SİBER GÜVENLİĞİN ETKİNLEŞTİRİLMESİNDE SÜREKLİ SÜREÇ DENETİMİ MODELİ*

Dr. Öğr. Üyesi Ali KESTANE**

İnceleme Makalesi / *Review Article*

Muhasebe Bilim Dünyası Dergisi

Aralık 2021, 23(4), 773-796

ÖZ

Modern çağın getirdiği teknolojik girişim işletmelerin faaliyetlerinin şeklini ve yönünü değiştirmiş ve dijital ekonomi ortaya çıkmıştır. E-ticaretin yoğun bir şekilde dünyanın geneline yayılması ile işletmelerin faaliyetlerini etkin ve verimli bir biçimde yerine getirerek varlıklarını koruma altına almaları noktasında Siber Güvelik kavramı ortaya çıkmış ve bu durumdan denetim faaliyetleri de kendisine düşen payı almıştır. Sermayenin uluslararası alanda hareket etmesi sonucunda işletme faaliyetlerinin farklı coğrafyalara taşınması, büyük veri yığınlarının oluşmasına yol açmış ve iç denetim faaliyetlerini güç hale getirmiştir. Bu bağlamda işletmelerin gerçekleştirmiş oldukları faaliyetlerine ilişkin alt işlem süreçlerinin sürekli olarak kontrol altına alınması ihtiyacı ortaya çıkmış ve Sürekli Süreç Denetimi kavramının doğmasına zemin hazırlamıştır. Değişen ve gelişen teknoloji ve yenilikler karşısında işletmelerin sürdürülebilirliklerini sağlamaları açısından; faaliyetlerine ilişkin en alt işlem süreçlerinden yola çıkılarak üretmiş oldukları veri ve bilgilerin korunması konusu siber güvenlik ve sürekli süreç denetimi konusunun kesişmesine neden olmuş ve söz konusu her iki uygulamanın yarattığı katma değer merak konusu olmuştur. Bu çalışmada siber güvenlik uygulamalarının etkinleştirilmesi üzerinde sürekli süreç denetiminin etkisinin belirlenmesi amaçlanmıştır. Uygulamada konunun yeni olmasından dolayı çalışma teorik bir perspektiften ele alınmış ve gelecekte yapılması gerekli görülen uygulamalara yönelik önerilerde bulunulmuştur.

Anahtar Kelimeler: Siber Güvenlik, İç Denetim, Sürekli Süreç Denetimi

Jel Sınıflandırması: O30, M40, M42

CONTINUOUS PROCESS AUDITING MODEL TO ENABLE CYBER SECURITY

ABSTRACT

The technological initiative brought by the modern era has changed the shape and direction of the activities of the businesses and the digital economy has emerged. As the e-commerce spread extensively throughout the world,

* Makale Geliş Tarihi (Date of Submission): 22.02.2021; Makale Kabul Tarihi (Date of Acceptance): 13.04.2021

** Kilis 7 Aralık Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü, alikestane@kilis.edu.tr, https://orcid.org/0000-0002-7049-0354

Atıf (Citation): Kestane, A. (2021). Siber Güvenliğin Etkinleştirilmesinde Sürekli Süreç Denetimi Modeli. *Muhasebe Bilim Dünyası Dergisi*, 23(4), 773-796. https://doi.org/10.31460/mbdd.884892.

the concept of Cyber Security has emerged in order to protect the assets of the businesses by performing their activities effectively and efficiently and the audit activities have taken its share from this situation. As a result of the international movement of capital, the relocation of business activities to different geographies has led to the formation of large masses of data and made internal audit activities difficult. In this context, the need for continuous control of sub-process processes related to the activities performed by businesses emerged and prepared the ground for the concept of Continuous Process Auditing. In order to ensure the sustainability of businesses in the face of changing and developing technologies and innovations; the protection of the data and information they have produced based on the lowest transaction processes of their activities has led to the intersection of cyber security and continuous process control and the added value created by these two applications has become a matter of curiosity. In this study, it is aimed to determine the effect of continuous process control on the activation of cyber security applications. Since the subject is new in practice, the study was handled from a theoretical perspective and suggestions were made for future applications.

Keywords: Cyber Security, Internal Audit, Continuous Process Audit

Jel Classiffication: O30, M40, M42

1. GİRİŞ

Dijital ekonomi çağının ileri teknoloji ürünlerinin işletmecilik faaliyetleri üzerinden iş dünyasına girmesi ile birlikte; iş dünyasının yönü e-platformlara doğru evrilmiş ve ticari faaliyetlerin gerçekleştirilmesinde yeni bir anlayış ortaya çıkmıştır. Söz konusu değişme ve gelişmeler karşısından bireyselden kurumsala iletişim ve bağlantı imkânlarının artması ulaşımı kolaylaştırmış olmasına rağmen güvenlik risklerini de beraberinde getirmiştir (Kestane 2020). Özellikle sermayenin uluslararası alanda e-platformlarda hareket ederek çeşitli coğrafyalara taşınması işletmecilik faaliyetlerinin kontrol ve denetlenmesi işlemlerini güç hale getirmiş yeni kontrol, denetim ve güvenlik risklerini ortaya çıkarmıştır (Kurnaz ve Kestane 2020, 1). Büyük ölçekli işletmelerin uluslararası sahnede faaliyetlerini genişleterek devam etmesi büyük veri yığınlarının oluşmasına neden olmuş söz konusu veri yığınlarının ise faaliyetlerinin etkili ve verimli bir şekilde yerine getirilmesi bakımından daha farklı yeni metotlar ile kontrol edilmesi gerekliliğini ortaya çıkarmıştır. İşletme faaliyetlerinin en alt işlem süreçlerinden yola çıkılarak; gerçekleştirilen faaliyetin niteliği, hacmi, genişliği, içinde bulunduğu birim ve güvenliği adına yeni risklerin oluşmasına yol açmış siber risk kavramının doğmasını tetiklemiştir. Söz konusu siber risklere bağlı olarak ortaya çıkan güven sorunu işletmelerin imajı üzerinde hayati bir öneme ulaşmış olup son yıllarda meydana gelen siber saldırılardan konunun önemi ve değeri açıkça görünür hale gelmiştir.

Siber güvenlik konusunun finansal tablo denetimin ötesinde işletmecilik faaliyetlerinin süreçlere kadar indirgenmesi ihtiyacı kendini belirtmiş; iç denetim faaliyetlerinden bağımsız denetime kadar olan denetim süreçlerinde süreç güvenliklerinin sağlanmasına yönelik anahtarlar oluşturulması ciddi bir

ihtiyaç olarak ortaya çıkmıştır. Bu bağlamda uluslararası meslek örgütleri ve denetim şirketleri konuya ilişkin çeşitli düzenlemeler yapmıştır ancak günümüzde eksik olan gereksinimler de hali hazırda mevcut bulunmaktadır. Siber güvenliğe yönelik olarak 2015 yılında Deloitte, COSO ile birlikte *Siber Çağda COSO* (COSO in the Cyber Age) adında bir rapor yayınlamış; söz konusu raporda siber risklerin işletmelerdeki değerlendirilme süreçlerine yönelik bir çerçeve sunulmuştur. (COSO 2015). Diğer taraftan; Uluslararası İç Denetçiler Enstitüsü, *Küresel Teknoloji Denetim Rehberi: Siber Risklerin Değerlendirilmesi: Üçlü Savunma Hattının Rolü* (Global Technology Audit Guide (GTAG): Assesing Cybersecurity Risk: Roles Of The Three Lines Of Defense) adlı bir rehber yayımlamıştır. Söz konusu rehberde, siber güvenlik riskleri karşısında iç denetçilerin güvence sağlamalarına yönelik hangi yetkinliklere sahip olmaları gerektiği üzerinde durulmuş; iç denetimin siber güvenlikteki açısından rolünü değerlendirilmiştir. (IIA 2016). Ayrıca, ISACA (Information System And System And Control Association) tarafından *Denetim: Siber Güvenlik* (Auditing: Cyber Security- Evaluating Risk and Auditing Controls) siber güvenlik kontrollerini, risk değerlendirme ve yönetim incelemelerini kapsayan bir rapor yayımlamıştır (ISACA 2017). Ayrıca, siber risklerin yönetilmesinde; ISO 27000, NIST (National Institute of Standards and Technology) ve COBIT (Control Objectivies for Information and Related Technology) gibi diğer düzenlemeler de yapılmıştır (COSO 2015). Türkiye'de ise Sermaye Piyasası Kurulu; 2018 yılı ocak ayında "*Bilgi Sistemleri Yönetim Tebliği* ve *Bilgi Sistemleri Bağımsız Denetim Tebliği"* yayınlanmış; söz konusu kapsamında bilgi sitemleri yönetimi ve denetimine yönelik açıklamalar yer almaktadır (SPK 2018).

