKCİ**

ÖZ

Blokzincir henüz yasal düzenlemeleri ve standartları net biçimde ortaya konulmamış olmakla birlikte tüm dünyada hızla gelişen, hem kamu hem de özel sektör tarafından yakından izlenen ve mevcut iş süreçlerinde köklü değişikliklere sebep olması beklenen bir teknolojidir. 2008 yılında ilk ortaya çıkmasından bu yana uygulama sahası sürekli olarak genişleyen bu teknolojinin ortaya koyduğu dönüşümün iç denetimin temel fonksiyonları olan denetim ve danışmanlık faaliyetlerini de etkilemesi öngörülmektedir. Teknolojinin sunmuş olduğu işlem şeffaflığı, silinmesi ya da değiştirilmesi mümkün olmayan işlem kayıtları, güvenilir bir üçüncü taraf onayı ya da kontrolü olmadan işlem gerçekleştirme gibi özellikler ve sürekli denetime çok uygun altyapısı en önemli avantajlar olarak öne çıkmaktadır. Bunun yanında yönetişim yapısının karmaşıklığı, teknolojinin anlaşılmasının güçlüğü, denetime olan bağımlılığı azaltma potansiyeli, mevcut sistemlerle entegrasyon problemleri ve yetersiz insan kaynağı gibi konular da riskli alanlar olarak değerlendirilmektedir. İç denetim faaliyetleri ve iç denetçi nitelikleri bakımından bu teknolojinin sunduğu fırsatlardan azami düzeyde faydalanmak, riskleri de olabildiğince iyi yönetmek için iç denetçilerin blokzincir teknolojisi konusunda yeterli düzeyde bilgi sahibi olmaları, dönüşüm sürecinde aktif rol alarak başlangıç aşamasında gerekli kontrollerin tasarlanmasına yardımcı olmaları kritik öneme sahiptir.

Blokzincir teknolojisinin teknik altyapısı, kullanım alanları, avantaj ve dezavantajları, mevcut süreç ve sektörlere potansiyel etkileri gibi birçok konuda çok sayıda çalışma olmasına karşın teknolojinin denetim mesleğine etkileri konusundaki çalışma sayısı kısıtlı ve daha çok muhasebe denetimleri odaklıdır. Bu çalışmada, kısıtlı sayıdaki bu çalışmalarla birlikte blokzincir teknolojisinin temel özelliklerinden bahsedilerek denetim mesleğine potansiyel etkileri konusunda daha geniş bir perspektif sunulması hedeflenmektedir.

Anahtar Kelimeler: Blokzincir, iç denetim, dağıtık kayıt defteri

JEL Kodlaması: H83, M42, O30.

ABSTRACT

Though the technical and legal regulations and international standards were not clearly defined yet, blockchain is a rapidly developing technology throughout the world. Both public and private sector are in hot pursuit of this newly emerging technology and it is expected to create radical changes in existing business processes. The transformation caused by this technology which has a consistantly expanding field of application since the first emergence in 2008, is predicted to affect the fundamental functions of internal auditing: audit and consulting. The most outstanding advantages of this technology are transparency, immutability, eliminating intermediaries and the favorable infrastructure for continuous auditing. Besides these advantages, it has some shortcomings such as the complexity of governance structure, difficulty in understanding the concept, the potential for diminishing the dependancy on the audit, problems in integration with the existing systems and insufficient resources of talent. It is so critical for internal auditors to have adequate knowledge on blockchain technology for taking the maximum advantages of the opportunities offered by this technology and for managing the risks as proper as possible. Another critical action is taking an active role in the transformation process for especially facilitating control design.

There are many researches on some specific topics of blockchain technology such as technical infrastructure of blockchain, use cases, advantages and disadvantages, potential impacts on existing business processes and sectors but the researches about the potential impacts on audit profession are very limited and mostly focused on accounting. In this paper, it is aimed to provide a wider perspective on the potential impacts of blockchain technology to the audit activities while referencing these limited researches and with the basic characteristics of blockchain.

Keywords: *Blockchain, internal audit, distributed ledger*

JEL Classification: *H83, M42, O30.*

*) İç Denetçi (CISA), T.C. Cumhurbaşkanlığı, Savunma Sanayii Başkanlığı, Ankara, Orcid:0000-0002-8697-9162, ckarahan@ssb.gov.tr

**) Doç. Dr., Enstitü Müdürü, Gazi Üniversitesi, Bilişim Enstitüsü, Ankara, Orcid:0000-0002-8669-276X, asli@gazi.edu.tr

Yazı Gönderim Tarihi: 03.04.2019, Yazı Kabul Tarihi: 10.04.2019

1. GİRİŞ

Denetim mesleğinde teknolojik yeniliklerin kullanımı günümüzde hızla artmaktadır. 1970'lere kadar kağıt, kalem ve hesap makinasından faydalanılıyorken günümüzde artık veri madenciliği, veri analitiği, sürekli risk izleme ve değerlendirme, blokzincir, yapay zeka gibi teknolojiler iç denetimde kullanılmaya başlanmıştır (Dai, 2017, s. 2).

Blokzincir teknolojisi ilk olarak 1 Kasım 2008 tarihinde, kriptografi, programlama ve matematik gibi konularda bilgi paylaşımları ve tartışmaların yürütüldüğü bir e-posta grubuna Satoshi Nakamoto takma adını kullanan bir üye tarafından gönderilen 'Bitcoin: Eşten-eşe Elektronik Nakit Ödeme Sistemi' başlıklı bir makale ile adını duyurmuştur. Aslında bu makalede blokzincir ifadesi doğrudan geçmemekte olup sistem tarif edilirken işlemlerin kaydedildiği yapı blok olarak, onaylanan her bir bloğun özel bir algoritma ile birbirine eklenmesi ise zincir olarak ifade edilmiş, blokzincir ifadesi daha sonra kullanılmaya başlanmıştır.

Son yıllarda gittikçe popülerliği ve bilinirliği artmakla birlikte henüz tam olarak potansiyeli ortaya çıkmamış olan blokzincir, ilk ortaya çıkmasının üzerinden on yılı aşkın bir süre geçmiş olmasına karşın henüz geniş kabul görmüş, üzerinde uzlaşılmış standartları bulunan ve kendini tam olarak ispatlamış bir teknoloji değildir. Bununla birlikte, çok da uzak olmayan bir gelecekte finans başta olmak üzere birçok sektörü ve kamu tarafından sunulan hizmetleri derinden etkileyeceği konusunda artık çok da fazla şüphe kalmamıştır. Uygulama alanı ve araştırma konuları çok hızlı bir şekilde genişleyen blokzincir teknolojisi hem özel hem de kamu sektörü için yıkıcı bir teknoloji olarak nitelendirilmektedir. Kuşkusuz ki iç denetim faaliyetleri de bu değişim ve dönüşümden etkilenecek, teknolojinin iç denetim mesleğine olumlu ve olumsuz bazı yansımaları olacaktır.

Blokzincir teknolojisinin yakın gelecekte birçok sektörü etkilemesi, günümüzdeki birçok iş alanının ortadan kalkmasına ya da dönüşmesine sebep olması öngörülmekte olup bu nedenle de yıkıcı bir teknoloji olarak adlandırılmaktadır. Dünya üzerinde birçok devlet, uluslararası kuruluş ve özel sektör temsilcisi bu teknolojinin doğrulanması ve uygulanması için çalışmalar yürütmekte olup bazı ülkeler gerçek hayat uygulamalarında bu teknolojiyi kullanmaya başlamışlardır.

Blokzincir teknolojisi, diğer sektörlerin yanı sıra muhasebe sektöründe de artan bir ilgi görmektedir. PwC bu teknolojiyi mevcut uygulamaları değiştirecek yeni nesil iş süreci geliştirme yazılımı olarak görmekte, Deloitte blokzincirin bireylerle işletmeler arasındaki işbirliğini, süreçlerin şeffaflığını büyük oranda artıracağını, bunun sonucunda da ekonominin verimliliği ve sürdürülebilirliğini geliştireceğini tahmin etmektedir (Dai, 2017, s. 59, 60).

Blokzincir teknolojisi ve iç denetim faaliyetlerine etkileri konusunda yapılmış olan akademik çalışmalar oldukça kısıtlı olup mevcut çalışmalar genel olarak muhasebe denetimleri ve mali denetimlere odaklanmıştır. Brender ve diğerleri (2018) blokzincir teknolojisinin yıkıcı etkileri konusundaki tartışmalarda denetim ve kontrol mesleklerinin pek ön plana çıkmadığını vurgulayarak bu teknolojinin denetim mesleği konusundaki yıkıcı etkisinin tam olarak öngörülemediği, daha küçük ölçekli denetim firmalarının ortaya çıkacak değişime ayak uydurabilmek için bir hazırlık yapmadıkları bulgularına ulaşmışlar, mesleğin muhasebeden daha çok Bilgi Teknolojileri (BT) alanına yöneleceğini ve denetçi profilinin değişmesinin beklendiğini belirtmişlerdir.

Birçok sektörde blokzincir teknolojisinin pilot uygulamaları geliştirilmiş ve teknolojinin kullanım senaryoları tartışılmış olmakla birlikte denetim alanındaki potansiyel katkıları henüz tam olarak değerlendirilmemiştir (Dai, 2017, s. 60).

2. BLOKZİNCİR TEKNOLOJİSİ

2008 yılındaki mali krizden sonraki Acil Ekonomik İstikrar Yasasının Amerikan mali sistemini çökmekten kurtardığı dönemde ortaya çıkan Bitcoin ile tarihte ilk defa maliyetli bir aracıya gereksinim duyulmadan birbirinden uzak ve birbirine güven duymayan iki taraf arasında güvenilir bir biçimde değer transferi gerçekleşmiştir (Catalini ve Gans, 2017, s. 1). Blokzincir, dijital bir varlık olan kripto para birimi Bitcoin'in temelini oluşturan teknolojidir.

Blokzincir teknolojisi için bankasız para, yöneticisiz şirket, politikacısız ülke benzetmesi yapılmaktadır

(Voshmgir, 2017). İlk ve en bilinen uygulaması Bitcoin olduğundan uzunca bir süre blokzincir sadece kripto paralarla ilgili bir terim olarak algılanmış, ancak zamanla algoritmanın içinde barındırdığı muazzam potansiyel fark edilmeye başlanmıştır. Satoshi Nakamoto (2008) bu sistemi herhangi bir finansal kuruluşun aracılığına ihtiyaç duyulmadan iki taraf arasında çevrim içi ödemeyi mümkün kılan tamamen eşten eşe bir elektronik para olarak tanımlamış, dijital imzanın bu sistemin bir parçası olduğunu, arada güvenilir bir üçüncü taraf olmadan birbirlerini tanımayan ve hatta birbirlerine güvenmeyen tarafların ihtiyaç duydukları güven mekanizmasının kriptografi ile sağlandığını, mükerrer harcama probleminin işlemleri kronolojik olarak sıralayan bir zaman damgası kullanılarak giderildiğini, kaydedilen işlemlerin geri döndürülmesinin hemen hemen imkansız olduğunu belirterek CoinMarketCap'ın 01.04.2019 tarihli verilerine göre (CoinMarketCap, 2019) toplam piyasa değeri yaklaşık 370 milyar dolar olan kripto para pazarının temelini atan sistemin teknik detaylarını 8 sayfalık makalesinde açıklamıştır.

Blokzincir teknolojisinin üzerinde uzlaşılmış tek bir tanımı bulunmamakla birlikte en temel ifadeyle tek bir kişi ya da kuruluşun kontrolünde olmayan, düğüm adı verilen çok sayıda bilgisayar tarafından yönetilen, işlemlerin doğrulanması için özetleme algoritmasını, onaylanması için ise mutabakat protokollerini kullanan, işlemleri zaman damgası ile sıralayan, onaylanmış işlemleri birbiri ardına kriptografi ve özetleme fonksiyonları ile bağlayarak tüm düğümlerde özdeş kopyasını tutan, içerdiği verilerin değiştirilmesi ve geriye çevrilmesi hemen hemen imkansız olan dağıtık bir veri kayıt sistemidir.

2008 yılında ilk ortaya çıkmasından bu yana blokzincir teknolojisi, 1.0, 2.0 ve 3.0 olarak üç evrede gelişim göstermiştir. Blokzincir 1.0 bilinen en yaygın örneği Bitcoin olan kripto para işlemlerinin gerçekleştirildiği, dijital para transferi ve dijital ödemeler gibi finansal uygulamaları içeren ilk dönemdir. Blokzincir 2.0, 2013 yılı sonlarında Ethereum adlı blokzincir platformunun ortaya çıkması ile ortaya atılan 'akıllı sözleşmeler' kavramının varlıkların dijital olarak transferinde kullanılmaya başlandığı dönemdir. Bu dönemde bilgisayar kodları biçiminde hazırlanarak belirli koşullar gerçekleştiğinde kendiliğinden çalışan sözleşmelerle blokzincir teknolojisinin yıkıcı etkileri ve kullanım alanları daha da genişlemiştir. Blokzincir 3.0 ise üzerinde net bir uzlaşı ve tanım bulunmamakla birlikte teknolojinin ölçeklenebilirlik problemlerinin giderilebildiği, finansal uygulamalarının ötesindeki uygulamaların geliştirildiği evredir.

Blokzincirin en önemli karakteristiklerinden biri dağıtık ve paylaşılan yapısıdır. Bu nedenle, blokzincire dayalı sistemler mevcut aracıların sebep olduğu maliyetleri ve ihtilafları ortadan kaldırma potansiyeline sahiptir. Böylelikle daha fazla veri bütünlüğü, dağıtıklık ve aracıya gerek duyulmayan bir güven ortamı ile daha düşük işlem maliyetleri vadetmektedir (Berryhill, Bourgery ve Hanson, 2018, s. 11).

Blokzincir aslında tek bir kavram değildir. İlk ortaya çıktıktan sonra birçok yönden gelişmiş, farklı şekiller almış ve sınırsız kullanım senaryolarına hitap etmiştir (Lyons, Courcelas, Grandsenne, Carrel ve Timsit, 2018, s. 6). Blokzincir teknolojisinin ilk ve en tanınan örneği olan *Bitcoin* özetleme, dijital imza, iş ispatı ve eşten eşe ağlar gibi çok büyük teknolojileri bir arada kullanmaktadır. Bunlardan hiçbiri yeni bir teknoloji olmamakla birlikte, bu mevcut teknolojilerin kombinasyonu blokzincirde yepyeni fonksiyonlar yaratmıştır (Nomura Research Institute, 2016, s. 13).

Casey ve Vigna (2018) blokzinciri "bilgisayar düğümlerinden oluşan bir ağda kopyaları kaydedilen, sürekli biçimde güncellemelerin bir yazılım yönlendirmeli mutabakatla belirlendiği, birbirlerine ardışık olarak bağlı ve kriptolojik olarak güvenliği sağlanmış, dijital imza ile kanıtlanabilir, dağıtık, sadece kayıt eklemeye izin verilen bir kayıt defteri" olarak tanımlamaktadır.

Blokzincir teknolojisinde veriler gruplanarak bloklar biçimde toplanır, işlem zamanlarına göre sıralanır ve daha sonra kriptografi kullanılarak bu bloklar birbiri üzerine eklenir. Her bir blok kendisinden önceki bloğun dijital bir parmak izine benzeyen özet değerini içerdiğinden bir bloktaki en küçük bir değişiklik kendisinden sonraki tüm blokların yapısını değiştirir. Böylelikle eski bir veriyi değiştirmek, takip eden tüm bloklardaki verileri değiştirmeyi ve bu değişikliği ağdaki tüm kullanıcılarda kaydedilen kopyalarda yinelemeyi gerektirir ve bu da pratikte çok zor bir işlemdir. Tamamlanan her blok ile birlikte en güncel zincir ağdaki tüm katılımcılar tarafından kendilerine kopyalanır. Herhangi bir katılımcıda hatalı, manipüle edilmiş ya da bozulmuş bir veri zincirinin bulunması

sistemi tehlikeye atmaz. İşlemi tamamlanan her bir blok ayrıca kendi zaman damgasını alır ve böylelikle bilgilerin bir sıra dahilinde kaydı sağlanarak çifte kayıt engellenir.

Blokzincirde güvenin inşa edilebilmesi için kimlik (kim kimdir?), sahiplik (kim neye sahiptir?) ve doğrulama (gerçek nedir?) biçiminde üç kilit unsur bulunmaktadır. Blokzincir kullanıcıların kimliklerini kolaylıkla ispatlamalarına, dijital varlıkların sahipliğinin korunmasına ve yüksek maliyetli bir aracı olmadan işlemlerin doğrulanmasına izin verir. Blokzincir kimlik problemini dijital imza kullanımıyla, sahiplik problemini kriptografik özetleme ile, doğrulama problemini ise program kodu aracılığı ile gerçekleştirilen ağdaki düğümlerin çoğunluğunun mutabakatını gözeten konsensüs mekanizmasıyla çözmektedir (Galen vd., 2018, s. 7, 8).

Blokzincir teknolojisinin tarihçesinden bahsedilirken haklı olarak Bitcoin ile başlanmakta birlikte 1970'li yıllara kadar yalnızca silahlı kuvvetler ve istihbarat servislerince kullanılan ancak 1976'da ilk defa herkese açık olarak kriptografi ve veri şifreleme konusunda iki makale yayınlayan Whitfield Diffie ve Martin Hellman ile 1980'lerin sonlarında bir grup yazılımcı aktivistin oluşturduğu bir e-posta grubu ile başlayıp 1992 yılında bir grup halini alan şifre anarşistlerinden de (*cypherpunks*) mutlaka bahsedilmelidir. Güven ve Şahinöz (2018) blokzincir teknolojisinin meydana getirdiği dönüşümü Avusturya asıllı Amerikalı iktisatçı J. A. Schumpeter'in 'her yeni icat yapıcı bir yıkıcılık barındırır' sözüne atıfla yaratıcı yıkım olarak tanımlamakta, kripto para, blokzincir teknoloji devrimi ve Bitcoin konusunda konuşulan ne varsa *Cypherpunks* adıyla bilinen bir avuç aktivist ile başladığını ileri sürmektedir.

Cypherpunk grubunun içerisinde *WikiLeaks* kurucusu Julian Assange, *BitTorent*'in yaratıcısı Bram Cohen, Bitcoin'in kurucusu Satoshi Nakamoto, ünlü kriptograf Hal Finney, Philip Zimmermann, Nick Szabo gibi birçok önemli isim bulunmaktadır (Cybersalon, 2013). Satoshi Nakamoto Bitcoin'i tasarlarken aslında yeni bir keşifte bulunmamış, kendisinin de içinde bulunduğu *Cypherpunks* grubunun diğer üyelerinin çalışmalarından, kriptografiden, oyun teorisinden, eşten eşe ağlardan, açık anahtarlı şifrelemeden, özetleme algoritmalarından ve dağıtık mimarilerden faydalanarak birçok farklı çözümü tek bir çatı altında, açık kaynak kodlu bir yazılımda toplayarak neredeyse kusursuz bir sistemi ortaya koymuştur.

Onbirinci Kalkınma Planı hazırlıkları kapsamında hazırlanmış olan özel ihtisas komisyonu ön raporunun bir kısmında da blokzincir teknolojisinden kısaca bahsedilmektedir (Onbirinci Kalkınma Planı Kamuda Kurumsal Yönetimde Yeni Yaklaşımlar Özel İhtisas Komisyonu, 2017):

> *"Özellikle son dönemde bitcoin gibi sanal para birimlerinin kullanımı ile gündeme gelen blok zinciri teknolojileri, aracı kurumların varlığını yazılım teknolojilerine dayalı bir kayıt sistemiyle geçersiz kılan yeni bir olanak sunmaktadır. Bu güvenilir kayıt sisteminin bireyler ve kurumlar arasındaki her tür kayıt sistemine uygulanabileceği düşünülmektedir. Bu alandaki gelişmeler bankacılık sisteminden kamudaki kayıtlara kadar çok geniş bir yelpazede tartışılmaktadır. Kamu yönetiminde bu teknolojilerin hangi alanlarda ve nasıl kullanılabileceğine ilişkin ciddi tartışmalar sürmektedir."*

2.1. Blokzincir teknolojisinin çalışma prensibi ve temel özellikleri

Blokzincir, veri bütünlüğünü sağlayan zincir şeklinde kayıt imzalama, verinin dağıtık biçimde bulunması ve sadece mutabakatla kayıt oluşturulabilmesi şeklinde üç temel kavramın birleşimi olarak tanımlanabilir. Bu üç maddeden en önemlisi ise mutabakat kısmıdır (T2 Yazılım A.Ş., Bankalararası Kart Merkezi A.Ş., 2018, s. 14).

Dijital bir sistem üzerinde mutabakat yapısı yazılımsal açıdan garanti altına alınmalıdır. Blokzincir teknolojisi bu noktada verinin iletişim ağları üzerinden, dağıtılmış şekilde saklanmasını ve bu süreç içinde verinin tüm noktalarda aynı kaldığına dair mutabakat yapılmasını sağlamakta, herkesin kendi verisini şifreleyeceği, böylelikle bu veriyi sadece kendisinin kullanacağı ve izin vermesi halinde diğer tarafların bu veriye erişebileceği bir yapı sunmaktadır (Usta ve Doğantekin, 2017, s. 45).

Blokzincir ve Dağıtık Kayıt Defteri Teknolojisi (*Distributed Ledger Technology – DLT*) bazen eşanlam-

lı olarak kullanılmakla birlikte tam olarak aynı şey değildir. Dağıtık Kayıt Defteri Teknolojisi gizli ya da herkese açık kayıtların ve bilginin dağıtılmasını sağlayan teknolojileri tanımlayan şemsiye bir kavramdır. Blokzincir ise ilk tam fonksiyonel Dağıtık Kayıt Defteri Teknolojisidir ve çok daha kapsamlı olan bu teknolojinin bir alt kategorisidir (Thake, 2018). Her blokzincir bir dağıtık kayıt defteridir ancak her dağıtık kayıt defteri bir blokzincir olmayabilir.

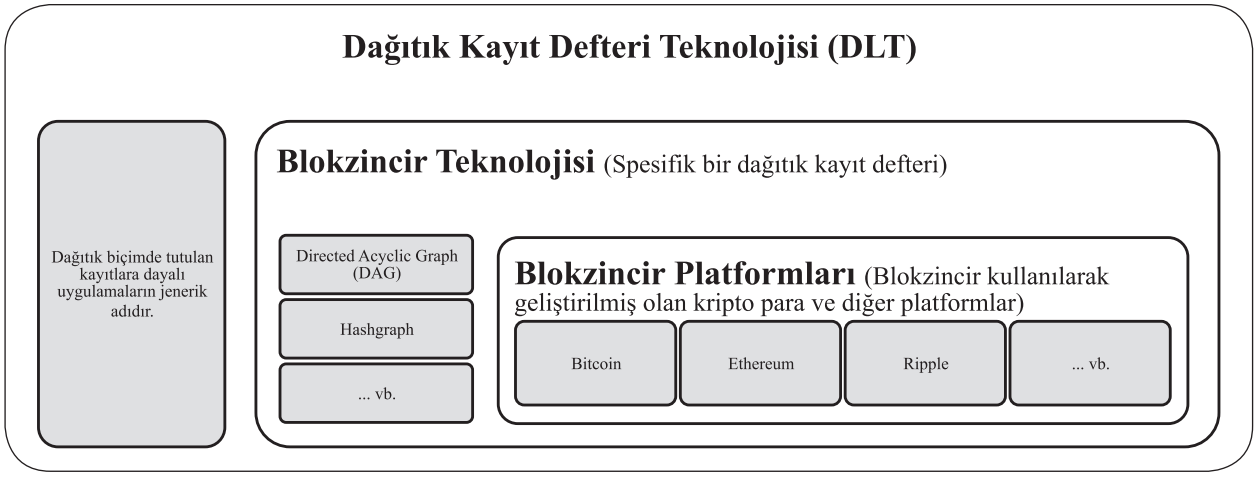
Blokzincir temel olarak sürekli büyüyen bir kayıtlar listesidir. Sadece veri eklemeye izin veren yapısı nedeniyle veri tabanına sürekli yeni kayıtlar eklenirken daha önce girilmiş olan verilerin silinmesi veya değiştirilmesi mümkün değildir. Bu özellikleri nedeni ile blokzincir teknolojisi olayların kaydı, kayıtların yönetilmesi, işlemlerin proses edilmesi, varlıkların izlenmesi ve oy kullanma konuları için çok uygundur (Ray, 2018).

Aşağıda verilmiş olan Şekil 1'de Bitcoin, blokzincir ve dağıtık kayıt defteri arasındaki ilişki gösterilmiştir.

Blokzincir teknolojisinde tüm bilgi blok adı verilen veri yapısında tutulur. Her bir blok işlem bilgileri ile birlikte kendinden önceki bloğun referans değerini de içinde barındırır. Blok içinde cevabı sadece ilgili bloğa özgü çözülmesi oldukça zor matematiksel bir bulmaca bulunur. Bu matematiksel problemin cevabı bulunmadan ağa yeni bir blok gönderilemez. Bu problem çözme süreci madencilik olarak adlandırılır ve madenciler soruyu ilk çözen olmak için yarışırlar. Çözümü ilk bulan madenci işlem doğrulama karşılığında ödül kazanır (teşvik mekanizması). Tüm işlem bilgileri, önceki bloğun referans değeri, zaman damgası ve işlem doğrulama için kullanılacak özel bir değer (*nonce* değeri) bir bloğu oluşturur ve bir özetleme algoritması ile tüm bu bilgilerin özet değeri (*hash*) alınarak o bloğun referans değeri oluşturulur. Blok içerisindeki verilerdeki en küçük bir değişiklik bile referans değerini değiştireceğinden bu değişiklik kendinden sonraki tüm blokları etkiler. Blokzincir ağındaki tüm katılımcılar (düğüm) tüm bloklardan oluşan zincirin tamamını kendilerine kopyalarlar. İşlemlerin gerçekleşmesi için oyun teorisine dayalı bir mekanizma ile uzlaşı sağlanması gerekir. Ağdaki her uç hem sunucu hem de istemcidir ve her birinde özdeş kopyalar tutulur. Açık anahtarlı kriptolama ve kriptolojik özetleme fonksiyonlarının kullanımıyla gizlilik ve şeffaflık sağlanır. Aşağıda verilmiş olan Şekil 2'de blokzincirin temel çalışma adımları basit biçimde verilmiştir:

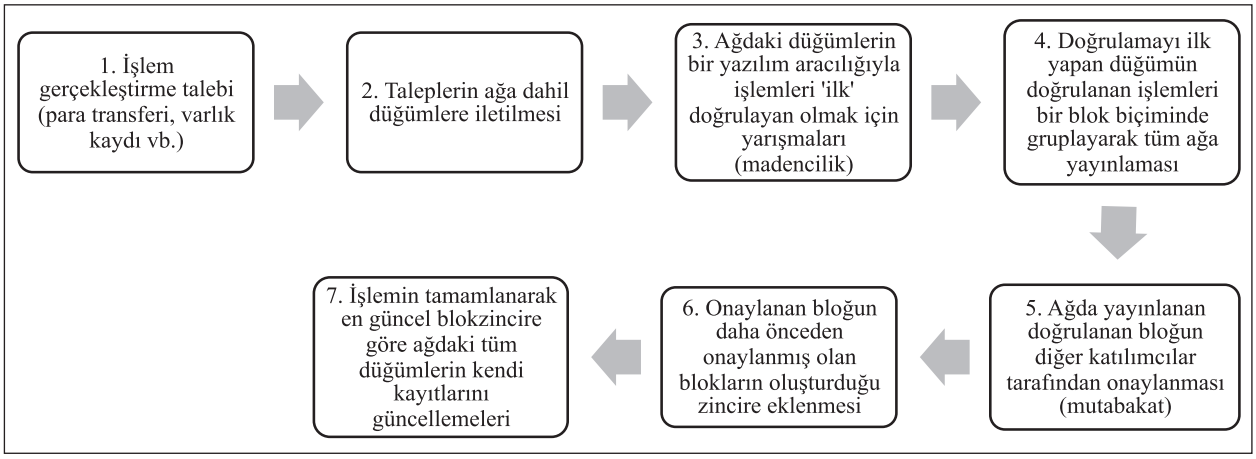
Blokzincir genellikle kayıt defterinin görünürlüğü ve erişim haklarının açıklığı bakımından kategorize edilmekte olup yaygın olarak görünürlük bakımından özel ve açık blokzincirler, erişim hakları bakımından da izin gerektiren ve gerektirmeyen blokzincirler olarak adlandırılmaktadır. Sadece yetkilendirilmiş kullanıcıların işlem geçmişi kayıtlarını görebildiği blokzincirler özel, sadece yetkilendirilmiş kullanıcıla-

Şekil 1. Dağıtık Kayıt Defteri Teknolojileri, Blokzincir ve Bitcoin Arasındaki İlişki



(Chartered Accountants Australia and New Zealand, 2017'dan uyarlanmıştır.)

Şekil 2. Blokzincir Teknolojisinin Temel Çalışma Adımları



(Yazarlar tarafından oluşturulmuştur.)

rın blokların geçerliliğinin onaylanması ve işlemlerin gerçekleştirilmesi ve doğrulanması mekanizmasında yer alabildiği blokzincirler de izin gerektiren blokzincirler olarak adlandırılır.

Deloitte 2019 yılı Mart ayında yayınlamış olduğu finans alanında blokzincirin kullanılması konulu rehberde bu teknolojinin finans alanında tanımlanmış olan süreçleri yeniden şekillendireceğini vurgulamakta, blokzinciri bir veya birden fazla tarafça kullanılan mevcut uygulamalar (Kurumsal Kaynak Planlama –ERP– sistemleri gibi) ile entegre olabilen dağıtık ve paylaşılan bir kayıt defteri olarak tanımlamaktadır. Kurumsal kullanım için tasarlanan özel blokzincir ağlarında ağa katılım izne tabi olup katılımcıların kimlikleri kriptografik anahtarlarla kontrol edilmektedir. Herhangi bir işlem bir blokzincir üzerinde kaydedilmeden önce mutabakat durumunu değerlendiren bir protokolle katılımcıların işlemin geçerliliğini doğrulamaları gerekir. Bir bloktaki her veri şifrelenmiştir ve her bir blok bir önceki bloğa benzersiz bir tanımlayıcı (hash – özet değeri) ile bağlanır. Blokzincirde kaydedilen işlemler ağ katılımcılarının bilgisayarlarında neredeyse eş zamanlı olarak güncellenir ve dağıtılır. Böylece blokzincir ağındaki her bir katılımcıda aynı veri kaydı bulunur. Eğer herhangi biri bloktaki veriyi değiştirmeye çalışırsa diğer katılımcılar blokları birbirlerine bağlamakta kullanılan özetleme mekanizması vasıtasıyla uyarılırlar.

Blokzincir teknolojisi bilgisayar bilimleri, kriptografi ve ekonomi alanlarının üzerine inşa edilmiştir. Bu teknoloji konusunda derinleşmek için bilgi sahibi olunması gereken konular temel olarak bilgisayar bilimleri alanında veri yapıları, kriptografi, dağıtık sistemler, ağ kurma, ekonomi alanında oyun teorisi, makroekonomi ve mikroekonomi başlıkları altında toplanmakta olup bunların yanında Bitcoin'in teknik altyapısı ile Ethereum ve akıllı sözleşme programlama konuları hakkında da bilgi sahibi olunmalıdır (Qureshi, 2018).

2.2. Blokzincir teknolojisinin avantajları ve problemli alanlar

Blokzincir teknolojisinin tasarımı itibariyle sunduğu en önemli avantajlar kayıtlı verilerin değiştirilememesi, tamamlanan her bir bloğun oluşturduğu zincirin ağdaki her bir katılımcıda özdeş ve eşzamanlı olarak dağıtık biçimde tutulması, işlemlerin doğrulanması ve onaylanması için merkezi bir otoriteye gereksinim duyulmaması ve herhangi bir kopyadaki bozulmuş ya da manipüle edilmiş veriyi içeren zincirin sistemi tehlikeye atmaması (güvenilirlik) biçimindedir.

Teknolojinin ortaya çıkış sürecinin altında yatan felsefe açık bir toplum için bireylerin mahremiyetinin korunması, şeffaflığın artırılarak merkezi otoritelere ve aracılara olan bağımlılığın ortadan kaldırılması ve üçüncü bir tarafa ihtiyaç olmadan tamamen kriptolojiye ve açık kaynak kodlu yazılımlara dayalı bir güven mekanizmasının inşa edilmesidir. İlk olarak Bitcoin ile ortaya konulan sistem bu felsefe ile hedeflenen temel unsurları başarıyla yerine getirmiştir.

Şeffaflık, gizlilik, dağıtık yapı ve güvenliğe ilave olarak blokzincir teknolojisinin sağladığı bazı önemli avantajlar aşağıdaki biçimde sıralanmaktadır:

- Aracılara gereksinim duyulmaması sonucunda işlem maliyetlerinde azalma,
- Çok düşük miktarlı ödeme ve transfer işlemlerini gerçekleştirebilme,
- Bankacılık sistemine dahil olmayan insanların finansal işlemlerden faydalanabilmesi için bir ortam sağlama (sosyal yardımların bankacılık sistemini kullanmadan blokzincir ile dağıtılabilmesi gibi),
- Gizli ve özel anahtarlı şifreleme ile insanların kendi verilerini yönetebilmeleri,
- Farklı birimler arasında veri paylaşımını kişisel mahremiyeti ihlal etmeden sağlayan yapı,
- Küçük ve orta ölçekli işletmelerin yerel ve ulusal yönetimlerle daha kolay iletişim kurabilmeleri,
- Yenilikçi fikirler ve projeler için kaynak toplamayı kolaylaştırması,
- Veri koruma maliyetinin düşürülmesi.

Blokzincir teknolojisi ihtilafların giderilmesi ve farklı birimler arasında mutabakat işlemlerinin yürütülmesi gibi manuel faaliyetleri azaltma veya ortadan kaldırma avantajını sunmaktadır. Kayıtların geriye dönük olarak değiştirilememesi, her işlemin birden fazla tarafça doğrulanması ve onaylanması gerekliliği bir taraftan geleneksel sistemlere göre etkinliği azaltırken bir taraftan da işlemlerde şeffaflığın artması, faaliyetlerin basitleşmesi ve yolsuzlukların en aza indirilmesi gibi avantajlar sunmaktadır (Chartered Accountants Australia and New Zealand, 2017).

Blokzincir yeni bir teknoloji olmasının ötesinde ölçeklenebilirlik, veri gizliliği, yetki/yargı uyuşmazlıkları ve dış kaynaktan temin edilen hizmetlere ilişkin sözleşmelerin performanslarından emin olunmaması gibi genel riskler taşımaktadır. Özellikle yetki problemleri blokzincirin dağıtık otonom kuruluşlara sahip olma özelliği yüzünden büyük kaygı doğurmakta, bir veri ihlali veya yasal bir anlaşmazlık durumunda yasal sorumluluğun kimde olacağı ve yetki sınırları ile ilgili düzenleme ve yasalarla nasıl başa çıkılabileceği soruları akla gelmektedir (Chalker, 2018).

Chalker (2018) diğer teknik riskleri; hesap güvenliği, akıllı sözleşmelerdeki kodlama hataları, iş süreçlerinin entegrasyon ihtiyacı, veriye ve şifreleme anahtarlarına erişim ve izinler, gerçek iş uygulamalarının azlığı biçiminde sıralamaktadır. Greenspan (2016) blokzincir ile klasik veri tabanlarının farklarını dört temel başlık altında değerlendirerek blokzincirin aracı ve merkezi otoriteyi ortadan kaldırması, yüksek hata toleransı (dayanıklılık) bakımlarından veri tabanlarının ise performans ve mahremiyet bakımlarından daha avantajlı olduğunu belirtmiştir.

Teknolojinin anlaşılmasının güçlüğü blokzincirin popülerleşmesinin önündeki bir diğer engeldir. Blokzincirin algoritmaları ve çalışma prensibi önemli miktarda sistem ve güvenlik bilgisi gerektirmektedir. Bu nedenle yöneticiler, muhasebeciler ve denetçiler bu teknolojiyi doğru ve etkin biçimde kullanabilmek için eğitim almalıdırlar (Dai, 2017, s. 82).

Değiştirilemezlik özelliği blokzincirin en temel ve en faydalı özelliği olmakla birlikte aynı zamanda pratik uygulamalarda en önemli kısıtlılığıdır. Blokzincir temel olarak hangi bilginin ilave edildiğini gösteren bir listedir. Günümüzde kamuda kullanılan geleneksel veri tabanlarından farklı olarak blokzincire eklenen bir verinin silinmesi mümkün değildir. Karar vericiler blokzincirin bu avantajının veri güncelleme ve silmenin imkansız hale gelmesine ağır basıp basmadığına karar vermeli, değiştirilemezlik özelliğinin kullanmak istedikleri alanda uygulanabilir olup olmadığını değerlendirmelidirler (Yaga, Mell, Roby ve Scarfone, 2018, s. 34).