E-uygulamalar ve ileri teknoloji ürünlerinin (bigdata, endüstri 4.0, yapaya zekâ, vs.) yoğun bir şekilde dünyanın geneline yayılması ile birlikte gelecekte işletmelerin varlıklarını sürdürülebilir olmaları açısından; faaliyetlerine ilişkin en alt işlem süreçlerinden yola çıkılarak üretmiş oldukları veri ve bilgilerin korunması konusu siber güvenlik ve sürekli süreç denetimi konusunun kesişmesine neden olmuş ve söz konusu her iki uygulamanın yarattığı katma değer önemli merak uyandırmıştır. Bu çalışmada siber güvenlik uygulamalarının etkinleştirilmesi üzerinde sürekli süreç denetiminin etkisinin belirlenmesi amaçlanmıştır. Türkiye'de siber güvenlik denetimleri üzerinde daha önce çeşitli araştırmalar yapılmış; fakat, Sürekli Süreç Denetimi konusunun daha önce ele alınmadığı görülmüştür. Ayrıca bu çalışmada söz konusu denetim modeli ile siber güvenlik denetimin bütünleşik olarak dikkate alınması konunun Türkiye için önemini ve diğer çalışmalardan farkını ortaya koymaktadır. Uygulamada konunun yeni olmasından dolayı çalışma teorik bir perspektiften ele alınmış ve çalışmanın teması kapsamında; ***"siber güvenliğin etkinleştirilmesine yönelik olarak sürek süreç denetiminin etkisi"*** araştırılmıştır ve gelecekte yapılması gereken uygulamalara yönelik önerilerde bulunulmuştur. Çalışma 2 ana bölümden oluşmakta olup birinci bölümde; siber risk, siber güvenlik ve sürekli süreç denetimi kavramlarının teorik çerçevesi oluşturulmuş, ikinci bölümünde ise siber güvenliğin etkinleştirilmesine

yönelik olarak sürek süreç denetimine yönelik bütünleşik bir model kurulmuş ve çalışma mantığı oluşturularak gelecekte yapılacak olan çalışmalara atıflarda bulunulmuştur.

2. SİBER RİSK KAVRAMI VE YÖNETİLMESİ

Günümüzde meydana gelen küresel rekabet koşullarına uyum sağlamak adına kamu ve özel sektörde bilgi teknolojileri yoğun bir şekilde kullanılmakta olup gerçekleştirilen işlemlerin elektronik ortama taşınması ile birlikte raporlamanın da biçim ve sunumunda farklılıklar meydana gelmiştir. Bu bağlamda kullanılan bilgi teknolojileri ile hem kamusal alanda hem de özel sektör kesiminde pek çok kolaylıklar sağlanabilmekte ve ortaya çıkan fırsatların yanında riskler ile de karşı karşıya kalınabilmektedir (Öztürk 2018, 208). Teknolojinin gelişmesine paralel olarak ortaya çıkan riskler arasında öne çıkan siber riskler; siber güvenlik kavramını ortaya çıkarmış ve PwC'nin 2018 yılında ortaya koymuş olduğu *"Küresel Ekonomide Suçlar ve Hile Araştırmaları"* başlıklı araştırmasında hile konusu 5 sınıfta ele alınmıştır. Söz konusu araştırmada en sık karşılaşılan hilelerden birisinin ise siber suçlar olduğu ifade edilmiştir (PwC 2018, 8). Yapılan araştırmadan hareketle siber risk kavramının işletmecilik alanına yeni bir unsur olarak doğduğu ve söz konusu risklerin belirlenmesi ve yönetilmesi bakımından önemini açıkça göstermektedir.

Siber risk kavramının açıklığa kavuşturulması ve siber güvenlik konusunun ele alınması noktasında konunun öneminin daha iyi anlaşılması bakımından yakın tarihte dünya genelinde ses getiren siber saldırılardan bahsetmek faydalı olabilecektir (KPMG 2019; Selimoğlu ve Altunel 2019, 7-8):

2012 – Linkedin: 6,5 milyon hesap ele geçirilmiştir,

2013 – Target: 110 milyon müşterinin kişisel bilgileri ele geçirmiştir,

2014 – JP Morgan: Milyonlarca banka hesabı verileri çalınmıştır,

Türkiye: Bir bankaya ait 2,7 milyon kredi kartı verisi çalınmıştır,

SONY: Kuzey Kore liderini aşağıladığı iddia edilen film nedeni ile SONY sunucuları hack'lenmiş ve film vizyona girememiştir,

2015 – Hilton: Hilton ve Starwood müşterilerinin kredi kartı verileri çalınmıştır,

2016 – Tesco Bank: 9000'i aşkın hesaptan 3,2 milyon dolar çalınmıştır,

Türkiye: Ülke genelinde yurtdışı kaynaklı DDOS saldırıları gerçekleştirilmiştir,

SWIFT: Türkiye, Bangladeş ve diğer ülkelerdeki bankalarda 100 milyon doları aşan tutarlarda paralar çekilmiştir,

2017 – Temmuz: Amerika'nın kredi birimi en büyük olan "Equfax"ın kayıtlarına erişilerek 145.5 milyon Amerikalı vatandaşın kişisel verileri çalınmıştır,

"Yahoo"ya ait ana şirket olan Verizon; 3 milyar yahoo kullanıcısının hesaplarının saldırıya uğradığını açıklamıştır,

"ShadowBrokers" isimli anonim şirket Amerikan Ulusal Güvenlik Merkezi'nin "hacking" araçlarını ifşa etmiştir,

64 ülkede Petya; fidye siber saldırısı gerçekleştirilmiştir. **Amazon**'nun bulut hizmetlerinde meydana gelen bir problemden dolayı 200 milyon Amerikan seçmenine ait kimlik bilgileri açık hale gelmiştir.

Yukarıda bahsedilen siber saldırıların temelinde yatan siber risk kavramı; herhangi bir kurum ya da kuruluşun sahip olduğu bilgi teknolojisi sisteminin işleyişinin durdurulması, kurumun itibarını kaybetmesine yönelik her türlü risk ile finansal kayıp yaşamasına neden olabilecek diğer riskleri ifade etmektedir. Söz konusu riskler (The Institute of Risk Management 2014, 8):

- Ajanlık, dolandırıcılık ya da para kazanma amacıyla bilgi sistemlerinin ele getirilmesine yönelik kasten gerçekleştirilen güvenlik ihlalleri,
- Kasıt olmadan ya da yanlışlıkla gerçekleştirilen güvenlik ihlalleri,
- İlgili sistemin tam olarak sağlam olmaması ve diğer unsurlardan dolayı ortaya çıkan fonksiyonel BT riskleri gibi eylemlerden ortaya çıkmaktadır.