Değiştirilemezlik özelliği nedeniyle kişisel bazı bilgiler blokzincirde kaydedilirse unutulma hakkı gerçekte uygulanamaz. Bununla birlikte, devletlerin tutmuş oldukları kimlik bilgisi ya da adli kayıtlar gibi bilgiler unutulma hakkı kapsamında olmayıp bu bilgilerin silinmesi talep edilemez. Ayrıca, çoğu kamu sektörü blokzincir uygulaması izin gerektiren yapıdadır ve sadece yetkilendirilmiş kamu çalışanları erişimi kontrol edebilirler (Berryhill, Bourgery ve Hanson, 2018, s. 29). Açık ağlarda veri paylaşan blokzinciri uygulamalarının hayata geçirilmesi halinde şifreleme metotlarının kullanıcı gizliliğini sağlama garantisi verilmelidir. Kişisel bilgilerin depolanmasının muhtemel olduğu durumlarda gizlilik ve mahremiyet en önemli önceliktir. Kurallar ve kanunlar bu tip bilgilerin korunması konusunda çok katıdır.

Kamu ve özel sektör kuruluşları genellikle büyük miktarda veriyi belgeler, görüntüler, videolar ve uygulamalar gibi farklı biçimlerde depolamak için veri tabanları kullanmaktadırlar. Blokzincir ise daha genel olarak bir işlemler listesidir ve çoğunlukla akıllı sözleşmeleri yönlendirmek ve çalıştırmak için küçük veri parçalarını içerirler. Genel veri depolama için tasarlanmamıştır (Yaga vd., 2018, s. 34). Bununla birlikte,

eğer işlem kayıtlarının güvenilir ve dağıtık biçimde yürütülmesi hedefleniyorsa blokzincir teknolojisi uygulanabilir bir çözümdür. İhtiyaçları giderecek, geleneksel veri depolama çözümleri ile blokzincir teknolojisini bir arada kullanan hibrit bir yaklaşım da pekala mümkündür. Sadece veri depolamak için bir çözüm aranıyorsa blokzincir teknolojisi uygun olmayabilir.

Blokzincir platformlarını en güçlü kılan özelliklerin başında kriptografi gelmektedir. Bu kapsamda kullanılan şifreleme yaklaşımları oldukça güçlü olsa da, kuantum bilişim (*quantum computing*) gibi alanlardaki gelişmelerle birlikte bu konuda gelecekte çeşitli zafiyetler görülebileceği düşünülmektedir. Bu sistemlerin kabul edilebilir sürelerde günümüzün gelişmiş ikili şifreleme yöntemlerini kırması mümkün olabilecektir. Bu blokzincir dünyası için hemen değil ama uzun vadede bir risk oluşturmaktadır (Usta ve Doğantekin, 2017, s. 105)

Belirli bir merkezi otoriteye bağlı olmaması istenmeyen durumlar ortaya çıktığında (hesaplara erişim şifresinin unutulması, hatalı işlemler vb.) kime başvurulacağı sorusunu ortaya çıkarmaktadır. Yazılım kodu geliştiricileri, blokzincir tasarımında doğrulama ve onaylama adımlarından sorumlu yetkili düğümler, kullanıcılar ve diğer karar vericilerin koordinasyonu konusunda henüz bir standart bulunmamaktadır.

Blokzincir teknolojisi ile ilgili yasal düzenleme ve standartlar henüz gelişim aşamasındadır. Akıllı sözleşmelerin hukuki altyapısı ve bağlayıcılığı, blokzincir denetim izlerinin mahkemelerde delil olarak kullanılıp kullanılamayacakları ve bu teknolojinin kullanımının bazı alanlarda zorunlu olup olmaması gibi konuların cevapları henüz belirsizliğini korumaktadır. Sistem dönüşümü için yüksek yatırım gereksinimi ve yeterli nitelikte insan kaynağının yetersizliği de diğer belirsizlik alanlarıdır.

Bu ölçüde hızlı bir büyüme bilgi teknolojileri karar vericilerinin karar vermesini güçleştirmektedir. Blokzincir teknolojisinin veya işlettiği ağın geniş kabul görmüş standartları bulunmamaktadır. Birçok blokzincir tedarikçisi küçük firmalar olduklarından bilgi teknolojileri ve satın alma birimleri için bu firmalarla birlikte proje yürütme kararı çok zordur. Aynı zamanda gizlilikle ilgili riskler de bulunmaktadır (Cheng, Daub, Domeyer ve Lundqvist, 2017).

İşlemlerin mutabakat algoritması ile doğrulanmadan önce tüm ağda dağıtılması gerektiğinden bant genişliği bir diğer önemli konudur. Kullanıcıların sayısı ve bunun sonucunda da işlem sayıları arttıkça daha iyi bir ağ bağlantısı gerekmektedir. İyi bir ağ bağlantısı ve büyük depolama kapasitesi etkin bir kayıt yönetimi gerektirmekte, daha fazla enerji tüketimi ve maliyete sebep olmaktadır (Brender, Gauthier, Morin ve Salihi, 2018, s. 10). 30 Mart 2019 tarihi itibariyle Bitcoin'in tahmin edilen yıllık elektrik tüketimi 52 terawatt/saat[1] olup bu miktar 5 milyona yakın Amerikan hanesinin ve Bangladeş gibi bazı ülkelerin elektrik tüketimine ve dünyanın elektrik tüketiminin %0,24'üne eşittir (Digiconomist, 2019). Ticari işler için ihtiyaç duyulan yüksek hacimle çok kısa zaman içerisinde başa çıkma kabiliyeti bakımından halihazırda kullanılan veritabanı sistemlerinin gerisindedir.

Ölçeklenebilirlik bir sistemin boyutunda veya hacminde meydana gelen değişim sonucunda o sistemin fonksiyonlarını aynı biçimde sürdürebilmesidir. Blokzincirde katılımcı sayısı arttıkça ölçeklenebilirlik problemi ortaya çıkabilmektedir. Tasarımı gereği bir blokzincir kayıt defteri ilk bloktan itibaren bütün işlemleri içermektedir. Bu nedenle kullanıcı ve işlemlerin sayısı arttıkça kayıt defterinin boyutu da büyümektedir. Bitcoin platformunda saniyede en fazla yaklaşık 7 işlem gerçekleştirilebilmektedir. Bu problem büyük oranda herkese açık olan blokzincirler için geçerli olup bazıları saniyede binlerce işlem gerçekleştirebilen özel blokzincirlerde bu problem çözülmüştür (Brender vd., 2018, s. 10).

Blokzincir teknolojisinde kullanılan açık-özel anahtar yapısındaki özel anahtarın saklanması kullanıcının sorumluluğundadır. Özel anahtarın kaybedilmesi ya da erişim şifresinin unutulması durumunda kullanıcının elinde şifrelenmiş işlemlerin sahipliğini doğrulayacak hiçbir bilgi kalmamaktadır. Bu nedenle bu anahtarların kaybedilmesi ilişkili varlığın da kaybedilmesi anlamına gelmektedir (Usta ve Doğantekin, 2017, s. 106).

Blokzincir teknolojisi yüksek güvenlikli işlemleri vadetmesine karşın yolsuzlukları tamamen ortadan kaldıramaz. Yanlışlıkla veya bilinçli olarak hatalı ya da yetkisiz bir adrese değer transferi yapıldığında bu işlemi tersine çevirmek imkansızdır. Blokzincir

1) Bir watt'ın 1 trilyon katına denk düşen terawatt büyük barajların üretimini ve ulusal çapta enerji tüketimini ölçmek için kullanılabilecek kadar büyük bir elektrik ölçü birimidir. Örneğin dünyanın en büyük hidroelektrik santrallerinden biri olan Atatürk Barajı'nın yıllık elektrik üretimi 8,9 terawatt civarındadır (Radore, 2017).

teknolojisini kullanan kuruluş bir oltalama saldırısına maruz kalırsa blokzincirin merkezi bir yönetimi olmadığı için bu olayın raporlanacağı bir dolandırıcılık departmanı yoktur. Özel anahtar kaybedilirse bu anahtarla ilişkili hesaba (ve varlığa) erişim artık mümkün olmaz (Psaila, 2017, s. 3)

Blokzincir teknolojisi her ne kadar klasik sistemlerdeki güvenilir bir aracı ihtiyacını ortadan kaldırıyor olsa da bazı durumlarda, özellikle akıllı sözleşme kullanımında bazı güvenilir bilgilere erişilmesi gerekmekte, bu durum da blokzincir teknolojisinin en temel özelliklerinden biri ile çelişkili bir durum ortaya çıkarmaktadır (İlkbahar, 2019). Bu çelişkili duruma örnek olarak belirli bir sıcaklık değerinin sağlanmasına yönelik olarak programlanmış bir akıllı sözleşmenin esas alacağı sıcaklık değerinin güvenilir bir kaynaktan sağlanması ihtiyacı verilebilir.

Teknolojinin finans ve sağlık kuruluşları gibi sektörlerce gerçekten çekicilik kazanması için birçok problemle başa çıkılmalıdır. Bunlar arasında veri güvenliği ve gizliliği, teknik uzman havuzunun yetersizliği, mevzuat ve uygunluk gereksinimlerinin bu yeni teknolojiye uygulanması bulunmaktadır. Bu güçlükler teknoloji olgunluğa eriştikçe giderilecek olup blokzincir teknolojisini kendi kuruluşlarında deneyimleyen geliştiricilerin dikkatini çekmeyen bir başka konu vardır: denetim güçlüğü. Blokzincir çözümleri geliştiren inovasyon ve strateji ekipleri ile yapılan çalışmalar sonucunda dört ana sorun tespit edilmiştir (Smith, 2018):

- Blokzincir oldukça yeni bir konudur. İlk uygulamanın üzerinden sadece 10 yıl geçmiştir ve birçok uygulama henüz olgunlaşmamıştır. Aksine, yönetimlerin güven duydukları sistemler on yıllardır denenmiştir ve bunları uygun biçimde kullanmak için spesifik kılavuz ve prensipler bulunmaktadır. Denetim ekiplerinin bu sistemden nasıl tam katkı elde edilebileceği konusunda uzmanlıkları bulunmamaktadır.
- Bu yeni teknolojinin içerdiği kontroller geleneksel kontrollerden oldukça farklıdır ve denetçilerin blokzinciri kimin kontrol ettiği, sisteme kimlerin erişim sağladığı, sunucuların nerede bulunduğu, hangi fiziksel ve dijital kontrollerin bulunduğu, faaliyetleri kimin izlediği, teknolojinin gerçekten de iddia edildiği biçimde çalışıp çalışmadığı gibi sorular sormaları gerekmektedir.
- Blokzincir teknolojisi konusunda teknik uzmanlık zayıftır. Blokzincir deneyimine sahip BT birimi sayısı çok azdır. 2017 Küresel Dijital IQ Anketi'nde finans servisleri yöneticilerinin %86'sı kuruluşlarında henüz yeterli blokzincir yetkinliğinin geliştirilmediğini ifade etmiştir. İç Denetim ekiplerinde bu sayı çok daha azdır.
- Blokzincir teknolojisinin ilk öne çıkan uygulaması Bitcoin olduğundan teknoloji konusunda olumsuz bir önyargı bulunmaktadır. Blokzincir teknolojisinin Bitcoin'den daha önemli bir konu olduğuna inanmakta genelde güçlük çekilmektedir.

Tüm bu teknik sıkıntılara ilave olarak PwC (2018) ve Deloitte'a (2018) göre blokzincirin kabulünün önündeki en büyük engel yasal düzenlemelerdeki belirsizliktir. Sistemlerin amaçlandıkları biçimde çalıştıklarından emin olunabilmesi için gerekli standartlar ve kontroller henüz yetersizdir. Örneğin; Avrupa Birliği'nde blokzincir projelerinin Genel Veri Koruma Kanunu (GDPR) gerekliliklerini nasıl karşılayabileceği henüz net değildir.

2.3. Blokzincir teknolojisinin kullanım alanları

Blokzincir teknolojisinin kullanım alanları farklı birçok yerde listelenmekle birlikte bu liste her geçen gün uzamakta, sürekli yeni kullanım alanları ortaya çıkmaktadır. Bu nedenle, sunulan her liste daima eksik olacaktır (Filipowski, 2018). Blokzincirin kamuda kullanımında üç konu öne çıkmaktadır: kimlik yönetimi, tapu kayıtları ve elektronik oylama (Killmeyer, White ve Chew, 2017, s. 14-15). Berryhill, Bourgery ve Hanson (2018) blokzincir konusundaki gelişmelerin yoğunlukla finans alanında yaşandığını ancak kamu sektöründe de son dönemde hızlı bir gelişim gösterdiğini öne sürerek kamu alanında yürütülen projelerde en sık rastlanan konuların dijital kimlikler, kişisel kayıtlar (sağlık, mali bilgiler), tapu kaydı, sosyal yardımların takibi, tedarik zinciri olduğunu belirtmektedir.

Nagpal (2017) blokzincirin çok faydalı olacağı üç konuyu; verinin aslına uygunluğu ve doğrulanması, akıllı varlık yönetimi ve akıllı sözleşmeler olarak sıralamaktadır.

Avrupa Parlamentosu'na sunulmak üzere 2017 yılında hazırlanmış olan raporda blokzincir teknolojisinin kullanımının öne çıktığı ve gelecekte de kullanım potansiyelinin yüksek olduğu konular dijital paralar, dijital içerikler ve telif hakları yönetimi, patentler,

elektronik oylama, akıllı sözleşmeler, tedarik zinciri yönetimi ve merkezi olmayan özerk kuruluşlar olarak belirtilmiştir (Boucher, Nascimento ve Kritikos, 2017).

Maupin'e (2018) göre hesap verebilir, güvenli, denetlenebilir ve şeffaf yapısı ile blokzincir teknolojisi tüm dünya vatandaşları için kapsayıcı küresel bir dijital ekonomi inşa edilmesi için kilit konumdadır. Devletlerin, vatandaşlarının sınır ötesi ekonomik işbirliğine inançlarını tesis etmeleri ve herkesin faydasına olan küresel ekonominin sağlanması için blokzincir kritik bir role sahiptir. Maupin bu teknolojinin ekonomik direncin geliştirilmesi, finansal kapsamın geliştirilmesi, vergilendirme, ticaret ve yatırım, istihdam, iklim, sağlık, sürdürülebilir gelişim ve kadının güçlendirilmesi gibi alanlara odaklanan politik amaçlar doğrultusunda kullanılmasını önermektedir.

Dünyadan kullanım örnekleri ve halihazırda yürütülmekte olan çalışmalar değerlendirildiğinde blokzincir teknolojisinin kullanılabilir olduğu konularda dijital kimlikler ve sertifikalar (yeterlilik belgeleri, lisanslar vb.), kişisel kayıtların tutulması ve yönetimi (sağlık bilgileri, sigorta, mali vb.), finansal hizmetler ve bankacılık, tapu kayıtları ve gayrimenkul işlemleri, tedarik zinciri yönetimi, varlık izleme ve envanter tutma, sosyal yardımların dağıtılması, hak sahiplikleri, telif hakları ve patentler, sözleşme ve tedarikçi yönetimi, yenilenebilir enerji, oy verme, kitlesel fonlama aracı olarak kullanım ve sadakat programları öne çıkmaktadır.

3. BLOKZİNCİR TEKNOLOJİSİ VE İÇ DENETİM

Teknolojinin içinde gömülü biçimde bulunan şeffaflık, izlenebilirlik, değiştirilemezlik ve kural ve prosedürlerin entegrasyonu özellikleri süreçleri ve bilgi üretimini zenginleştirerek denetim ve kontrol prosedürlerini önemli ölçüde değiştirmekte, hatta bazı durumlarda işe yaramaz hale getirmektedir. Aynı zamanda bu özellikler denetçiler için en iyi uygulamaların yeniden tasarlanması, kural ve prosedürlerin güncellenmesi, yeni standartların tanımlanması gibi fırsatlar da yaratmaktadır (Brender vd., 2018, s. 3).

Blokzincir teknolojisi birçok kamu hizmeti için güvenli, şeffaf, hızlı ve düşük maliyetli çözümler vadetmekte olup kurumları için maksimum katkıyı sağlamayı amaçlayan iç denetçiler için de bazı fırsatlar ve zorluklar ortaya çıkarmaktadır. Bu zorlukların üstesinden gelmek ve fırsatlardan faydalanmak için iç denetim birimleri denetçilerin hem blokzincir teknolojisi hem de blokzincir projeleri konusunda iyi biçimde eğitilmelerini sağlamalıdır (Rooney, Aiken ve Rooney, 2017, s. 41).

Blokzincir ile geliştirilen uygulamaların sayısındaki artış kayıt saklamayı gerektiren her şeyde olduğu gibi iç denetimi de etkileyecektir. İç denetim blokzincirin teknik mimarisinin detaylı analizini gerçekleştirmek için hazırlıklı olmalı, yeterli düzeyde şeffaflığı gerçekleştirmek ve blokzincir uygulamalarının amaçlandığı biçimde çalıştığını doğrulamak için stratejiler geliştirilmelidir (Pelletier, 2018).

İç denetim bakış açısı ile blokzincire dayalı uygulamalarda devrimsel olan şey bilgi ve işlemlere ilişkin gerçeğin bulunmasında yepyeni bir yaklaşım sunmasıdır. Blokzincirin ortaya çıkmasına dek gerçeğin kanıtı spesifik kayıt defterlerinin ya da veritabanlarının tutulmasına dayanan bir sistem ve bu sistemi yöneten güvenilir bir üçüncü taraf iken blokzincir ile bu yapı kökünden değişmektedir.

3.1. Blokzincir teknolojisinin iç denetim faaliyetlerine ve iç denetim mesleğine potansiyel etkileri

Denetim mesleğine özgü olarak blokzincir teknolojisi değiştirilmesi mümkün olmayan bir kayıt defteri ve gerçek zamanlı olarak işlemlerin tüm anakütlesi üzerinde testleri gerçekleştirme fırsatı sunmaktadır. Bu nedenle, blokzincir konusunda danışmanlık ve güvence hizmetleri sunan büyük dörtlü (*Deloitte*, *EY*, *KPMG* ve *PwC*) olarak da bilinen firmaları da içeren geniş bir kitlenin ilgisini çekmektedir (Sheldon, 2018, s. 1). Örneğin; PwC (2018) tarafından henüz patent süreci devam etmekte olan bir risk çerçevesi ve sürekli denetim yazılımını içeren 'Blokzincir Doğrulama Çözümü' adı verilen bir çerçeve geliştirildiği duyurulmuştur.

Sheldon'a (2018) göre blokzincir kullanımı kuruluşların güçlü BT yönetişimine ihtiyaç duyduğu gerçeğini değiştirmeyecek, hatta bazı durumlarda bu yönetişim çok daha karmaşık bir hale gelecektir. Sheldon (2018) "Özel ve İzin Gerektiren Blokzincir Denetiminde Bilgi Teknolojileri Genel Kontrolleri" başlıklı çalışmasında blokzincir denetimleri için BT genel kontrollerini üç kategoride incelemiştir: (1) Program Geliş-

tirme ve Değişiklik Yönetimi, (2) Bilgisayar İşlemleri, (3) Programlara ve Veriye Erişim.

Blokzincir tasarımındaki değişiklikler mutabakat protokolü, iletişim protokolü, akıllı sözleşmeler, dağıtık uygulamalar (Dapps) veya programın kaynak kodu ile gerçekleşebilir. Birden fazla kuruluşun katılımıyla oluşturulmuş olan konsorsiyum tipi blokzincir ağlarında bu tasarım değişiklikleri konusunda tüm üyelerin mutabakatı ve değişikliklerin hedeflenen biçimde uygulandığından emin olunmasını sağlayan bir mekanizmanın bulunması gerekmektedir. Denetçiler bu nedenle değişikliklerin kabul edilmesi ve kabulden sonra uygulanması konusunda üyelerin mutabakatlarına ilişkin mekanizmanın tasarımını ve işleyişini dikkate almalıdırlar.

Kuruluşlar blokzincir kullanmaya başladıkça eski sistemlerinden ve hatta üçüncü taraf bulut esaslı sistemlerden veri toplanması ve bu verilerin işlenmesinde bir geçiş dönemi yaşanacaktır. Bu sistemler blokzincirle bir arayüz oluşturacak, nihai olarak blokzincire yüklenen verileri üreteceğinden eski uygulamalar ve süreçlere ilişkin mevcut politika ve prosedürlerin sürdürülmesi ve hatta daha da geliştirilmesi gerekecektir. Blokzincire kaydedilen veriler artık değiştirilmeye karşı korumalı olsa da blokzincirin dışında iken genel BT risklerine karşı hala savunmasızdır. Verilerin bir üst sistemden blokzincire iletimindeki geçiş arayüzü bu yeni ortamdaki en hassas kontrol noktalarından biri olacaktır. Denetçilerin, kendine özgü BT ortamında bu veri geçişinin en kontrollü biçimde nasıl yapılabileceğinin belirlenmesi konusunda sorumlu birimlerle birlikte çalışmaları gerekecektir. Blokzincir iş sürekliliği ve felaket kurtarma planlaması konusundaki birçok endişeyi giderme potansiyeline sahiptir. Denetçiler, blokzincir arayüzü görevini üstlenen eski sistem erişilemez olduğunda hangi prosedürlerin izleneceğini görmek için iş sürekliliği/felaket kurtarma planlarını değerlendirmek isteyecektir (Sheldon, 2018, s. 7,8,9).

Kripto paraların ortak problemi özel bir anahtarla ilişkilendirilmiş dijital varlıklara bu anahtarın kaybedilmesi halinde erişilememesidir. Bu nedenle, blokzincir üzerinde dijital varlık hareketini kontrol etmek için açık ve gizli anahtar kullanılıyorsa denetçiler bu anahtarların saklanma sürecini ve özel anahtarın çalınması ya da başkası tarafından ele geçirilmesi halinde bu anahtarla ilişkili dijital varlığın kontrolünü yeniden ele geçirme sürecini ve anahtarla ilişkilendirilmiş varlıklara erişmeye artık gereksinim duyulmadığında bu varlıkların güvenliğinin sağlanması konusunu da dikkate almalıdırlar (Sheldon, 2018, s. 9).

Blokzincir güvenli veri işleme, değiştirilemez kayıtlar ve sağlam yapısı ile yeni bir teknoloji olmakla birlikte halen BT altyapısının bir bileşeni olduğu akıldan çıkarılmamalıdır. Etkin BT genel kontrolleri olmadan blokzincir tarafından üretilen verilerin güvenilirliği tam olarak sağlanamayacağından mutlaka düzgün işleyen BT genel kontrolleri ile desteklenmelidir.

Blokzincirde tutulan verilere dayanarak karar alan kullanıcılar verinin nasıl kontrol edildiği, sorgulandığı ve hedeflenen kapsama ne derecede uygun olduğunun anlaşılması konusunda çok dikkatli olmalıdır. İç denetçiler de hizmet sundukları tarafları blokzincirin her sorunun çözümü olmadığı konusunda uyarmalı, blokzincirin sağlayacağı katkının paylaşılan bir veri tabanı ya da bir ERP sisteminden fazla olduğundan emin olunmasının önemini vurgulamalıdırlar (Sheldon, 2018, s. 11). Blokzincir teknolojisi halen tam olgunlaşmamış ve gelişimini devam ettiren bir teknolojidir. Karar vericiler bu noktada teknolojiden faydalanmak konusunda erken davrananlardan veya kendini ispatlamış teknolojik çözümleri kullanmaya devam ederek bu yeni teknoloji için bekle ve gör yaklaşımını benimseyenlerden olmak konusunda bir karar vermelidirler.

Brender ve diğerlerinin (2018) İsviçre'deki 23 denetim firmasından 34 mali ve BT denetçisi ile yüz yüze görüşme yolu ile yaptıkları anket sonucunda denetçilerin hemen hemen tamamının orta vadede denetim mesleğinde bir değişim olmasını bekledikleri, yarısından fazlasının ise denetim fonksiyonlarının çok daha fazla BT yönelimli olacağını bekledikleri sonucuna ulaşılmıştır. Görüşülen bazı denetçiler denetçilerin programlama gibi spesifik BT yeteneklerine sahip BT mühendis denetçileri olacakları hipotezini öne sürmüşler, hatta bir kısmı 'blokzincir denetçisi' ifadesinden bahsetmiştir.

Brender ve diğerlerine (2018) göre denetim mesleği bir dönüm noktasındadır ve teknolojinin bu konudaki potansiyel yıkıcı etkileri tam olarak tahmin edilememektedir. Daha küçük ölçekli denetim firmaları bu değişikliklerle yüzleşmek için yeterli donanıma sahip değildir. Bu yıkıcı etkiler denetim mesleği paradigmasını daha fazla BT odaklı olacak biçimde değiştirecek, dolayısı ile denetçilerin profili de değişecektir.

Birçok denetçiye göre yeni denetim ve muhasebe standartları ve yeni gelişmeler konusunda güncel ka-

lınmaya gerek duyulmakta, dahası BT yeteneklerinin geliştirilmesi gerekmektedir. Denetçilerin büyük bölümünün daha derin BT kabiliyeti konusunda eğitim ihtiyacı bulunmaktadır. Denetçiler kodlama, özetleme algoritmaları, kriptografi, akıllı sözleşmelerin teknik ve hukuki boyutu gibi konularla yeteneklerini genişletmeli, özellikle yeni ortaya çıkan yönetişim problemlerini anlamak için kendilerini güncellemelidirler (Brender vd., 2018, s. 17, 22; Chalker, 2018).

İç denetim mesleğinin üst yönetime destek verme fonksiyonu dikkate alınarak blokzincir risklerini izlemek ve değerlendirmek için yeterli kaynaklara sahip olunup olunmadığı konusu değerlendirilmelidir. Bu kaynaklar ilave personel, dış kaynaktan temin edilecek uzmanlar, BT veya siber güvenlik birimleriyle daha yakın ilişkiler veya denetim personelinin gerekli eğitimi almaları için sağlanacak ilave bütçe olabilir (Kelly, 2019, s. 3).

Blokzincir teknolojisinin denetim mesleğine potansiyel etkileri değerlendirilirken iki farklı durum göz önünde bulundurulmalıdır; denetlenen tarafın blokzincir teknolojisini iş süreçlerinde kullanmaları sonucunda blokzincir sisteminin denetlenmesi ihtiyacı ve teknolojinin bir denetim aracı olarak kullanılması.

Dikkate alınması gereken bir diğer konu bazı durumlarda birden fazla kuruluşla işbirliği içinde çalışma ihtiyacıdır. Blokzincirlerin her biri kendi yönetişim yapısına sahiptir ve bir blokzincir birden çok kuruluşa ait çok sayıda paydaşı içerebilir. Bu durumda, tüm paydaşların gereksinimlerinin karşılanıp karşılanmadığından emin olmak için farklı kuruluşlardaki iç denetçilerin birlikte çalışmaları gerekecektir (Rooney, Aiken ve Rooney, 2017, s. 42).

Doğanay'a (2019) göre gelişen teknolojilerle birlikte iş dünyası iki önemli riskle karşı karşıya kalmıştır; yeni teknolojilerin tam olarak anlaşılıp uygulanamaması, dijitalleşmenin beraberinde getirdiği siber risklerin anlaşılamaması. Bu durum denetim mesleği için de geçerlidir.

Chalker (2018), uygun yönetişim, risk yönetimi ve kontrollerin başlangıçta inşa edilmesinin bir problem ortaya çıktıktan sonra uygulamaktan çok daha kolay olduğu düşüncesinden hareketle denetçilerin blokzincir süreçlerine erkenden dahil olmaları gerektiğini düşünmektedir. Blokzincir uygulamaları kurumun geleneksel BT yapısının dışında gerçekleşebileceğinden denetçiler, kurum BT organizasyonunun çok daha ötesine bakmalıdırlar.

3.2. Blokzincir teknolojisinin iç denetim faaliyetlerine sunduğu fırsatlar

Unerman ve O'Dwyer (2004), 2001 yılındaki *Arthur Andersen* ile bağlantılı *Enron* skandalı gibi bazı olumsuz tecrübelerin sadece bu firmaları değil küresel denetim endüstrisini olumsuz etkileyerek bu mesleğin en önemli varlığı olan kamu güveninin zedelenmesine yol açtığını belirtmektedir. Bu güvenin yeniden sağlanması için muhasebe ve denetim standartları gibi yeni düzenlemeler getirilmiş, bu düzenlemelerin getirdiği zorunluluklar firmalar için bazı işlemlerin karmaşıklığının artması, kontrol faaliyetlerinin ve raporlamaların maliyetlerinin yükselmesine neden olmuştur. Günümüzde, blokzincir teknolojisi kurumsal işletmelere dijital etkileşimlerini veya işlem kayıtlarını şeffaf, güvenli, denetlenebilir, etkili ve kesintilere karşı dayanıklı bir biçimde gerçekleştirme imkanı sunmaktadır.

Bu teknolojinin verilere daha etkin bir biçimde erişimi mümkün kılacağı açıktır. Herhangi bir varlığın ya da belgenin kodlanabilmesi veya bir kayıt defteri aracılığı ile referanslanabilmesi denetçilerin ve muhasebe çalışanlarının işlerini kolaylaştıracak, manuel işlemleri azaltacak, tüm işlemlerin izlenebilirliğini sağlayacaktır (Schatsky ve Muraskin, 2015, s. 2,3). Büyük uluslararası denetim firmaları bir denetimi gerçekleştirmek için gerekli olan zaman ve maliyetin kayda değer miktarda azalacağını öngörmektedir (Brender vd., 2018, s. 7). Bu teknoloji ile günümüz sistemlerinde her gün rutin olarak yürütülen bazı işler -farklı sistemlerdeki kayıtların mutabakat işlemleri gibi- gereksiz hale gelecektir (Rooney, Aiken ve Rooney, 2017, s. 42).

Blokzincir, bilgisayar işlemleri ile ilgili birçok riski azaltma ya da ortadan kaldırma potansiyeline sahiptir. Birçok kuruluş veri yedeklemesi için iç kontrollere ve süreçlere sahiptir. Blokzincir ile veriler kalıcı bir kayıt defterinde depolandığından artık veri yedeklemeye gerek kalmayacaktır. Bir düğümle ilgili bir ihlal gerçekleştiğinde kalan diğer düğümlerde de kayıt defterinin tamamı, ilgili protokoller ve kaynak kodları bulunduğundan işlemler devam edecektir (Diedrich, 2016).

Blokzincirde işlemlerin grup işleme (*batch processing*) ile yayınlanması için bir çizelgeleme gereksinimi de yoktur. İşlemler iletişim ve mutabakat protokolleri tarafından belirlenen biçimde neredeyse gerçek zamanlı olarak gerçekleştirilir ve kaydedilir. Blokzincir

felaket kurtarma bakımından da önemli avantajlar sunmaktadır. Coğrafi olarak farklı bölgelerdeki düğümlerde tutulan kayıtlar bir felaket durumunda çalışmaya devam edecektir. Felaket durumu sona erdiğinde bundan etkilenen düğümler yeniden blokzincir ağına dahil olarak en güncel kayıtları kendilerine kopyalayabilirler (Diedrich, 2016).

Blokzincirin kayıtların değiştirilemezlik özelliğinden dolayı kaydedilen verilerin korunması için ilave kontrollere gerek yoktur. Tüm işlemlere ait kayıtlara anlık olarak erişilebilir. Tüm işlemler ayrıca otomatik olarak teknolojinin kendisi tarafından doğrulanarak onaylanmaktadır. Bu nedenle denetçilerin temel odak noktaları zaten teknoloji tarafından yerine getirilen, işlemlerin mevcudiyetini, kanıtların bulunmasını, doğruluğunu ve tamlığını garanti etmek olmayacaktır (Sheldon, 2018, s. 10; Brender vd., 2018, s. 20). Blokzincir teknolojisi eski verilerin silinmesi veya değiştirilmesine ilişkin riskleri de hemen hemen ortadan kaldırmaktadır. Bir blok onaylanıp zincire eklendikten sonra zincirdeki eski verilerin değiştirilmesi blokzincir ağındaki düğümler değişiklik konusunda tamamen mutabık olmadıkça imkansızdır.

Blokzincir teknolojisi şeffaf bir teknolojidir, maliyetleri düşürebilir, daha hızlı ve daha ucuz biçimde işlemler gerçekleştirebilir. Ayrıca asla değiştirilmesi mümkün olmayan işlem kayıtları sunarak denetim izlerini (*log*) otomatik hale getirmektedir. Bu durum denetimlerin gelecekte daha etkin biçimde gerçekleştirilmesi için bir fırsattır (Whitehouse, 2018). Kelly'ye (2019) göre blokzincir teknolojisi tam potansiyelini yansıttığında her çeşit işlem için kusursuz ve değiştirilmesi mümkün olmayan bir şeffaflık sağlayacak, tüm endüstrinin çalışma şeklini değiştirecek, hatta denetim mesleğini dönüştürecektir.

Kelly (2019) ve Rooney ve diğerleri (2017) blokzincir teknolojisi ile tüm işlemlere her an ulaşılabileceğinden örneklemeye ihtiyaç duyulmayacağını ileri sürmektedir.

Blokzincir teknolojisinin iş süreçlerinde kullanımının denetim iş yükünü azaltması ve bu ve benzeri teknolojilerin denetimlerde daha yoğun kullanılması ile denetçilerin daha fazla katma değer sağlayıcı faaliyetlere odaklanmaları da mümkündür. Operasyonel ve finansal bilgilerin blokzincire sürekli olarak kaydedilmesi sayesinde bu bilgi istendiği anda analiz edilebilir ve gerçek zamanlı denetimler gerçekleştirilebilir.

Psaila (2017) blokzincir teknolojisinin denetim bakımından fırsatlarını kaydedilen verilerin değiştirilememesi, işlemlerin sürekli olarak doğrulanabilmesi ve şeffaflık, doğrulama sürecinin otomasyonunun denetim ortamında maliyet etkinliği sağlaması, örneklem seçimi yerine tüm anakütlenin denetlenebilmesi ve sağlanan güvencenin artması, sürekli denetimi mümkün kılması biçiminde sıralamaktadır.

Nesnelerin interneti gibi diğer bazı teknolojilerle birlikte kullanıldığında blokzincir teknolojisi bazı fiziksel varlıkların hareketlerinin de gerçek zamanlı olarak izlenebilmesini mümkün kılmaktadır. Bu teknoloji ile aynı zamanda, neredeyse gerçek zamanlı olarak kullanıcı rolleri ve taleplerine göre farklı biçimde içerikleri düzenlenmiş olan blokzincir kayıtlarını yöneticiler, denetçiler ve diğer bazı paydaşlar gibi ilgili taraflara sürekli olarak yayınlamak da mümkündür (Dai, 2017, s. 60, 61).

Tysiac (2018) blokzincirin yaygınlaşması ile denetçiler için akıllı sözleşme denetçisi, konsorsiyum blokzincirlerin kontrol etkinliğinin denetimi, katılım için izin gerektiren blokzincirlerde erişim izni yöneticisi, blokzincir ağı katılımcılarının arasındaki olası ihtilaflar için arabulucu gibi yeni rollerin ortaya çıkabileceğini öne sürmektedir.

Blokzincir teknolojisi ile tutulan muhasebe kayıtları sayesinde herhangi bir kişi istediği zaman işlemleri bir gelir tablosu ve bilanço biçiminde toplayabilir ve firma veya denetçileri tarafından hazırlanan üç aylık mali durum raporlarının beklenmesi gerekmez. Mali raporlamadaki bu radikal değişikliğin bir maliyeti olmakla birlikte çok önemli iki katkısı bulunmaktadır: Onaylı bilgilerin dışarıya açılmasıyla firmanın verilerinin doğruluğuna duyulan güvenin artması, firmanın kayıtları ve belgelerinin doğruluğu konusunda güvence vermek için işe alınan ve yolsuzluğa da açık bir süreç yürüten yüksek maliyetli denetçilere gerek kalmaması (Yermack, 2017, s. 24).

Yermack'a göre (2017) blokzincirde gerçek zamanlı tutulan kayıtlar sayesinde şüpheli varlık transferleri ve çıkar çatışması anlamına gelebilecek bazı diğer işlemlerin anında fark edilmesi sağlanabilecek, gerçek zamanlı muhasebe kayıtlarının tutulabilmesi ile denetim firmalarının rolleri azalacak, bu teknolojiye dayanan akıllı sözleşmelerin kullanımıyla finansal problemlerin beklenen maliyetleri ve dava açma ihtiyacı azalacaktır.

Blokzincire dayalı sürekli denetim kavramı bu otonom ve kendi kendini düzenleyen paradigma içerisinde denetim mesleğinin rolü ile ilgili tartışmaları da beraberinde getirmektedir. Denetçilerin işlemlerin doğruluklarına dair güvence verme rolleri azalsa da hükümleri, görüşleri ve içgörüleri çok daha gerekli hale gelecektir. Denetimin odağı kayıtların izlenmesi ve doğrulanmasından sistemik değerlendirme, risk değerlendirme, önleyici denetimler ve yolsuzlukların tespiti gibi daha karmaşık analizlere doğru kayacaktır (Dai, 2017, s. 76).

Blokzincir önemli ancak düşük değerli olan doğrulama zamanında kayda değer miktarda azalmaya neden olarak denetçilerin zamanlarını blokzincirin kullanımı konusundaki yönetişim rollerinin değerlendirilmesi, "akıllı" ve "gerçek zamanlı" denetimlerin gerçekleştirilmesi, blokzincir sonrası çağda diğer karmaşık iç kontrol mekanizmaları ve risk yönetimi stratejisi konularında tavsiyelerde bulunmak gibi katma değeri daha fazla olan alanlara tahsis edebilirler. Bu, iç denetçilerin kuruluşlardaki güvenilir danışmanlar olma fonksiyonlarını pekiştirecektir (Yeung, 2017).

Kelly'ye (2019) göre yönetim kurulları hızlı bir biçimde blokzincir ile kripto paralar arasındaki farkları, blokzincir tasarım tiplerinin birbirlerinden farklarını öğrenmeli, teknoloji risk komitesi oluşturulması veya yeni ortaya çıkan teknolojiler ve blokzincir konusunda yetkin yeni yöneticilere yönetim kurullarında yer verilmesi konusunu dikkate almalıdırlar. Burada, iç denetim birimlerinin bu kavramlar hakkında yeterli düzeyde bilgi sahibi olarak yeni ortaya çıkan riskler ve teknolojinin detayları konularında üst yönetime eğitim ve danışmanlık vermek üzere hazırlıklı olmaları hem denetim mesleği hem de hizmet verilen kuruluş için önemli bir fırsattır.

3.3. Blokzincir teknolojisinin iç denetim faaliyetleri bakımından risk ve tehditleri

Geçmişte, ERP ve EDI (Electronic Data Interchange - Elektronik Veri Alışverişi) gibi yıkıcı teknolojiler kurumların verimliliğine önemli katkıda bulunmuş, maliyetleri düşürmüştür. Bununla birlikte teknolojik karmaşıklık, önemli miktarda finansal yatırım ve zaman gereksinimi, teknolojinin diğer paydaşlara yaygınlaştırılmasındaki güçlükler ve süreçlerde değişiklik gerekliliği gibi unsurlar bu yeni teknolojilerin benimsenmesini engelleyebilmektedir (Dai, 2017, s. 79).

Blokzincir teknolojisi kuruluşların iş görme biçimlerinde büyük değişiklikler gerçekleştirmek konusunda büyük vaatler sunmanın yanında üst yöneticiler ve yönetim kurulları için bazı sorunlara yol açma potansiyelini de taşımaktadır. Teknolojinin yol açacağı dönüşümün neler olabileceği konusunda hiç kimsenin gerçekten bilgisi bulunmamaktadır. 1994 yılındaki internet veya 2005 yılındaki sosyal medyayı hatırlamak gerekirse; herkes teknolojinin bazı büyük ve önemli etkilerinin olacağını bilmekte, ancak hiç kimse bunun nasıl olacağını kesin olarak bilememektedir (Kelly, 2019, s. 1).

Protiviti'nin 2019 yılında kurumsal riskler konusunda yapmış olduğu ankette yönetim kurulu başkanları ve diğer üst yöneticilerin en büyük endişesinin inovasyon ve yeni teknolojileri kucaklamakta yetersiz kalmak olduğu ortaya çıkmıştır (Kelly, 2019, s. 1). Karar vericilerin blokzincir teknolojisini de içeren yeni teknolojiler konusunda karşı karşıya oldukları en önemli risk temkinli davranmaları durumunda teknolojinin gerisinde kalmaları ve fırsatları kaçırmaları, öte yandan erken davranarak bu fırsatları yakalamak stratejisini seçmeleri durumundaysa olumsuz bir senaryoda gereksiz yatırım yapılması ve kaynakların israf edilmiş olması durumudur. Bu riskleri en uygun biçimde yönetebilmek için konu hakkında yeterli ve güncel bilgiye sahip olarak ilerlemeleri yakın biçimde takip etmek gerekmektedir.

Blokzincir teknolojisi genellikle önemli depolama ve hesaplama kaynaklarına ihtiyaç duyduğundan, büyük şirket sistemlerinde benimsenmesi, daha büyük depolama sistemlerinin öngörülen gelişimine, veri iletimi için daha geniş bant genişliğine ve hesaplama gücünün önemli ölçüde genişlemesine bağlı olacaktır (Dai, 2017, s. 80).

Deloitte Kanada'dan muhasebede blokzincir teknolojisinin kullanımı konusunda çalışan kıdemli danışman Spoke (2015) blokzincir teknolojisinin sağladığı otomatik üçüncü taraf doğrulaması ile finansal işlemlerin testi için denetime olan bağımlılığı azaltacağını düşünmektedir.

Blokzincir ve veri analitiği, süreç otomasyonu, dijitalleşme, robotlaşma, yapay zeka (AI) gibi teknolojiler farklı karakteristiklere sahip olmalarına ve her birinin denetim mesleğine potansiyel etkileri farklı olmasına karşın önemli denetim standartları kurumları (IAASB ve PCAOB) bu teknolojileri birbirinden ayırt

etmeden yeni teknolojileri araştırmak için çalışma grupları kurmaktadırlar (Brender vd., s. 15). Denetim standartları bakımından bu tip bir ayrımın yapılmaması gelecekteki bu teknolojileri içeren denetim faaliyetlerinde bazı güçlüklere ve standart olmayan uygulamalara yol açabilecektir.

Büyük dörtlü olarak bilinen firmaların dışındakiler henüz bu konu ile ilgili çalışmaya başlamamış olup bekle ve gör stratejisini izlemektedirler. Deneyimsiz denetçiler tarafından yürütülen testler ve manuel süreçlerin otomatik hale gelmesiyle artık günümüzdeki kadar yeni mezun denetçi (*junior*) ihtiyacı kalmayacaktır. Artık daha uzman, daha deneyimli profesyoneller aranacaktır. Bu durum da denetim organizasyonundaki piramit yapısını ve firmaların kariyer planlamalarını etkileyecektir. İşe yeni alınan denetçilerin kıdemli denetçiliğe yükselmeleri süreci olumsuz etkilenecektir (Brender vd., 2018, s. 18).

Blokzincirin başarılı bir biçimde adaptasyonu çalıştığı ortamın güvenliğine yüksek derecede bağımlıdır. Makul düzeyde güvence verebilmek için, denetim süreçleri iç BT kontrollerinin işletim etkinliğinin değerlendirilmesi yönünde bir değişim göstermek zorundadır (Psaila, 2017, s. 3). Bu dönüşümün sağlanabilmesi için denetim birimlerinin insan kaynağının yeterliliğinin değerlendirilmesi ve bu doğrultuda güçlendirilmesi gerekmektedir.

Blokzincirin sunduğu fırsatlardan en büyük kazancın sağlanması bu teknolojinin geniş biçimde kabul görmesi ile mümkün olacaktır. Birçok blokzincir platformu veri güvenliğinin sağlanabilmesi için büyük miktarda depolama alanı ve hesaplama gücüne ihtiyaç duymaktadır. Çok hacimli kurumsal verilerin böyle bir sistemde tutulması oldukça zorlu ve potansiyel olarak da pahalı olabilir (Dai, 2017, s. 81).

Güvenilir bir blokzincirde yer alan işlemin doğrulanarak onaylanması kesin mali durum açıklamaları için yeterli bir kanıt olabilir ancak işlemin doğası gereği yeterli bir denetim kanıtı işlevi görmeyebilir. Yani, blokzincir üzerinden bir değer transferi yapıldığında değerin teslim edildiği doğrulanabilir ancak bu değer karşılığında teslim edilmesi gereken ürünün teslim edilip edilmediği belirlenemeyebilir. İlave olarak, blokzincirin yönetimi denetlenen tarafından kontrol edilmiyor da olabilir (Tysiac , 2018 ; Bible vd., 2017).

Bu konuyu karmaşıklaştıran bir diğer husus da blokzincirin tek bir ürün veya uygulama olmamasıdır. Henüz kabul edilmiş standartları bulunmamaktadır ve blokzinciri kullanan 20 kuruluşa gidilse belki 16'sında farklı tip yazılım ve yarım düzine farklı mimari ile karşılaşılacaktır (Whitehouse, 2018).

Bazı yayınlarda blokzinciri teknolojisinin muhasebe denetmenlerince yürütülen mali durum tabloları denetimlerine ihtiyacı ortadan kaldıracağını iddia edilmektedir. Tüm işlemler geri döndürülemez ve değiştirilemez bir blokzincirde saklandıktan sonra denetim veya denetçiye gerek kalmayabileceği öne sürülmektedir (Bible, Raphael, Taylor ve Valiente, 2017).

Denetçiler hangi düğümlerin mutabakat mekanizmasına katıldıklarını, mutabakat mekanizmasını, işlemleri doğrulayan düğümlerin hesaplama güçlerinin dengeli dağıtılıp dağıtılmadığını, tek bir düğüm ya da küçük bir grubun usulsüzlük ya da %51 saldırısı ile zararlı faaliyetlerde bulunma risklerini değerlendirmelidir (Sheldon, 2018, s. 5). Bu konuları değerlendirmek için derinlemesine teknik bilgi ve denetçilerin bu güne kadar aşina olmadıkları bazı konularda yetkinlik kazanmaları gerekecektir.

4. SONUÇ VE ÖNERİLER

Henüz kamu uygulamaları oldukça kısıtlı, kamudaki bilinirliği nispeten az ve yakın gelecekte operasyonel kamu hizmetlerini üstlenme beklentisi düşük olmakla birlikte, teknolojinin bu güne kadar ivmesi sürekli artan gelişim hızı göz önüne alındığında, blokzincir teknolojisinin getireceği dönüşüme karşı hazırlıklı olunması, bu dönüşümün fırsatlarının kaçırılmaması ve risklere karşı gerekli tedbirlerin alınabilmesi için çok önemlidir. Bu hazırlığın etkin biçimde yapılabilmesi için de ön şart teknoloji hakkında yeterli düzeyde bilgi sahibi olmak ve dünyadaki gelişmeleri yakından takip etmektir.

Bu teknoloji, tüm sektörleri olduğu gibi kaçınılmaz olarak denetim faaliyetlerini de etkileyecektir. Bu etki hem olumlu hem de olumsuz unsurlar içermektedir. Denetim faaliyetleri bakımından blokzincir teknolojisinin sunduğu fırsatlar sürekli ve gerçek zamanlı denetimleri mümkün kılması, kaydedilen verilerin

silinememesi ve değiştirilememesi nedeniyle güvenilir kanıtlar sunması, manuel işlemleri azaltması, tüm anakütleyi denetleme imkanı vererek örneklem seçme gerekliliğini ortadan kaldırması, denetimin iş yükünü azaltarak denetçilerin katma değer sağlayıcı diğer faaliyetlere daha fazla odaklanmalarını sağlaması biçiminde özetlenebilir. Öte taraftan, bu teknolojinin denetim faaliyetleri bakımından potansiyel tehdit içeren özellikleri ise tasarımı ve mimarisi nedeniyle anlaşılmasının güçlüğü, süreçlerin yeniden tasarlanmasını gerektirmesi, yönetişim yapısının karmaşıklığı, denetlenebilmesi ve denetimlerde kullanılabilmesi için teknik bilgi gerektirmesi, denetim sürecinde daha çok rutin testleri gerçekleştiren deneyimsiz denetçilere olan ihtiyacı ortadan kaldırması ve henüz mevzuatının ve standartlarının bulunmaması biçimindedir.

Uluslararası iç denetim standartları uyarınca (2120 – Risk Yönetimi ve 2130 - Kontrol) iç denetim faaliyeti, kurumun yönetişim süreçlerinin, faaliyetlerinin ve bilgi sistemlerinin maruz kaldıkları riskleri değerlendirmek ve bu risklere karşılık olarak tasarlanmış kontrollerin etkinlik ve verimliliklerini değerlendirerek etkin kontrollerin tasarlanması ve uygulanması konusunda kurumlarına yardımcı olmak zorundadır. Bu standart gereğince, iç denetim birimleri blokzincir gibi teknolojilerin stratejik ve operasyonel risklerini değerlendirmeli, bilgilerin güvenilirliği ve doğruluğunun, faaliyetlerin etkinliği ve verimliliğinin, mevzuat, politika ve prosedürlere uyumun sağlanması için gerekli kontrollerin tasarlanmasında yönlendirici ve kolaylaştırıcı rol üstlenmelidirler.

Risk ve kontrollere yönelik rollerinin yanı sıra iç denetim birimleri kurum içerisinde münferit olarak yürütülen ve üst yönetimin dikkatini çekmemiş olan çalışmalar varsa bunları tespit ederek üst yönetimi bilgilendirebilir, konu hakkındaki yetkinlik düzeyine paralel olarak bu çalışmaları değerlendirebilir, kurumsal risk yönetimi ve stratejik yönetim kapsamında blokzincir teknolojisinin dikkate alınması için gerekli kurul ve birimleri bilgilendirebilir. Bu bağlamda bu teknolojiye ilişkin çalışmalarda öncü rol üstlenmek iç denetim birimleri ve iç denetim faaliyetleri konusunda kurumlardaki farkındalığın artırılması, itibarın ve danışmanlık fonksiyonunun geliştirilmesi bakımlarından bir fırsat olarak değerlendirilmektedir.

Üst yönetim ve karar alıcılar, blokzincir teknolojisini kullanacak kuruluşların tedarikçisi konumunda bulunan işletmelerin zorlanabilecekleri konular, ihtiyaç duyulabilecek yeni teknolojiler, eski teknolojilere entegrasyon, ihtiyaç duyulacak nitelikli insan kaynağı, en uygun kulanım alanları konularına cevap bulmak konusunda önemli bir sorumluluk yüklenmektedirler. Bu sorumluluk ve karar alma konusundaki iyimser öngörü karar verici konumdaki yöneticilerin blokzincir teknolojisi konusunda yeterli bilgilerinin olduğu varsayımına dayanmaktadır. İç denetim fonksiyonu, üst yönetimi bu kararlarda destekleyici bir rol üstlenebilir.

İç denetim birimleri olarak teknolojinin mesleğe etkilerine karşı hazırlıklı olunması bakımından iç denetimin kurumdaki blokzincir projelerine dahil edilip edilmediği, kurumdaki bu projelerden haberdar olunup olunmadığı, bu teknolojinin nasıl ve nerede kullanılabileceği, sunacağı fırsatların ve getireceği risklerin neler olduğu sorularına cevap aranması gerekmektedir.

İç Denetim Standartlarına göre (1210 – Yeterlilik) iç denetçiler bireysel görevlerini yerine getirebilmek için gerekli bilgi, yetenek ve diğer vasıflara sahip olmak zorundadır. Bu standart doğrultusunda, blokzincir teknolojisinin geniş kabul görerek yaygınlaşmasından önce iç denetim birimleri iç denetçilerin bu yeni teknoloji konusunda eğitim almalarını sağlamalıdır. Konu hakkında belirli bir yetkinliğe eriştikten sonra görev yaptıkları kurumlarda olası blokzincir uygulamalarının planlama aşamalarına dahil olarak uygulamanın yönetişim, risk yönetimi ve kontrollerin henüz tasarım aşamasında sisteme entegre edilmesini sağlamalıdırlar. Teknolojinin büyük avantajlar sağlayacağı beklentisi ile birlikte blokzincirin kurumdaki belirli süreçler için en uygun seçim olup olmadığı da değerlendirilerek teknolojinin kullanılma kararı konusunda azami mesleki özen gösterilmelidir. Aşırı temkinli davranarak fırsatları kaçırmak ile çok aceleci davranıp gereksiz maliyetlere neden olmak arasındaki denge çok iyi kurulmalıdır. Bu dengenin kurulması için en kritik nokta ise teknoloji konusunda yeteri kadar bilgi edinerek karar vermeyi destekleyici donanıma sahip olmaktır. İç denetçiler bu yeni teknolojiye karşı açık ve kucaklayıcı olmalı, getireceği problemlerle birlikte fırsatları da anlayarak gelecekteki yıkıcı değişikliklere karşı hazırlıklı olmalıdır.

Kaynakça

Berryhill, J., Bourgery, T., & Hanson, A. (2018). *Blockchains Unchained: Blockchain Technology and its Use in the Public Sector, OECD Working Papers on Public Governance, No. 28.* Paris: OECD Publishing. http://dx.doi.org/10.1787/3c32c429-en adresinden alındı.

Bible, W., Raphael, J., Taylor, P., & Valiente, I. O. (2017). *Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession.* Toronto: Deloitte Development LLC.

Boucher, P., Nascimento, S., & Kritikos, M. (2017). *How blockchain technology could change our lives.* Brussels: Scientific Foresight Unit (STOA), European Parliament.

Brender, N., Gauthier, M., Morin, J.-H., & Salihi, A. (2018). *The Potential Impact of Blockchain Technology on Audit Practice.* Geneva: University of Applied Sciences and Arts Western Switzerland.

Casey, M., & Vigna, P. (2018). *The Truth Machine: The Blockchain and the Future of Everything.* New York: St. Martin's Press.

Catalini, C., & Gans, J. (2017). Some Simple Economics of the Blockchain. *Rotman School of Management Working Paper No. 2874598; MIT Sloan Research Paper No. 5191-16.*

Chalker, A. (2018, 6 12). *Why Internal Auditors Must Care About Blockchain*. 3 25, 2019 tarihinde The Protiviti View: https://blog.protiviti.com/2018/06/12/internal-auditors-must-care-blockchain/ adresinden alındı.

Chartered Accountants Australia and New Zealand. (2017). *The Future of Blockchain: Applications and Implications of Distributed Ledger Technology.* Sydney: Chartered Accountants Australia and New Zealand.

Cheng, S., Daub, M., Domeyer, A., & Lundqvist, M. (2017, 2). Digital McKinsey. *Using blockchain to improve data management in the public sector*.

CoinMarketCap. (2019, 4 1). *Coin Market Capitalization*. 3 22, 2019 tarihinde https://coinmarketcap.com/coins/views/market-cap-by-total-supply/ adresinden alındı.

Cybersalon. (2013, 9 5). *Cypherpunks, Bitcoin & the Myth of Satoshi Nakamoto*. 5 16, 2019 tarihinde Cybersalon: http://cybersalon.org/cypherpunk/ adresinden alındı.

Dai, J. (2017, 10). A Dissertation for the degree of Doctor of Philosophy. *Three Essays on Audit Technology: Audit 4.0, Blockchain, and Audit App*. New Jersey: The State University of New Jersey.

Deloitte. (2018). *Breaking blockchain open Deloitte's 2018 global blockchain survey.* Deloitte Development LLC.

Deloitte. (2019). *Unleashing blockchain in finance.* Deloitte Development LLC.

Diedrich, H. (2016). *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations.* Wildfire Publishing.

Digiconomist. (2019, 3 30). *Bitcoin Energy Consumption Index*. 3 31, 2019 tarihinde Digiconomist: https://digiconomist.net/bitcoin-energy-consumption adresinden alındı.

Doğanay, S. (2019, 3 15). Yeni ve gelişen teknolojilerin yarattığı dönüşüm. Türkiye Kimya Petrol Lastik ve Plastik Sanayii İşverenleri Sendikası. 3 2019 tarihinde https://kiplas.org.tr/dr-sertac-doganay-ile-gelisen-teknolojiler-uzerine-konustuk/ adresinden alındı.

Galen, D., Brand, N., Boucherle, L., Davis, R., Do, N., El-Baz, B., . . . Lee, J. (2018). *Blockchain for Social Impact Moving Beyond the Hype.* Stanford: Stanford Graduate School of Business.

Greenspan, G. (2016, 3 17). *Blockchains vs centralized databases*. 3 27, 2018 tarihinde https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/ adresinden alındı.

Güven, V., & Şahinöz, E. (2018). *Blokzincir, Kripto Paralar, Bitcoin.* İstanbul: Kronik Kitap.

İlkbahar, R. (2019, 3 5). *Araştırma Şirketlerinin Gözünden Blokzincir'in Geleceği*. Medium: https://medium.com/@recepilkbahar/arastirma-sirketlerinin-gozunden-blokzincirin-gelecegi-5bc15045bc50 adresinden alındı.

Kelly, M. (2019, 2). Boards Look to Harness Blockchain Disruption. *Tone at the Top*. The Institute of Internal Auditors.

Killmeyer, J., White, M., & Chew, B. (2017). *Will blockchain transform the public sector?* Deloitte University Press.

Lyons, T., Courcelas, L., Grandsenne, J., Carrel, E., & Timsit, K. (2018). *Blockchain Innovation in Europe.* European Union Blockchain Observatory and Forum.

Maupin, J. (2018). *The G20 Countries Should Engage with Blockchain Technologies to Build an Inclusive, Transparent, and Accountable Digital Economy for All.* Max Planck Institute.

Nagpal, R. (2017, 9 9). *#8 Steps to Build a Blockchain Solution*. 6 1, 2018 tarihinde Entrepreneur - Start, run and grow your business: https://www.entrepreneur.com/article/300077 adresinden alındı.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Nomura Research Institute. (2016). *Survey on Blockchain Technologies and Related Services FY2015 Report.* Tokyo: Japan's Ministry of Economy, Trade and Industry (METI).

Onbirinci Kalkınma Planı Kamuda Kurumsal Yönetimde Yeni Yaklaşımlar Özel İhtisas Komisyonu. (2017). *Onbirinci Kalkınma Planı Kamuda Kurumsal Yönetimde Yeni Yaklaşımlar Özel İhtisas Komisyonu Ön Raporu.*

Pelletier, J. (2018, 4 5). *A Blockchain Primer for Internal Audit*. 3 26, 2019 tarihinde IA Online: https://iaonline.theiia.org/blogs/Jim-Pelletier/2018/Pages/A-Blockchain-Primer-for-Internal-Audit.aspx adresinden alındı.

Psaila, S. (2017). *Blockchain: A game changer for audit processes?* Malta: Deloitte.

PwC. (2018). *Global blockchain survey.* PricewaterhouseCoopers Limited.

PwC. (2018, 3 6). *PwC Blockchain Validation Solution*. 3 14, 2019 tarihinde PwC: Audit and assurance, consulting and tax services: https://www.pwc.com/us/en/about-us/new-ventures/pwc-blockchain-validation-solution.html adresinden alındı.

Qureshi, H. (2018, 1 28). *The authoritative guide to blockchain development*. 5 31, 2018 tarihinde freeCodeCamp: https://medium.freecodecamp.org/the-authoritative-guide-to-blockchain-development-855ab65b58bc adresinden alındı.

Radore. (2017, 1 31). *Elektrik ve Elektrik Birimleri Nelerdir?* 3 31, 2019 tarihinde Radore Blog: https://radore.com/blog/elektrik-birimleri-nelerdir.html adresinden alındı.

Ray, S. (2018, 2 19). *The Difference Between Blockchains & Distributed Ledger Technology*. 2 10, 2019 tarihinde Towards Data Science: https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92 adresinden alındı.

Rooney, H., Aiken, B., & Rooney, M. (2017). Q&A. Is Internal Audit Ready for Blockchain? *Technology Innovation Management Review*, 7(10): 41-44.

Schatsky, D., & Muraskin, C. (2015). *Beyond bitcoin Blockchain is coming to disrupt your industry.* Deloitte University Press.

Sheldon, M. D. (2018, 12 5). A Primer for Information Technology General Control Considerations on a Private and Permissioned Blockchain Audit. *American Accounting Association Journal*.

Smith, A. M. (2018, 3 15). *The blockchain challenge nobody is talking about*. 3 26, 2019 tarihinde PwC Next in Tech: https://usblogs.pwc.com/emerging-technology/the-blockchain-challenge/ adresinden alındı.

Spoke, M. (2015, 6 11). *How Blockchain Tech Will Change Auditing for Good*. 3 25, 2019 tarihinde CoinDesk: https://www.coindesk.com/blockchains-and-the-future-of-audit adresinden alındı.

T2 Yazılım A.Ş., Bankalararası Kart Merkezi A.Ş. (2018). *Keşif: Blockchain'in Sırları BBN Faz 1.* İstanbul: Bankalararası Kart Merkezi A.Ş.

Thake, M. (2018, 2 8). *What's the difference between blockchain and DLT?* 2 10, 2019 tarihinde Medium: https://medium.com/nakamo-to/whats-the-difference-between-blockchain-and-dlt-e4b9312c75dd adresinden alındı.

Tysiac , K. (2018, 3 15). *How blockchain might affect audit and assurance*. 3 22, 2019 tarihinde Journal of Accountancy: https://www.journalofaccountancy.com/news/2018/mar/how-blockchain-might-affect-audit-assurance-201818554.html adresinden alındı.

Unerman, J., & O'Dwyer, B. (2004). Enron, WorldCom, Andersen et al.: a challenge to modernity. *Critical Perspectives on Accounting, 15*, 971-993.

Usta, A., & Doğantekin, S. (2017). *Blockchain 101.* İstanbul: Kapital Medya Hizmetleri A.Ş.

Voshmgir, S. (2017). Disrupting governance with blockchains and smart contracts. *Strategic Change, Vol.26*, 499-509.

Whitehouse, T. (2018, 4 3). *Auditors develop early plans for how to audit blockchain*. 3 24, 2019 tarihinde Compliance Week: https://www.complianceweek.com/news/news-article/auditors-develop-early-plans-for-how-to-audit-blockchain#.W_R1cOgzY2w adresinden alındı.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview.* United States National Institute of Standards and Technology.

Yermack, D. (2017, 1). Corporate Governance and Blockchains. *Review of Finance*, 7-31.

Yeung, E. (2017, 6 9). *Blockchain 101 for Internal Audit*. 3 22, 2019 tarihinde LinkedIn: https://www.linkedin.com/pulse/blockchain-101-internal-audit-eric-yeung/ adresinden alındı.

NESNELERİN İNTERNETİ: RİSK TEMELLİ YAKLAŞIM

(INTERNET OF THINGS: RISK-BASED APPROACH)

Mine ZEYBEK* / Ercan Nurcan YILMAZ**

ÖZ

Son yıllarda hızla popüler bir teknoloji konsepti haline gelen "nesnelerin interneti" (Internet of Things, IoT), hali hazırda bazı zorluklar ve aşılması gereken problemleri olsa da özellikle 5G teknolojisinin de katkısıyla günlük hayatımızda önemli bir yer tutacaktır. Temel olarak basitten karmaşığa bir takım ana işlevleri olan ürün ya da cihazlar; birçok algılayıcı ve haberleşme arabirimi donanımı eklenerek algoritmalar ile desteklenmesi sonucunda matematiksel ve mantıksal özellikleri olan ve birbirleri ile "konuşabilen" akıllı cihazlar haline dönüşmüştür. Ancak bu yeni teknolojide güvenlik ve mahremiyet kavramları da dikkatle ele alınması gereken en önemli sorunlardandır. Güvenlik konusunda yapılan çok sayıda çalışma ve akademik tartışma bulunmasına rağmen, bahsi geçen akıllı cihazların ortak bir donanım, algoritma ya da arayüze sahip olmaması; hemen hepsi için geçerli bir güvenlik protokolü geliştirilmesinin önündeki en büyük engel olarak görünmektedir. Bu sebeple "nesnelerin interneti" teknolojisine sahip cihazların yaygınlaşıp ev ve işyerlerinde yerlerini almasıyla birlikte, yeterli önlemler alınmazsa, son yıllarda sayısı oldukça artan ve küresel çapta gerçekleştirilmeye başlanan siber saldırılarda, başka bir boyuta geçilmesinin önünü açacağı düşünülmektedir. Makale kapsamında nesnelerin internetinin güvenliği konusunda yapılan çalışmalar incelenmiş, nesnelerin internetinin yapısı ve mimarisinden bahsedilip, nesnelerin internetine yönelik güvenlik tehditleri ile yaşanmış olaylar ele alınmış ve nesnelerin internetinin denetiminde değerlendirilebilecek kontroller belirtilerek, nesnelerin internetinin güvenliğine yönelik alınabilecek önlemler sunulmuştur.

Anahtar Kelimeler: Nesnelerin interneti, siber güvenlik, mahremiyet, bilgi güvenliği, siber saldırı, denetim kontrolleri.

JEL Kodlaması: K42

ABSTRACT

Internet of Things (IoT), which has become a popular technology concept in recent years, will have an important place in our daily lives with the help of 5G technology, even though it already has some difficulties and problems to be overcome. In this new technology, basically, devices including from simple to complex main functions; security and privacy concepts are two of the most important issues to be handled with due to the fact that it is transformed into smart devices that have mathematical and logical features and can be talked to each other through the addition of many sensors and communication interface hardware. Although there are numerous studies and academic discussions about security of IoT, because of the fact that there is no common hardware, algorithm, or interface of these smart devices; developing a commonsecurity protocol for all of them is the biggest obstacle to achieve it. For this reason, devices with IoT technology take their places in the houses and workplaces, and if sufficient measures are not taken, it is thought that the cyber attacks, which have been increasing in recent years and are being carried out on a global scale and organized, will pave the way for another dimension. The previous studies on the security of the IoT were examined within the scope of this article. In addition, the structure, architecture and security threats of the IoT were discussed. The controls that can be evaluated for the audit of the Internet of Things are pointed out and also, the measures to ensure the safety of the IoT were presented.

Keywords: *Internet of Things, cyber security, privacy, data security, cyber attack, audit controls.*

JEL Classification: *K42*

---

*) İç Denetçi, İçişleri Bakanlığı, İç Denetim Birimi Başkanlığı, Ankara, Orcid: 0000-0002-8652-2082, mine.zeybek@icisleri.gov.tr

**) Doç. Dr., Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği Bölümü, Ankara, Orcid: 0000-0001-9859-1600, enyilmaz@gazi.edu.tr

Yazı Gönderim Tarihi: 02.04.2019, Yazı Kabul Tarihi: 05.04.2019

1. GİRİŞ

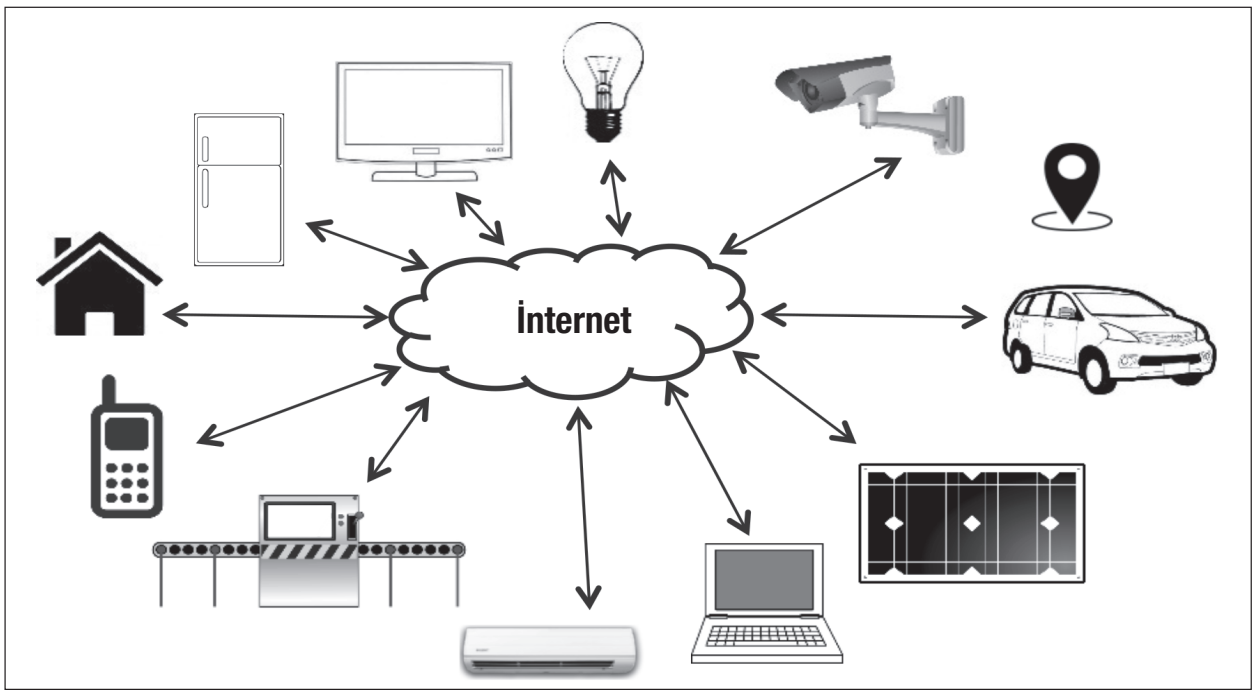
"Nesnelerin interneti" (Internet of Things, IoT) için, birbirlerine oldukça yakın olarak ifade edilen birden fazla tanım yer almaktadır. İlk olarak 1998 yılında Kevin Ashton tarafından yapılan bir sunumda kullanılan bu terim, internet benzeri bir yapıda birbirleri ile haberleşebilen cihazları tanımlamıştır (Weber, 2010) .

Gartner tarafından yayınlanan bir raporda (Gartner, 2017), sadece 2017 yılında internete bağlı olan, dünya çapında 8,4 milyar "nesne" kullanılacağı belirtilmektedir. Bu sayının 2016 yılı verilerinden %16 daha fazla olduğu ifade edilirken 2020'ye kadar 31 milyar cihaza, 2025'te ise 75 milyar cihaza ulaşması beklenmektedir (Brandon, 2016) (Claveria, 2019). Günümüzde ortalama bir akıllı cihaz tüketicisi yaklaşık 4 adet internete bağlı cihaza sahiptir (Buckle, 2016). Teknoloji, gelişmeye ve ilerlemeye devam ederken, nesnelerin interneti bireyin günlük hayatının birçok yönüne nüfuz ettiği için, büyümeyi yönlendiren belirli bir sektör yoktur. 2017 yılında 125.5 milyon olan giyilebilir cihaz sayısının, 2021 yılında 240.1 milyona ulaşması beklenmektedir (Lamkin, 2017). Otomotiv endüstrisinde de, 2020 yılında yeni araçların % 75'inin, internete bağlanabilmek için gerekli donanıma sahip olacağı tahmin edilmektedir (Greenough, 2015).

IoT cihazlarını üreten şirketlerin, cihazların güvenliğini sağlamak için ortalama bütçelerinin sadece % 11'ini harcadıkları ve şirketlerin % 67'sinin veri şifrelemeyi birincil güvenlik yöntemi olarak ele aldıkları rapor edilmektedir (Lohrmann, 2017). Bununla birlikte, 2017 yılında bir anket ile tüketicilerin IoT ile ilgili mevcut güvenlik kaygıları araştırılmıştır. Anket sonucunda tüketicilerin % 65'inin bir korsan tarafından IoT cihazlarının kontrolünün ele geçirebileceğinden, % 60'lık bir kesiminin ise verilerin sızdırılmasından veya çalınmasından endişe ettiği ve ortalama 2 adet akıllı cihaza sahip kullanıcılardan sadece %14'ünün bu cihazların güvenliği konusunda son derece bilgili olduklarına inanıldıkları tespit edilmiştir (Gemalto, 2017).

Bu verilerden de görüleceği üzere, IoT pazarı, akıllı telefonlar ve bilgisayarların benimsenmesiyle başlayarak akıllı saat ve bileklikler, akıllı televizyonlar, akıllı ev aletleri ve hatta akıllı otomobiller de dâhil olmak üzere gittikçe büyümekte ve günlük hayatımızın birçok bölümünde giderek daha yaygın hale gelmektedir (Şekil 1).

Şekil 1. IoT kullanım alanları



(Yazarlar tarafından oluşturulmuştur.)

Bu cihazlar temel olarak hayatlarımızı daha iyi ve daha kolay hale getirmeyi amaçlamakla birlikte, tüketicilerin çoğu zaman fark etmedikleri şey, hızlı büyüyen ağ bağlantılı cihazlarla, göz ardı edilmesi giderek zorlaşan ve giderek artan bir güvenlik riskidir. Son birkaç yılda IoT cihazlarının güvenlik açısından tehlikeye girdiği ve istismar edildiği birçok durum meydana gelmiştir.

Bu çalışmada literatürdeki IoT güvenliği konusundaki mevcut çalışmalar ile IoT'nin genel yapısı ve mimarisi incelenmiş, olası riskler ile son birkaç yılda meydana gelen saldırılar ele alınmış, IoT denetimi için önerilen kontroller belirtilmiş ve son olarak IoT güvenliğinin sağlanmasına yönelik alınması gereken tedbirler ve çözüm önerileri sunulmuştur.

Çalışmanın 2. bölümünde literatür araştırması yapılmış, 3. bölümünde IoT kullanım alanları, mimari yapısı, bileşenleri ve bu bileşenlere yönelik olası saldırılar ve riskler ele alınmıştır. 4. bölümde yaşanmış IoT saldırı vakaları belirtilmiş, 5. bölümde IoT denetimine yönelik kontrol listesi verilmiştir. 6. bölümde ise IoT güvenliğinin sağlanmasına yönelik çözüm önerileri üzerinde durulmuş ve son olarak araştırma sonucu elde edilen sonuçlar 7. bölümde tartışılmıştır.