Siber risk kavramının açıklığa kavuşturulması ile birlikte yaşanmış olan siber saldırılar dikkate alındığında ilgili bilgi sistemlerine yönelik ortaya çıkan siber tehditler aşağıdaki biçimlerde olabilmektedir (Kumar ve diğerleri 2005, 5-6):

- **Kimlik Doğrulama Suçları:** Kimlik doğrulama noktasında şifrelerin çalınması sonucunda ortaya çıkan suçlardır. Söz konusu problemin çözülebilmesi açısından birden fazla şifre ya da ilave bilgilere sahip olunması gerekmektedir.
- **İnkâr Edememe:** Göndericinin, göndermiş olduğu mesajın takip altına alınarak söz konusu mesajın gönderilmediğine dair iddia engellenebilmektedir. Fakat web sayfasına ulaşan bir kullanıcının yerinin tespit edilmesi güç bir durumdur.
- **Truva Atları ve Virüsler:** Truva atları; yüksek bir düzeyden daha düşük bir düzeye bilgi taşıyabilmekte iken virüsler; ilgili cihaz içerisinde yayılarak çeşitli özelliklerdeki birçok dosyayı silebilmektedir.
- **Sabotaj:** Hacker'ler sistemlere erişimi sağlayarak uygun olmayan mesajlar yollayabilmektedirler.

- **Hizmet ve Altyapısal Engellemelere Yönelik Saldırılar:** Telekomünikasyon, güç ya da enerji sistemleri gibi sistemlerden oluşan alt yapılar erişime açık hale getirilerek zarar ortaya çıkabilmektedir. Söz konusu saldırıların ilgili hizmetlerin sunulmasında önemli engel oluşturmaktadır.
- **Doğal Afetler:** Deprem, kasırga ya da yangın gibi doğal felaketler bilgisayar ağlarının zarar görmesine neden olabilmekte olup söz konusu durumun önlenmesine yönelik veri tabanlarının güncellenmesi ya da iyileştirilmesi faydalı olabilecektir.

Bahsedilen siber tehditlere ek olarak; web sayfası hırsızlığı, hukuka uygun olmayan içerik sunulması, sosyal mühendislik, sistem güvenliğine zarar verilerek erişim sağlanması, talep edilmeden alınmış olunan elektronik e-postalar, zararlı yazılımlar, bukalemun, mantık bombaları, salam tekniği, çöpe dalma, süper darbe ile bilgi ve veri aldatmacası gibi tehditler de söz konusu olabilmektedir (Aslay 2017, 25-26). Bu bağlamda işletmelerin karşı karşıya kalmış oldukları siber risklerinin belirlenmesi ve yönetilmesi; amaç ve hedeflere ulaşılması, imaj kaybının yaşanmaması ve zarara uğranılmaması adına büyük önem taşımaktadır. Bu bağlamda öncelikle konuya ilişkin farkındalık oluşturulması önemli bir başlangıç adımı sayılabilmektedir. Bu doğrultuda farkındalık algısının belirlenmesine yönelik Türkiye'de gerçekleştirilen bir çalışmada; 501 kullanıcının %96,3'ünün bilgi güvenliğinin önemine yönelik hassasiyete sahip olmasına rağmen söz konusu kullanıcıların %51,5'inin kullanmış oldukları teknolojik ürün ya da cihazlara ilişkin olarak tehditlerin farkında olmadıkları tespit edilmiştir. Dolayısıyla Türkiye adına öncelikle bireysel olarak daha sonra kamu ya da özel sektör fark etmeksizin siber tehdit ya da saldırılar hakkında farkındalık oluşturulması önemli bir gereklilik olarak ortaya çıkmaktadır. Özellikle işletme sahiplerinin çalışanlarına siber risklere yönelik farkındalık eğitimi sağlaması, teknolojinin hızlı ilerleme kaydetmesinden dolayı farkındalığın etkin bir şekilde yönetilmesi ve sürekliliğinin sağlanması büyük önem taşımaktadır (Erol ve Sağıroğlu 2018, 107-109).

İç Denetim Enstitüsü (IIA- The Institute of Internal Auditing) tarafından gerçekleştirilen çalışma dikkate alındığında siber ile ilişkili olan riskleri çözmek ve problemleri aşmak üzere; lider ekibinin caydırıcı önlemler geliştirmesi, söz konusu önlemlerin ise eğitim ve bilinçlendirme etkinlikleri ile uygulamaya koyulmasının faydalı olacağından bahsedilmektedir. Bu bağlamda farkındalığın artırılması amacıyla tedarikçilerden çalışanlara, işletme ortaklarından yüklenicilere dek eğitim verilmesi gerekmekte ve siber güvenlik önlemlerine ilişkin alınması gereken önlemler ve protokoller konusunda kendilerinden neyin beklendiğinin açıkça ortaya koyulması ve anlaşılmasının sağlanması gerekmektedir (IIA 2018, 7). Bu noktada siber risklerin belirlenerek yönetilmesi aşağıdaki biçimde özetlenebilmektedir (KPMG 2016, 7):

- İşletmelerin sahibi oldukları ağların korunmasına yönelik; anti-virüs sistemleri kurularak güvenlik duvarlarının oluşturulması, siber olay yönetimi politikalarının uygulamaya koyularak kullanıcı eğitimine önem verilmesi,

- Yönetim kurulunun bilgi risklerine karşı olan sorumluluğu siber güvenliğin merkezinde yer almakta olup dolayısıyla ilgili işletmenin önemli görülen bilgi varlıklarının neler olduğunun tespit edilmesi ve söz konusu varlıklara ilişkin risklerin yönetilmesi,
- Siber güvenlik projelerinde; insan unsuru temel alınarak kültür ve iş süreçleri ile teknik güvenlik konularını kapsayacak bütünleşik yaklaşımların ortaya koyulması,
- Siber güvenliğin teknik bir konu olmasının yanında güvenliğin sağlanmasına yönelik siber olaylara hazırlık yapmaktan başlanarak saldırı sonrasındaki müdahalelere ilişkin entegre bir yapılanma sağlanması,
- Güvenlik açığı penceresinden bakıldığından çalışanlar birincil faktör olarak görülebilir ancak bu anlamda kendilerine gerekli eğitim ve yetkinliklerinin kazandırılmasına yönelik teşvik uygulamalarının hayata geçirilmesi ve de
- Siber güvenlik sisteminin sağlıklı bir biçimde çalışmasına yönelik uygun bir yönetim yapısının oluşturularak araştırma sistemlerinin kurulması.

3. SİBER GÜVENLİK VE DENETİM

Siber olayların günümüzde artan sayıda meydana gelmesi ve medyanın söz konusu olaylara kilitlenmesi hemen her kurum yöneticisinin dikkatini çekmiş olup siber güvenlik kavramı öne çıkmıştır (Hermans ve Diemont 2017, 109). Siber teknolojinin son yıllarda hızlı bir gelişme kaydetmesi; bilgisayar sistemlerinde yer alan verilerin korunmasına yönelik alınan önlemleri artırmış ve sonucunda olası tehdit ve saldırılara karşı sistem güçlendirmesine olanak sağlanmıştır. Ağlarda yer alan veri sızıntılarından sistemlerin çökmesine kadar ciddi zararlara yol açan siber güvenli ve gizlilik olayları geçmiş yıllara kıyasla günümüzde daha çok meydana gelmekte; söz konusu durum ise günümüz toplumun en büyük tehdit mekanizmalarından birisi olarak karşılanmaktadır (Li ve diğerleri 2019, ix). Günümüzde birbirine bağlı ve bağımlı bir bilgi teknolojisi ortamının varlığı, siber güvenlik olaylarından ileri gelen ticari etkilerin artmasına yol açmakta; dinamik süreç olmasından dolayı ise riski azaltmak adına siber güvenlik bilgi sistemlerinin kurulması yaşamımızda olmazsa olmaz bir rol almaktadır (Wyatt 2017, 336).