2. LİTERATÜR ARAŞTIRMASI

IoT güvenliği üzerine bugüne kadar yapılan çalışmalar değerlendirildiğinde IoT ve ilgili sistemlerin güvenlik gereklilikleri, zorlukları ve bu sistemlere yönelik saldırılar ile güvenlik çözümleri üzerinde durduğu görülmektedir. Bu bölümde IoT'de zafiyet olarak görülebilecek unsurlar ile güvenliğin sağlanabilmesi amacıyla yapılan çalışmalar incelenmiştir.

Yapılan bir çalışmada nesnelerin internetinin kullanıldığı akıllı evlerin tasarımı aşamasında farkındalığın olması gerektiği vurgulanmış ve akıllı bina sistemlerinden istenilen verimi elde etmek için, tasarımcıların sistemin gücünün farkında olması ve sistemin deneyimli kişiler tarafından işletilmesi gerektiği ifade edilmiştir. Söz konusu çalışmada akıllı ev uygulamaları için eğitim seti tasarlanmış ve geliştirilen bu sistem sayesinde; kursiyerlerin akıllı bina sistemini öğrenme ve kendi özel sistemlerini geliştirme fırsatı bulacakları belirtilmiştir (Yılmaz, 2011).

Bir başka çalışmada ise IoT için düşünülen güncel protokol parçaları tanıtılarak, oluşabilecek güvenlik zafiyetleri, protokol yığınının her katmanı için irdelenmiştir. Aynı çalışmada, IoT güvenliğinin, yeni nesil internet güvenliğinin ayrılmaz bir parçası olarak düşünülmesi gerektiği ve bu bağlamda düşük karmaşıklığa ve yüksek güvenilirliğe sahip çözümlerin IoT ağları için yapılandırılması gerektiği belirtilmiştir. Ayrıca, interneti oluşturacak 6LoWPAN, 6TiSCH, CoAP ve benzeri protokollerin, güvenliğin ön planda olduğu bir anlayışla tasarlanması gerektiği de vurgulanmıştır (Görmüş vd., 2018).

Rizvi ve arkadaşları tarafından yapılan bir çalışmada da, IoT'nin yoğun olarak kullanıldığı kritik alanlardan bahsedilmiş ve IoT'nin şu anda karşı karşıya olduğu güvenlik gereklilikleri, zorlukları ve mevcut güvenlik çözümlerinden bazılarının tanımlanmasına yardımcı olacak sınıflandırma üzerinde durulmuştur (Rizvi vd., 2018).

Săndescu ve arkadaşları tarafından yapılan çalışmada ise, IoT bağlamında var olan güvenlik açıkları ve saldırıları ele alınmış, dinamik bir IoT Sistemi Güvenlik Testi (DISST) modelinin araştırma ve geliştirme çalışmalarının tamamlanıp hayata geçirileceği belirtilmiştir (Săndescu vd., 2018) .

Hussain ve Abdullah yaptıkları çalışmada IoT'nin büyümesinden dolayı güvenlik ve gizlilik gereksinimlerinin değiştiğinden ve geleneksel şifreleme ve şifre çözme tekniklerinin yetersiz kaldığından söz etmiş ve gelecekteki ihtiyaçları karşılamak için hafif şifreleme teknikleri gerektiğini ifade ederken, güvenlik saldırıları karmaşıklaştıkça bunların da gelecekteki ihtiyaçlara çözüm olamayabileceğini belirtmişlerdir (Hussain ve Abdullah, 2018).

Reyna ve arkadaşlarının yaptığı çalışmada ise, blok zincirin ve IoT'nin başarılı bir şekilde birlikte çalışabilmeleri için ele alınması gereken ana zorlukların bir analizi yapılmış ve blok zincir teknolojisinin nesnelerin interneti uygulamalarını geliştirmeye yardımcı olabileceği önemli noktalar belirlenmiştir. Ek olarak bu konudaki mevcut platformlar ve uygulamalar da incelenerek yasal mevzuatın benimsenmesinin, blok zincir ve IoT'nin, hükümet altyapısının bir parçası olarak dahil edilmesinin anahtarı olduğu ve vatandaş, hükümet ve şirketler arasındaki etkileşimi hızlandıracağı belirtilmiştir. IoT ve blok zincir entegrasyonun,

mevcut kağıt parayla aynı seviyede kripto para birimleri kuracak şekilde, blok zincir kullanımını büyük ölçüde artıracağı da vurgulanmıştır (Reyna vd., 2018).

Banerjee ve arkadaşları, nesnelerin internetinde paylaşılan verinin bütünlüğünü sağlamada blok zincir kullanımının potansiyelini ortaya koydukları çalışmada aynı zamanda, 2016'dan beri yayımlanan IoT ve ilgili sistemler için tasarlanmış güvenlik tekniklerini gözden geçirmişlerdir. Mevcut tehditleri tespit edebilmenin önemli olduğu ancak yakın gelecekte potansiyel tehdit ve saldırıları tahmin etme kabiliyetinin çok daha önemli olduğu vurgulanarak, dokuz potansiyel araştırma sorusuna yer verilmiştir (Banerjee vd., 2018).

Han, Jeon ve Kim yaptıkları çalışmada, akıllı ev sistemini oluşturan bileşenlerin temel güvenlik fonksiyonlarını gizlilik, bütünlük ve kullanılabilirliğe göre sınıflandırmış ve tanımlamışlardır (Han vd., 2015).

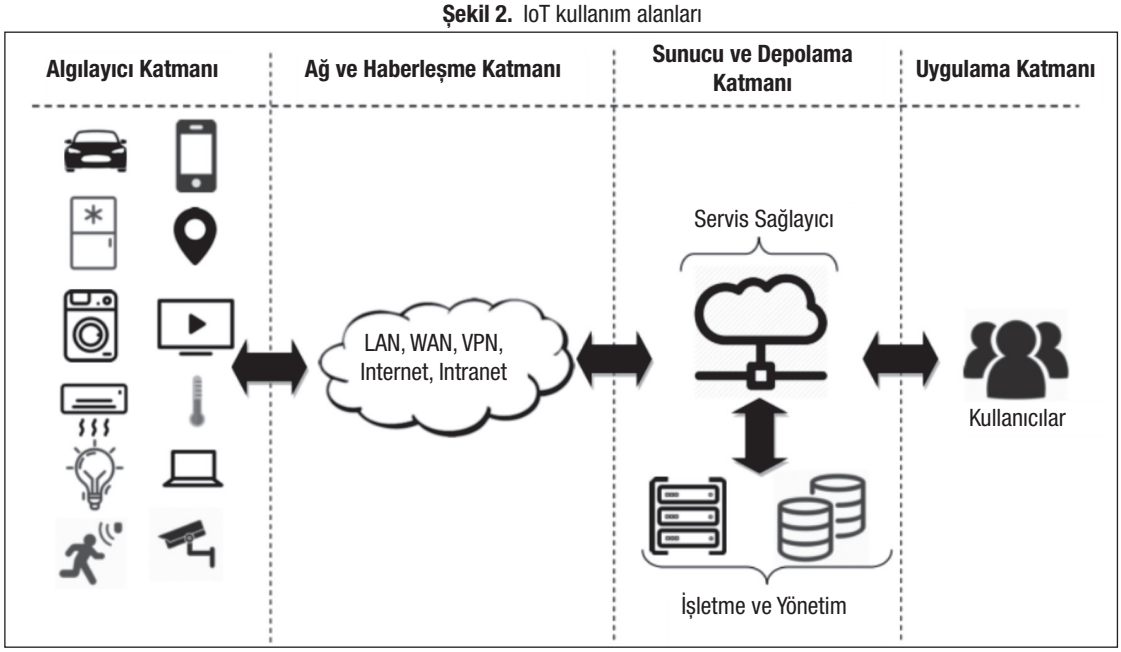
Şenol ve Arslan'ın yaptıkları çalışma ise IoT objelerinin donanımsal olarak çok çeşitli olmasından dolayı ortak bir güvenlik protokolü uygulamasının zor olduğunu, bu yüzden de tüm IoT objelerinin ağ üzerinden TCP/IP protokolü ile haberleşebildiği ve tüm zorlu güvenlik protokollerinin ağ geçidi cihazı üzerinde bulunduğu güvenli bir IoT Güvenli Ağ Geçidi tasarımını önermektedir. Önerilen bu sistemde objeler ve güvenli ağ geçidi arasında, güvenli bir ilişkinin kurulması gerektiği ve bu ilişkinin de iki tarafın da güvendiği bir sertifika otoritesi tarafından sağlandığı belirtilmektedir (Şenol ve Arslan, 2016).

3. NESNELERİN İNTERNETİNİN YAPISI

IoT kavramının terminolojideki tanımı üzerine birçok farklı görüş bulunmaktadır. Bu farklılığın sebebi aslında kavramı oluşturan iki sözcükten gelmektedir. Çeşitli ticari şirketler ve araştırma kurumları kendi altyapılarına, ilgi alanlarına göre ya internet kısmına ya da nesne kısmına ağırlık vererek tanım oluşturmuşlardır (Atzori vd., 2010).

Örneğin, Atzori vd., (2010) yaptıkları çalışmada, standart iletişim protokollerine dayalı, birbirine bağlı ve eşsiz olarak adreslenebilen evrensel nesneler ağı olarak, Madakam vd. (2015) ise çalışmalarında çevre şartlarına göre davranabilme, bilgi, veri ve kaynak paylaşabilme, otomatik organize olabilme yeteneklerine sahip açık ve kapsamlı akıllı nesneler ağı olarak ve Alam vd (2016) ise, bilgi toplama için mevcut ve gelişen bilgi ve iletişim teknolojilerine dayalı, birbirine bağlı nesneler tarafından gelişmiş hizmetler sağlayan küresel bir altyapı olarak tanımlamışlardır.

Şekil 2. IoT kullanım alanları



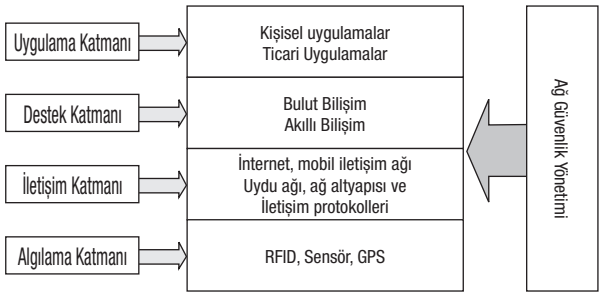
(Yazarlar tarafından oluşturulmuştur.)

E-sağlık, ev otomasyonu, akıllı çevre, akıllı su, akıllı tarım, akıllı hayvancılık, akıllı enerji, akıllı şehirler, akıllı ölçüm, endüstriyel kontrol, güvenlik ve acil durumlar, alışveriş ve lojistik gibi birçok alanda karşımıza çıkan IoT (Gökrem ve Bozuklu, 2016), Şekil 2'de görülebileceği üzere, algılayıcılar ya da harekete geçiriciler gibi fiziksel nesnelerin ağ katmanı üzerinden uygulamalar aracılığıyla son kullanıcılara ulaşması şeklinde özetlenebilecek sistemler bütünüdür (Çavdar ve Öztürk, 2017). Bu bütüne ait iş akışı aşağıdaki şekilde ifade edilebilir.

1) Nesne algılama, nesneye özgü bilgilerin tanımlanması ve iletilmesi. Algılayıcıların türüne bağlı olarak sıcaklık, yönlendirme, hareket, titreşim, hızlanma, nem, havadaki kimyasal değişiklikler gibi veriler algılanmakta ve tanımlanmaktadır. Akıllı hizmetlerin tasarımı için farklı algılayıcıların bir kombinasyonu kullanılabilmektedir.
2) Bir eylemin başlatılması. Alınan nesne bilgisi, çağrılacak otomatik bir işlemi belirleyen bir akıllı cihaz / sistem tarafından işlenmektedir.
3) Akıllı cihaz sistem yöneticisine mevcut sistem durumunu ve gerçekleştirilen eylemlerin sonuçları hakkında geri bildirim sağlayan bir mekanizma içermektedir.

Şekil 3'te de literatürde ortaya konulan IoT güvenlik mimarisi verilmiştir (Suo vd., 2012). Burada; algılama katmanında RFID okuyucu veya algılayıcılar yardımıyla ortamdaki veriler toplanmakta, ağ katmanında nesneler arasında kablolu veya kablosuz bağlantılarla veriler iletilmektedir. Destek Katmanında kullanıcı ve uygulamalar için bir hizmet oluşturulup, hizmet yönetimi sağlanmakta, kullanıcılar da uygulama katmanı yardımıyla IoT sistemine erişebilmektedir.

Şekil 3. IoT güvenlik mimarisi



(Security in the internet of things: a review, Suo vd., 2012)

3.1. Olası IoT Saldırıları

Artan IoT kullanımı ile birlikte savunmasız yapısı da göz önüne alındığında, bu sistemlere yapılan siber saldırılar da giderek artmaktadır. Bu kapsamda IoT güvenliği konusunda yapılan akademik çalışmalarda; potansiyel tehditler ve saldırganlar incelenmiş ve güvenlik ile mahremiyet açısından üç grup saldırgan bulunduğu belirtilmiştir. (Atamli ve Martin, 2014):

- Kötü niyetli kullanıcı: Üreticinin sırlarını öğrenmek ve kısıtlanmış fonksiyonlara erişim sağlamak için saldırı gerçekleştiren kullanıcıdır. Sistemden gizli bilgileri öğrenerek bu sırları farklı firmalara satabilir ya da elde ettiği bir güvenlik açığını aynı özellikteki diğer cihazlarda kullanabilir.
- Kötü niyetli üretici: Ürünlerini sattıkları kullanıcılar ya da onların kullandığı diğer cihazlar hakkında bilgi toplamak için ürün geliştiren üretici firmalardır. Tasarımda cihazlar üzerinde oluşturulan arka kapı ya da zararlı yazılımlar sayesinde topladığı bilgileri casusluk amaçlı kullanabilirler. Ayrıca ortamdaki diğer internete bağlı nesneler ile iletişim kurup zarar vererek onları üreten firmaların güvenilirliğini zedeleyebilirler.
- Dış saldırganlar: Cihaz üzerinde herhangi bir erişimi ve yetkisi olmayan kötü niyetli kişilerdir. Farklı türde saldırılar uygulayarak kullanıcı hakkında bilgi toplamak, maddi zarar vermek gibi amaçları olabilir. Tehdit kaynakları arasında en yüksek orana sahip gruptur.

Literatürde yapılan çalışmalarda; IoT ağlarındaki cihazların kısıtlı bant genişliği, hafıza ve hesaplama yeteneğine sahip olmaları, onları tehditlere karşı savunmasız bıraktığı ifade edilmiştir. Bundan dolayı, bu cihazların geleneksel güvenlik tekniklerini kullanarak internetin ortaya koyduğu güvenlik sorunlarıyla başa çıkmalarının mümkün görülmediği ve IoT mimarisini oluşturan katmanların farklı özellikteki saldırılara karşı savunmasız olduğu belirtilmiştir (Wood ve Stankovic, 2002) (Karlof ve Wagner, 2003) (Görmüş vd., 2018).

Şekil 2'de görüldüğü üzere; IoT sisteminde; alınan ve işlenen veri, cihazlar yani donanım, iletimde kullanılan ağ, verilerin saklandığı bilgisayar/sunucu, kullanıcıların kullandığı uygulamalar ve tabii ki kullanıcı

olmak üzere 6 temel bileşen yer almaktadır. IoT güvenliğinin sağlanabilmesi için, bahsedilen saldırganlar tarafından gerçekleştirilebilecek saldırıların hedef alabileceği tüm bileşenlerin güvenliklerinin sağlanması gerekmektedir. Bu kapsamda IoT sisteminde en önemli bileşen veridir. Verinin temininden kullanıcıya ulaşmasına kadar gizliliğinin ve bütünlüğünün sağlanması gerekmektedir. Algılama katmanında bulunan algılayıcıların, RFID cihazı gibi donanım açısından düşük işlemcili, düşük kapasiteli ve düşük maliyetli olması, bilgi güvenliği ihlali ihtimalini de arttırmaktadır (Gubbi vd., 2013). Ağ ve haberleşme katmanı, farklı ağlardaki verinin aktarımını sağlamakta ve bu sayede değişik yapıdaki cihazlarla çeşitli teknolojiler bir arada kullanılabilmektedir (Ray, 2018). Bu yüzden de; ağ bileşeni gerek içeriden gerekse dışarıdan birçok saldırıya maruz kalabilmektedir. IoT'de sunucular, istenildiği zaman kullanılabilen, her yerden erişim sağlanabilen, ihtiyaca göre hizmet veren ve yönetimi kolay olan bulut bilişim üzerinde organize edilmektedir. Bulut bilişimde de veri bütünlüğüne, gizliliğine, transferine yönelik riskler söz konusu olabilmektedir (Chou, 2015). Uygulama katmanı en üst katman olup, kullanıcıların ihtiyaçlarına istinaden hizmet vermekte ve Sunucu ve Depolama Katmanında bulunan sistem yönetimi ve işletimi ile etkileşim içinde çalışabilmesi için çeşitli yazılımlar bulundurmaktadır. Burada kullanılan yazılımlara karşı gerçekleştirilebilecek saldırılar sistemin yönetiminin yetkisiz kişilerce ele geçirilmesi veya sistemdeki verilerin ele geçirilmesine neden olabilmektedir. Gerek sistemin kurulu bulunduğu kurumda çalışan kişiler, gerekse kurum dışından kişiler tarafından bilinçli ya da bilinçsiz olarak sisteme zarar verilebilmektedir. IoT'nin karmaşık yapısı göz önüne alındığında kullanıcı bileşenine yönelik de saldırı gerçekleştirilmesi söz konusudur.

IoT bileşenlerine yönelik olası saldırılar sınıflandırılmış (Ülker vd., 2017) olup, açıklamaları ve oluşturacağı riskler (İDKK, 2014) ile birlikte Tablo 1'de verilmiştir.

Tablo 1. Olası Saldırılar, Oluşturacağı Riskler ve İlgili Bileşenler

Saldırı Adı	Saldırı Açıklamaları	Saldırı Sonucu Oluşan Risk	Veri	Donanım	Ağ	Sunucu	Uygulama	Kullanıcı
ACK (Acknowledgement) Saldırısı	Saldırgan Kaynak IP adresini hedef IP adresi olarak gösterip SYN paketi yollar ve alıcının hedef SYN paketi yollamadığı halde ACK yoklamasıyla gerçekleşen saldırı türüdür.	Hedef sistemin hizmet veremez hale gelme riski vardır.			X	X		
Arka Kapı	İşletim Sistemi ya da uygulamalarda açıklık oluşturmaya yönelik gerçekleştirilen saldırı türüdür.	Veri kaybı, veri sızıntısı, veri hırsızlığı, veri bütünlüğünün bozulması, kritik donanımlara yetkisiz erişim, zararlı yazılımların bilgi sistemine iletilmesi riski vardır.	X				X	
DNS (Domain Name Server) Zehirlenmesi	Önbellek veri tabanına veri ekleme silme değiştirme ile hedefi şaşırtmaya yönelik saldırı türüdür.	Veri kaybı, veri sızıntısı, veri hırsızlığı, veri bütünlüğünün bozulması, kritik donanımlara yetkisiz erişim, zararlı yazılımların bilgi sistemine iletilmesi, kullanıcının gitmeye çalıştığı siteden farklı bir siteye yönlendirilmesi riski vardır.			X			
E Posta Sahteciliği	Sahte e posta adresini güvenilir olarak gösterilerek gerçekleştirilen saldırı türüdür.	Veri kaybı, veri sızıntısı, veri hırsızlığı, kritik donanımlara yetkisiz erişim riski vardır.	X					
Fiziksel Saldırı	Doğrudan ağın çalışmasını sağlayan donanımlara zarar vermeye yönelik saldırılardır.	Sunuculara, cihazlara veya ağa zarar vererek sistemin hizmet veremez hale getirilmesi riski vardır.		X	X	X		

Saldırı Adı	Saldırı Açıklamaları	Saldırı Sonucu Oluşan Risk	Veri	Donanım	Ağ	Sunucu	Uygulama	Kullanıcı
IP Sahteciliği	Saldırganın gizli dinleme sonucu edindiği paketin şifreli olmaması durumunda kaynak IP adresini değiştirerek hedef sistemi yanıltmasıdır.	Sistemin hizmet dışı kalması, DDoS da zombi cihaz olma riski vardır.	X		X	X	X	
Keylogger (Tuş Kaydedicisi)	Klavyeye basılan tuşları kaydetmeyi amaçlayan yazılımdır.	Veri kaybı, veri hırsızlığı riski vardır.	X					
Oltalama	e posta yardımıyla kişisel bilgileri ele geçirmeye yönelik gerçekleştirilen saldırı türüdür.	Veri kaybı, veri hırsızlığı riski vardır.	X					X
Ortadaki Adam Saldırıları	Haberleşen iki uç arasına girerek veriyi dinlemeye, yakalamaya yönelik gerçekleştirilen saldırı türüdür.	Veri kaybı, veri hırsızlığı riski vardır.	X		X			
Oturum Çalma	İstemci ile sunucu arasına girerek kullanıcı oturumunu ele geçirmeye yönelik gerçekleştirilen saldırı türüdür.	Veri kaybı, veri hırsızlığı, kullanıcılar tarafından bilinçli ya da farkında olmadan bilgi sistemleri üzerinde erişim yetkisi arttırma işlemlerinin gerçekleştirilmesi riski vardır.	X					
Ölümcül Ping	Saldırganın büyük boyutlu paketleri hedef sisteme göndererek hizmet dışı kalmasına neden olan saldırı türüdür.	Hedef sistemin hizmet veremez hale gelme riski vardır.		X	X	X		
Reklam Yazılımı	Reklam görüntülemek ve kişilerin ilgi odağına göre veri toplanılmasına yönelik yazılımdır.	Kişiler ve kişilerin ilgi alanları hakkında bilgi toplanması riski vardır.	X					X
Smurf Saldırısı	Saldırganın ağdaki bilgisayarlara hedef sistemin IP adresinden ICMP (Internet Control Message Protocol) paketi yollayarak alıcı bilgisayarların sürekli ACK mesajı yollamasına neden olan saldırı türüdür.	Hedef sistemin hizmet veremez hale gelme riski vardır.		X	X	X		
Solucanlar	Ağ bağlantısı üzerinden bulaşarak sistemdeki dosyalara zarar verme, bilgisayarın işleyişini bozmayı hedeflemektedir.	Veri kaybı, veri sızıntısı, veri hırsızlığı, veri bütünlüğünün bozulması, kritik donanımlara yetkisiz erişim, zararlı yazılımların bilgi sistemine iletilmesi, hedef sistemin zarar görmesi riski vardır.	X			X	X	
Sosyal Mühendislik	Hedef sistemdeki kişi hakkında bilgi edinebilmek için kişilerin kandırılması yöntemiyle gerçekleştirilen saldırı türüdür.	Kritik donanımlarda yetkisiz erişimlerin görülmesi, veri kaybı, veri hırsızlığı, zararlı yazılımların sisteme yüklenmesi, kritik veri, bilgi ve cihazların bilinçli ya da farkında olmadan değiştirilmesi riski vardır.	X					X
Spam	Herhangi bir amaç doğrultusunda hedef sistemin e postalarına gelen iletilerdir.	Amacına göre değişmekle birlikte; kritik donanımlarda yetkisiz erişimlerin görülmesi, veri kaybı, veri hırsızlığı, zararlı yazılımların sisteme yüklenmesi, kritik veri, bilgi ve cihazların bilinçli ya da farkında olmadan değiştirilmesi riski vardır.	X					X

Saldırı Adı	Saldırı Açıklamaları	Saldırı Sonucu Oluşan Risk	Veri	Donanım	Ağ	Sunucu	Uygulama	Kullanıcı
SQL (Structured Query Language) Enjeksiyonu	SQL sorgularına müdahale ederek hedef sistemin bilgilerini edinmeyi amaçlar.	Veri kaybı, veri hırsızlığı, veriler üzerinde değişiklik yapılarak bütünlüğün bozulma riski vardır.			X			
SYN (Synchronize) Saldırısı	Saldırgan hedef sisteme ardışık olarak SYN bayraklı TCP (Transmission Control Protocol) paketi göndererek hizmet veremez hale getirir.	Hedef sistemin hizmet veremez hale gelme riski vardır.		X	X	X		
Tekrarlama Saldırıları	Haberleşen iki uç arasındaki paketin saldırgan tarafından ele geçirilerek tekrar tekrar alıcıya iletilmesiyle gerçekleşen saldırıdır.	Verilere yetkisiz erişim riski ile sistemin hizmet veremez hale gelme riski vardır.	X		X			
Truva Atları	Bilgisayar yazılımı olup, bulaştığı bilgisayardaki bilgileri dışarı sızdırmaktadır. Saldırgan ağ bağlantısı üzerinden kurbanın bilgisayarını kontrol etmektedir.	Kritik donanımlarda yetkisiz erişimlerin görülmesi, veri kaybı, veri hırsızlığı, zararlı yazılımların sisteme yüklenmesi, sistemin zarar görmesi riski vardır.	X				X	
UDP Saldırısı	Saldırının temel prensibi farklı bir IP adresini kullanarak hedef sistemin portlarına büyük boyutlu UDP (User Datagram Protocol) paketleri yollamaktır.	Hedef sistemin hizmet veremez hale gelme riski vardır.			X	X		
Virüsler	Zararlı bilgisayar yazılımı olup bilgisayarın işleyişini değiştirmektedir.	Kritik donanımlarda yetkisiz erişimlerin görülmesi, veri kaybı, veri hırsızlığı, zararlı yazılımların sisteme yüklenmesi, sistemin zarar görmesi riski vardır.	X		X	X	X	
Web Sahteciliği	Güvenilen bir web sitesinin sahtesini kullanarak gerçekleştirilen saldırı türüdür.	Veri kaybı, veri sızıntısı, veri hırsızlığı, kritik donanımlara yetkisiz erişim riski vardır.	X					

(Ülker vd., 2017 ve İDKK, 2014 kaynaklarından faydalanılarak yazarlar tarafından oluşturulmuştur.)

4. YAŞANMIŞ OLAYLAR

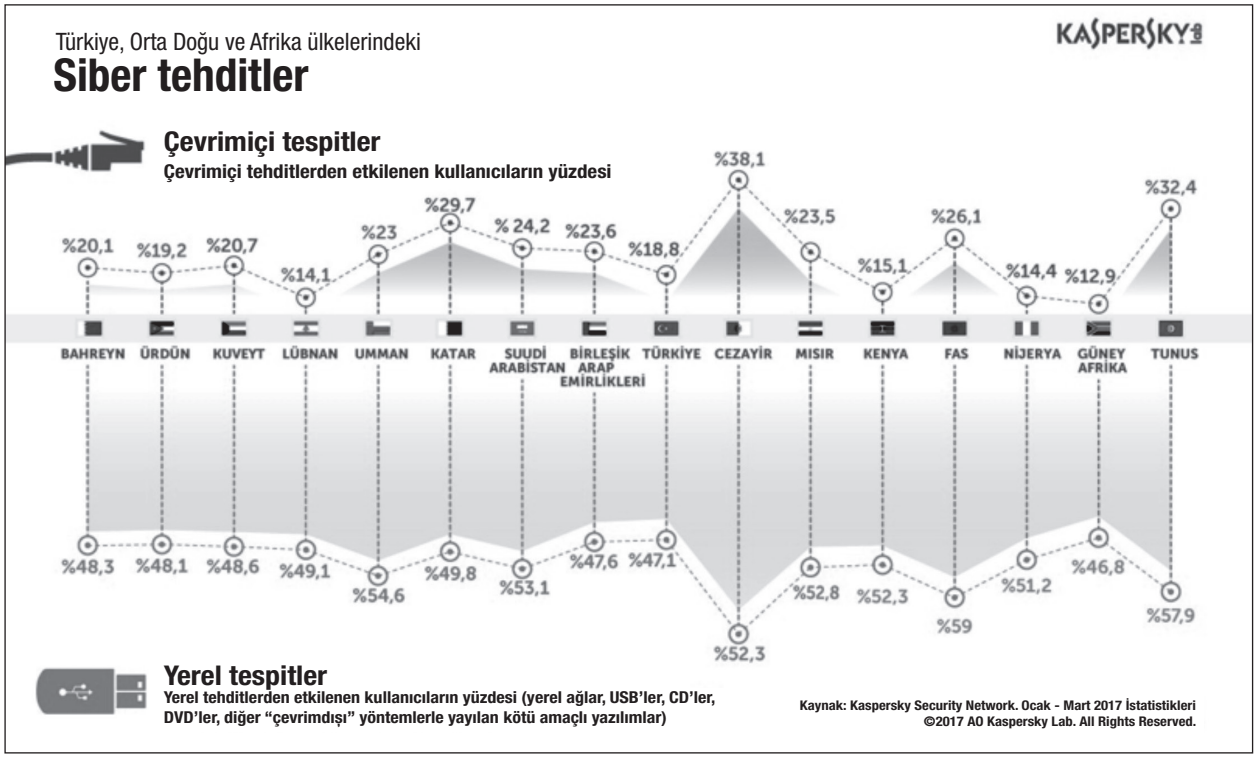
Trend Micro firmasının yayınladığı Akıllı Ev Ağı Güvenlik Özeti (Smart Home Network Security Summary) adlı raporda, IoT güvenlik zafiyetlerinin oluşturduğu tehditlerden en çok etkilenen 10 ülke açıklanmıştır (Trendmicro, 2017). Rapor incelendiğinde ABD, Çin ve İngiltere'nin %28, %7 ve %7 ile ilk üç sırayı aldığı, listede onları Hong Kong, Kanada, Avustralya, İsveç, Hollanda, Tayvan ve Rusya'nın izlediği görülmektedir. Bu ülkelerde yaşanan siber saldırıların, dünya genelinde yaşanan saldırıların %70'ini oluşturduğu ifade edilen raporda, son dönemde özellikle BitCoin üretimi için kullanılan ve birbirleriyle konuşan cihazların da siber suçlular için sömürülecek yeni bir pazar oluşturduğu belirtilmiştir.

Kaspersky firmasının 2017 yılında yayınladığı IoT güvenlik raporu da içerdiği veriler açısından oldukça çarpıcı sonuçlara yer vermektedir (Kaspersky, 2017).

Kaspersky tarafından paylaşılan rapora göre; beyaz eşyadan endüstriyel sistemlere kadar geniş ölçekte kullanılan IoT cihazlarının ülkemizin de içerisinde bulunduğu bölgede %45 oranında siber saldırılara maruz kaldığı görülmektedir. Bunun yanı sıra %47,1 oranında çevrimdışı yerel saldırılara maruz kalındığı tespit edilen ülkemizin %18,8 oranında da çevrimiçi saldırıya maruz kaldığı iletilmiştir.

2016 yılında gerçekleştirilen ve yakın tarihin en büyük siber olaylarından olan DDOS saldırısının hedefi doğrudan dünya çapında internet erişimiydi (Karakullukçu, 2017). Yapılan saldırılar sırasında, o güne

Şekil 4. Siber güvenlik tehditlerine ilişkin tespitler



(Kaspersky Security Network. Ocak – Mart 2017 İstatistikleri)

kadar kullanılan cihazlardan farklı olarak IoT cihazlarının yoğun sayıda kullanıldığı tespit edilmiştir. Mirai isimli bir kötücül yazılım kullanan siber saldırganlar yine bu yazılım sayesinde yaklaşık 620 GB'lık bir veri trafiği oluşturmayı başarmışlardır. Ana hedefi ABD olmasına rağmen ülkemizde de birçok internet servisine erişimde sıkıntılara neden olmuştur.

2017 yılında Amerikan Gıda ve İlaç İdaresi (FDA) tarafından yapılan açıklama ile ülke genelinde yaklaşık 500.000 kalp pilinin, kritik güvenlik açığı nedeniyle geri çağrıldığı duyurulmuştur. Bu geri çağırmaya sebep olan ana neden ise; hayati öneme sahip bu IoT cihazlarının kötü niyetli kişiler tarafından kontrol edilebileceği ya da kullanılmaz hale getirilebileceği endişesi olmuştur (FDA, 2017). Sonrasında cihaz için yayımlanan yazılım güncellemesi ve daha sonraki partilerde üretilen cihazların da güncel yazılım ile kullanıma sunulması bu zafiyetin kapatılmasını sağlamıştır.

2016 yılında gerçekleşen bir başka örnek de, kalp hızı ve egzersiz aktivitesi seviyesi gibi kullanıcı bilgilerini izleyen giyilebilir bir teknoloji olan Fitbit cihazı ile ilgilidir. Bilgisayar korsanları birçok müşterinin hesaplarına sızarak bilgi edinebilmişlerdir. Bu saldırı, cihazın IoT ekosisteminin bir parçası olmasının doğrudan bir sonucu olmasa da, Fitbit'in bu giyilebilir cihazının internete bağlanması nedeniyle faillere sunulan bilgiler büyük oranda artmıştır. Bilgisayar korsanları yalnızca müşteri bilgilerine erişmemişler, aynı zamanda belirli kullanıcıların akşam koşularındaki kullanabileceği popüler rotaları görmelerine izin veren GPS geçmişi gibi bilgilere de ulaşabilmişlerdir. Birçok kişi bu bilginin elde edilebileceğinin farkında olmadığı gibi ve bu türden güvenlik açıklarının farkına varmak, müşterilerin bu ürünleri kullanmak istememesindeki en büyük etkenlerden biridir. Buna ek olarak, bu gibi güvenlik ihlalleri, ele geçirilmiş hesapların çok zayıf şifrelere sahip olmasından dolayı, şirketlerin olduğu kadar tüketicilerin de kusuru olduğu ifade edilmiştir (McGee, 2016).

Bir başka IoT cihazlarındaki açıklardan kaynaklı kötüye kullanım için örnek de (Greenberg, 2017), ses tanıma özelliğini "akıllı asistan" ile birleştiren bir akıllı

hoparlör olan, Amazon Echo cihazıdır. Mark Barnes adında bir İngiliz araştırmacı, kötü niyetli bir kişinin, bu cihazda kötü amaçlı yazılımları kolayca çalıştırabildiğini ve iz bırakmadan "gizlice dinleme mikrofonu" haline getirebileceğinin farkına varmıştır. Bu; kötü niyetli kişilerin, insanların evlerinde yani kendilerini güvenli hissettikleri bir ortamda, izinsiz ve gizlice konuşmalarını dinlemesine olanak sağlayacaktır. Bu tür cihazlar genellikle ofis ve otel odalarında dışarıda gözetim altında olmadan bırakabildiği için oldukça kolay bir şekilde cihaza müdahale edilebilmektedir. Amazon, bu sorunu 2017 model Echo cihazlarında düzeltebilmiştir; ancak, bu önceden satın alınan herhangi bir Echo cihazını güvenli hale getirememiştir. Amazon konu hakkında yorumda bulunduğunda, sadece; Echo cihazının kullanıcılarına güvenliğini "güvenilir perakendecilerden satın aldıkları" ve "yazılımlarının güncel olmasını sağladıkları sürece" iyi olacağını garanti etmekle yetinmiştir.

Otomobillerin internete daha çok bağlanması ve toplumun sürücüsüz araçları benimsemesi sayesinde, bu araçlar da çeşitli saldırıların hedefleri olabilmektedir. Alman Güvenlik Konferansı DIVMA'da, Trend Macro adlı bir güvenlik firması, siber saldırganların, bir aracın dahili ağını kullanmasına ve araç içinde mesaj gönderen bileşenlere müdahale etmesine izin veren, az bilinen bir korsanlık tekniğini vurgulamıştır. Buna göre, bir bilgisayar korsanı bu güvenlik açığından yararlanabilirse, hava yastığını ve kilitlenmeyi önleyici frenleri devre dışı bırakabilecek, aracın kilidini açabilecek ve hatta arabanın çalınmasına izin verebilecektir (Greenberg, 2017). Charlie Miller ve Chris Valasek adında iki araştırmacı ise, yaptıkları çalışmada (Drozhzhin, 2015), standart bir Jeep SUV'un kablosuz internet erişim sistemine girebilmişler ve daha sonra otomobilin kontrol alan ağına erişim sağlayarak ana sistemi ele geçirmişlerdir. Bu aşamadan sonra, otomobili hızlandırabilmek, yavaşlatmak ve hatta yoldan saptırabilmek için aracı kontrol edebildiklerini göstermişlerdir.