Siber güvenlik kavramı; *"siber ortamlarda karşılaşılabilecek tehdit ve tehlikeler ile oluşabilecek riskleri önceden öngörüp bunlara karşı önceden önlem alma girişimi"* ya da *"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 edilebilmektedir (Sağıroğlu 2018, 26). Yapılan tanımlamalardan yola çıkıldığında siber güvenlikte temel amaç; güvenliğin makul seviyede sağlanması olarak karşımıza çıkmaktadır. Bu noktada yüz yüze sağlanan bir

güvenlikten bahsetmenin yok denecek kadar imkânsız olmasına dikkat edilmesi önemli bir gerekliliktir. Bu bağlamda siber güvenliğin sağlanması bakımından siber risklerin belirlenerek doğru bir biçimde yönetilmesi kritik bir unsur olarak karşılanmaktadır. Dolayısıyla, risklerin tespit edilerek giderilmesi açısından etkili bir risk yönetimi sağlanarak; mevcut olan teknolojiler, teknikler, standart, politika ve çözüm uygulamaları hayata geçirilerek siber güvenlik çalışmalarının pratikte aktif hale getirilmesi gerekmektedir (Selimoğlu ve Altunel 2019, 9). Bu bağlamda siber güvenlik uygulamalarında aşağıdaki unsurların yer alabildiği görülmektedir (Sağıroğlu 2018, 44):

- Güvenlik politikasının oluşturularak uygulamaya koyulması,
- Gerekli olduğuna inanılan koruma ilkelerinin uygulanması,
- Etkili bir risk analiz ve yönetimi,
- Belirli periyotlarla ilgili sistemlere ilişkin; hatalar, eksiklikler ve açıklıklar ile zafiyetlerin engellenmesine yönelik testlerin gerçekleştirilmesi,
- Sistem içerisinde yer alan kullanıcılara asgari düzeyde hak tanınması,
- Siber güvenliğin etkin bir şekilde hayata geçirilmesi bakımından ilgili düzenlemelerin (Siber Çağda COSO, ISO 27000 vs.) uygulamaya koyulması
- İçinde bulunulan elektronik platformların güvenlik açısından her zaman risk taşıdığına dikkat edilmesi gerekmekte ve bilgilerin kullanımı açısından yedekleme ve kurtarma sistemlerinin oluşturulması ve uygulamaya koyulması,
- Güncel tehlike ya da tehdit unsurlarının takip edilerek olası tehdit ve tehlikelere karşı öngörülebilir mekanizmaların oluşturulması ve işletilmesi,
- Güvenlik gerektiren unsurların ya da birimler tanımlanarak; sayısının minimum düzeye indirilmesinin ilke edinilmesi,
- Siber güvenlik sistemleri ilişkili olan uzmanlarının eğitimlerinin artırılmasına imkân verilmesi gibi uygulamalar söz konusu olabilmektedir.

Siber risklerin yönetilmesinden hareketle siber güvenliğin sağlanması konusunda denetim faaliyetlerinin nasıl yerine getirileceği ile ilgili önemli hususların ortaya koyulması yararlı görülmektedir. Denetim faaliyetlerinde kontrol uygulamalarının nasıl hayata geçirileceği, iç ve dış tehdit unsurlarının tespit edilmesi ile birlikte denetim faaliyetlerinin gerçekleştirileceği ortamların nasıl olması gerektiği konularına aşağıda Tablo 1'de açıklık getirilmektedir.

Yeterli olmayan kontrollerin ve güvenlik uygulamalarının bulunduğu alanlarda para kazanmayı hedefleyen kesimlerden ziyade politik menfaat elde etmek isteyen kişiler ya da kesimler tehdit unsuru oluşturabilmektedir. Ayrıca, sistemin çevresinde yer alan taraflar ya da içerisinde yer alan çalışanlar kaynaklı tehditler de ortaya çıkabilmektedir. Dolayısıyla saldırılar, işletmelerin çevresel güvenlik sistemlerine karşı sınırlı kalmamaktadır. Aynı zamanda işletmelerin bilgisayar sistemlerinin birçok

katmanında yer alan zafiyetleri kullanan siber suçlulardan da kaynaklanabilmektedir (City of Vancouver 2016, 1).

Tablo 1. Siber Güvenlik Denetimlerinde Anahtar Unsurlar

KONTROLLER	Siber saldırıların önlenmesinde kullanılan araçlar ve kontroller; i) Güvenlik ve anti virüs programları, ii) çalışanlara şifre kullanım eğitimi verilmesi, iii) Düzenli olarak yedekleme yapılması, iv) Güvenlik uygulamalarının düzenli bir biçimde güncellenmesi ve v) Düzenli olarak siber güvenlik denetimlerinin yerine getirilmesi şeklinde sıralanabilmektedir. Bu bağlamda işletmelerin ilgili süreçleri en iyi biçimde tasarlamış olması ve güncel olarak yerine getirmesi konusunda emin olmaları gerekmektedir. İşletmelerin ihtiyaçları doğrultusunda siber güvenlik denetimlerinin yapılması önemlidir. Bu noktada beklentilerin net bir şekilde belirlenmesi, denetimlerin başlangıç ve bitiş tarihlerinin sistematik olarak ortaya koyulması gerekmektedir.
TEHDİTLER	Kontrollerin olmadığı bir ortamda; gizlilik, bütünlük ve kullanılabilirlik unsurlarının iç ve dış tehditler tarafından etkilenmesi muhtemeldir. Bu bağlamda uygulamaya koyulan yeni yasal mevzuat ve düzenlemeler işletmeler için ayrı bir tehdit oluşturabilmektedir. İnsan kaynaklı ortaya çıkan tehditler birçok maniplasyonu bünyesinde bulundurmaktadır. Kötü niyetli olarak hazırlanan yazılımlar, kodlar, yetkisiz erişim sağlanması ile donanım hataları ile birlikte pek çok etmen tehdit unsuru taşımaktadır.
VERİ ORTAMI	İşletmelerin bulut, Nesnelerin İnterneti (IoT), mobil, büyük veri analitikleri üzerinde çalışıp çalışmadıkları bağlamında karşı karşıya kaldıkları tehditlerin miktarı ya da önemi de değişim göstermektedir. Bilgilerin yer değiştirmesi durumunda (örneğin, mobil ortamdan buluta geçerken), bilginin yeni konumuna hitap edebilmek adına yeni kontrol ortamlarına ihtiyaç duyulacaktır. Yeni kontrol ortamları da gerek güncellenmelere gerekse de denetimlere ihtiyaç duyacağı açıktır.

Kaynak: Öztürk 2018, 220

Siber güvenlik değerlendirme süreçleri ve denetimleri siber güvenliğin sağlanmasına katkı sağlayabilmektedir. Bu noktada işletmelerin yönetimi, risk yönetim uzmanları ve iç denetçiler denetimin yürütücüleri olarak karşılanmaktadır (ISACA 2004). Dolayısıyla siber güvenlik denetimlerin hangi aktörler tarafından nasıl yürütüldüğünün açıklanmasına fayda bulunmaktadır (Tablo 2).