Günümüzde evler de, IoT güvenlik açıkları dikkate alındığında güvenli görünmemektedirler. "Akıllı kilitler" veya bluetooth özellikli bir cihazla (cep telefonu gibi) kilitlenebilen ve kilidi açılabilen kilitler kısa bir süre önce DEF CON olarak bilinen bir siber saldırı sözleşmesinde kullanılmıştır (Wollerton, 2016). İki Mercurlite güvenlik çalışanı olan Anthony Rose ve Ben Ramsey, 16 farklı tip akıllı kilitten 12'sini nispeten rahatlıkla kırmayı başarmışlardır. Bu cihazları kilitlemek için kullanılan şifrelerin şifrelenmemiş olduğunu, daha doğrusu düz metinde saklandığını tespit etmişler ve yaklaşık 100 $ için, bu kilitleri ele geçirmeyi, şifreyi keşfetmeyi ve kapıyı açmayı başarmışlardır.

Bir başka örnek olarak, Nest firmasına ait kullanıcıların evlerini bulundukları yerden kolayca izleyebilmelerini sağlayan bluetooth özellikli bir güvenlik kamerası verilebilir (Estes, 2017). Bir güvenlik araştırmacısı olan Jason Doyle, kameranın bluetooth bağlantısını amacı dışında kullanmanın bir yolunu bulmuştur. Söz konusu kameralar internete bağlı olduklarından, bir bilgisayar korsanının basit bir bluetooth komutuyla kamerayı kolayca kapatıp ve işe yaramaz hale getirebileceğini tepsit etmiştir. Bu sayede iz bırakmadan hırsızlık amacıyla bir eve girilebileceği gibi, evdeki internet ağına girilebilmesine bile imkan verecektir. IoT'nin bir parçası olan masaüstü ya da dizüstü bilgisayarlar ile web kameraları da saldırıların hedefi olabilmektedir. Rezitech Inc. isimli bilgisayar firmasında teknisyen olarak çalışan Trevor Harwell, teknik servise tamir için gelen bilgisayarlara kurduğu uzaktan erişim programı (remote acces tool, RAT) ile bilgisayarın dahili algılayıcılarından bir tanesinin arızalandığını bildiren sahte bir mesaj görüntüleyerek kullanıcılardan bilgisayarlarını sıcak buharın yanında birkaç dakika beklettikleri takdirde sorunun düzeleceğini söylemiş ve inanması zor gelse de birçok kullanıcı banyo yaptıkları sırada bilgisayarlarını da yanlarında götürmüş, RAT sayesinde birçok görüntü ve videolarının izinleri dışında kaydedilmesine engel olamamışlardır. CamCapture yazılımı ile görüntüleri adres gösterdiği sunucuya yükleyen saldırgan, eylemleri sonucunda 1 yıl hapis cezası almıştır (Plummer, 2011).

Ayrıca bebek kamerası olarak kullanılan internet üzerinden izlenebilen IP kamera ve monitörlerin de kötü niyetli kişiler tarafından ele geçirildiğini belirten birçok haber bulunmaktadır. Bununla birlikte internete bağlı yazıcılardan buzdolaplarına, termostatlara kadar birçok "akıllı" cihaz siber saldırıların hedefi olabilmektedir (Wang, 2018).

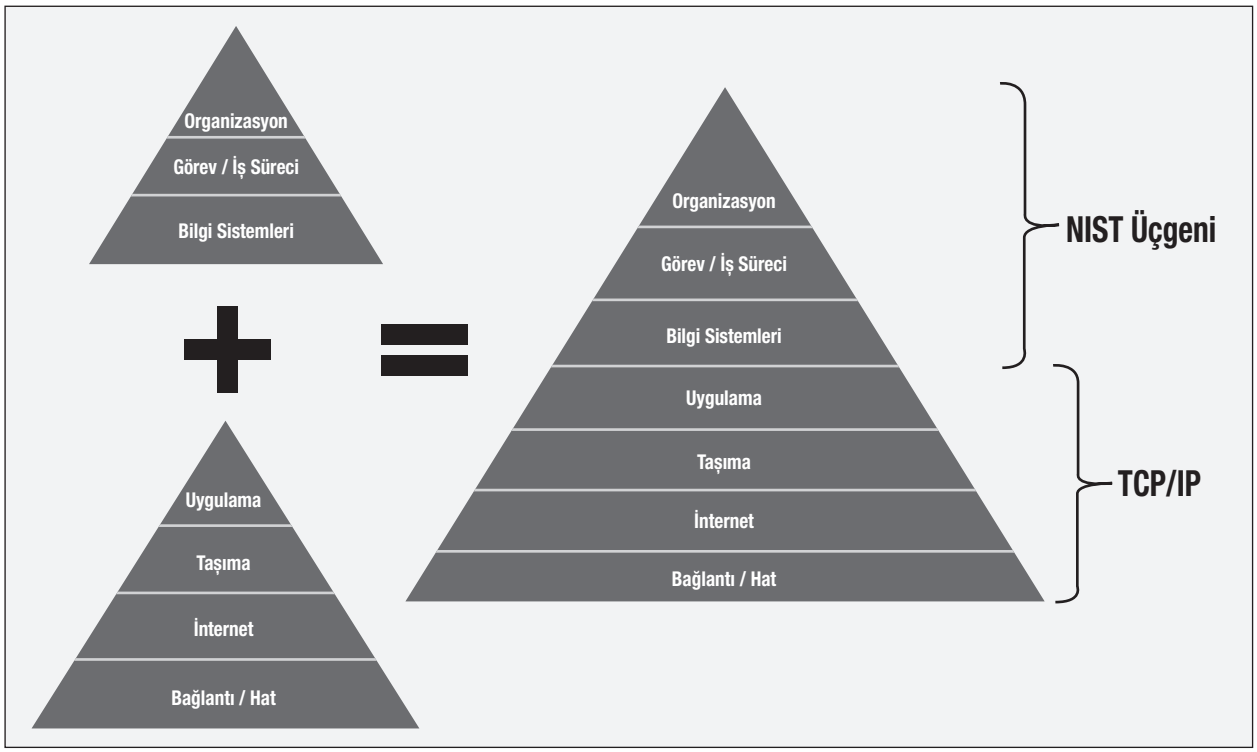
5. IoT DENETİMİNE YÖNELİK KONTROL LİSTESİ

Önceki bölümlerden de görüldüğü üzere IoT giderek artan kullanımıyla artık hayatımızın büyük bölümünde yer almakta olup, birçok saldırının da hedefi olmaktadır. Bu yüzden ilgili sektörlerin, güncel siber güvenlik stratejileri ve operasyonlara yapılacak büyük değişiklikler için hazırlıklı olması gerekmektedir. IoT'nin getirdiği zorluklar sağlam planlama, iyi güvenlik stratejileri ve sıklıkla yapılan IoT denetim değerlendirmeleriyle; ileriye dönük bir şekilde çözülmelidir (Gonzalez, 2015). IoT denetimi için genel bir denetim modelinin benimsenmesi ve mevcut belgelerden uygulanabilir kontrollerin seçilmesi tavsiye edilmektedir (Cooke ve Raghu, 2018). Bu kapsamda Jekot ve Pavlosoglou tarafından yapılan çalışma (Jekot ve Pavlosoglou, 2017) ile bir denetim yöntemi önerilmiştir. Bu yöntemde öncelikle IoT cihazının uçtan uca kullanım durumu, Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (Ulusal Standartlar ve Teknoloji Enstitüsü, NIST) SP 800-53'ün kontrol listesine göre incelenmekte, yüksek öncelikli (P1- Priority 1) atanmış kontroller seçilmektedir. Söz konusu kontrollerde "bilgi sistemi" ifadesi "IoT cihazı", "Organizasyon" ifadesi ise "kullanım ortamları" veya "üretici" olarak değiştirilmiştir. Daha sonra NIST SP 800-53 standardında IoT cihazının kullanım amacı ve kullanım alanı düşünülerek kontroller "uygulanabilir" olarak işaretlenmiştir. Burada IoT'ye özgü kontrollerin listesi elde edilirken ilgili olmayan maddeler ise çıkarılmıştır. Kontroller gruplanırken, IoT cihazlarının ortak TCP/IP yığını ve gerçekleştirilmesi gereken işin amacı özelliklerinin birleştirilmesi düşünülerek oluşturulan ve Şekil 5'te gösterilen TCP/IP yığını ile NIST'in "Organizasyon, Görev ve Bilgi Sistemi Görünümü" katmanlarından seçilerek türetilmiştir.

Bu gruplama ile ortaya çıkan kalıplara dayanarak kullanım durumu için geçerli kontrollerin 12 madde olarak listelenmesi sağlanmıştır.

1. Fiziksel Erişim Kontrolü (NIST 800-53/PE-3):
   - Üretici;
     - IoT cihazına fiziksel erişim yetkilerini zorunlu tutar.
     - IoT cihazına erişim izni vermeden önce bireysel erişim yetkilerini doğrular.
     - Giriş/çıkışı kontrol eder.

Şekil 5. NIST SP 800-39 ile TCP/IP büyütme modeli



(An IoT Control Audit Methodology Jekot ve Pavlosoglou, 2017)

- Fiziksel erişim denetleme kayıtlarını tutar.
- IoT cihazındaki alanlara erişimi kontrol eder.
- Kombinasyonlar tehlikeye girdiğinde IoT cihazındaki kombinasyonları ve anahtarları değiştirir.

2. İletim Gizliliği ve Bütünlüğü (NIST 800-53/SC-8):
   - IoT cihazı, iletilen bilgilerin gizliliğini ve bütünlüğünü korur. Bu kontrol hem iç hem de dış ağlar ve bilginin aktarılabileceği algılayıcı, mobil cihaz, giyilebilir teknolojiler, yazıcı, fotokopi makinesi gibi her türlü IoT bileşeni için geçerlidir.
3. Sınır Koruması (NIST 800-53/SC-7):
   - IoT cihazı:
     - Sistemin dış sınırındaki ve sistem içindeki temel iç sınırlarda iletişimi izler ve kontrol eder.
     - İç kullanım ortamından ayrılmış halka açık sistem bileşenleri için alt ağlar kurar.
     - Harici ağlara veya bilgi sistemlerine, yalnızca üreticinin güvenlik mimarisine uygun olarak düzenlenmiş sınır koruma cihazlarından oluşan yönetilen arayüzler üzerinden bağlanır.
4. Cihaz Tanımlama ve Doğrulama (NIST 800-53/IA-3):
   - IoT cihazı, yerel, uzak veya ağ bağlantısı kurmadan önce diğer cihazları benzersiz bir şekilde tanımlar.
   - Üretici, IoT cihazlarının güvenlik kategorileri tarafından istenen kimlik doğrulama mekanizmalarının gücünü belirler ve ayrıca, doğrulamaya dayalı cihaz tanımlama ve doğrulamanın üretici tanımlı konfigürasyon yönetimi süreçleri tarafından yapılmasını sağlar.
5. Ortak Bilgi İşlem Cihazları (NIST 800-53/SC15):
   - IoT cihazı:
     - Üreticinin açık bir şekilde izin verdiği durumlar haricinde ortak bilgi işlem cihazlarının uzaktan etkinleştirilmesini yasaklar.
     - Cihazlarda fiziksel olarak mevcut olan kullanıcılara açık bir kullanım göstergesi sağlar. (Örneğin, açık kullanım göstergesi, ortak bilgi işlem cihazı etkinleştirildiğinde kullanıcıya sinyal verir.)
6. Kimlik ve Kullanıcı Kimlik Doğrulama (NIST 800-53/IA-2):
   - IoT cihazı, üretici kullanıcılarını (veya üretici kullanıcıları adına hareket eden işlemleri) benzersiz şekilde tanımlar ve doğrular. Üretici, grup hesaplarındaki bireylerin benzersiz tanımlanmasını veya bireysel faaliyetlerin ayrıntılı hesap verebilirliğini talep edebilir. Üretici, kullanıcı kimliklerini doğrulamak için şifreleri, jetonları veya biyometreleri ya da çok faktörlü doğrulama durumunda, bunların bir kombinasyonunu kullanır.
7. Hesap Yönetimi (NIST 800-53/AC-2):
   - Üretici;
     - Görevleri/işletme işlevlerini desteklemek için sistem hesaplarını tanımlar ve seçer.
     - Hesap yöneticileri atar.
     - Grup ve rol üyeliği için koşullar belirler.
     - Her bir hesap için yetkili kullanıcıları, grup ve rol üyeliğini ve erişim yetkilerini belirtir.
   - Üretici veya cihaz sahibi;
     - Üretici tarafından tanımlanan prosedürlere veya koşullara uygun olarak cihaz hesaplarını oluşturur, etkinleştirir, değiştirir, devre dışı bırakır ve kaldırır.
     - Hesap yöneticilerini bilgilendirir, hesap yönetimi gereksinimlerine uyması için hesapları yetkilendirir ve hesapları inceler.
     - Grup kimlik bilgilerini yönetir.
8. En Az İşlevsellik (NIST 800-53/CM-7):
   - Üretici;
   - IoT cihazını sadece temel yetenekleri sağlayacak şekilde yapılandırır.
   - Bir dizi tanımlanmış fonksiyon, port, protokol ve / veya hizmet kullanımını yasaklar veya kısıtlar.
9. Cihaz Beklemedeyken Bilgilerin Korunması (NIST 800-53/SC-28):
   - IoT cihazı, bekleme konumunda iken de hem kullanıcı hem de sistem bilgilerinin gizliliğini ve bütünlüğünü korur.
10. Sistem Güvenlik Planı (NIST 800-53/PL-2):
    - Üretici;
      - Kurumsal mimarisine uygun bir güvenlik planı geliştirir ve izin sınırlarını açıkça tanımlar.

- Cihazın operasyonel bağlamını ve operasyonel ortamını görevler ve iş süreçleri açısından açıklar.
- Sistem için güvenlik gereksinimlerine genel bir bakış sunar.
- Sebepleri de dâhil olmak üzere bu gereklilikleri karşılamak için uygulanan güvenlik kontrollerini açıklar.
- Cihazdaki ve/veya çalışma ortamındaki değişikliklerin veya plan uygulaması veya güvenlik kontrol değerlendirmeleri sırasında tespit edilen sorunların ele alınması için planı günceller.
- Güvenlik planını izinsiz açıklama ve değişiklikten korur.

11. Misyon/ İş Süreci Tanımı (NIST 800-53/PM-11):
    - ➢ Üretici;
        - Bilgi güvenliği ve kullanım ortamı, üretici varlıkları, bireyler, diğer üreticiler ve kullanıcılar için oluşan çevre riskini göz önünde bulundurarak görev/iş süreçlerini tanımlar.
        - Belirlenen görev/iş süreçlerinden kaynaklanan bilgi koruma gereksinimlerini belirler ve ulaşılabilir koruma ihtiyaçları elde edilene kadar gereken süreçleri gözden geçirir.
12. Bilgi Güvenliği Program Planı (NIST 800-53/PM-1):
    - ➢ Üretici;
        - Bir bilgi güvenliği programı planı geliştirir ve yayar.
        - Güvenlik programına ilişkin gereksinimlere genel bir bakış ve bu gereksinimleri karşılamak için yürürlükte olan veya planlanan güvenlik programı yönetim kontrollerinin ve ortak kontrollerin bir tanımını sunar.
        - Bilgi güvenliğinin farklı yönlerinden sorumlu olan örgüt varlıkları arasında koordinasyon sağlar.
        - Planın, riske karşı sorumluluk ve hesap verebilirliği olan üst düzey bir yetkili tarafından onaylanmasını sağlar.

Kullanım durumlarına dayanarak, bu kontrollerin değerlendirilmesi eksiksiz bir denetimin gerçekleştirilmesi için yeterli bir temel teşkil edecektir ancak böyle bir denetimi geçecek bir IoT cihazı henüz geliştirilmemiştir. IoT endüstrisi geliştikçe boşluklar belirlenirse, gerektiğinde söz konusu yönteme daha fazla kontrol eklenebilecektir (Jekot ve Pavlosoglou, 2017).

6. IoT GÜVENLİĞİ İÇİN ÖNERİLER

IoT cihazları; arabalar, oyuncaklar, giyilebilir teknolojiler ve elektrikli ev aletleri gibi çeşitlilik göstermektedir. IoT ekosistemindeki çeşitlilik ve karmaşıklık, güvenlik çalışmalarının farklı seviyelerde ve farklı paydaşlarca yapılmasını gerektirmektedir.

Cihaz güvenliğine, cihazların tasarım ve üretim aşamasından başlanmalıdır. Bu aşamada donanımsal olarak güvenlik önlemi alınabileceği gibi varsayılan parolaların değiştirilmesi ve zor parola seçilmesi gibi bazı kullanıcı ayarları varsayılan olarak zorunlu hale getirilebilir.

Kullanıcıların ve cihazların erişim ayrıcalıklarının sağlanması için kimliklerin doğrulanma, yetkilendirilme ve denetlenme mekanizmaları sağlanmalıdır. Bir ağın güvenli bölümlere ayrılması ile IoT cihazlarının ana bilgi işlem cihazlarından ayrılmasına yardımcı olarak güvenlik artırabilir (BizTech, 2017).

Mümkün olduğunca IoT cihazlarını internetten gizlemek de, internette arama yaparken cihazların keşfedilememesini sağlayacaktır.

Cihaz ve şebeke arasında şifrelenmiş bir sanal özel ağ (VPN) bağlantısı kurmak, cihazdan ağa verilen bilgilerin bütünlüğünü tehlikeye atacak üçüncü kişilerin erişim ihtimalini azaltacaktır.

IoT sistemi, İzinsiz Giriş Tespit Sistemleri (IDS) ile sürekli izlenmelidir.

IoT cihazları kuruluşlara entegre edildiğinden, mevcut bilgi teknolojileri politika ve prosedürleri bu cihazları kapsayacak şekilde genişletilmelidir.

Güvenlik kontrolleri uygulanmalı ve IoT cihazlarının, ağlarının ve altyapısının geçirgenliği değerlendirilmeli ve güncel olmalıdır.

IoT ekosistemi kurumlara entegre edildiğinden, getirdikleri risk de yönetilebilir bir şekilde değerlendirilmelidir.

Bunlarla birlikte, IoT ekosisteminde kullanılan kamera gibi farklı cihazlara özgü güvenlik önlemeleri de alınmalı ve kullanıcı farkındalığı artırılmalıdır.

Ayrıca, Tablo 1'deki bileşenlere yönelik saldırı türlerine karşın alınabilecek önlemler de şu şekildedir (Ülker vd., 2017):

ACK, UDP saldırılarına karşın; zaman aşımı (timeout) değerini düşürmeli, saldırı tespit sistemi ve güvenlik duvarı kullanılmalı, yönlendirme seviyesinde koruma sağlanmalıdır.

Arka Kapı, reklam yazılımı, solucanlar, spam, truva atları ve virüs saldırılarına karşın; anti-virüs ve güvenlik duvarı kullanılmalıdır.

DNS zehirlenmesine karşın; saldırı tespit sistemi kullanılmalıdır.

E-posta sahteciliğine karşın; e-posta doğrulama mekanizması, alan adı anahtarı kimlik doğrulama mekanizması, tek kullanımlık şifre, şifreleme algoritması kullanılmalıdır.

IP sahteciliğine karşın; zaman aşımı değeri düşürülmeli, kaynak IP adresini doğrulama mekanizması ve Hop sayısını filtreleme (HCF) kullanılmalıdır.

Tuş kaydedicisine (keylogger) karşın; anti-casus yazılım ve güvenlik duvarı kullanılmalıdır.

Oltalama (phishing) saldırısına karşın, oltalama saldırıları saptama mekanizması kullanılmalı ve kullanıcılar bilinçlendirilmelidir.

Ortadaki adam (man in the middle) saldırısına karşın; şifreleme algoritması, güvenlik duvarı ve sızma önleme sistemi (IPS) kullanılmalıdır.

Oturum çalma saldırısına karşın; güvenli protokol kullanımı sağlanmalı, koruma mekanizması ve şifreleme algoritması kullanılmalıdır.

Ölümcül ping ve yoğun paket gönderimi (smurf) saldırılarına karşın; saldırı tespit sistemi, güvenlik duvarı ve anti-virüs programı kullanılmalı, yönlendirme seviyesinde koruma sağlanmalıdır.

Sosyal mühendislik saldırısına karşın, kullanıcılarda farkındalık sağlanmalıdır.

Yapılandırılmış Sorgu Dili (Structured Query Language, SQL) Enjeksiyonu saldırısına karşın; güvenli veri tabanı konfigürasyonu ile saldırı tespit sistemi kullanılmalıdır.

Eşzamanlı (SYN) saldırısına karşın; SYN çerezleri (cookies), SYN ön bellek (cache), SYN ağ vekili (proxy) güvenlik duvarı, IPS ve IDS kullanılmalı ve yönlendirme seviyesinde koruma sağlanmalıdır.

Tekrarlama saldırısına karşın, şifreleme algoritması ve güvenlik duvarı kullanılmalıdır.

Web sahteciliği saldırısına karşın; tek kullanımlık şifre ve şifreleme algoritması kullanılmalıdır.

7. SONUÇ

Sensörlerin ve diğer IoT cihazlarının, sağladıkları gerçek zamanlı veriler sayesinde giyilebilir teknolojilerin yanı sıra; güvenlik, otomasyon, tarımsal üretim, meteoroloji, envanter, akıllı ev, hastane, eğitim, aydınlatma, iletişim ve altyapı, kritik altyapılarda kontrol, yapay zeka destekli güvenlik ve takip sistemleri ile başta otomotiv ve ulaşım sektörleri olmak üzere endüstride çokça kullanılmakta olduğu ve hayatımızın her alanında gün geçtikçe daha sık yer aldığı aşikardır.

Kullanımının bu denli yaygınlaştığı IoT cihazlarını içerisinde barındıran söz konusu sistemlere karşı; veri hırsızlığı, veriler üzerinde değişiklik yaparak veri bütünlüğünü bozma; sunuculara, cihazlara, kritik alt yapılara ve bunların iletişiminde kullanılan ağlara zarar vererek bu sistemlerin hizmet veremez hale getirilmesi, kritik donanımlara yetkisiz erişim kritik verilerin ve bilgilerin değiştirilmesi ve/veya silinmesi gibi amaçlarla yapılan saldırılar olmaktadır. Bu saldırıların planlı olabileceği gibi bilinçsiz kullanıcılar tarafından farkında olmadan da doğrudan yapılabildiği ya da yapılan saldırıların parçası olarak gerçekleşebilmektedir. Bu noktada bu tür saldırıların kişisel veya kurumsal olarak maddi ve manevi zarara yol açacağı da çok açık şekilde görülmektedir.

Bu düzeyde kritik öneme sahip olmasına karşın, Internet of Business (2017) tarafından yapılan bir ankette, IoT kullanıcılarının %48'inin, bilgisayarlarının kötü niyetli kişiler tarafından ele geçirilebileceğinin ve geniş çaplı siber saldırıların başlatılmasında kullanılabileceğinin farkında olmadıkları ortaya çıkmıştır. Buna ek olarak, ankete katılan beş kişiden yaklaşık dördünün, IoT saldırılarıyla ilgili bir haber görmedikleri veya okumamış oldukları ve uyarılara rağmen, katılımcıların %78'inin ise IoT güvenliğine olan güvensizlikleri göremedikleri ifade edilmiştir (Fearn, 2017).

Bu çalışmada ortaya konulan önerilerin doğru algılanması IoT sistemlerin güvenliği, bu sistemlerin etkileşim içerisinde olduğu diğer sistemlerin güvenliği ve kurumsal güvenlik konularına katkı sağlayacaktır. Örnekleri verilen gerçekleşmiş olayların bilinmesi-

nin, bireysel ve kurumsal kullanıcıların bu nesneleri satın alırken güvenlik konusunda daha hassas davranmalarına ve hatta kişisel ve kurumsal güvenliklerini kurarken daha doğru önlemler almalarına da olanak sağlayabileceği değerlendirilmektedir.

Bu kapsamda iç denetçiler, IoT cihazlarının üretim aşamasında fabrikalarda olduğu kadar, kullanım aşamasında da kurumlarında gerek risk analizi ve farkındalık konularında danışman, kolaylaştırıcı ya da eğitici gibi roller ile gerekse bu yeni teknolojilerin bilgi teknolojilerine bütünleşik olarak çalıştığını göz önünde bulundurarak yaptıkları denetimlerde, bu konudaki risklerin uygun şekilde kontrol edildiğine dair makul güvence sağlamak suretiyle üst yönetime yardımcı olabilecek, aynı zamanda IoT cihazlarının kullanımı sayesinde ortaya çıkan fırsatların değerlendirilmesine de katkı sağlayabilecektir.

Kaynakça

Alam F., Mehmood R., Katib I., Albeshri A. (2016). Analysis of eight data mining algorthms for smarter internet of things (IoT). *Procedia Computer Science*, 437-447.

Atamli A.W. ve Martin A. (2014). Threat-Based Security Analysis for The Internet of Things. *IEEE*, 35-43.

Atzori L., Iera A., Morabito G. (2010). The Internet Of Things: A survey. *Elsevier B.V.*

Banerjee M., Lee J., Choo K. K. R. (2018). A blockchain future for internet of things security: a position paper. *Digital Communications and Networks*, 149-160.

Chou, D. C. (2015). Cloud computing risk and audit issues. *Computer Standards & Interfaces*, 137-142.

Çavdar T., Öztürk E. (2017). Nesnelerin interneti için yeni bir mimari tasarımı. *Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 39-48.

Gökrem L., Bozuklu M. (2016). Nesnelerin İnterneti: Yapılan Çalışmalar ve Ülkemizdeki Mevcut Durum. *Gaziosmanpaşa Bilimsel Araştırma Dergisi*, 47-68.

Görmüş S., Aydın H., Ulutaş G. (2018). Nesnelerin interneti teknolojisi için güvenlik: var olan mekanizmalar, protokoller ve. *Gazi Üniversitesi Mühendislik Mimarlık Fakütesi Dergisi,* 1247-1272.

Gubbi J., Buyya R., Marusic S., Palaniswami M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems*, 1645-1660.

Han J., Jeon Y., Kim J. (2015). Security Considerations for Secure and Trustworthy Smart Home System in the IoT Environment . *IEEE*, 1116-1118.

Hussain R., Abdullah İ. (2018). Review of Different Encryptionand Decryption Techniques Used for Security and Privacy of IoT in Diffirent Applications. *IEEE*, 293-297.

İDKK (İç Denetim Koordinasyon Kurulu). (2014). *Kamu Bilgi Teknolojileri Denetimi Rehberi,* Ankara.

Karlof C. ve Wagner D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *IEEE*, 113-127.

Madakam S., Ramaswamy R., Tripathi S. (2015). Internet Of Things(IoT):A Literature Review. *Journal of Computer and Communication*, 167-173.

Ray, P. P. (2018). A Survey on Internet of Things Architectures. *Journal of King Saud University-Computer and Information Sciences*, 291-319.

Reyna A., Martín C., Chen J., Soler E., Díaz M. (2018). *On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems*, 173-190.

Rizvi S., Pfeffer J., Kurtz A., Rizvi M. (2018). Securing the Internet of Things (IoT): A Security Taxonomy for IoT. *IEEE*, 163-168.

Săndescu C., Grigorescu O., Rughinish R., Deaconescu R., Călin M. (2018). Why IoT security is failing. The Need of a Test Driven Security Approach. *IEEE*.

Suo H., Wan J., Zou C., Liu J. (2012). Security in the internet of things: a review. *IEEE*, 648-651.

Şenol S., Arslan K.S. (2016). Secure Trusted IoT Gateway (STIG). *Information Security Conference 2016.* Ankara: researchgate.

Ülker M., Canbay Y., Sağıroğlu Ş. (2017). Nesnelerin İnternetinin Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Açisindan İncelenmesi. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, 28-41.

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *ScienceDirect*, 23-30.

Wood A.D. ve Stankovic J.A. (2002). Denial of Service in Sensor Networks. *IEEE*, 48-56.

Yılmaz, E. N. (2011). Education set design for smart home applications. *Wiley*, 631-638.

İnternet Kaynakları

BizTech (2017, 09 28). https://biztechmagazine.com/article/2017/09/5-keys-foolproof-iot-security adresinden alındı.

Brandon, J. (2016, 06 01). *CSO*. https://www.csoonline.com/article/3077537/security-concerns-rising-for-internet-of-things-devices.html adresinden alındı.

Buckle, C. (2016, 02 18). *Globalwebindex*. https://blog.globalwebindex.com/chart-of-the-day/digital-consumers-own-3-64-connected-devices/ adresinden alındı.

Claveria, K. (2019, 3 7). *VisionCritical*. https://www.visioncritical.com/blog/internet-of-things-stats adresinden alındı.

Cooke I., Raghu R.V. (2018). ISACA . https://www.isaca.org/JOURNAL/ARCHIVES/2018/VOLUME-5/Pages/auditing-the-iot.aspx?utm_referrer= adresinden alındı.

Drozhzhin, A. (2015, 8 6). Kaspersky. https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/ adresinden alındı.

Estes, A. C. (2017, 03 22). https://gizmodo.com/this-nest-security-flaw-is-remarkably-dumb-1793524264 adresinden alındı.

FDA. (2017, 08 29). https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm adresinden alındı

Fearn, N. (2017, 2 1). internetofbusiness. https://internetofbusiness.com/consumers-security-risks-iot-devices/ adresinden alındı.

Gartner. (2017, 2 7). https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 adresinden alındı.

Gemalto. (2017, 10 31). gemalto. https://www.gemalto.com/press/Pages/Gemalto-survey-confirms-that-Consumers-lack-confidence-in-IoT-device-security-.aspx adresinden alındı.

Gonzalez, M. H., Djurica J. (2015). ISACA. https://www.isaca-istanbul.org/nesnelerin-interneti-buyuk-firsat-saglarken-daha-cok-risk-ortaya-cikarir/ adresinden alındı.

Greenberg, A. (2017, 8 2). https://www.wired.co.uk/article/amazon-echo-alexa-hack adresinden alındı.

Greenberg, A. (2017, 8 16). https://www.wired.com/story/car-hack-shut-down-safety-features/ adresinden alındı.

Greenough, J. (2015, 02 19). Businessinsider. https://www.businessinsider.com/connected-car-statistics-manufacturers-2015-2 adresinden alındı.

Karakullukçu, E. (2017). Webtekno. https://www.webtekno.com/hackerlar-buyuk-hack-saldirisinda-evlerdeki-akilli-cihazlari-kullanmislar-h21383.html adresinden alındı.

Kaspersky. (2017, 05 20). https://www.kaspersky.com.tr/about/press-releases/2017_turkiye-yi-de-kapsayan-bolgenin-siber-tehdit-trenleri-aciklandi adresinden alındı.

Lamkin, P. (2017, 06 22). *Forbes*. https://www.forbes.com/sites/paullamkin/2017/06/22/wearable-tech-market-to-double-by-2021/#6aaf9b03d8f3. adresinden alındı.

Lohrmann, D. (2017, 11 5). *GT*. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/lack-of-trust-in-iot-security-means-more-regulation-is-coming.html adresinden alındı.

Jekot M., Pavlosoglou Y. (2017). *ISACA*. https://www.isaca.org/Journal/archives/2017/Volume-6/Pages/an-iot-control-audit-methodology.aspx adresinden alındı.

McGee, M. K. (2016, 01 11). https://www.databreachtoday.com/fitbit-hack-what-are-lessons-a-8793 adresinden alındı.

NIST 800-53/AC-2. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/AC-2 adresinden alındı.

NIST 800-53/CM-7. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/CM-7 adresinden alındı.

NIST 800-53/IA-2. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/IA-2 adresinden alındı.

NIST 800-53/IA-3. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/IA-3 adresinden alındı.

NIST 800-53/PE-3. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/PE-3 adresinden alındı.

NIST 800-53/PL-2. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/PL-2 adresinden alındı.

NIST 800-53/PM-1. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/PM-1 adresinden alındı.

NIST 800-53/PM-11. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/PM-11 adresinden alındı.

NIST 800-53/SC15. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/SC-15 adresinden alındı.

NIST 800-53/SC-28. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/SC-28 adresinden alındı.

NIST 800-53/SC-7. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/SC-7 adresinden alındı.

NIST 800-53/SC-8. (tarih yok). NIST: https://nvd.nist.gov/800-53/Rev4/control/SC-8 adresinden alındı.

Plummer, M. (2011, 6 10). *abcnews*. https://abcnews.go.com/US/california-computer-technician-trevor-harwell-suspected-spying-women/story?id=13806697 adresinden alındı.

Trendmicro. (2017, 08 15). https://newsroom.trendmicro.com/press-release/commercial/trend-micro-reveals-top-ten-regions-affected-iot-security-threats adresinden alındı.

Wang A. B. (2018, 12 20). *washingtonpost*. https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/?noredirect=on&utm_term=.4b3cea98a13b adresinden alındı.

Wollerton, M. (2016, 8 9). https://www.cnet.com/news/have-a-smart-lock-yeah-it-can-probably-be-hacked/ adresinden alındı.

COSO 2017 KURUMSAL RİSK YÖNETİMİ ÇERÇEVESİNE KONTROL ÖZ DEĞERLENDİRME YAKLAŞIMIYLA BAKIŞ VE BİR KURUM UYGULAMASI-II[1]

(OVERVIEW THROUGH CONTROL SELF-ASSESSMENT APPROACH TO COSO 2017 ENTERPRISE RISK MANAGEMENT FRAMEWORK AND APPLICATION OF AN ORGANIZATION-II)

Alptuğ GÜLER* / Ali Kasım ARKIN**

ÖZ

Dünyadaki sosyal ve teknik değişim hiç olmadığı kadar ivme kazanmış durumdadır. Bu değişime bağlı olarak da belirsizlikler ve riskler hem nicelik, hem de nitelik olarak artmakta, kurumları ve çalışanları kontrol edilemez bir yöne taşımaktadır. Kurumlar, riskleri kontrol edebildiği sürece sürdürülebilirliklerini sağlayabilmektedir. Kontrol Öz Değerlendirme sürdürülebilirlik ve risklere karşı öngörülebilecek kontrol araçlarını geliştirmek için etkin bir bakış açısı sağlamakta ve Kurumsal Risk Yönetimi için sağlam bir zemin oluşturma potansiyeli taşımaktadır. COSO (The Committee of Sponsoring Organizations of the Treadway Commission) 2017 yılında mevcut çerçevesini güncelleyerek Kurumsal Risk Yönetiminin kurumun tüm süreçlerine entegre edilmesinin önemini vurgulamıştır. Bu entegrasyon; örgütün yönetişim, strateji, h edef belirleme ve günlük operasyonlarına ilişkin karar alma süreçlerini iyileştirecek, performansı artıracak ve örgütsel sürdürülebilirliğe katkı sağlayacaktır. Yenilenen COSO çerçevesinin kurum bünyesinde içsellik kazanması için örgütlerin yapması gereken ilk adım, belirsizliklerini ve risklerini tespit etmesidir. Bunun en etkin yolu örgüt bünyesinde bir risk çalıştayı yapıp, çalıştay sonuçlarını Kurumsal Risk Yönetimi için yol haritası yapmaktan geçmektedir.

Bu makalede, Kontrol Öz Değerlendirme yöntemleri ile yenilenen COSO Kurumsal Risk Yönetim Çerçevesi açıklanmış ve Düzce Üniversitesi Risk Evreninin Belirlenmesi Çalıştayı örneğiyle kuruma sağlayacağı katkılar değerlendirilmiştir. Bir vaka analizi olarak Çalıştay, Kontrol Öz Değerlendirmenin kurum genelinde risk-kontrol ve hedef için bir farkındalık oluşturma kapasitesini göstermektedir.

Anahtar Kelimeler: Kurumsal Risk Yönetimi, Risk Çalıştayı, Kontrol Öz Değerlendirme, COSO KRY 2017 Çerçevesi

JEL Kodlaması: G32, L21, M12, M42

ABSTRACT

Social and technical change in the world has gained more momentum than ever before. Due to this change, uncertainties and risks increase in both quantity and quality and carry the institutions and employees to an uncontrollable direction. Institutions can ensure their sustainability as long as they can control the risks. Control Self-Assessment provides an effective perspective for developing control tools that can be predicted for sustainability and risks, and has the potential to be a solid ground for enterprise risk management. In 2017, COSO (The Committee of Sponsoring Organizations of the Treadway Commission) updated its existing framework and emphasized the importance of integrating enterprise risk management into all processes of the organization. This integration will improve the decision-making processes of the organization's governance, strategy, goal setting and daily operations, improve performance and contribute to organizational sustainability. The first step that organizations need to make for the internalization of the renewed COSO framework within the organization is to identify the uncertainties and risks. The most effective way to do this is to carry out a risk workshop within the organization and make the results of the workshop a roadmap for enterprise risk management.

In this article, Control Self-Assessment methods and renewed COSO Enterprise Risk Management Framework are explained, and the contributions to be provided to the organization by the example of Düzce University Risk Universe Workshop were evaluated. As a case study, the Workshop demonstrates the capacity of the Control Self-Assessment to establish an awareness for the risk-control and objective across the organization.