Tablo 2. Siber Güvenlik Denetimlerinin Aktörleri

YÖNETİM	Yönetim, işletme hakkında alınan riskli kararların nihai sahibidir. Dolayısıyla, siber güvenlik kontrollerinin var olması ve etkin bir biçimde çalıştırılması konusunda teşvik edici bir rol üstlenmektedir. Risk yönetiminden elde edilen bilgiler ışığında sağlıklı kararlar alınabilmektedir.
RİSK YÖNETİMİ	İşletmelerde risk yönetimi genellikle sorumlu bir birim tarafından sağlanmakta ve yönetim ise ilgili süreci yürüterek karar alabilmektedir. Risk değerlendirme eyleminin iki temel amacı bulunmaktadır. Risk seviyesinin belirlenmesi ve anlaşılması bakımından ilgili risk hakkında toplantı yapılarak fikir birliğinin sağlanması gerekmektedir. İzleyen aşamada ise risklerin nasıl giderilebileceğine dair yöntemlerin belirlenmesi önemlidir. Söz konusu durum riskin tespit edilmesinden problemin çözülmesi konusuna ilişkin olumsuz etkenleri ortadan kaldırabilecektir. Diğer taraftan siber güvenlik konusunda riskli alanlar sürekli olarak değişebilmektedir. Bu noktada yeterli kaynaklara ve yönetim çerçevesine sahip olmak gereklidir. Çünkü işletmenin etkin bir biçimde yönetilmesi, liderliğin sağlanması ve ortaya çıkan tehditler ile baş edilebilmesi bu hususa bağlı olarak şekillenmektedir.
İÇ DENETİM	Günümüz dijital ekonomi ortamında işletmelerin koruma altına alınması hayati önem taşımaktadır. İç denetim departmanı işletmelerin birçoğunda; siber güvenlik denetimleri konusunda çok önemli bir pozisyona sahiptir. Bununla birlikte işletmenin yönetim kurulu ve denetim kuruluna bağımsız bir görüş bildirilmesi bakımından çapraz raporlama ilişkisine ve yetkisine sahiptir. Çapraz raporlamada yönetim kuruluna bilgilendirme yapılmaktadır. Denetim kuruluna da rapor verilmektedir. İç denetim, kontrollerin objektif olarak değerlendirilmesinde, iyileştirilmesinde, yönetim kurulu ile üst yönetimin siber riskleri anlamasında ve ilgili durumlara tepki vermesinde ve son olarak siber tehditleri yönetme konusunda önemli katkılar sağlamaktadır.

Kaynak: ISACA 2004, 2; Öztürk 2018, 221-222

Siber güvenlik denetimlerinin yukarıda belirtilen aktörler tarafından uygulamaya geçirilmesi bakımından çeşitli araçlara, teknik donanım ve teknolojik ekipmanlara gereksinim duyulmaktadır.

Dolayısıyla siber suçların önlenmesi ve giderilmesine yönelik kullanılan teknik denetim araçları ve ilgili vakalarda kullanılan dokümantasyon araçları aşağıdaki biçimde sıralanabilmektedir (Poonia 2014, 17-20).

Kullanılan Teknik Araçlar: i) Bilgisayarların ana belleklerinin zarara uğraması durumunda kullanılan yazılım olarak ifade edilen veri kurtarma programları; ***ii)*** Bilgi sistemlerine yönelik gerçekleştirilmesi olası olan siber saldırıların belirlenmesi bakımından oluşturulan tuzak sunucu olan bal küpleri; ***iii)*** Siber suçların kayıt altına alınması ve takip edilmesi konusunda IP adreslerinin izlenmesi ve ***iv)*** internette gerçekleştirilen görüşmelerde suçlu tespitinin yapılabilmesi bakımından sohbet odalarının izlenmesi şeklinde sıralanabilmektedir.

Kullanılan Dokümantasyon Araçları: i) Bilgi sistemlerinde yer alan veri işlemlerine ait olan süreçlere ilişkin veri akış diyagramları; ***ii)*** Örgütsel sistem faktörlerinin birbirleri ile ilgili ilişkilerine ilişkin varlık ilişki diyagramları; ***iii)*** Kararların ve olası sonuçlarının ağaç şeklinde bir biçimle ifade eden karar ağaçları; ***iv)*** Bir algoritmaya ilişkin adımların sırasını oklar ile ifade eden şemalar olan akış şemaları ve ***v)*** Hangi sistemlerde hangi verilerin kullanıldığı ile söz konusu verilerin daha önce farklı bir sistemde kullanılıp kullanılmadığını ifade eden veri kalemleri toplamı olan veri sözlükleri şeklinde sıralanabilmektedir.

4. İÇ DENETİMİN SİBER GÜVENLİK AÇISINDAN ROLÜ

Günümüzde yaşanan siber saldırılardan hareketle siber risklerin sadece bir teknoloji riski olarak dikkate alınmasından öte iş riski olarak karşılanması; karmaşık ve hızla değişime uğrayan bir konu olarak siber güvenlik konusu hakkında iç denetçiler ile iç denetim yöneticilerinin (İDY) ya da iç denetim birim başkanlarının ilgili konu ile yakından ilgilenmesi ve konu hakkında bilgi sahibi olmalarının önemi artarak devam etmektedir. Siber risklerin geniş bir alanda kendisine yer edinmesi iç denetçilerin konu ile ilgili rolünü daha fazla önemli hale getirmiş; bu noktada elde edilecek olan başarının, yönetim ve denetim komitesinin konuya ne kadar hassasiyet gösterdiğine ve İDY'nin bu konudaki tutumuna bağlı olduğunu göz önünde bulundurmakta fayda vardır. Siber güvenlik denetim faaliyetlerinin gerçekleştirilmesine ek olarak İDY; bağlı olduğu söz konusu kurum ya da kuruluşa geleceğe dönük stratejik kararların alınmasında fikir üretme pozisyonu ile güvenilir bir danışmanlık hizmeti sunmakla sorumludur (IIA 2016, 4).

Siber güvenlik konusunun bütünleşik bir yaklaşımla sistemli bir biçimde ele alınması ve değerlendirilmesi gerekliliği; 2016 yılında Uluslararası İç Denetçiler Enstitüsü tarafından "Global Perspektif ve Anlayışlar: Güvenilir Siber Danışmanlık için İç Denetim" kitapçığında açıkça vurgulanmıştır. Belirtilen yaklaşımın olmaması durumunda, işletmelerin günlük faaliyetlerini dahi

yerine getiremeyebileceği, fikri mülkiyet hakları ve imajları konusunda zarar meydana gelebileceği ve dolayısıyla siber güvenliğin sağlanamayabileceği açıkça görülebilmektedir (IIA 2016). Söz konusu açıklamalardan hareketle siber güvenlik konusunu meydana karmaşık alanlar üzerinde iç denetim faaliyetlerinin doğrudan etki yaratabileceği dört kritik alan belirtilebilmektedir (IIA 2017, 10):

- Siber tehdit olaylarına karşılık ön hazırlık ve olaylara müdahale etme hakkında güvence sağlamak,
- Kurumun karşı karşıya kalmış olduğu riskler hakkında; karşılaşılan risklerin düzeyi ve risklere verilen cevapların düzeyi hakkında yönetim kuruluna bilgi vermek,
- BT ve diğer birimler ile birlikte hareket ederek etkili bir savunma ve müdahale mekanizması oluşturmak üzere çalışmak,
- Organizasyon içerisinde yer alan taraflar hakkında risklere ilişkin olarak iletişimi ve koordinasyonu etkili hale getirmek şeklindedir.