Keywords: *Entreprise Risk Managemeent, Risk Workshop, Control Self Assessment, COSO ERM 2017 Framework*

JEL Classification: *G32, L21, M12, M42*

1) Yazının 1. kısmı Denetişim Dergisinin 18. sayısında yayımlanmıştır.

*) İç Denetçi (CGAP), Düzce Üniversitesi, Orcid: 0000-0001-8439-9511, alptugguler@duzce.edu.tr

**) İç Denetçi (CGAP,CCSA), Düzce Üniversitesi, Orcid: 0000-0002-6826-0998, aliarkin@duzce.edu.tr

Yazı Gönderim Tarihi: 19.10.2018, Yazı Kabul Tarihi:31.10.2018

4. BİR UYGULAMA ÖRNEĞİ OLARAK DÜZCE ÜNİVERSİTESİ RİSK BELİRLEME ÇALIŞTAYI

Kurum çapında risk yönetimi süreçleri üzerinde üst yönetiminin liderliğinin olmaması, risk yönetimi değerlendirmelerinde ve iş birimlerinde risklere verilmesi gereken yanıtlarda kültürel farklılıklara ve kurum genelinde risk yönetimi uygulamalarında tutarsızlıklara yol açmaktadır. Kurumsal Risk Yönetimi üzerindeki üst düzey yönetici liderliği, kurumun risk felsefesi ve stratejisini risk yönetimine tutarlı bir şekilde tüm örgüt boyunca iletme ve entegre etme konusunda yardımcı olmaktadır (Beasley vd., 2008: 314). Düzce Üniversitesi'nde yürütülen Risk Belirleme Çalıştayının başlangıç aşamasında üst yönetimin desteği alınmış ve çalışma bu destekle yürütülerek tamamlanmıştır.

Temel yaklaşım olarak üniversitenin karşı karşıya olduğu veya olabileceği risklerin tespit edilmesi üzerine odaklanılmıştır. Çalıştay, üniversitenin misyon, vizyon ve temel değerleri doğrultusunda kurumsal hedeflerine ulaşmasına engel olabilecek risklerin belirlenmesiyle başlamış ve tespit edilen risklerin yönetilebilmesi için mevcut bulunan kontroller ve konulması gereken kontrol veya stratejilerin değerlendirilmesiyle devam etmiştir. Çalıştayın nihai hedefi, üniversitenin kurumsal hedefleri açısından mevcut risklerin belirlenmesi ve değerlendirilmesi olmuştur.

Düzce Üniversitesi İç Denetim Birimi olarak 2018 Yılı İç Denetim Programı'na "Düzce Üniversitesi Bünyesindeki Tüm Birimleri Kapsayan Risk Evreninin Belirlenmesi Faaliyeti- Kontrol Öz Değerlendirme" başlıklı Risk Temalı Çalıştay odaklı danışmanlık faaliyeti alınmıştır. Bu kapsamda bir takvim doğrultusunda 02 Temmuz 2018 tarihinde Cumhuriyet Konferans Salonunda yapılan genel sunum ile Düzce Üniversitesinin Teşkilat Şemasında tanımlı bulunan Genel Sekreterlik- İdari Birimler, Enstitüler, Koordinatörlükler, Bölümler, Fakülteler, Yüksekokullar, Meslek Yüksekokulları ve Araştırma ve Uygulama Merkezlerinden; her birimden ayrı ayrı olmak üzere; bir personelin birim yöneticisi pozisyonunda, diğer personelin ise Stratejik Planlama Kurulu Birim Temsilcisi (zorunlu) olduğu, en az üç personelin hazır bulunduğu Düzce Üniversitesi Risk Evreninin Belirlenmesi Çalıştayı başlamıştır.

Çalıştay öncesinde; 18-29.06.2018 tarihleri arasında çalışma grupları belirlenmiş ve 25.06.2018 tarihinde yapılacak olan çalışmanın genel şemasını da içeren bir Risk Yönetim Rehberi yayınlanmıştır.

Çalıştayın 2. aşamasında, 10-27.07.2018 tarihleri arasında ekip çalışması formatında, Üniversitenin 2 iç denetçisinin kolaylaştırıcı olarak görev aldığı Operasyonel Süreçlerin Belirlenmesi, Ana ve Alt Faaliyetler ile Yönetim Faaliyetlerinin Tespit Edilmesi ve Çalışma Gruplarıyla Birimler Temelinde Risk-Kontrol Çalışması faaliyetleri yerine getirilmiştir.

Çalıştayın 3. aşamasında, 01-09.08.2018 tarihleri arasında yine ekip çalışması formatında, Üniversitenin 2 iç denetçisinin kolaylaştırıcı olarak görev aldığı Risk Evreni Konsolidasyon Çalışması faaliyeti yerine getirilmiştir.

4.1. Risk Belirleme Çalıştayının Veri Toplama Aşamaları

02 Temmuz 2018 tarihinde Cumhuriyet Konferans Salonunda başlayan ve tüm gün süren Çalıştayın sunum içeriğini; Çalıştayın Düzenlenme Sebebi, Risk Yönetim - Risk Değerlendirmesi, Risk Yönetimi, Kurumsal Risk Yönetimi, İç Kontrol-Kontrol Öz Değerlendirme, İç Denetim, Süreç Yönetimi ve Risk Evrenini Belirme Çalışması-Örnek Uygulama konuları oluşturmuştur.

Çalıştayın 1. aşamasını oluşturan sunum bölümüne 99'u akademik ve 73'ü idari olmak üzere toplam 172 personel katılmıştır. Çalıştayın 2. ve 3. aşamalarına ise 69'u akademik ve 102'si idari olmak üzere toplam 171 personel katılmıştır.

Çalıştay öncesi yayınlanan Risk Yönetimi Rehberinde kurumsal yönetimin temel bileşenlerinden olan risk yönetimi için temel bilgiler verilmiş ve rehberin temel amacı Düzce Üniversitesi bünyesindeki tüm birimleri kapsayan risklerin tespit edilerek Üniversitenin Risk Evreninin belirlenmesi olarak ifade edilmiştir. Bu temel amacın dışındaki ikincil amaçlar;

- Düzce Üniversitesi genelinde risk kültürünün oluşturulması,
- Düzce Üniversitesi çalışanlarına Kontrol Öz Değerlendirme yönteminin tanıtılması,

- Üniversitenin tüm faaliyet alanlarında görülebilecek Stratejik, Operasyonel, İtibar, Finansal, Yasal (Uygunluk), Bilgi Sistemleri, Raporlamalar ve Sağlık ve Güvenlik risklerinin kategorik olarak belirlenmesi,
- Üniversitenin stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek öncelikli risklerin belirlenmesi,
- Risklerin analiz edilmesi, değerlendirilmesi, sınıflandırılması ve önceliklendirilmesi,
- Risklere yönelik stratejilerin ve uygulanacak kontrol faaliyetlerinin belirlenmesi,
- Risklerin hem birimlerce ve hem de İç Denetim Birimi tarafından izlenmesi ve raporlanması,
- Üniversitesinin Kurumsal Risk Yönetiminde rol ve sorumlulukları bulunan yöneticiler ve çalışanlar için temel bir farkındalık ve paylaşım kanalının oluşturulması,
- Üniversitenin risk yönetimi, iç kontrol ve iç denetim üçgenin etkin bir şekilde oluşturulması

olmuştur.

Üniversitenin risk evrenini belirlemek amacıyla ilgili birimlerden verileri toplamak ve ekip çalışmalarında kullanmak üzere Microsoft Office Excel programından faydalanılmıştır. Ekip üyelerinin rahatlıkla kullanabileceği birbirine entegre 3 sayfadan meydana gelen bir excel dosya formu tasarlanmıştır. Formun içeriğini aşağıda belirtilen üç ana başlık oluşturmaktadır:

- Risk Belirleme
- Risk Analizi
- Risk Yönetimi

Formun doldurulması yukarıda belirtilen sıra dahilinde olmuştur. İş tekrarını önlemek amacıyla bazı veriler sayfalar arasında otomatik olarak aktarılmıştır. Üniversite birimleri, tüm çalışanların katılımını ve riskin etkin yönetimini sağlamak amacıyla aşağıda örneği bulunan Birim Risk Profil Kartını (Şekil 6) kendi çalışanlarına dağıtarak Çalıştaya doğrudan katılmayanlardanda gerekli verileri toplayabilmişlerdir.

4.1.1. Risk Belirleme Sayfası

Risk belirlemesi, kontrol listelerinin tamamlanması, risklerin tanımlanması için toplantılar yapılması ve arşivlenmiş belgelerin analiz edilmesi ile sağlanır (Dinu, 2012: 68). Çalışmada kullanılan Risk Belirleme sayfası 4 ana başlık (sütun) içermektedir (Şekil 7). Risk No sütununa, riski kolayca tanımlamak için

Şekil 6. Birim Risk Profil Kartı

Birim Adı	
Anahtar Risk Göstergesi	
Detaylı Risk Açıklaması	
Risk Kategorisi (Türü)	Stratejik operasyonel (faaliyet), finansal (mali), yasal (uygunluk), itibar, bilgi sistemleri, raporlama ve sağlık - güvenlik
Risk Etki Değerlendirmesi	Çok yüksek, yüksek, orta, düşük ve çok düşük
Risk Olasılık Değerlendirmesi	Çok yüksek, yoksek, orta, düşük ve çok düşük
Risk Oranı (risk etki ve olasılık sıralaması, 5*5 matris)	Önem derecesi çok yüksek, yüksek, orta ve düşük
Risk Yönetimi Stratejisi	Kabul et, kontrol geliştir, transfer et, kaçın, faydalan
Kontrol Faaliyeti / Strateji Açıklaması	Riske karşı oluşturulan kontrol faaliyetinin / stratejisinin açıklanması
Risk Sorumlusu	
Riskin Ait Olduğu Süreç / Faaliyet	
Riskin Ait Olduğu Alt Süreç /Alt Faaliyet	
Riskin Kontrolüne Ait Mevzuat ve/ veya Politika Belgesi	

(Yazarlar tarafından oluşturulmuştur.)

manuel olarak risk numarası girişi yapılmıştır. Anahtar Risk Göstergesi sütununa, manuel olarak kısaca risk olayının spesifik göstergesi tanımlanmıştır. Detaylı Risk Açıklaması sütunu için, manuel olarak risk olayını (mevcut veya olabilecek bir durumu) ve olası olumsuz sonuçları açıklayan ayrıntılı bir açıklama yapılması istenmiştir. Son olarak Risk Kategorisi sütunu ile açılır listeden, Tablo 2'de verilen skalaya uygun olacak şekilde, riskin içeriğini taşıyan uygun bir risk kategorisi seçimi sağlanmıştır.

Tablo 2. Risk Kategorisi

Risk Kategorisi	Açıklama
Stratejik Risk	Stratejik riskler iş hedeflerinin peşinde - ya fırsatlardan yararlanarak ve/veya tehditleri azaltarak - ortaya çıkmaktadır (Emblemsvåg ve Kjølstad, 2002: 847). Üniversitenin belirlemiş olduğu amaç ve hedefleri doğrudan olumsuz etkileyebilecek risklerdir.
Operasyonel Risk (Faaliyet Riski)	Operasyonel risk gibi kategoriler, düzenleyici ve yönetsel bir vizyon sürecinde önemli bir rol oynar, uygulamaların yeniden düzenlenmesi için geçici haritalar ve örgüt seviyesinde değişim ajanları için yeni diller ve fikirler sağlar (Power, 2005: 578). Üniversitenin yetersiz sistemlerinden, süreçlerinden, çalışanlarından, faaliyetlerinden ya da dış etmenlerden kaynaklanabilecek kayıplar ve işleyişi aksatabilecek risklerdir.
Finansal (Mali) Risk	Örgüt genelinde finansal risk yönetiminin büyüme faaliyetinin her geçen gün arttığı ve daha önemli bir hale geldiği finansal riske ait sorulabilecek temel sorulardan biri; finansal risk değerlendirmelerinin kurumun genel stratejik planına entegre edilmiş ve genel merkezden mi yönetildiği, yoksa bireysel işletim birimleri tarafından merkezi olmayan bir şekilde mi yönetildiğidir (Dolde, 1993: 33). Üniversite bünyesinde mali boyutta bir kayba neden olabilecek potansiyel olay, koşul ya da durumlardan kaynaklaan risklerdir.
Yasal / Uygunluk Riski	Herhangi bir kriz meydana geldiğinde, örgütler için potansiyel olarak halkla ilişkiler ve hukuki anlamda bazı sonuçlar meydana gelir. Krizlerle yüzleşen kurumlar, hem maddi menfaat sahipleri güvenilirliğini yitirirken hem de kötü eylemler iddiasıyla yasal yükümlülük altına girme riskini de taşımaktadırlar (Fitzpatrick, 1995: 33). Üniversitenin yasal mevzuattan ve mevzuatın değişmesinden kaynaklanabilecek yükümlülükleri yerine getirememesi, zamanında yerine getirememesi, eksik olarak yerine getirmesi veya mevzuatın yanlış yorumlanmasından dolayı meydana gelebilecek risklerdir.
İtibar Riski	İtibar riskleri, yalnızca insan yapımı bir toplumsal etkileşim ve iletişim ürünü olmaları bakımından diğer risk türlerinden farklıdır (Power, Scheytt, Soin ve Sahlin, 2011: 316). Üniversitenin iç ve dış paydaşları ya da genel kamuoyu nezdinde imajına zarar verebilecek risklerdir.
Bilgi Sistemleri Riski	Çalışanların günlük işlerinde bilgi kaynaklarıyla çalışmaları durumunda oluşabilecek kurum içi güvenlik tehditlerine daha fazla önem verilmesi durumunda, personel tarafından bilgi sistemleri güvenlik ihlallerinin oluşması azaltılabilir. Bilgi sistemleri güvenliğini yönetmeye yönelik organizasyonel çabaların tipik olarak çalışanlar, politikalar, süreçler ve kültür gibi diğer zayıflık kaynaklarını yönetme yerine donanım, yazılım ve ağ gibi teknolojik varlıklardaki güvenlik açıklarına odaklanma eğilimi vardır (Spears ve Barki, 2010 :503). Kullanıcılar bilgi sistemlerinin güvenlik risklerini yönetmede değerli bir kaynak olabilmektedir (Spears ve Barki, 2010: 504). Üniversitenin sahip olduğu bilgi teknolojilerinin kullanıma bağlı olarak herhangi bir kayba neden olabilecek potansiyel olay, koşul ya da durumlardır.
Raporlamalar Riski	Maddi olarak yanlış beyan edilen finansal tabloların olasılığının, yöneticilerin iş dışı davranışları ile sezgisel ve ilgi çekici bir şekilde değişime uğradığı ve finansal raporlama riskine ilişkin çeşitli kanıtlar mevcuttur (Davidson, Dey ve Smith,2015: 25).Üniversitenin ürettiği raporlara bağlı olarak iç ve dış paydaşları ya da genel kamuoyu nezdinde üniversitenin imajına zarar verebilecek risklerdir.

Sağlık ve Güvenlik Riski	Sağlık ve güvenlik risklerinin doğasını ve büyüklüğünü bilmek, önceliklerin belirlenmesinde ve aynı zamanda rekreasyonel faaliyetlerin, işlerin ve günlük yaşamın diğer yönlerinin takip edilmesiyle ilgili kararlar vermede yardımcı olacaktır. "Risk-risk" durumları riskli alternatifler arasından seçim yapılmasını gerektirir. "Ne kadar güvenli" durumlar, daha fazla güvenlik için diğer istenen faaliyetlerin ne kadarının feda edilmesi konusunda daha genel bir seçim gerektirir. "Ne kadar güvenli" durumların yönetilmesi doğal olarak daha zordur, çünkü bunlar bulanık düşünme ve retoriğe tabidir. Mevcut tahminlerin büyük belirsizlikleri, mantıklı kararlara varmak için açıkça iletilmelidir (Lave, 1987: 291). Üniversite bünyesinde iş sağlığı ve güvenliği kurallarına uyulmaması nedeniyle iç ve dış paydaşların maruz kalabileceği risklerdir.
Operasyonel ve Yasal Risk	Üniversitenin hem yetersiz sistemlerinden, süreçlerinden, çalışanlarından, faaliyetlerinden ya da dış etmenlerden kaynaklanabilecek kayıplar ve işleyişi aksatabilecek operasonel riski ve hem de üniversitenin yasal mevzuattan ve mevzuatın değişmesinden kaynaklanabilecek yükümlülükleri yerine getirememesi, zamanında yerine getirememesi, eksik olarak yerine getirilmesi veya mevzuatın yanlış yorumlanmasından dolayı meydana gelebilecek yasal risklerdir.
Operasyonel ve Finansal Risk	Üniversitenin hem yetersiz sistemlerinden, süreçlerinden, çalışanlarından, faaliyetlerinden ya da dış etmenlerden kaynaklanabilecek kayıplar ve işleyişi aksatabilecek operasyonel riskleri ve hem de üniversite bünyesinde mali boyutta bir kayba neden olabilecek potansiyel olay, koşul ya da durumlardan kaynaklanan finansal risklerdir.
Karma Risk	Yukarıda bahsedilen risk kategorilerden aynı anda iki veya daha fazla başlık altında değerlendirilebilecek risklerdir (Örneğin, operasyonel, yasal ve itibar riskinin aynı anda mevcut olma durumu).

(Yazarlar tarafından oluşturulmuştur.)

Risk Belirlemesinde, üniversite birimlerinin hassas görevler değerlendirmeleri, stratejik plana yönelik yapılan çalışmalar, birimlerin uymakla yükümlü olduğu yasal mevzuat, birimlerin iş akış şemaları, sunmakta oldukları faaliyet alanları ile ilgili hizmetler göz önünde bulundurulmuştur. Birimlerin faaliyetleri, çevresel yapıları, sunduğu hizmetleri, maruz kalabileceği risklerin kaynağı için bir temel oluşturmaktadır.

Şekil 7. Risk Belirleme Sayfası

(Ekran görüntüsü)

4.1.2. Risk Analizi Sayfası

Modern dünyada karşı karşıya kalınan riskler üç temel yolla ele alınmaktadır. Duygular olarak ele alınan risk, tehlikeye yönelik hızlı, içgüdüsel ve sezgisel tepkilere işaret eder. Analiz olarak ele alınan risk, mantıksal nedene dayanır ve bilimsel yönetimin tehlike yönetimine katılmasını sağlar (Slovic vd., 2004: 311). Çalışmada Risk Analizi sayfası 6 ana başlık (sütun) içermektedir (Şekil 8). Sayfanın ilk üç sütun bilgisi Risk Belirleme sayfasından otomatik olarak gelmektedir. Etki sütununda, riskin neden olduğu yaklaşık etki çok düşük- düşük-orta- yüksek ve çok yüksek olmak üzere 5'li likert ölçeğinden uygun seçeneğin seçilmesini sağlayacak şekilde açılır listeden seçim yapılmaktadır. Olasılık sütununda da etki sütununa benzer bir biçimde, oluşan riskin yaklaşık olasılığı çok düşük-düşük-orta-yüksek ve çok yüksek olmak üzere 5'li likert ölçeğinden uygun seçeneğin seçilmesini sağlayacak şekilde açılır listeden seçim yapılmaktadır. Son olarak Risk Oranı sütununa, seçilen etki ve olasılık değerlerine göre düşük-orta-yüksek ve çok yüksek olmak üzere Excel hesaplama yapmakta ve veri girişi otomatik gerçekleşmektedir.

Şekil 8. Risk Analizi Sayfası

	A	B	C	E	G	I
1	RİSK ANALİZİ					
2	RİSK NO	Detaylı Risk Açıklaması	Risk Kategorisi	Etki	Olasılık	Risk Oranı
3	Otomatik	Otomatik	Otomatik	Açılır Liste	Açılır Liste	Otomatik
15						
16						
17						
18						
19						
20						

Risk Evreni Çalışması | Risk - Belirleme | Risk - Analizi | Risk - Yönetimi

(Ekran görüntüsü)

4.1.3. Risk Yönetimi Sayfası

Geleneksel olarak kurumlar, stratejik öğeler için birden çok kaynak kullanarak ve güvenlik stoğu tutarak, çevrelerindeki mevcut risklere karşı tampon oluşturan stratejiler benimsiyorlardı. Bu tamponlar operasyonel performansları kısıtlayabilmekte ve rekabet avantajını olumsuz yönde etkileyebilmektedir. Yeni yaklaşımlar, potansiyel kayıpları tanımlamayı, potansiyel kayıpların olasılığını anlama ve bu kayıplara önem vermeyi içeren resmi bir süreç olan risk yönetimini içermektedir (Giunipero ve Eltantawy, 2004: 699). Çalışmanın Risk Yönetimi sayfası 12 ana başlık (sütun) içermektedir (Şekil 9). Sayfanın ilk üç sütun bilgisi Risk Belirleme sayfasından otomatik olarak gelmektedir. Risk Yönetimi Stratejisi sütununa, belirlenen risk için uygun cevap ölçüsü (Kabul et, Kontrol geliştir, Transfer et, Kaçın, Faydalan) açılır listeden seçilmektedir. Kontrol Faaliyeti / Strateji Açıklaması sütununa, belirlenen riske karşı oluşturulan / oluşturulabilecek kontrol faaliyetinin / stratejisinin açıklaması yapılmıştır. Risk Sorumlusu sütununa, tanımlanan risk için ilgili birim risk sorumlusu girilebilmektedir. Riskin Ait Olduğu Süreç / Faaliyet sütununa, Birim bazında riskin ait olduğu süreç veya faaliyet yazılmaktadır. Riskin Ait Olduğu Alt Süreç / Alt Faaliyet sütununa, Birim bazında varsa riskin ait olduğu alt süreç veya alt faaliyet yazılmaktadır. Risk kontrolüne ait Mevzuat ve / veya Politika Belgesi sütununa,

Riskin kontrolü için kullanılan mevzuat, rehber, plan, politika belgesi, akış şeması gibi dokümanlar yazılmaktadır. Kontrol Önlemleri Sonrası Risk Değerlendirmesi Grubunda bulunan etki, olasılık ve risk oranı için sırasıyla; etki sütununa, seçilen müdahale eylemi / stratejisi hesaplanarak riskin neden olduğu yaklaşık etki çok düşük-düşük-orta-yüksek ve çok yüksek olmak üzere 5'li likert ölçeğinden uygun seçeneğin seçilmesini sağlayacak şekilde açılır listeden seçim yapılmaktadır. Olasılık sütununa, seçilen müdahale eylemi / stratejisi hesaplanarak, oluşan riskin yaklaşık olasılığı çok düşük- düşük-orta-yüksek ve çok yüksek olmak üzere 5'li likert ölçeğinden uygun seçeneğin seçilmesini sağlayacak şekilde açılır listeden seçim yapılmaktadır. Son olarak Risk Oranı sütununa, seçilen etki ve olasılık değerlerine göre düşük- orta- yüksek ve çok yüksek olmak üzere Excel hesaplama yapmaktadır. (Otomatik veri yerleşimi yaptığından herhangi bir veri bulunmamaktadır.)

Şekil 9. Risk Analizi Sayfası

A	B	C	D	E	F	G	H	I	K	M	O
RİSK YÖNETİMİ											
RİSK NO	Anahtar Risk Göstergesi	Risk Kategorisi	Risk Yönetimi Stratejisi	Kontrol Faaliyeti / Strateji Açıklaması	Risk Sorumlusu	Riskin Ait Olduğu Süreç /Faaliyet	Riskin Ait Olduğu Alt Süreç / Alt Faaliyet	Riske ait Mevzuat ve/veya Politika Belgesi	Kontrol Önlemleri Sonrası Risk Değerlendirmesi		
									Etki	Olasılık	Risk Oranı
Otomatik	Otomatik	Otomatik	Açılır Liste	Manuel	Manuel	Manuel	Manuel	Manuel	Açılır Liste	Açılır Liste	Otomatik

(Ekran görüntüsü)

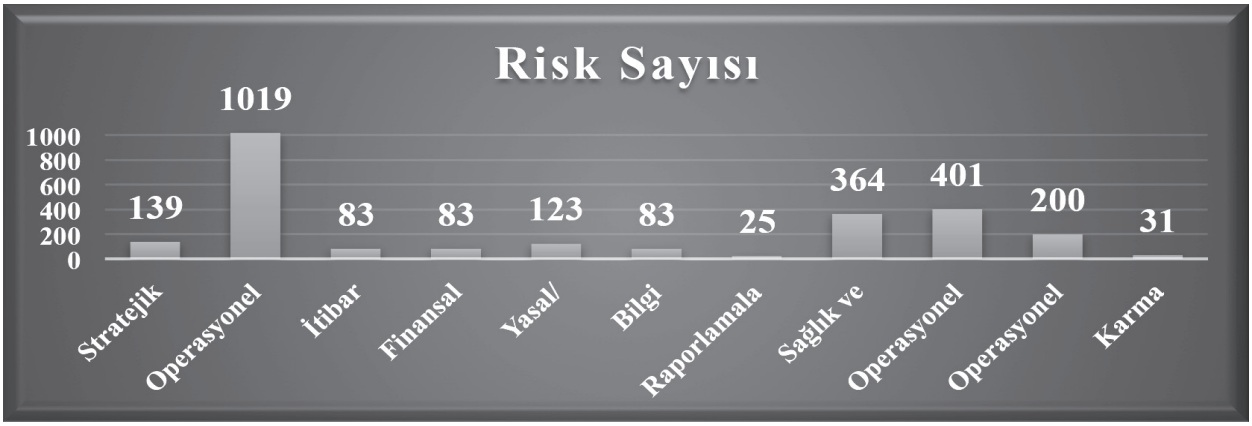
4.2. Risk Belirleme Çalıştayının Raporlama Aşaması ve Sonuçları

Çalıştayın raporlama aşamasında Fakülteler, Yüksekokullar, Enstitüler, Bölümler, İdari Birimler, Araştırma ve Uygulama Hastanesi, Koordinatörlükler ve Araştırma ve Uygulama Merkezlerinden gelen veriler konsolide edilmiş ve bu konsolidasyon sonrası Üniversitesi Genel Risk Raporu, Kısımlar Bazında Risk Raporu, Isı (Risk) Haritası, Risk Kategorileri Bazında Risk Raporu ve Çalıştay Metriklerini de kapsayan Düzce Üniversitesi Risk Evreninin Belirlenmesi Çalıştayı Raporu hazırlanmıştır.

Düzce Üniversitesi Risk Evreninin Belirlenmesi Çalıştayı sonucunda 69 üniversite biriminden; 139 adet Stratejik, 1019 adet Operasyonel, 83 adet İtibar, 83 adet Finansal, 123 adet Yasal / Uygunluk, 83 adet Bilgi Sistemleri, 25 adet Raporlamalar, 364 adet Sağlık ve Güvenlik, 401 adet Operasyonel ve Yasal, 200 adet Operasyonel ve Finansal ve 31 adet Karma risk kategorisinde toplam 2551 adet risk raporlanmıştır (Grafik 1).

Üniversite bünyesinde Operasyonel Risklerin baskın bir ağırlığının bulunması, birimlerin faaliyet alanla-

Grafik 1. Kategorilerine Göre Risk Sayısı

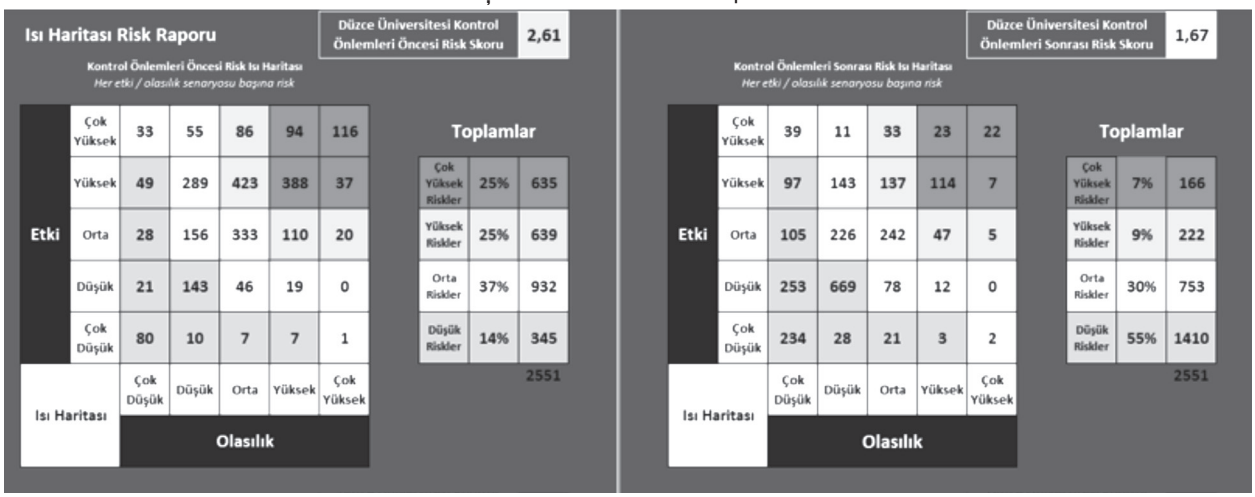


(Ekran görüntüsü)

rına daha fazla odaklanması ihtiyacını gün yüzüne çıkarmış ve risk yönetiminin omurgasının Operasyonel Riskler ağırlıklı olarak kurgulanması ihtiyacını doğurmuştur. Sağlık ve güvenlik risklerinin belirgin ağırlığı; bir taraftan İş Sağlığı ve Güvenliği (İSG) konusunda üniversite genelinde bir farkındalığın oluştuğunu göstermekte ve diğer yandan 6331 sayılı İş Sağlığı ve Güvenliği Kanunu temelinde, kurumsal bakış açısını yansıtan İSG yapılanma ihtiyacını işaret etmektedir.

Çalıştayın ikinci önemli sonucu olarak; toplanan veriler ışığında kontrol önlemleri öncesi ve sonrası durumu gösteren 2 adet ısı haritası risk raporu (Şekil 10) hazırlanmıştır. Bu haritalara göre; Düzce Üniversitesi Kontrol Önlemleri Öncesi Risk Skoru 2,61 değeri ile "*Yüksek*" ve Düzce Üniversitesi Kontrol Önlemleri Sonrası Risk Skoru 1,67 değeri ile "*Orta*" olmuştur. Çalıştay katılımcıları risklere karşı mevcut ve alınacak aksiyonlar (kontrol önlemleri) sonucunda yaklaşık 1 puanlık bir risk değer azaltımı öngörmüşlerdir.

Şekil 10. Isı Haritası Risk Raporu



(Ekran görüntüsü)

Isı haritasındaki riskler kendi aralarında konsolide edildiğinde üniversite genelindeki riskler; kontrol önlemleri öncesi 346 adet Düşük, 931 adet Orta, 639 adet Yüksek ve 635 adet Çok Yüksek risk oranlarına (Grafik 2) sahip olmuştur. Bu riskler için geliştirilecek kontrol önlemleri ve stratejiler sonucunda mevcut risk dağılımı 1410 adet Düşük, 753 adet Orta, 222 adet Yüksek ve 166 adet Çok Yüksek risk (Grafik 3) olacaktır. Isı haritasının etki ve olasılık sağ-üst hattındaki yoğunluk kontrol önlemleri sonra belirgin bir şekilde sol-alt hatta konumlanmaktadır.

Son yorum olarak risklere karşı geliştirilmesi gereken risk yönetimi stratejisinde ağırlıklı oran, Kontrol Geliştir seçeneği (Grafik 4) olmuştur. Özellikle "Çok Yüksek" ve "Yüksek" riskler öncelikli olarak odaklanılması gereken bir risk portföyünü oluşturmaktadır. Woods'a (2009: 74) göre; "Çok Yüksek" ve "Yüksek" riskler, iş hedeflerinin karşılanması ve hizmet sunumunun sağlanması için acil bir kontrol iyileştirmesinin yapılması gereken bir durum olarak tanımlanır. Yüksek ve çok yüksek etki veya yüksek olasılıklı tüm riskler çok yüksek olarak sınıflandırılır ve bu riskler ve ilgili kontroller hakkındaki bilgiler organizasyonel hiyerarşide bir sonraki seviyeye kadar otomatik olarak yükselir. Diğer bir deyişle, bir birim yöneticisi bir faaliyette ciddi bir risk görüyorsa, bu durum daha sonra, riski azaltmak için eylem planlarının tasarlanmasını sağlama sorumluluğunu üstlenen bir üst yönetici tarafından bilinecektir. "Çok Yüksek" ve "Yüksek" riskler, ilgili birim bünyesinde haftalık toplantıların ve eylem planlarının konusu olmalıdır. Eylem planları, mevcut kontrollerin etkinliği, hangi ilave kontrollerin gerekli olduğu ve bunlardan kimin sorumlu olduğu hakkında yorumlar içermelidir.

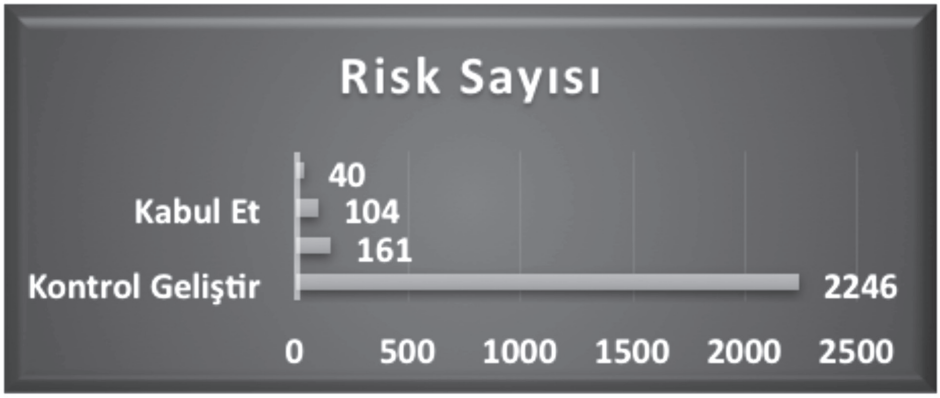
Grafik 2. Kontrol Önlemleri Öncesi Risk Oranı

(Ekran görüntüsü)

Grafik 3. Kontrol Önlemleri Sonrası Risk Oranı

(Ekran görüntüsü)

Grafik 4. Risk Yönetimi Stratejisine Göre Risk Sayısı



(Ekran görüntüsü)

5. SONUÇ

Örgüt varlık bulduğu habitatta sürekliliğini korumak zorundadır. Örgütün sürekliliği, belirsizlikler ve risklerle dolu dünyada eylemlerinin ne kadar etkin olduğuna bağlıdır. Çalışmada bu etkin eylemler için örgütün risk, kontrol ve hedef formasyonunu odağına alan Kontrol Öz Değerlendirme yaklaşımı ele alınmıştır. Bu yaklaşım ile örgütün risklerini belirlemesi, belirlenen risklerin etkin kontrolünün sağlanması ve bunlara bağlı olarak örgütsel hedeflere ulaşması için kurum bünyesinde oluşturulabilecek yol haritalarının içeriklerinin belirlenmesi sağlanmıştır. Kontrol Öz Değerlendirme yöntemi örgüt içinde ister dikey isterse yatay olarak kurulabilecek ağlar vasıtasıyla ve kurumsal negatif entropi üretme kapasitesiyle hem iş görenler ve hem de yönetim kademsinde bulunanlar için etkin bir kurumsal yönetme gücü sağlayabilmektedir. Ancak bu gücün örgütün sahip olduğu kültür kadar olacağı unutulmamalıdır. Örgüt kültürünün hedef-risk-kontrol formülasyonun kurulumu için Kontrol Öz Değerlendirme anlayışını bünyesinde içselleştirmesi gerekmektedir.

Kontrol Öz Değerlendirme sağladığı bakış açısı ile Kurumsal Risk Yönetimi için proaktif bir yönetim potansiyeli taşımaktadır. Örgütlerin etkin bir Kurumsal Risk Yönetimi için COSO güçlü bir çerçeve sağlamaktadır. Bu çerçeve COSO küpündeki paradigma değişimi sonucunda Kurumsal Risk Yönetimini daha uyarlanabilir bir yapıyı gösteren sarmal boyuta taşınmış ve bu boyut artık strateji, risk ve performans arasında daha kuvvetli bir bağ oluşturmuştur.