Uluslararası İç Denetim Enstitüsü'nün yapmış olduğu araştırma ve açıklamalar doğrultusunda işletmelerin kurumsal olarak siber riskler karşısında bilinçli ve hazırlıklı olmasının gerekliliği açıkça görülebilmektedir. Günümüzde birçok kurum ya da kuruluş siber risk kavramının varlığının bilincinde ancak konu hakkında gerektiği biçimde bir hazırlık çalışmalarının olmadığı da görülmektedir. Bu bağlamda işletmelerin en azından herhangi bir siber saldırı karşısında; siber tehdit ya da saldırıları, engelleme, önleme ya da direnme ya da en az hasarla saldırıdan kurtulabilecek donanıma sahip olması gerekmektedir. Bu bağlamda ise işletmelerin söz konusu alanda kendilerine yetenek kazandırmalarının iç denetim fonksiyonu ile mümkün olacağının hatırlatılmasında önemli fayda görülmektedir.

Siber risklere (kullanıcı-kimlik doğrulama/çalma, yetkisiz erişim, casusluk, vs.) yönelik yaşanan saldırılar neticesinde endişelerin artması ile beraber ilgili kurum ya da kuruluşun paydaşları siber risk programlarını izlemekte ve sonuç olarak; yönetim kurulları iç denerim biriminden siber riskler karşısında güvence talep etmektedir. Bu bağlamda iç denetim biriminin rolünün şekli ve yönü dijital alanlara yönelmekte ve dolayısı ile yeteneklerini bu yönde geliştirmeleri büyük önem taşımaktadır. Ayrıca, yönetim kurullarının siber risklere ilişkin güvence talep etmelerinin altında işletme faaliyetlerine ilişkin alt süreçlerin kontrol altına alınması konusunun da önemle üzerinde durulması gerektiği sinyalini vermektedir.

Siber güvenlik konusunda meydana gelen açıklar karşısında iç denetim fonksiyonun rolünün genişlemesinin gerekliliği ortaya çıkmış olup bu bağlamda; risk değerlendirme stratejilerinin siber güvenlik açıkları dikkate alınarak yeniden yapılandırılması ve tüm riskleri kapsayacak bir biçimde ilgili politika, prosedür ve iç kontroller ile uyum sağlayacak şekilde güvence yaratması gerekmektedir. Siber saldırılara yönelik iç denetim biriminin, işletmenin faaliyetlerine ilişkin alt süreçlerine hâkim olabilecek

bir *süreç denetim modeli* oluşturmalı; söz konusu modelin ise iç kontrol sistemi tabanında uygulamaya koyulması gereklilik arz etmektedir.

Hali hazırda iç denetim fonksiyonu savunmaya yönelik kontrollerin etkinliğini değerlendirmekte (Kurnaz ve Dindaroğlu 2015); BT genel kontrollerinin ise siber güvenlik riskleri karşısında etkili bir çözüm önerisi getirmediği bilinmektedir. Bu bağlamda riskleri izleme, suiistimalleri tespit etme ve onarıcı eylemlerin uygulamaya koyulması noktasında siber risklerin karmaşıklığı göz önünde bulundurulmak suretiyle ek kontrol katmanlarının ya da mekanizmalarının olması gerektiğine ihtiyaç duyulmaktadır (IIA 2016). Bu noktada iç denetim birimi ile yönetim kurulunun etkili bir iletişim ve koordinasyon içerisinde olması gerçekleştirilecek olan faaliyetlerin etkin olmasını sağlayabilecektir. Siber güvenlik ile ilgili gelişmelerin sürekli takip altına alınması ile birlikte ilgili kurum ya da kuruluşun kırılganlık düzeyinin doğru bir şekilde analiz edilebilmesi mümkün hale gelebilecektir. Sonucunda ise öngörülebilir bir siber güvenlik planının oluşturulmasına katkı sağlanabileceği vurgulanabilmektedir (IIA 2018, 6-9).

Yukarıda bahsedilen siber güvelik ve iç denetim ilişkisine yönelik olarak işletmelerin dijital dönüşüm uygulamalarına ağırlık vermeler ile birlikte gerçekleştirmiş oldukları faaliyetlerinin dijital uygulamalara evrildiği ve söz konusu faaliyetlere ilişkin süreçlerin ise gün ışığına çıktığı ve güvenlik tehditlerine açık hale geldiği günümüz iş dünyasında açıkça görülebilmektedir. Bu bağlamda işletmelerin etkili bir siber risk haritası oluşturması, öngörülebilir güvenlik önlemlerinin alınması ve doğru bir şekilde uygulamaya koyabilmeleri bakımından; faaliyetlerine ilişkin alt süreçlere ait iş ve işlemleri kontrol altına alarak sürekli bir süreç denetimi mekanizmasına ihtiyaç duyulmaktadır. Bu noktada, iç denetçilerin dijital uygulamalar ile karşı karşıya kalması ve kontrol araçlarının bu yönde değişmesi ve gelişmesi ile birlikte süreçlere hâkim olmaları önemli bir gereklilik olarak görülebilmektedir. Çalışmanın izleyen aşamalarında denetim alanına yeni bir bakış açısı getiren *Sürekli Süreç Denetimi Modeli*'nin işleyişi hakkında doyurucu bir bilgi sunularak söz konusu modelin siber güvenliğin etkinleştirilmesindeki rolüne yönelik bir model önerisi sunulmaktadır.