COSO yenilenen çerçevesi ile günümüz çalışma dünyasına daha esnek bir yapılanma biçimine bürünmüş, ağaç şeklindeki bir metaforik bakışla Kurumsal Risk Yönetiminin köklerine yönetişim ve kültür kavramlarını oturtmuştur. Bu metaforda ağacın gövdesini; strateji ve hedef belirleme (örgütün hedeflerinin risk iştahı ile stratejiyle uyumlu ve onu destekleyecek şekilde kurgulanması, örgütün her seviyesindeki risklerinin göz önünde bulundurulması), performans (risklerin belirlenmesi, şiddetinin değerlendirilip önceliklendirilmesi ve buna bağlı olarak risk yanıtlarıyla portföy bakış açısının oluşturulması), gözden geçirme ve revize etme (örgütün, önemli değişimler ışığında, hedeflerine göre performansını nasıl sonuçlandırdığı, kurumsal yönetim uygulamalarının etkin ve verimli çalışıp çalışmadığı, kuruma ne kadar değer kattığı ve değer katmaya süreklilik kazandırıp kazandırmadığı ve düzeltilmesi gereken faaliyetler bulunup bulunmadığı) oluşturmaktadır. COSO Kurumsal Risk Yönetimin dallarını ise bilgi, iletişim ve raporlama oluşturmuştur. Bu dallar aracılığıyla örgüt içinden ve dışından bilgi elde edilip, kurum içinde gerekli paylaşım sağlanmaktadır. Örgüt bilgi ve veriyi faaliyetlerinde kullanmakta, işlemekte, bilgi sistemlerinden faydalanmakta ve bunu bir süreç mantığıyla işletmektedir. Son olarak örgüt yönetişim, risk, kültür ve performansa ait raporlama yapmakta ve bunu paylaşmaktadır. COSO'nun yeni çerçevesinin örgüt bünyesinde işlerliğinin sağlanması için ilk adım olarak örgütün bir risk envanterinin elde hazır bulunması gerekmektedir.

Risk envanterini çıkarmak için için en kullanışlı yol, örgüt bünyesinde bir risk çalıştayı düzenlemek olmaktadır. Bu çalıştay aracılığıyla; örgütsel hedeflerin gerçekleştirilmesini engelleyen riskler belirlenip bir listesi oluşturulabilmekte, belirlenen risklerin nasıl yönetilebileceğine veya uygun şekilde yönetilip yönetilmediğine karar verilebilmesi için kontrol süreçleri izlenebilmekte veya tasarlanabilmektedir. Çalıştay yalnızca örgütün maruz kaldığı riskleri tespit etmekle kalmamakta ayrıca örgüt kültürünün risk ve kontrol kavramlarıyla tanışmasına aracılık etmekte ve buna bağlı olarak örgüt iklimini riske-kontrole-yönetişime odaklı bir yapıya çevirebilmektedir. 2018 yılı içinde gerçekleştirilen Düzce Üniversitesi Risk Evreninin Belirlenmesi Çalıştayı ile örgüt hem Kontrol Öz Değerlendirme ve hem de risk-kontrol-hedef bütünlüğü kavramlarıyla tanışmış oldu. Kurumun insan kaynaklarının yapısı ve teknik altyapısının yeterliliğine, faaliyetlerinin karmaşıklık düzeyine, stratejik hedeflerinin değişkenliğine bağlı olarak farklı birimlerden çok farklı iş pozisyonlarından katılımın sağlandığı Çalıştay sonucunda, uzun soluklu bir çalışma olarak risk evreni ortaya çıkarılmış ve böylece Kurumsal Risk Yönetiminin geliştirilmesi için ilk kök kazanılmıştır. Özgün bir uygulama olduğu düşünülen söz konusu Çalıştayın, Düzce Üniversitesinde risk yönetimi konusunda bundan sonra yapılacak çalışmalara yön vermesi ve diğer kurumlara da örneklik oluşturması beklenmektedir.

Kaynakça

Abrams C., Von kanel J., Muller S., Pfitzmann B., ve Ruschka-Taylor S., (2007) "Optimized Enterprise Risk Management", *IBM Systems Journal*, 46(2), 219–234.

Anderson D., (2017, Ekim) "COSO ERM Getting Risk Management Right", *Internal Auditor*, 38-43.

Akçakanat Ö., (2012) "Kurumsal Risk Yönetimi ve Kurumsal Risk Yönetim Süreci", *Süleyman Demirel Üniversitesi Vizyoner Dergisi,* 4(7), 30-46.

Barr P. S., Stımpert J. L. ve Huff A. S., (1992) "Cognitive Change, Strategic Action, and Organizational Renewal" *Strategic Management Journal*, 13(S1), 15–36.

Bartlett C. A. ve Ghoshal S., (2002) "Building Competitive Advantage Through People: Human, Not Financial, Capital Must Be The Starting Point and Ongoing Foundation of A Successful Strategy", *MIT Sloan Management Review*, 43(2), 34+.

Beasley M., Pagach D., ve Warr R., (2008) "Information Conveyed in Hiring Announcements of Senior Executives Overseeing Enterprise-Wide Risk Management Processes", *Journal of Accounting, Auditing & Finance*, 23(3), 311–332.

Bhatt G. D. ve Grover V., (2005) "Types of Information Technology Capabilities and Their Role in Competitive Advantage: An Empirical Study", *Journal of Management Information Systems*, 22(2), 253–277.

Callahan C. ve Soıleau J., (2017) "Does Enterprise Risk Management Enhance Operating Performance?", *Advances in Accounting*, 37, 122-139.

COSO, (2004) *Enterprise Risk Management Framework*, http://www.coso.org/documents/COSO_ERM_Execut iveSumm ary.pdf. Erişim Tarihi: 01.08.2016.

COSO, (2017) *Integrating with Strategy and Performance Executive Summary*, https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf Erişim Tarihi: 12.09.2018.

D'arcy, S. P., (2001) "Enterprise Risk Management", *Journal of Risk Management of Korea*. 12(1).

Davıdson R., Dey A. ve Smıth A., (2015) "Executives' "Off-The-Job" Behavior, Corporate Culture, and Financial Reporting Risk", *Journal of Financial Economics*, 117(1), 5-28.

Dınu A. M., (2012) "Modern Methods of Risk Identification in Risk Management", *International Journal of Academic Research in Economics and Management Sciences*, 1(6), 67-71.

Dolde W., (1993) "The Trajectory of Corporate Fınancial Risk Management", *Journal of Applied Corporate Finance*, 6(3), 33–41.

Emblemsvåg J. ve Kjølstad L.E. ,(2002) "Strategic Risk Analysis – A Field Version", *Management Decision*, 40(9), 842-852.

ERM, (2018) *Applying Enterprise Risk Management to Environmental, Social and Governance-Related Risks*, https://www.coso.org/Documents/COSO-WBCSD-Release-New-Draft-Guidance-Printer-friendly.pdf Erişim Tarihi: 11.10.2018.

Fıtzpatrıck K. R., (1995, Summer) "Ten guidelines for reducing legal risks in crisis management", *Public Relations Quarterly*, 40(2), 33-38.

Flamholtz E., (2001) "Corporate Culture and the Bottom Line", *European Management Journal,* 19(3), 268–275.

Gıunıpero L.C. ve Eltantawy R.H., (2004) "Securing The Upstream Supply Chain: A Risk Management Approach", *International Journal of Physical Distribution & Logistics Management*, 34(9), 698-713.

GLEIM CPA REVIEW, (2018) *Updates to Business Environment and Concepts.*

Hallikas J., Karvonen I., Pulkkınen U., Vırolaınen V.M. ve Tuomınen M., (2004) "Risk Management Processes in Supplier Networks", *International Journal of Production Economics*, 90(1), 47–58.

Hamıd A.R.A., Majıd M.Z.A. ve Sıngh, (2008) "Causes of Accidents at Construction Sites", *Malaysian Journal of Civil Engineering*, 20(2) : 242 - 259.

Hubbard L., (2000) *Control Self-Assessment A Practical Guide*, the IIA.

Joseph G. ve Engle T., (2005) "The Use of Control Self-Assessment by Independent Auditors", *The CPA Journal*, 38-43.

Kıral H. ve Hatipoğplu İ.İ., (2017) "Risk Yönetiminde Kontrol Öz Değerlendirme Yaklaşımı ve Strateji Geliştirme Birimlerinin Bu Kapsamda Üstlenebilecekleri Roller", *Amme İdaresi Dergisi*, 50(4), 115-133.

KİDDER, (2014) *CCSA Sınavı Hazırlık Kursu Notları*, Ankara: Kamu İç Denetçiler Derneği.

Kurt G. ve UYSAL T.U., (2018) "COSO Kurumsal Risk Yönetimi Çerçevesi Güncelleme Projesinin Getirdiği Yenilikler", *Muhasebe ve Denetime Bakış*, 54, 19-34.

Lave L., (1987) "Health and safety risk analyses: information for better decisions", *Science*, 236(4799), 291–295.

Levın A.C., (2008) "Solving the Right Problem: A Strategic Approach to Designing Today's Workplace", *Building Design Strategy: Using Design to Achieve Key Business Objectives*, ed.: LOCKWOOD T. ve WALTON T., New York: Allworth Press.

Lıebenberg A. P. ve Hoyt R. E., (2003) "The Determinants of Enterprise Risk Management: Evidence From the Appointment of Chief Risk Officers", *Risk Management Insurance Review*, 6(1), 37–52.

Lundqvist S. A., (2015) "Why Firms Implement Risk Governance – Stepping Beyond Traditional Risk Management to Enterprise Risk Management", *Journal of Accounting and Public Policy*, 34(5), 441–466.

Lyon B.K. ve Hollcroft B., (2012, Aralık) "Risk assessments: Top 10 pitfalls and tips for improvement", *Professional Safety*, 57(12), 28-34.

Lyon B.K. ve Popov G., (2016, Mart) "The Art of Assessing Risk", *Professional Safety*, 61(3), 40-51.

Mcnally J., (2007) "Control Self-Assessment: Everybody Pitching in with Internal Controls", *Pennsylvania CPA Journal*, 78(3), 33-35.

Moeller R., (2015) *Brink's Modern Internal Auditing–A Common Body of Knowledge*, 8th Edition, New Jersey: John Wiley&Sons.

Norrman A. ve Jansson U., (2004) "Ericsson's Proactive Supply Chain Risk Management Approach After a Serious Sub-Supplier Accident", *International Journal of Physical Distribution & Logistics Management*, 34(5), 434–456.

O'reılly C., (1989) "Corporations, Culture, and Commitment: Motivation and Social Control in Organizations", *California Management Review*, 31(4), 9–25.

Phinicharomma S., (2018) *Risk Base Internal Controls & Audit: What's New under COSO-ERM 2017 Framework?*

Power M., (2005) "The Invention of Operational Risk", *Review of International Political Economy*, 12(4), 577-599.

Power M., (2009) "The Risk Management of Nothing", *Accounting, Organizations and Society*, 34(6-7), 849-855.

Power M., Scheytt T., Soın K. ve Sahlın K., (2011) "Reputational Risk as A Logic of Organising in Late Modernity", *Organisation Studies*, 30(2&3), 301–324.

Prewett, K. ve TerrY, A., (2018) "COSO's Updated Enterprise Risk Management Framework—A Quest for Depth and Clarity", *Journal of Corporate Accounting & Finance*, 29(3), 16-23.

Sadu I., (2017, Ekim) "Assessing Soft Controls", *Internal Auditor*, 57-60.

Schwenk C. R., (1984) "Cognitive Simplification Processes in Strategic Decision-Making" *Strategic Management Journal*, 5(2), 111–128.

Slovıc P., Fınucane M.L., Peters E. ve Macgregor D.G., (2004) "Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality", *Risk Analysis*, 24(2), 311-322.

Spears J. L. ve Barkı, H., (2010) "User Participation in Information Systems Security Risk Management", *MIS Quarterly*, 34(3), 503-522.

Touam Z., (2016, Aralık) "Control Self-Assessment, Techniques and Strategies", *IA Internal Auditor Middle East*, 18-20

TURNBULL REPORT, (2005) Internal Control - Revised Guidance for Directors on The Combined Code, London:Financial Reporting Council.

Türedi H. ve Karakaya G., (2015) "COSO İç Kontrol Modeli ve Kontrol Ortamı", *Finans Politik & Ekonomik Yorumlar*, 52(602), 67-76 .

Woods M., (2009) "A contingency theory perspective on the risk management control system within Birmingham City Council", *Management Accounting Research*, 20(1), 69-81.

Wu D. D. ve Olson D., (2009) "Enterprise Risk Management: a DEA VaR Approach in Vendor Selection", *International Journal of Production Research*, 48(16), 4919–4932.

SİGORTA SEKTÖRÜNDEKİ İÇ DENETİM UYGULAMALARINDA YASAL MEVZUATIN ROLÜ

(THE ROLE OF THE LEGAL REGULATIONS ON THE INTERNAL AUDIT APPLICATIONS IN THE INSURANCE SECTOR)

Rasim HACIOĞLU* / Günay Deniz DURSUN**

ÖZ

Bünyesinde bulundukları kurumların faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif güvence ve danışmanlık faaliyetleri olan iç denetim fonksiyonu, kurumların risklerinin etkin şekilde yönetilerek varlıklarının etkili ve verimli olarak sürdürülebilmesinde kritik öneme sahiptir. Bu önem, çeşitli tür ve seviyeden risklerle sürekli olarak karşı karşıya kalan ve esasen bir risk yönetimi işi olan sigortacılık alanında ise çok daha yüksek seviyeye çıkmaktadır. İç denetim faaliyetlerinin sigortacılık alanındaki bu öneminin yanı sıra, iç denetim sisteminin oluşturularak denetim faaliyetlerinin gerçekleştirilmesi ülkemizde yasal olarak da zorunluluk taşımaktadır. Bu çalışmada iç denetim faaliyetlerinin ülkemiz sigortacılık mevzuatındaki yeri, önemi ve mevcut durumu incelenmiş ve iç denetim sisteminin daha etkili ve verimli şekilde oluşturularak, denetim faaliyetlerinin de daha etkin şekilde yürütülebilmesi amacına yönelik olarak, yasal mevzuattaki gelişim alanları araştırılmış ve yapılan tespitlere bağlı olarak çözüm önerileri sunulmuştur.

Anahtar Kelimeler: Sigorta, Mevzuat, İç Denetim, Risk Yönetimi

JEL Kodlaması: M42, H83, G22, G32, G38

ABSTRACT

The internal audit function which aims to provide independent and objective assurance and consulting activities to the corporates has critical importance for managing the risks effectively and sustaining the efficiency and profitability of corporate entities. The mentioned importance increases in insurance area due to the insurance is a risk management activity and depending on the sector companies meet with the risks which have various types and levels as consistently. As well as this importance of internal audit function in insurance sector, it is a legal obligation in Turkey to constitute an internal audit system and perform audit activities in insurance companies. In this study, the place, importance and existing status of internal audit function in Turkish insurance legislation have been searched and by the search it is aimed to detect the improvement areas in the legislation and make the recommendations to the related parties to be able to increase the effectiveness of internal audit activities in the insurance sector.

Keywords: *Insurance, Legislation, Internal Audit, Risk Management.*

JEL Classification: *M42, H83, G22, G32, G38*

*) Dr., Aman Takaful Sigorta A.Ş., İç Denetim Bölümü Yöneticisi (CIA, SMMM, CFE, CRMA), İstanbul, Orcid: 0000-0002-9878-3685, rasimhacioglu@yahoo.com

**) Dr. Öğr. Üyesi, İstanbul Aydın Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Muhasebe ve Finans Yönetimi Bölümü, İstanbul, Orcid: 0000-0002-1079-2879, gunaydenizdursun@aydin.edu.tr

Yazı Gönderim Tarihi: 11.03.2019, Yazı Kabul Tarihi:28.03.2019

1. GİRİŞ

Sigortacılık bir risk yönetimi işidir (Şenel, 2006:299). En yalın haliyle, zarara veya kayba uğrama tehlikesi şeklinde tanımlanabilen ve bireysel, toplumsal ve kurumsal hayatın her alanında karşılaşılan risk kavramının, genel kabul görmüş tek bir tanımı bulunmamakta, ekonomi, siyaset, sağlık, teknoloji, tarım, çevre gibi farklı alanlarda farklı algı ve etkileri oluşmakta, bu sebeple de kullanıldığı alana ve iş koluna göre çok çeşitli risk tanımlamaları yapılmaktadır (Shaw, 2003:23). Sigortacılık alanında risk, herhangi bir tehdidin bir kıymette veya kurumun kendisinde zarara yol açma ihtimali bulunan olay(lar) olarak tanımlanmakta ve sigortanın varoluş nedenleri arasında sayılmaktadır (Kaya ve diğ., 2014:16-17).

Sigortanın temel varlık sebebi olan risklerin etkin olarak yönetimi, bu alandaki işletmelerin varlığı, kurumsallığı, sürdürülebilirliği ve kârlılığı açısından hayatî önem taşımaktadır. Risklerin yönetiminden, yönetim kurullarına karşı işletme üst yönetimleri sorumlu olup, işletme yönetimleri bu amaç doğrultusunda çeşitli istatistik, yöntem ve fonksiyonlardan yararlanmaktadır. İç denetim fonksiyonu, gerek yapısı ve doğası sebebiyle ve gerekse ülkemiz sigortacılık mevzuatının yüklediği sorumluluklara bağlı olarak, sigorta işletmelerindeki iç kontrol ortamları, finansal yapı ve durumları ile operasyon etkinlikleri ve verimliliklerinin değerlendirilmesinde en önemli risk yönetimi araçlarından biri olarak öne çıkmaktadır.

Bu çalışmada, ülkemiz sigortacılık mevzuatının iç denetim fonksiyonu ile ilgili hüküm ve yükümlülükleri incelenerek, sigorta işletmelerinde risklerin yönetimi ve iç kontrol ortamlarının değerlendirilmesinde yasal mevzuat açısından iç denetim fonksiyonlarının etkinliğini etkileyebilecek hususlar araştırılmış ve tespit edilen bulgular ışığında iç denetim faaliyetlerinin etkili ve verimli şekilde yürütülebilmesi için ilgili taraflara çözüm önerilerinde bulunulmuştur.

2. SİGORTANIN KAVRAMSAL ÇERÇEVESİ

2.1. Sigorta Kavramı ve Sigortanın Önemi

Sigorta, belirli bir prim karşılığında yapılan ve belirsiz bir ya da birçok riskin gerçekleşmesi halinde sigortacının sigortalıya ödemeyi taahhüt ettiği para ya da diğer teminatlara ilişkin sözleşmedir (https://www.lloyds.com, 2019).

Sigorta ile az sayıdaki insan veya kurumun başına gelen zararlar, aynı riske maruz bulunan tarafların tümü tarafından birlikte paylaşılıp daha kolay telafi edilmektedir. (SEGEM, 2014:10). Risklerin etkilerini azaltan, vatandaşları ve katılımcıları koruma altına alan, sosyal güvenlik sistemini destekleyen, mali istikrara, ekonomik kalkınmaya ve büyümeye katkıda bulunan sigorta, toplumsal ve ekonomik alanlarda çok önemli faydalar sunmaktadır. Dolayısıyla sigorta, temelinde risk yönetimi işi olmakla birlikte, yalnızca risklere karşı oluşturulmuş bir koruma sistemi olmayıp, kişileri, kurumları, toplumları ve devletleri muhtemel risklere karşı koruyan, bunların hem kişisel ve sosyal hem de ticari hayatta daha esnek olmalarını sağlayan ve bu suretle gelişimlerine ve büyümelerine destek olan sosyal bir paylaşım aracıdır (Grant, 2012:3).

2.2. Sigorta Türleri ve Özellikleri

Sigorta, en temel haliyle sosyal ve özel sigortalar olmak üzere iki farklı kola ayrılmaktadır. Sosyal sigortalar devletler tarafından ve genellikle de mecburi olarak uygulanmakta ve kapsamına aldığı tüm çalışanlar için sosyal tehlikelere karşı bir güvenlik müessesesi olarak işlev görmektedir (İleri, 1998:166). Sosyal sigortalar yoluyla teminata alınan risklerin neler olduğu yasal olarak da belirlendiğinden, bu tür sigortalar, kapsamındaki risklerin haricinde bir sosyal teminat içermemekte ve bu yönleriyle özel sigortalardan tamamen farklılaşmaktadır (Topçuoğlu ve Öztürk, 2009:5). Bu durumda sosyal sigortalar kapsamı dışında kalan pek çok riske ilişkin korumanın ancak özel sigortalar ile sağlanabileceğini söylemek mümkündür. Özel sigorta kapsamına, gerçek veya tüzel kişilerin risklerini transfer etmek amacıyla ihtiyari veya zorunlu olarak sigorta şirketlerinden satın aldıkları sigorta ürünleri girmektedir (Çipil, 2013:101).

Özel sigortalar konuları bakımından; can & mal & sorumluluk sigortaları, zorunlu & ihtiyari sigortalar,

zarar & meblağ sigortaları gibi türlere ayrılabilmekle birlikte, en genel kabul gören ayrım ise hayat ve hayat dışı (elementer) şeklinde yapılan branş bazlı sınıflandırmadır (SEGEM, 2014:24). Bu sınıflandırmada, insan hayatının sigortalanmasıyla ilgili sigorta ürünleri hayat branşı altında yer alırken, bunun dışındaki diğer sigorta ürünleri elementer branşlar altında toplanmaktadır (Çipil, 2013:105).

Sigorta kavramı ve tanımı göz önüne alındığında sigortayı diğer sektörlerden farklı kılan temel ve ortak özellikler ortaya çıkmaktadır. Bunlar; "sigortacı, sigortalı (sigortalı, sigorta ettiren veya lehtar), sigorta sözleşmesi, belirsizlik, prim ödenmesi, tazminat ödeme taahhüdü ile risk ve riskin transferi" şeklindeki unsurlardır (Özkan, 1998:10-11). Genel itibarıyla herhangi bir zamanda ve şekilde oluşması ihtimali olan çeşitli tehlikeler şeklinde tanımlanabilecek olan risk kavramı, sigortanın varoluş sebebi olması sebebi ile bu unsurların en önemlisi olarak öne çıkmaktadır (Göğüş, 2012:17).

2.3. Sigortacılıkta Risk ve Risk Yönetimi

Yukarıda hem genel hem de sigortacılık açısından tanımına değinilen risk kavramının, tanımlanması, sınıflandırılması ve yönetimi faaliyetleri, sigortacılığın risklerin transferine ilişkin bir ticaret alanı olması sebebiyle, diğer alanlara nazaran çok daha fazla önem taşımaktadır. Sigorta şirketlerinin karşılaştığı riskleri sınıflandırmada genel kabul görmüş bir sistem olmayıp, sigortacılığa ilişkin uluslararası çeşitli düzenleme taraflarının farklı şekillerde yaptıkları ayrımlar bulunmaktadır (Tiryaki ve Gözüaçık, 2007:23-24). Bununla birlikte sigortacılıkta risk kavramını temelde iki açıdan ele almak mümkündür. Bunlardan biri sigorta şirketinin yüklendiği, başka bir deyişle teminat verip çeşitli olasılıkların gerçekleşmesine bağlı olarak oluşan riskler, diğeri verilen teminatların dışında kurumun faaliyetleri, stratejileri, yatırımları, dış etkenler ve benzeri türdeki risklerdir (Karabulut, 2011:4).

Sigorta şirketleri, varlıklarını sürdürülebilir kılmaları ve de kârlılıklarını, etkinliklerini ve verimliliklerini devam ettirebilmeleri için karşılaştıkları tüm bu riskleri etkin şekilde tanımlamak, sınıflamak, ölçmek, kontrol altına almak, bir diğer ifade ile etkin risk yönetimi gerçekleştirmek durumundadır.

Sigortacılıkta risk yönetimi, sigorta işletmelerinde sigortalıların risklerini karşılayabilecek miktarda sermayenin bulunmasının yanı sıra, ülkenin finansal kurum ve kuruluşlarının ve de diğer tüm paydaşların hak ve menfaatlerini koruyacak idari yapının kurulmasını ifade etmektedir (Yazıcı ve Yanık, 2010:8). Dolayısıyla, sigorta şirketleri açısından önleyici kontroller içeren, iyi şekilde kurgulanmış ve şirketin amaçlarına uygun bir risk yönetim sistemiyle, esasen kurumsal risk yönetiminin kastedildiği söylenebilmektedir (Acharyya, 2008:39). Kurumsal risk yönetimi, kurumu etkileyebilecek potansiyel olayları açıklamak, kurumun risk alma profiliyle uyumlu şekilde riskleri yönetmek ve kurumun hedeflerine erişmesine ilişkin makul düzeyde güvence sağlamak amacıyla geliştirilmiş; kurumun yönetim kurulundan, üst yönetiminden ve diğer çalışanların tamamından etkilenen ve strateji belirlemede kullanılan, kurumun bütününde uygulanan sistemli bir süreçtir (COSO, 2004:2).

Sigortacılık sektöründe risk yönetimi çeşitli yöntemlerle yapılabilmekle beraber, en temel haliyle risk yönetimi sistemini; iş kabul/üretim limit ve yetkileri, standartlar ve raporlar, yatırım rehberi ve stratejileri ile tazminat yönetimi uygulamaları oluşturmaktadır. Söz konusu araçlar sayesinde risklerin yönetimine ilişkin tanımlar, prosedürler, limitler, yetkiler ve yöntemler belirlenmekte ve risk yönetimi faaliyetlerinin kurumun amaç ve hedeflerine uygun şekilde sürdürülmesi sağlanmaktadır (Babbel ve Santomero, 1996:7-8).

Bununla birlikte iç denetim fonksiyonu da, sağladığı güvence ve danışmanlık hizmetleri ile birlikte, gerek işletmelerin süreç yönetimleri ve gerekse üst yönetimleri için risk yönetimi faaliyetlerinin etkili, verimli, doğru ve yeterli şekilde gerçekleştirilmesine yönelik önemli katkılar sunmaktadır. Gerek iç denetimin yüksek katma değeri ve gerekse ülkemizdeki yasal düzenlemelerin iç dene-

tim fonksiyonuna yüklediği sorumluluklar dikkate alındığında, iç denetimin kurumlardaki en önemli risk yönetimi araçlarından biri olduğunu söylemek mümkündür.

3. SİGORTACILIKTA İÇ DENETİM

3.1. İç Denetimin Sigorta Sektöründeki Yeri ve Önemi

İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyeti olup; kurumun risk yönetim, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olan bir fonksiyondur (http://www.theiia.org, 2019).

Son zamanlarda her alanda görülen büyük ve önemli değişimler ile artan rekabet ortamı, dar ve kısıtlı şekilde algılanan, değerlendirilen ve uygulanan iç denetim fonksiyonu kavramının anlamını önemli ölçüde değiştirerek iç denetimi, kurumun amaçlarına ulaşmasında yönetimin en önemli yardımcılarından birine dönüştürmüştür (http://www.denetimnet.net, 2019). Sürekli artan riskler nedeniyle günümüzde organizasyonların güçlü kalabilmesi ve sürdürülebilir bir başarı sağlayabilmesi için ihtiyaç duydukları temel unsurlardan biri iç denetimdir. Kurumlarda üst yönetimin başarısını, güvenilirliğini ve hesap verebilme gücünü artırma işlevi gören iç denetim, gün geçtikçe önemini daha da artırmaktadır. İç denetim dünyadaki birçok ülkenin hem özel sektöründe hem de kamu yönetiminde yasal bir zemine kavuşmuştur. Hâlihazırda iç denetim uluslararası standartlarda yürütülen bir yönetim disiplini halini almıştır (Aslan, 2010:63).

Sigorta ise, günümüzün gelişmiş ekonomik ve sosyal dünyasında mikro anlamda, risklerin gerçekleşmesinden sonra oluşabilecek zararları aynı riskin tehdidi altında bulunan taraflara dağıtarak sosyoekonomik çöküşlere engel olurken, makro anlamda, ekonomik gelişme ve büyüme sürecinde bir nevi katalizör görevi görerek sosyal, ekonomik ve politik istikrara katkı sağlamaktadır (Uralcan, 2012:125).

Sigorta sektörü; malî yapısı, riskleri, kârlılıkları, gelir üretme şekilleri, organizasyon yapılanmaları, faaliyetleri ve operasyonları itibarı ile diğer sektörlerden ayrışmaktadır (Uzun ve diğ., 2005:6). Sektörün kendine has yapı ve dinamikleri, önemli yükümlülükler içeren yasal mevzuat, farklı muhasebe sistemi, yoğun rekabet koşulları, artan, çeşitlenen ve farklılaşan riskler, bu risklere bağlı olarak değişen ve gelişen müşteri talepleri, büyüyen organizasyonlar, karmaşıklaşan işlemler, teknolojik gelişmeler, politik/doğal/çevresel/ekonomik olaylar gibi temel sebeplere bağlı olarak işletmelerin varlıkları, kârlılıkları, sürdürülebilirlikleri, faaliyetleri ile yönetsel karar ve stratejilerini etkileyen sigorta pazarına özgü ve/veya genel çok çeşitli ve kritik riskler ortaya çıkmaktadır. Söz konusu risklerin yönetiminde iç denetim fonksiyonu hem kavramsal ve yapısal olarak hem de mevzuat yükümlülüğü sebebi ile önemli işlevler üstlenmekte ve buna bağlı olarak iç denetimin sağladığı bağımsız ve tarafsız, danışmanlık ve güvence hizmetlerinin önemi diğer sektörlere nazaran sigortacılık alanında çok daha fazla önem taşımaktadır.

3.2. Sigorta Sektöründe İç Denetim Mevzuatı

Sigortacılık, finansal alanda faaliyet gösteren sektörlerden biridir ve bu sebeple devletin sıkı yasal düzenlemeleri ve takibine tabi tutulmaktadır. İşleyişi ve özellikleri itibari ile diğer sektörlerden farklılık gösteren sigorta sektörü, ülkemizde Hazine ve Maliye Bakanlığı bünyesinde yer alan iki birim tarafından sektör şartlarına ve özelliklerine uygun olarak düzenlenmekte ve denetlenmektedir (Dursun ve Kablan, 2017:70). Bunlardan Sigortacılık Genel Müdürlüğü, temel olarak sigortacılıkla ilgili konularda mevzuatı hazırlamak, uygulamak ve ilgililer tarafından uygulanmasını izlemek ve yönlendirmek, ülke sigortacılığının gelişmesi ve sigortalıların korunması için tedbirler almak, bu tedbirleri bizzat uygulamak veya ilgili kuruluşlarda uygulanmasını izlemek faaliyetlerinden sorumludur. Sigorta Denetleme Kurulu ise, ilgili kanun ve yönetmelikler kapsamında kendisine verilen denetim, inceleme ve soruşturma faaliyetlerini yürütmek ve sonuçlandırmak, denetim sonuçlarını ve alınacak önlemleri incelemek ve değerlendirmek, sigortacılıkla ilgili denetim gerektiren ihbar ve şikâ-

yetleri incelemek ve sonuçlandırmak sigortacılık piyasası ile ilgili raporlar hazırlamak ve ilgili taraflara raporlamak ve mütalaa vermek görevlerini gerçekleştirmektedir (https://www.hmb.gov. tr, 2019).

Türkiye'de devletin sıkı kontrolü altında faaliyet gösteren sigortacılık sektöründeki devlet müdahalelerinin amaçlarını şu şekilde sıralamak mümkündür (http://www.aktuerya.hacettepe.edu.tr, 2019):

- Sigortacılığın bütünüyle güvene dayalı bir sistem olması,
- Verilen taahhütlerin gerçekleştirilmesine yönelik şirketlerin ödeme kabiliyeti, mali yeterlilik ve şirket sürekliliği sağlayabilmesi,
- Sigortalılarla beraber üçüncü şahısların ve yatırımcıların hak ve menfaatlerinin korunması,
- Sektörün sahip olduğu istihdam kapasitesinin geliştirilmesi,
- Ekonomi politikalarını belirleme konusunda yol gösterici olması.

Bu amaçlar doğrultusunda sigorta sektörü ülkemizde; kanunlar, kanun hükmünde kararnameler, yönetmelikler, genelgeler, tebliğler, Bakanlar Kurulu kararları, klozlar, genel şartlar, tarifeler ve talimatlardan oluşan çok sayıdaki düzenleme aracılığı ile yürütülmektedir.

Ülkemizdeki sigortacılık faaliyetlerinin temellerini yasal anlamda Sigortacılık Kanunu ile Türk Ticaret Kanunu oluşturmaktadır. Türk Ticaret Kanunu'nda sigortacılık faaliyetleri altıncı kitapta düzenlenmiş ve sigortanın temel kavramları, tarafları ve yükümlülükleri, türleri, prensipleri ve çeşitli hükümlerini düzenleyen genel çerçeve çizilmiştir (Türk Ticaret Kanunu, 14.02.2011 tarih ve 27846 sayılı Resmî Gazete). Sigortacılık Kanunu ile de *"ülkemiz sigortacılığının geliştirilmesini sağlamak, sigorta sözleşmesinde yer alan kişilerin hak ve menfaatlerini korumak ve sigortacılık sektörünün güvenli ve istikrarlı bir ortamda etkin bir şekilde çalışmasını temin etmek üzere bu Kanuna tâbi kişi ve kuruluşların, faaliyete başlama, teşkilât, yönetim, çalışma esas ve usulleri ile faaliyetlerinin sona ermesi ve denetlenmesine ilişkin hususlar ve sigorta sözleşmesinden doğan uyuşmazlıkların çözümlenmesine yönelik olarak sigorta tahkim sistemi ile ilgili usul ve esasları düzenlemek"* amacı güdülmüştür (Sigortacılık Kanunu, 14.06.2007 tarih ve 26552 sayılı Resmî Gazete). Bununla birlikte, Karayolları Trafik Kanunu, Karayolu Taşıma Kanunu, Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, Tarım Sigortaları Kanunu, Türk Borçlar Kanunu, Afet Sigortaları Kanunu ile Tüketicinin Korunması Hakkında Kanun da sigortacılık faaliyetlerini düzenleyen temel (birincil) mevzuatı oluşturmaktadır (https://www.tsb.org.tr, 2019).

1959 tarihli Sigorta Murakabe Kanunu esas alınarak oluşturulan ve sigortacılık alanındaki iç denetim faaliyetlerinin güncel değişim ve gelişmelere uyumunun sağlanması amacını güden "Sigorta ve Reasürans Şirketlerinin Kuruluş ve Çalışma Esasları Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik" 2004 yılında yayımlanmış ve böylece sigorta sektöründe iç denetim faaliyetlerine yönelik önemli ve resmî bir dayanak ortaya konmuştur. Buna göre "sigorta şirketleri bünyesinde, faaliyetlerinin kapsamı ve yapısıyla uyumlu, değişen koşullara cevap verebilecek nitelik, yeterlilik ve etkinlikte iç denetim sistemlerinin bulunmaması; bu şirketlerin mali durumlarının, sigortalıların hak ve menfaatlerini tehlikeye düşürecek şekilde zayıfladığı hallerden sayılacağı" hükmü konmuştur (Sigorta ve Reasürans Şirketlerinin Kuruluş ve Çalışma Esasları Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik, 27.01.2004 tarih ve 25359 sayılı Resmi Gazete). Yine aynı dönemde **"Sigorta ve Reasürans Şirketlerinin İç Denetim Sistemlerine İlişkin Genelge"** yayımlanmış ve söz konusu yönetmelikte yer alan iç denetim sistemi kavramına ilişkin açıklamalar yapılarak; iç denetim birimi görevleri, iç denetimin kapsamı, personelin yetki ve sorumlulukları, iş akış ve prosedürleri konularında genel bir çerçeve çizilmiştir (https://www.tsb.org.tr, 2019).

Sigorta şirketlerinde iç denetim zorunluluğu birincil mevzuat kapsamında Sigortacılık Kanunu ile birlikte ortaya konmuştur. Buna göre *"sigorta şirketleri ile reasürans şirketleri; tüm iş ve işlemlerinin, sigortacılık mevzuatı ve ilgili diğer mevzuata, şirketin iç yönergeleri ile yönetim stratejisi ve politikalarına uygunluğunun sürekli kontrol edilmesi, denetlenmesi ile hata, hile ve usulsüzlüklerin tespiti ve önlenmesi amacıyla risk yönetim sistemleri de dahil olmak üzere etkin bir iç denetim sistemi kurmak zorundadır"* (Sigortacılık Kanunu, md. 4/8).

Sigorta sektöründe zorunlu tutulan iç denetim çalışmalarına ilişkin iç denetim fonksiyonunun yapı ve faaliyetlerinin çerçevesi ise ikincil mevzuat kapsamında "Sigorta ve Reasürans ile Emeklilik Şirketlerinin İç Sistemlerine İlişkin Yönetmelik" ile çizilmiştir. (21.06.2008 tarih ve 26913 sayılı Resmî Gazete). Sigortacılık Kanunu'na dayandırılarak hazırlanmış olan ve iç denetimin yanı sıra iç kontrol ve risk yönetimi faaliyetlerini de kapsayarak toplu şekilde iç sistemler adı altında birleştiren söz konusu yönetmelik; hayat dışı, hayat, emeklilik ve reasürans alanında faaliyet gösteren sigorta şirketlerinin tamamını kapsamaktadır. Buna göre şirketler, karşı karşıya kaldıkları riskleri izlemek ve kontrolünü sağlamak amacıyla, kurum faaliyetlerinin kapsam ve yapısıyla uyumlu, değişen şartlara uygun, merkez ve taşra tüm birimlerinde uygulanan yeterli ve etkin iç sistemler oluşturmak, uygulamak ve geliştirmek zorundadırlar.