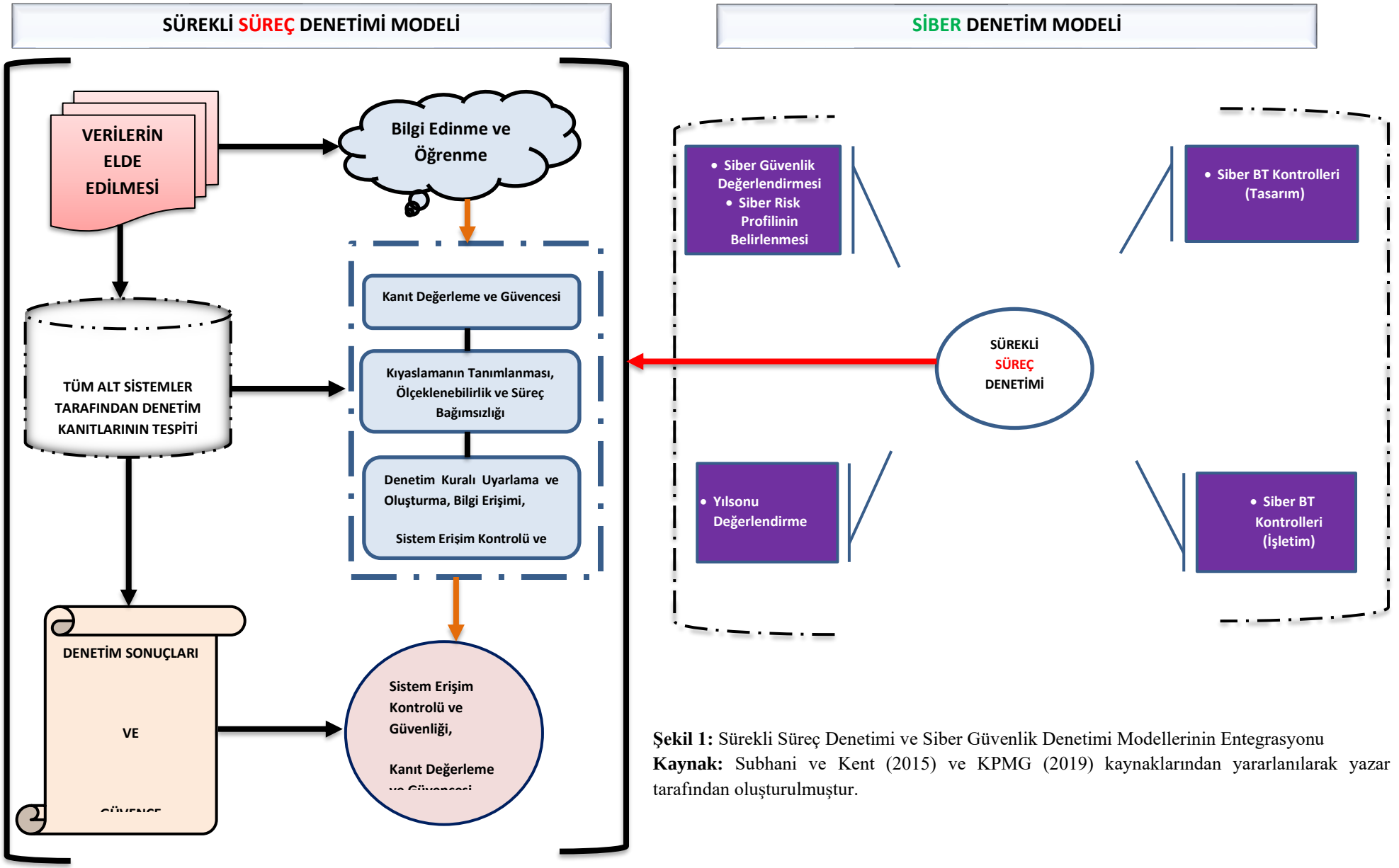
5. SİBER GÜVENLİĞİN ETKİNLEŞTİRİLMESİNDE SÜREKLİ SÜREÇ DENETİMİ MODEL ÖNERİSİ

Bilgi güvenliği yönetiminin kilit oyuncusu kabul edilen, ekonomi içerisinde yer alan kurum ve kuruluşlar ile birlikte devlet kurumlarının; uygulamalarının ve sistemlerin varlığı, *iş süreçlerinin* gizliliği ve bütünlüğüne karşılık olarak artan tehdit olaylarının engellemek üzere iç denetim tarafından pratikte hayata geçirilen yeni bir uygulama *Siber Güvenlik Denetimi* karşılanmaktadır. Dolayısıyla ortaya koyulan güvencelerin ve bilgi güvenliği konusunda süreçlerin düzenli aralıklar ile gözden geçirilmesi ile gerçekleştirilen işlemlerin tamlığı, güncelliği, etkinliği hakkında fikir üretmek mümkün

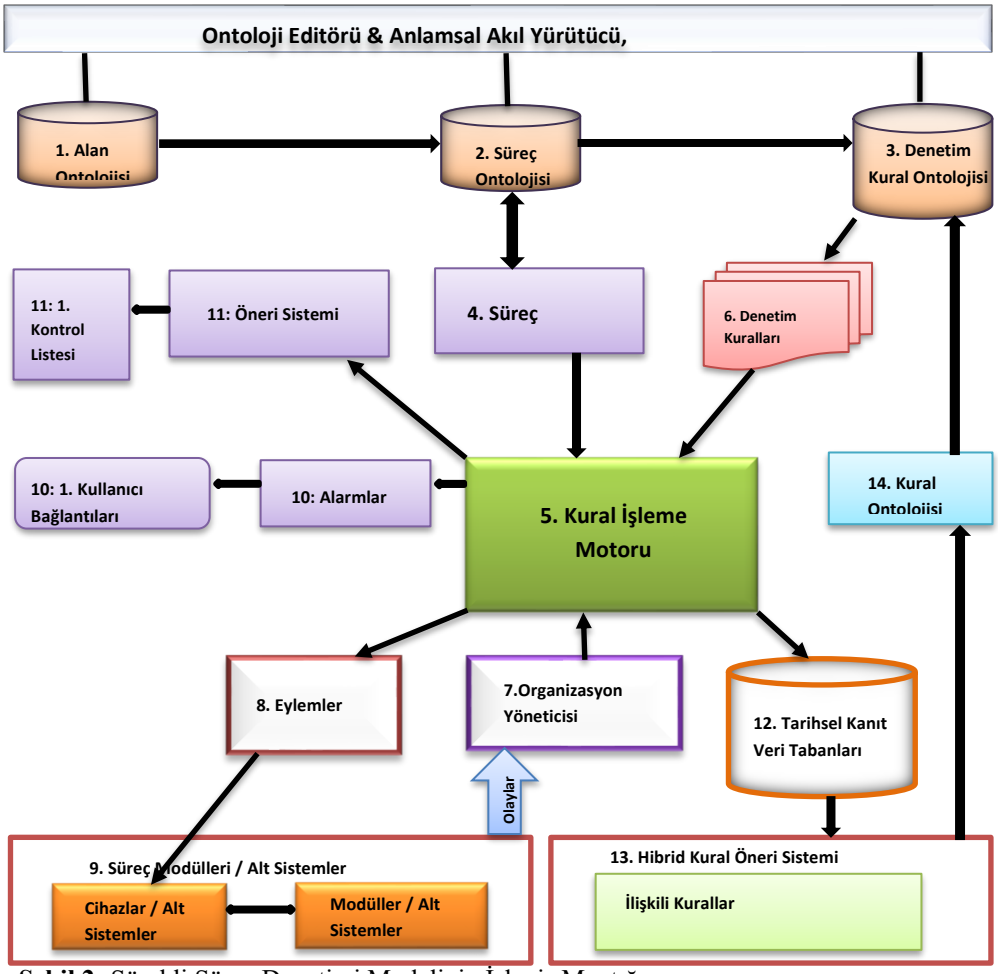
hale gelmektedir (BSI 2008, 5). Diğer taraftan, siber güvenliğin etkin hale getirilmesinde iş süreçlerine ilişkin sistemlerin bütünlüğünü ve gizliliğini korumak ile beraber dijital hizmet kullanımını aktif olarak yerine getirmek; karşılaşılan en temel zorluklardan birisidir. Bu bağlamda, karşı karşıya kalınan siber risklerin temel özellikleri ile birlikte riski azaltıcı yönde kullanılan kontrollerin sürekli olarak izlenmesi gerekmektedir. Dolayısıyla sistemlerin 7/24 online olarak çalışmasından dolayı organize olarak gerçekleştirilen siber saldırılara karşı koymak daha güç hale gelmekte; dolayısıyla, koruma uygulamalarının kurum ya da kuruluşlarının tabana yayılması büyük önem taşımaktadır (Sunde 2017, 272).

Yukarıdaki açıklamalardan hareketle önemli miktarda modern iş faaliyetleri çoğunlukla süreç odaklı olduğundan iş süreçlerinin otomasyonu arttıkça, bu sadece prosedürlerin denetiminde değil, süreçlerin denetlenmesinde de değişime yol açmaktadır. E-ticaret işletmeleri için web teknolojilerine bağımlılık, sistem denetiminin gerçekleştirilmesini güçleştirmekte olup e-ticaret sistemlerinin belirli protokollere ve gereksinimlere sahip olmasından ve geleneksel kâğıt tabanlı sistemlerden ayrılması bu konuda büyük önem taşımaktadır.