Yönetmelik, iç denetim sisteminin amacını "üst yönetime şirket faaliyetlerinin Sigortacılık Kanunu ve ilgili diğer mevzuat ile şirket içi strateji, politika, ilke ve hedefler doğrultusunda yürütüldüğü ve iç kontrol ve risk yönetimi sistemlerinin etkinliği ve yeterliliği hususunda güvence sağlamak" şeklinde tanımlamıştır. Buna göre, şirkette iç denetim birimi ya da teftiş kurulu tarafından yürütülecek iç denetim faaliyetlerinin gerçekleştirilebilmesi için, şirketin büyüklüğüne, faaliyetlerinin karmaşıklığına, yoğunluğuna, kapsamına ve risk düzeyine bağlı olarak, Sigortacılık Kanunu ve ilgili mevzuat ile şirket içi düzenlemelerde öngörülen denetim hizmetlerinin aksatılmadan ve bu hizmetlerin gerektirdiği seviyede yerine getirilmesi amacıyla yeterli sayıda iç denetçi veya müfettiş çalıştırılmalı ve iç denetim biriminin doğrudan yönetim kuruluna bağlı ve idari açıdan bağımsız olarak örgütlenmesi sağlanmalıdır. İç denetim birimi; genel müdürlüğün tüm birimleri, bölge müdürlükleri ve şubeleri ile taşra teşkilatı için en az yılda bir, tüm acenteleri için ise en az üç yılda bir defa raporlama yapmalı, fakat bankalar hariç tutulmak üzere şirketin toplam prim üretimindeki payı en az %5 ve daha fazla olan ya da tahsilâtı düşük olan acenteler için en az yılda bir defa yerinde denetim yapmalıdır. Söz konusu denetimlerle ilgili planlama risk değerlendirmelerine göre, üst yönetimin görüşü de alınarak oluşturulmalı ve ilgili iç sistemlerden sorumlu yönetim kurulu üyesinin uygun gördüğü planlar yönetim kurulunun onayıyla yürürlüğe girmelidir. Düzenlenmiş olan tüm raporlar, yönetim kurulunun gündemine alınmalı ve rapor sonuçlarına göre yapılacak işlemlere karar verilmelidir. İç denetim sistemiyle beklenen hedefe ulaşabilmek için şirketin yurt içinde ve yurt dışındaki şube, bölge müdürlüğü, acente ve genel müdürlük birimlerinin tamamı ile tam konsolidasyona tabi ortaklıkları gözetiminde yapılan dönemsel ve riske dayalı denetimlerde aşağıda sıralanan faaliyetler gerçekleştirilmelidir:

- İç kontrol ve risk yönetimi birimlerinin uygulamaları ile yeterlilik ve etkinliklerinin değerlendirilmesi,
- Muhasebe kayıtları ile finansal raporların doğruluğu ve güvenirliğinin incelenmesi,
- Operasyonel faaliyetlerin, belirlenmiş olan usullere uygunluğu ile bunlara ilişkin iç kontrol uygulama usullerinin işleyişinin test edilmesi,
- Elektronik bilgi sistemi güvenilirliğinin gözden geçirilmesi,
- İşlemlerin, Kanuna ve ilgili diğer mevzuata, şirket içi strateji, politika ve uygulama usulleri ile diğer iç düzenlemelere uygunluğunun denetlenmesi,
- Şirket içi düzenlemeler çerçevesinde yönetim kuruluna yapılan raporlamalar ile Müsteşarlığa yapılan raporlamaların doğruluğu, güvenilirliği ve zaman kısıtlamalarına uygunluğunun denetlenmesi,
- Eksiklik, hata ve suiistimallerin ortaya çıkarılması; bunların yeniden ortaya çıkmasının önlenmesine ve şirket kaynaklarının etkin ve verimli olarak kullanılmasına yönelik görüş ve önerilerde bulunulması,
- Ana hizmetlerin uzantısı veya tamamlayıcısı niteliğinde olan hizmet alımlarının iç denetim sistemi kapsamında değerlendirilmesi,
- Dönemsel ve riske dayalı denetimler haricinde, yönetim kurulunun veya Müsteşarlığın talebi üzerine, iç denetimin amacına uygun olarak özel denetimlerin gerçekleştirilmesi.

Yukarıda sayılan kanun, yönetmelik ve genelgeler, sigorta sektöründeki iç denetim faaliyetlerine yönelik temel ve esas mevzuatı oluşturmakta olup, bun-

ların yanı sıra iç denetim faaliyetlerine çeşitli atıfların yapıldığı birtakım düzenlemeler bulunmaktadır. 24.08.2007 tarihli ve 26623 sayılı Resmî Gazete'de yayımlanan "Sigorta Şirketleri ve Reasürans Şirketlerinin Kuruluş ve Çalışma Esaslarına İlişkin Yönetmelik" ve de 07.08.2007 tarihli ve 26606 sayılı Resmî Gazete'de yayımlanan "Sigorta ve Reasürans ile Emeklilik Şirketlerinin Mali Bünyelerine İlişkin Yönetmelik" bu düzenlemelerden olup, genel itibarı ile sigorta şirketlerinde iç denetim sisteminin gerekliliğini ortaya koymaktadır (https://www.murathanbayri.com.tr, 2019).

4. SİGORTACILIKTA İÇ DENETİM FAALİYETLERİNE İLİŞKİN MEVZUATIN DEĞERLENDİRİLMESİ

Sigorta sektöründeki iç denetim faaliyetleri ve kapsamlarının düzenlendiği "Sigorta ve Reasürans ile Emeklilik Şirketlerinin İç Sistemlerine İlişkin Yönetmelik" ve "Sigorta ve Reasürans Şirketlerinin İç Denetim Sistemlerine İlişkin Genelge" incelendiğinde, iç denetim faaliyetlerinin etkinliği etkileyebilecek birtakım hususların ve bunlara ilişkin gelişim alanlarının bulunduğu değerlendirilmektedir.

Bunlardan birincisi, söz konusu mevzuat yükümlülüklerinin sigorta sektöründe yer alan şirketlerin tür ayrımı olmadan tamamına uygulanacak şekilde oluşturulmuş olmasıdır. Sigorta sektöründeki şirketler hayat dışı, hayat, emeklilik ve reasürans alanlarında faaliyet göstermekte ve nihayetinde sigortacılık faaliyeti gerçekleştirmekle birlikte; faaliyetlerinin içerikleri, şekilleri, ürünleri, hizmetleri, sunulan teminatları/kapsamları, iş operasyonları, organizasyon yapıları, taşıdıkları riskler ve bu risklerin belirsizlik ve olasılıkları itibarıyla birbirinden önemli farklılıklar göstermektedir. Örneğin hayat dışı branşlarda faaliyet gösteren bir şirketin üstlendiği risklerin çeşit ve seviyeleri ile emeklilik alanında faaliyet gösteren bir şirketin riskleri birbiri ile aynı olmadığı gibi, bu risklerin etki, olasılık ve belirsizlikleri de benzer özelliklerde değildir. Yine örneğin bir reasürans şirketinin ürünleri kurumsal müşterilere yönelik iken, hayat dışı, hayat ve emeklilik şirketlerinin hem bireysel hem de kurumsal müşterileri bulunabilmekte ve dolayısıyla da taşıdıkları riskler birbirinden farklılaşmaktadır. Bununla birlikte, sigorta sektöründeki şirketler aynı alanlarda faaliyette bulunsalar dahi, organizasyon yapıları, büyüklükleri, operasyonları, branş dağılımları, portföy yapıları, finansal durumları gibi göstergelerinin birbirinden farklılıklar göstermesi sebebiyle riskleri de farklılaşmaktadır. Örneğin hayat dışı sigortacılık alanında faaliyet gösterip üretiminin oto branşlarında yoğunlaştığı bir şirket ile yangın/doğal afetler branşlarına yönelik üretimin ağırlıkta olduğu bir şirketin riskleri birbirinden önemli oranda farklılaştığı gibi, üretim yapılan branşlarının benzer olması durumunda dahi, yukarıda da sayıldığı gibi finansal durum, üretim hacmi, portföy yapısı, organizasyon yapısı, risk algı ve iştahı, yönetim kararları gibi birçok kritere bağlı olarak bu şirketlerin riskleri de farklılaşmaktadır. Tüm bu sebeplere bağlı olarak mevzuatta iç denetim faaliyetleri, kapsamları ve uygulamalarına ilişkin yükümlülüklerin, şirketlerin alan, branş, hacim, finansal durum, pazar payı, üretim/reasürans yapıları, hasar uygulamaları, organizasyon yapılanmaları ve benzeri türünde kriterler dikkate alınmadan ve herhangi bir ayrım yapılmadan sigortacılık alanındaki tüm şirketler için ortak olarak belirlenmesi, bu şirketlerin iç denetim yapı ve faaliyetleri açısından tekdüze uygulamalara maruz bırakılmasına sebep olmakta ve buna bağlı olarak iç denetim fonksiyonundan beklenen katma değerin sağlanamaması riski ortaya çıkmaktadır.

Gelişim alanı olabilecek bir diğer husus, iç denetim faaliyetlerinin risk odaklı olarak gerçekleştirilmesine ilişkindir. Risk odaklı iç denetim, klasik denetim anlayışından farklı olarak bir organizasyondaki süreç, operasyon ve işlemlere ilişkin risklerin tespiti, derecelendirilmesi ve kontrollerinin değerlendirilerek çözüm önerilerinin sunulması faaliyetleridir (Adiloğlu, 2011:67). Risk odaklı iç denetim anlayışı sayesinde iç kontrollerin uygunluğunu ve yeterliliğini incelemek, riskin izlenmesi sürecinde ihtiyaç duyulacak bilgileri temin etmek ve bir iş alanında geçerli olan en iyi uygulamaları tanımlamak mümkün olabilmektedir (Türedi ve diğ., 2015:4). Söz konusu mevzuat ise, bir yandan sigorta işletmelerinde iç denetim faaliyetlerinin risk esaslı yapılmasını şart koşmakta iken, diğer yandan da bir malî dönem içinde işletmelerdeki tüm bölüm ve bölge yöneticiliklerine ilişkin faaliyetlerin incelenmesini zorunlu tutmaktadır. Risk odaklı denetimin temelinde ise, denetim çalışmalarının kurumlardaki tüm alanlarda değil, ağırlıklı şekilde riskli olarak değerlen-

dirilen noktalarda yoğunlaştırılması bulunmaktadır. İç denetim faaliyetlerinin aynı anda hem risk odaklı olarak hem de bir dönem içerisinde tüm bölüm/bölgelerde gerçekleştirilmesi mümkün olabilmekle birlikte, sigortacılık gibi çeşitli tür ve seviyeden risklerle sürekli olarak karşı karşıya olan bir alanda bu yükümlülüğün gerçekleştirilebilmesi oldukça güçtür. Bunun için öncelikle yetkin, tecrübeli ve yeterli sayıda denetçiden oluşan bir kadro ve ayrıca sistemsel destek gerekmekte ve bunlar da finansal kaynak gerektirmektedir. Bu durum işletmeler için ek maliyetler anlamına gelmekte olup, sigorta işletmeleri gibi maliyet odaklı kurumlarda ise bu tür ek maliyetlerin oluşması üst yönetimler tarafından istenmeyebilmektedir. Bu durumda mevzuatın uygulanabilirliği açısından bir tezat oluştuğu ve denetimlerin hem risk esaslı olarak ve hem de bir dönemde tüm birimlerde gerçekleştirilmesi yükümlülüklerinin birbirini engelleyebilecek birer koşul olabileceği değerlendirilmektedir.

Mevzuatta risk esaslı denetim faaliyetlerine ilişkin bir diğer gelişim alanı da bu faaliyetlerin şekil ve kapsamı ile ilgilidir. Söz konusu yönetmelikte riske dayalı olarak gerçekleştirilmesi şart koşulan denetimlerin, risk esaslı iç denetim kavramında yer alan kriterleri nasıl sağlayacağı belirtilmemiştir. Bir diğer ifade ile risk esaslı denetim faaliyetlerinin iç denetim birimleri tarafından nasıl planlanacağı, hangi alanların önceliklendirilmesi gerektiği, risklerin nasıl derecelendirileceği, süreç ve operasyonlar bazında hangi risk türlerine ve kontrol noktalarına hangi kaynaklarla ne kadar zaman ayrılacağı ve hangi denetim teknikleri/faaliyetlerinin uygulanabileceği konularında ayrıntı ve açıklamalar bulunmamaktadır.

Bununla birlikte, mevzuattaki bir başka gelişim noktası ise iç denetim faaliyetlerinin kalite seviyeleri ile iç denetçilerin performans takiplerine ilişkindir. Uluslararası İç Denetim Standartları gereği de hazırlanması ve sürdürülmesi gereken kalite güvence ve geliştirme programları; gerçekleştirilen faaliyetlerin iç denetimin tanımına ve standartlara uygun olarak değerlendirilmesini ve iç denetçilerin etik kurallarını uygulayıp uygulamadığının değerlendirilmesini mümkün kılmak amacıyla tasarlanmakta ve iç denetim faaliyetlerinin verimliliğini ve etkililiğini değerlendirerek gelişim alanlarını belirlemektedir. Yine uluslararası standartlar gereği hem iç hem de kurumdan bağımsız dış değerlendirmelerden oluşması gereken kalite güvence faaliyetleri, iç denetim çalışmalarının etkinliği ve yeterliliği ile iç denetçilerin performansları, bağımsızlıkları, tarafsızlıkları ve yetkinliklerini dönemsel olarak etkin ve objektif şekilde ölçmeli ve sonuçları da dönemsel olarak işletme üst yönetimleri ve yönetim kurullarına iletilmelidir (IIA, 2010:10-12). Bu açıdan değerlendirildiğinde, mevzuatta iç denetim faaliyetlerinin kalitesine ve iç denetçilerin performansına ilişkin ölçücü ve seviye arttırıcı araç ve yöntemler ve bunların kullanımları ile ilgili daha ayrıntılı hükümlere ihtiyaç bulunduğu anlaşılmaktadır.

İlgili mevzuata ilişkin tüm bu faktörlere bağlı olarak; sektörde yer alan şirketlerin yönetim anlayışına, iç denetimin yapısı, personel yetkinliği ve tecrübesine, iç denetim algısına ve işletme faaliyetlerine bağlı olarak iç denetim uygulamalarında, çalışmaların kalite seviyelerinde, denetim faaliyetleri ve iç denetçilerin performans takip, sonuç ve ölçümlerinde farklılıklar ve eksiklikler yaşanması risklerinin oluşabileceği, iç denetim mevzuatı gereğince yapılması zorunlu tutulan risk odaklı iç denetimlerin gerçekleştirilemeyebileceği veya istenen kapsam, etki ve verimde olamayabileceği değerlendirilmektedir.

5. SONUÇ VE ÖNERİLER

Günümüzün bireysel, sosyal, çevresel, politik ve ekonomik dünyasının getirdiği şartlara bağlı olarak birey ve kurumlar sürekli olarak risklerle karşılaşmakta ve varlıklarını sağlıklı şekilde sürdürebilmek için bu riskleri etkin ve doğru olarak yönetmek durumunda kalmaktadır. Birey ve kurumların risklerini en etkin şekilde yönetebilmelerini sağlayan araçların başında özel sigortacılık hizmetleri gelmektedir. Bu hizmetleri sağlayan sigorta şirketleri, çok sayıda ve türde riski üstlenmekte ve esasen kümülatif risk yönetimi faaliyetleri gerçekleştirmektedir. Bu sebeple sigortacılık alanı diğer sektörlere kıyasla risklerle doğrudan ve sürekli olarak karşı karşıya olan ve bu risklerin de doğru, etkili ve verimli olarak yönetilmesi gereken sektörlerin başında gelmektedir. İç denetim fonksiyonu sigortacılık alanındaki şirketlerde risklerin etkin şekilde yönetilmesinde sağladığı güvence ve danışmanlık hizmetleri ile yönetim kurulları ve şirket üst yönetimlerinin kararlarında önemli ölçüde yol gösterici olmaktadır. Bununla birlikte, iç denetim siste-

minin kurgulanması ve denetim faaliyetlerinin gerçekleştirilmesi ülkemizde yasal olarak da zorunluluk taşımaktadır. Halihazırda Sigortacılık Kanunu, Sigorta ve Reasürans ile Emeklilik Şirketlerinin İç Sistemlerine İlişkin Yönetmelik ve de Sigorta ve Reasürans Şirketlerinin İç Denetim Sistemlerine İlişkin Genelge, sigortacılık sektöründeki iç denetim faaliyetlerini düzenleyen mevzuat olarak öne çıkmaktadır. Bu çalışma kapsamında söz konusu mevzuat incelenmiş ve iç denetim faaliyetlerinin etkinliğini etkileyebilecek birtakım hususların bulunduğu değerlendirilerek çözüm önerileri sunulmuştur.

Buna göre, sigorta işletmelerindeki iç denetim faaliyetlerine ilişkin tekdüze yükümlükler içeren mevcut yönetmeliğin güncellenerek, işletmelerin faaliyetleri, branşları, yapıları, pazar payları, üretim/hasar/reasürans yapıları ve bunlara ilişkin risklerin sınıf ve seviyelerini dikkate alacak şekilde ayrıntılı olarak düzenlenmesi ve işletme yapılarına ve risklerindeki artış oranına bağlı olarak, iç denetim yapı ve faaliyetlerine ilişkin yükümlülüklerin de arttırılması iç denetimin etkinliğinin sağlanmasında fayda sağlayabilecektir.

Diğer yandan, mevzuatta şart koşulan riske dayalı denetimlerin nasıl yapılabileceğine, hangi alanlara, süreçlere, kontrol noktalarına ve risk türlerine hangi denetim teknikleriyle yaklaşılabileceğine ve kaynakların nasıl kullanılabileceğine yönelik açıklayıcı mahiyette ek yasal mevzuatın oluşturulması, mevcut mevzuatın daha iyi anlaşılması ve uygulanması için yararlı olabilecektir. Ayrıca incelemelerin riske dayalı olarak daha etkin şekilde yapılabilmesi için işletmelerdeki tüm bölüm ve bölge/taşra yönetimlerinin bir dönem içerisinde incelenmesinin zorunlu tutulması yerine, yapılacak risk analizlerine bağlı olarak yüksek riskli alanların daha sık, düşük riskli alanların ise daha seyrek olarak denetlenmesine olanak sağlayacak şekilde güncellenmesi faydalı olabilecektir.

İç denetim faaliyetlerinin belirli bir usulde yapılabilmesi için planlama, icra, raporlama ve bulgu takip konularında belirli ve ayrıntılı standartların mevzuata konulması da fonksiyon etkinliğinin arttırılmasına yönelik katkı sağlayabilecektir. Bununla birlikte, iç denetim personeline yönelik istihdam esaslarının kapsamlı olarak belirlenmesi yanı sıra performans ölçüm ve takiplerinin yapılması ve faaliyetlere ilişkin kalite standartlarının sağlanmasına yönelik güvence programlarının uygulanması konusunda yükümlülüklerin ilgili mevzuatta ayrıntılı şekilde yer bulması da denetim faaliyetlerinin ve iç denetçilerin etkinliği, bağımsızlığı ve tarafsızlığının sağlanmasında yararlı olabilecektir.

Böylelikle, yasal mevzuat desteğinin geliştirilmesi suretiyle sigorta sektöründeki iç denetim fonksyonunun daha da güçlendirileceği, etkinliğinin ve katma değerinin arttırılmasına katkı sağlanabileceği değerlendirilmektedir.

Kaynakça

Acharyya, M. (2008), 'An Empirical Study on Enterprise Risk Management in Insurance', New Frontiers in Enterprise Risk Management, *Springer Berlin Heidelberg*, ss.39-55.

Adiloğlu, B. (2011), *İç Denetim Süreci ve Kontrol Prosedürleri,* İstanbul: Türkmen Kitabevi.

Aslan, B. (2010), 'Bir Yönetim Fonksiyonu Olarak İç Denetim', *Sayıştay Dergisi*, Sayı:77, Nisan-Haziran 2010, ss.63-86.

Babbel, D.F. & Santomero, A.M. (1996), 'Risk Management by Insurers: An Analysis of the Process', *The Wharton Fınancıal Instıtutıons Center*, 96-16, ss.1-36.

COSO (2004), 'Enterprise Risk Management – Integrated Framework' *Executive Summary,* September 2004.

Çipil, M. (2013), *Yeni Sigortacılık Mevzuatı ve Türk Ticaret Kanunu ile Uyumlu Risk Yönetimi Ve Sigortacılık*, Ankara: Nobel Yayıncılık, 2. Basım.

Dursun, G.D. & Kablan, A. (2017), 'Sigorta Şirketlerinde Karşılıklar ve Muhasebeleştirilmesi', *Marmara Sosyal Araştırmalar Dergisi*, Sayı:12, ss.68-76.

Göğüş, H.S. (2012), *Risk Odaklı İç Denetimde Risklerin Saptanması Ve Değerlendirilmesi*, İstanbul: Türkmen Kitabevi.

Grant, E. (2012), 'The Social and Economic Value of Insurance', *The Geneva Association Paper*, Sept. 2012.

IIA – The Institute of Internal Auditors (2010), 'Uluslararası İç Denetim Standartları', 2010.

İleri, H. (1998), 'Türkiye›de Sosyal Güvenlik Sisteminin Değerlendirilmesi', *Selçuk Üniversitesi Sosyal Bilimler Meslek Yüksekokulu Dergisi*, Sayı:1, ss.163-188.

Karabulut, H. (2011), 'Hayat Sigortası Şirketlerinde ve Emeklilik Şirketlerinde Finansal Risklerin Yönetimi', *Reasürör Dergisi*, Sayı:79, ss.4-25.

Kaya, F. ve diğ. (2014), *Sigortacılık*, İstanbul: Beta Basım, 4. Baskı.

Özkan, M. (1998), *Sigorta İşlemleri ve Muhasebesi*, İstanbul: Bilim Teknik Yayınevi.

SEGEM (2014), *Sigorta Acenteleri Teknik Personel Eğitimi Ders Notları,* 2014.

Shaw, J.C. (2003), *Corporate Governance & Risk A Systems Approach*, New Jersey: Wiley Finance.

Şenel, S.A. (2006), 'Sigorta Şirketlerinde Mali Yeterlilik', *Afyon Kocatepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* Cilt:8, Sayı:2, ss.297-315.

Tiryaki, T. & Gözüaçık, G. (2007), 'Elemanter Sigorta Şirketlerinde Risk Faktörleri', *Reasürör Dergisi*, Sayı:63, ss.16-37.

Topçuoğlu, M. & Öztürk M. (2009), 'Özel Sigorta Girişiminin Sosyal Güvenlik Sistemi Açısından Önemi', *Süleyman Demirel Üniversitesi E-Dergi*, ss.1-16.

Türedi, H. ve diğ. (2015), 'Risk Odaklı İç Denetim', *Muhasebe ve Finansman Dergisi*, Sayı:66, Nisan 2015, ss.1-20.

Uralcan, Ş. (2012), 'Sigorta Faaliyetlerinin İşlevsel Açıdan Değerlendirilmesi ve Türk Sigorta Sektörünün Bu Bağlamda Dünya Sigorta Şirketleriyle Karşılaştırılması', *Sosyal ve Beşerî Bilimler Dergisi*, Cilt:4, Sayı:1, ss.125-134.

Uzun, A.K. ve diğ. (2005), 'Sigorta ve Reasürans Şirketlerinin Kurumsal Yönetim Güvencesi: İç Denetim', *TİDE İç Denetim Dergisi*, Sayı:11, Bahar 2005, ss.6-11.

Yazıcı, S. & Yanık, S. (2010), 'Sigorta Sektöründe Kurumsal Yönetim ve Kurumsal Yönetim Komitesi'nin Rolü', *İktisat Fakültesi Mecmuası,* Cilt:60, Sayı:2, ss.1-22.

İnternet Kaynakları

Https://www.lloyds.com/help-and-glossary/glossary-and-acronyms?Letter=I, (Erişim tarihi: 10.01.2019).

http://www.theiia.org/guidance/standards-and-guidance/ippf/definition-of-internal-auditing/?search%C2%BCdefinition, (Erişim tarihi: 15.01.2019).

http://www.denetimnet.net/Pages/kriz_ic_denetim.aspx, (Erişim tarihi: 15.01.2019).

https://www.hmb.gov.tr/, (Erişim tarihi: 04.02.2019).

http://www.aktuerya.hacettepe.edu.tr/duyurular/seminerler/risk_gunleri/3.pdf, (Erişim tarihi: 04.02.2019).

https://www.tsb.org.tr/kanunlar-ve-khk.aspx?pageID=415, (Erişim tarihi: 04.02.2019).

https://www.tsb.org.tr/genelge-teblig-ve-sektor-duyurulari-2004.aspx?pageID=629, (Erişim tarihi: 05.02.2019).

https://www.murathanbayri.com.tr/wp-content/uploads/2018/05/Turk-Sigortacilik-Sektorunde-ic-Denetimin-Yasal-Cercevesi.pdf, (Erişim tarihi:05.02.2019).

HAKEMLİ Denetişim
Ortak Aklın Harmanı

ABONELİK FORMU

☐ Denetişim Dergisine 1 yıl abone olmak istiyorum. (KDV Dahil) 100 TL

☐ Denetişim Dergisine 2 yıl abone olmak istiyorum. (KDV Dahil) 180 TL

(Denetişim Dergisinin satış fiyatı KDV dahil 35 TL'dir. Yılda üç sayı yayımlanır.)

ABONELİK BİLGİLERİ (KİŞİSEL ABONELER İÇİN)

AD SOYAD : .....

DERGİNİN GÖNDERİLMESİ İSTENİLEN ADRES : .....

.....

TELEFON (EV/İŞ) : .....

CEP TELEFONU : .....

E-POSTA ADRESİ : .....

DOĞUM TARİHİ : .....

MESLEĞİ : .....

KURUMU : .....

ABONELİK BİLGİLERİ (KURUMSAL ABONELER İÇİN)

AD SOYADI : .....

DERGİNİN GÖNDERİLMESİ İSTENİLEN ADRES : .....

.....

TELEFON : ..... **FAKS:** .....

FATURADA YER ALMASI İSTENİLEN BİLGİLER : .....

.....

ÖDEME BİLGİLERİ

Abonelik bedelinin; Ziraat Bankası Başkent Şubesi nezdindeki TR 82 0001 0016 8358 7849 3750 01 No'lu IBAN'a yatırıldığını gösterir dekontun ve derginin gönderilmesi istenen posta adresinin iletilmesi yeterlidir.

YAZIŞMA ADRESİ

Kamu İç Denetçileri Derneği
Meşrutiyet Caddesi Konur Sokak No: 36/6 Kızılay ANKARA
www.kidder.org.tr • denetisim@kidder.org.tr

DENETİŞİM DERGİSİ YAZIM KURALLARI

A- GENEL ESASLAR

1. Denetişim Dergisi, TÜBİTAK ULAKBİM kriterlerini gözeten bilimsel içerikte "hakemli dergi"dir ve 4 ayda bir yayımlanır. Yayım dili Türkçedir.
2. Gönderilen yazılar, daha önce hiçbir yayın organında tam metin olarak yayımlanmamış veya yayımlanmak üzere gönderilmemiş olmalıdır. Daha önce ulusal ya da uluslararası kongre ya da sempozyumlarda sunulmuş ve özet metni basılan çalışmalar, bu nitelikleri belirtilerek gönderilebilir.
3. Gönderilen yazılar derginin kapsamı ile ilgili olmalıdır. İç denetim, iç kontrol, risk yönetimi, yönetişim, süreç yönetimi, performans yönetimi vb. gibi iç denetimle doğrudan ilişkili konularda yazılan makaleler öncelikli olarak yayımlanır.
4. Gönderilen yazılar, Yayın Kurulu tarafından bir ön değerlendirmeye (intihal sorgulaması vb. yönlerden) tabi tutulduktan sonra yazar(lar)ı gizlenerek bir Yayın Kurulu üyesi ve iki bağımsız hakemin değerlendirmesine sunulur; hakem değerlendirme sistemindeki süreçlerin tamamlanmasından sonra Yayın Kurulunun belirlediği sıraya göre yayım sürecine alınır. Değerlendirme sonucunda yayımlanması uygun görülmeyen eserlerle ilgili olarak yazar(lar)ına bilgi verilir.
5. Yayımlanması kabul edilen yazıların bütün hakları Denetişim Dergisine aittir. Yazıların içeriğinden yazarları, reklâmların içeriğinden ilan sahipleri sorumludur. Yazıların araştırma ve yayın etiğine uygun olması esas olup, bu hususta COPE (Committee On Publication Ethics) standartları gözetilir.
6. Dergimizde yayımlanan yazılardan "Denetişim Dergisi" kaynak gösterilerek alıntı yapılabilir.
7. Yayımlanmasına karar verilen yazılardaki basit yazım ve dizim hataları, yazara gönderilmeksizin Yayın Kurulunca re'sen düzeltilebilir.
8. Yayımlanan her bir yazı için 150,00 TL' den 250,00 TL'ye kadar telif ücreti ödenir. Ödenecek telif ücretinin tutarı, yayımlanan yazının türü ile bilimsel özgünlüğü ve araştırma yoğunluğu dikkate alınarak Yayın Kurulu tarafından belirlenir. Telif ücretinin ödenmesi yazının yayımlanmasını müteakiben yapılır.
9. Yazılar, elektronik ortamda "denetisim@kidder.org.tr" adresine word dosyası formatında gönderilmelidir. Gönderilen e-posta metninde, yazarın isim ve unvanı, açık adresi, telefon numarası, e-posta adresi ile telif ücreti ödenebilmesi için gerekli olan T.C. kimlik numarası ve banka hesap numarası bilgileri belirtilmelidir.
10. Aynı sayı içerisinde, aynı yazara ait tek yazarlı birden fazla eser yayınlanamaz.

B- YAZIM KURALLARI

1. Gönderilen yazılar;
   - Türkçe olmalıdır. İngilizce yazılmış makaleler de yayımlanabilir.
   - Özet bölümü hariç 4000 kelimeden az 8000 kelimeden çok olmamalıdır.
   - "Times New Roman" yazı tipinde, 10 punto büyüklüğünde, tek satır aralıklı olacak şekilde iki yana yaslı/dayalı biçimde yazılmalıdır.
   - "Normal" sayfa yapısında, üstten ve alttan 3 cm, sağdan ve soldan ise 2 cm kenar boşluğu olacak şekilde, cilt payı bırakılmadan ve 1 cm satır girintisi ile yazılmalıdır.
   - Bilimsel makale yazım kurallarına ve Türk Dil Kurumunca belirlenmiş imla ve yazım kurallarına uygun olmalıdır.
2. Yazı; Türkçe ve İngilizce başlık, Türkçe ve İngilizce özet (öz), makalede ele alınan ana konuları belirten anahtar kelimeler, giriş, gelişme, konuyla ilgili değerlendirme ve önerilerin özetlendiği sonuç bölümlerinden oluşmalıdır. İlgili bölümler aşağıdaki şekilde düzenlenmiş olmalıdır.
   - Başlık ve Yazar Adı: Yazı başlığı, makalenin içeriğini yansıtacak şekilde kaleme alınmalı ve 10 kelimeyi geçmeyecek şekilde 14 punto büyüklüğünde, tümü büyük ve kalın harfli, sayfaya göre ortalanmış olmalıdır. Bu başlığın bir satır altına ise başlık ile aynı biçimde ve parantez içinde olacak şekilde İngilizce makale başlığı da yazılmalıdır. Yazar ya da yazarların adları, İngilizce başlığın bir satır altına, sağa dayalı, italik/eğik, 11 punto büyüklüğünde ve kalın harfli olacak şekilde yazılmalıdır. Yazar adının ilk harfi büyük sonraki harfleri küçük, soyadının ise tümü büyük harflerden oluşmalıdır. Soyadı bitiminden sonra üzerine * simgesi konulup, bu simge ilk sayfanın altına dipnot şeklinde belirtildikten sonra, yazar ya da yazarların unvanları, çalıştıkları kurumlar, Orcid numaraları ve e-posta adresleri, aralarına virgül konularak 10 punto büyüklüğünde ve italik olarak yazılmalıdır.
   - Öz: Bu kısımda, yazıda ele alınan konu ile öneri ve sonuçlar 250 kelimeyi geçmeyecek şekilde Türkçe olarak özetlenmelidir. Özet kısmı 9 punto büyüklüğünde ve kalın harflerle iki yana yaslı olacak biçimde yazılmalıdır.
   - Anahtar Kelimeler: Bu bölümde yazıda ele alınan ana konuları belirtecek anahtar sözcüklere yer verilmelidir. Anahtar kelimeler 3'ten az ve 5'ten çok olmamalıdır.
   - Jel Kodları : Bu bölümde yazıda ele alınan konulara ilişkin JEL kodlarına yer verilmelidir.
   - Öz (Abstract), anahtar kelimeler (keywords) ve jel kodlarının (JEL Classification) İngilizceleri aynı sırayla ve anlam farkı olmaksızın yer almalıdır.
   - Giriş: Giriş bölümünde yazının konusu, konu ile ilgili özet arka plan, yazının amacı ve ele alınan konular ile yönteme yer verilmelidir.
   - Konuya İlişkin Açıklama, Tartışma ve Değerlendirmeler: Bu kısımda yazının konusu ile ilgili mevcut durum analizi yapılmalı, mümkünse bu alandaki ulusal ve uluslararası uygulama ve standartlar ile gelişmelere yer verilerek mevcut durumun eksiklikleri ve geliştirilmesi gereken yönleri olarak ele alınmalı ve bu amaca yönelik somut öneriler geliştirilmelidir.
   - Sonuç: Yazıda ele alınan konu bu kısımda çok öz bir şekilde ele alınmalı, değerlendirme ve öneriler özetlenmelidir.
3. Ekler, Tablo ve Şekiller aşağıdaki kurallara göre belirtilmelidir.
   - Tablo, şekil, grafik ve resimlerin adları; bu nesnelerin sınırlarını aşmayacak şekilde, "Times New Roman" yazı tipinde, 10 punto büyüklüğünde, sözcüklerin baş harfleri büyük ve 1 satır aralıklı olarak nesnelerin üzerine yazılmalıdır. Bu nesneler alıntı yapılarak kullanılmışsa; alıntı yapılan kaynak nesnenin hemen altında, bu nesnenin sınırlarını aşmayacak şekilde, "Times New Roman" yazı tipinde, 10 punto büyüklüğünde ve 1 satır aralıklı olarak yazılmalıdır. Bu husus ayrıca kaynakça kısmında mutlaka belirtilmelidir.
   - Ekler, Kaynakça'dan önce verilmelidir. Bunlara metin içinde yapılan göndermeler; (EK Tablo:1), (EK Şekil:7) ya da (EK Grafik:5) şeklinde yapılmalıdır.
4. Dipnot ve yararlanılan kaynaklar belirtilmeli, dipnotlar sayfanın altında verilmeli, yararlanılan kaynaklara metin içinde parantez içinde, metnin sonunda ise Kaynakça bölümünde yer verilmelidir. Dipnotlar ve Kaynakça aşağıdaki kurallara uygun olmalıdır.
   - Yararlanılan kaynaklar "Times New Roman" yazı tipinde, 9 punto büyüklüğünde, metin içi kaynak gösterme yöntemiyle (APA stilinde) yazılmalı ve makalenin sonunda Kaynakça bölümünde yer almalıdır.
   - Kaynakçada yazarların önce soyadları ilk harfleri büyük diğerleri küçük şekilde, sonra adlarının sadece ilk harfleri büyük harfle kısaltma yapılmak suretiyle yazılmalıdır.
   - Kaynakçada yararlanılan kaynaklar yazar soyadına göre alfabetik olarak sıralanmalıdır.
   - İnternet üzerinden yararlanılan kaynaklarda yazar ismi bulunmuyorsa, bu kaynaklar, yazarı belirli kaynaklar sona erdikten sonra, "İnternet Kaynakları" başlığı altında ve erişim tarihlerinin kronolojik sıralaması dikkate alınarak yazılmalıdır.

Çeşitli kaynaklardan yapılan alıntılamalar için kullanılabilecek örnekler aşağıda sunulmuştur.

Kitap:

i. Kepekçi C. (1998). *Bağımsız Denetim* (3. Baskı). Ankara: Siyasal Yayınevi.

ii. İnalcık, H. (2017) *Osmanlı imparatorluğu klasik çağ (1300-1600)* (24. baskı). İstanbul: Yapı Kredi Yayınları.

Çeviri Kitap:

iii. Müftüler M. (2001) *Türkiye ve AB: Soğuk Savaş Sonrası İlişkiler.* (Coşkun Coşar, Çev.). İstanbul: Astra Yayınları.

Yukarıdaki yazım kurallarına ve makale şablonuna http://www.kidder.org.tr/?page_id=112 adresinden ulaşabilirsiniz.

HAKEMLİ Denetişim
Ortak Aklın Harmanı

Kamu İç Denetçileri Derneği
Meşrutiyet Caddesi Konur Sokak No: 36/6 Kızılay - ANKARA
www.kidder.org.tr • denetisim@kidder.org.tr