Sürekli Süreç Denetimi: Süreçlerin kontrollerinin izlendiğine ve verilerin sürekli olarak güvence altına alındığına dair sürekli bir güvence sağlamak için, hizmet tabanlı bir denetim yaklaşımı olarak ifade edilebilmektedir. Süreç tabanlı küçük ve orta ölçekli işletmeler, sürekli denetim ve gözetim hizmetlerine; süreçlerin kendisine tanımlanan görevleri ve olayları yürüttükleri zaman ihtiyaç duymaktadır. Bir hizmet olarak Sürekli Süreç Denetimi, yalnızca belirli süreçler için değil, tüm denetim ihtiyaçlarına yönelik her türlü süreç için uygulanabilir ve maliyet etkin bir yöntemdir (Subhani ve Kent 2015, 1-6; Alles ve diğerleri 2008). Denetime konu olan işlem ve olaylara ilişkin süreçlerin gerçek zamanlı olarak güvenlik ve gözetiminin değerlendirilmesine olanak sağlamaktadır. Denetimde insan faktöründen kaynaklanan hatalar ve zaman kayıplarından ziyade süreç kaynaklı ortaya çıkan sorunların tespit edilmesi ve giderilmesinde önemli bir role sahiptir. Ayrıca, denetime olan güvenin, denetimin etkinliğinin ve veriminin arttırılabilmesinin sağlanmasında rol üstlenen Sürekli Süreç Denetimi; işletmeler için kontrol ve risk değerlendirmelerinin otomatik olarak gerçekleştirebilmektedir. Teknoloji odaklı bütün süreçlerde etkili olabilmektedir. Günümüzde yeni bir yaklaşım olarak ortaya çıkan sürekli süreç denetiminin işleyiş aşamaları KPMG (2019) ile Subhani ve Kent (2015)'in çalışmasından uyarlanarak aşağıda Şekil 1'de açıklanmış ve sistematize edilerek siber denetim modeline entegre edilmiştir.



Şekil 1: Sürekli Süreç Denetimi ve Siber Güvenlik Denetimi Modellerinin Entegrasyonu
Kaynak: Subhani ve Kent (2015) ve KPMG (2019) kaynaklarından yararlanılarak yazar tarafından oluşturulmuştur.



Şekil 2: Sürekli Süreç Denetimi Modelinin İşleyiş Mantığı

Kaynak: Subhani ve Kent 2015, 3

Sürekli süreç denetimine ilişkin belirtilen Şekil 1'deki modelin ana bileşenleri; Alan Bilgisi ve Süreç Olarak Denetim Kural Ontolojisi, Süreç Modelleme ve Karakterizasyonu, Denetim Kurallarının Oluşturulması ve Uyarlanması ve Denetim Kuralları Süreci ve Kurallar Motoru şeklinde aşağıda açıklanmaktadır.

Alan Bilgisi ve Süreç Olarak Denetim Kural Ontolojisi: Ontolojiler, bir bilgi alanını modellemek için bir dizi temsili ilkelerin (sınıflar veya kümeler, sosyo-demografik özellikler ya da özellikler ve sınıflar arasındaki ilişkiler) tanımlarının paylaşılmış hali olarak ifade edilebilmektedir. Paylaşılabilir bir bilgi modeli oluşturmak için bu tür ontolojiler (alan, süreç ve denetim kuralı) önerilmektedir. ***Alan ontolojileri,*** mal ve hizmetlerin üretimi veya sunulması konusunda finans veya endüstri gibi belirli gerçek dünya alanlarının ve süreçlerinin kavramsallaştırılmasını belirtmeyi amaçlamaktadır (Ünalır ve diğerleri 2010, 240-243; Gruber 1995). Alan ontolojisinin yanı sıra, Hybrid Katmanlı Ontoloji'yi oluşturan diğer üç bileşen vardır (Subhani ve Kent, 2015).

Süreç Ontolojileri (SO), tanımlanmış kavramların ve homojen veya heterojen olabilecek veri tabanları ile her bir süreç için (Jiang ve Tan 2010; Can ve Ünalır 2010, 205) ve süreç denetim kuralları için hibrid tabakalı ontolojinin oluşturulması amacıyla süreç ontolojileri için bir uzman sistem eşleştirilmektedir (Gürbüz ve Demirörs 2016, 698). ***Denetim kuralları***, insan tarafından gerçekleştirilen denetim kapsamında bir faaliyet veya bileşen için tanımlanmaktadır. Denetim kuralları, bir kuruluşun hiyerarşik yapısına ve zorunlu işletme kontrollerine dayanmaktadır. ***Bir Süreç Olarak Denetim Kural Ontolojisi (SODKO),*** diğer sistem ve sistemlerin hizmeti ile bilginin, değiş tokuş edilmesini ve muhakemesini de sağlayabilmektedir. Bilgi tabanlı yapı kullanan ontoloji veri tabanlarında depolanan bilgi, süreç modellemesinde tarihsel veri tabanları / kanıt bankaları ile birlikte kullanılabilmektedir.

Süreç Modelleme ve Karakterizasyonu: Süreçlerin önceden tanımlandığı varsayılmakta ve sistemin belirli sürecin sıralı prosedürüne ve özellik tercihlerine uyarlanması, bu modülün ana odak noktası kabul edilmektedir. Sistemi sürekli değişen davranışlarına göre ayarlayabilmek için süreçleri karakterize etme seçenekleri mevcuttur. Süreç modelleyicisi bileşeni, bir hizmet olarak denetim sistemi ile farklı süreçler ve bunların modülleri arasındaki ara bağlantıların tanımlanmasına odaklanmaktadır (DeCesare 2014). Süreç modelleyicisi alan ontolojisinden, süreç ontolojisinden ve tarihsel veri tabanlarından bilgi almaktadır. Tarihsel kanıt bankası, geçmişte keşfedilen kanıtları kural motoru ve uzman sistemler tarafından depolamakta ve söz konusu kanıtların analizi çeşitli araçlar tarafından yapılmaktadır (Coşkunçay ve diğerleri 2014, 233).

Denetim Kurallarının Oluşturulması ve Uyarlanması: Yeni denetim kurallarının oluşturulması veya yeni denetim kurallarının gerekli olduğuna ya da mevcut olanların değiştirilmesi veya yeni süreç modüllerinin gelişimine uyum sağlamak için mevcut kurallardan bazılarının değiştirilmesi, uyarlanması ve gözden geçirilmesine karar veren üst düzey yöneticiler ya da alan uzmanları tarafından süreç ontolojisinde süreç modülleri eklenebilmekte veya süreç dizileri değiştirilebilmektedir. Bu yeni denetim kuralları ve değişiklikler doğrudan alan uzmanları veya eğitimli yöneticiler tarafından eklenebilmektedir. Veri madenciliği teknikleri ya da alana özel öneri sistemleri aracılığıyla tarihsel veri tabanlarından denetim kurallarının otomatik oluşturulması mümkündür. Oluşturulan denetim kuralları, denetim kuralı süreci için kural motoruna uyarlanacak; denetim kurallarının depolanması ve denetim kural ontolojisinin gelişimi ise süreç denetim kuralları ontolojisine bağlı olacaktır (Subhani ve Kent 2015, 4).

Denetim Kuralları Süreci ve Kurallar Motoru: SSD modelinin ana bileşeni, mevcut süreç durumlarından sonuçlar üretmekten sorumlu olan Denetim Kuralları İşleme Motoru' dur (Forgy 1982). ***Kurallar motoru,*** işlem modellerinden ve organizasyon yöneticisinden bilgi almakta ve sonuçlarını alarmlar, eylemler ve öneriler biçiminde üretmektedir. Öneriler, alana özgü öneri sistemi kullanılarak

uygulama sunucusu aracılığıyla kontrol listeleri şeklinde oluşturulmakta, ayrıca durumların üstesinden gelinmesine olanak sağlanmaktadır (Subhani ve Kent 2015, 5).

Günümüzde veri olaylarının ya da yığınlarının büyüklüğü artmaya devam etmekte olup en önemli gelişmelerden birisi söz konusu artış eğiliminin arkasındaki karmaşıklık düzeyidir. Bu bağlamda siber saldırı düzenleyenler daha fazla karmaşık yöntemler kullanarak hem hedefleri hem de iş modelleri değişime uğramıştır (McCarthy 2017, 4). Siber saldırganlar hedef aldıkları kurum ya da kuruluşlara yönelik plan yaparken bütünleşik bir yaklaşım sergilemekte; ulaşmak istedikleri bilgileri elde etmek adına kurumların savunma mekanizmalarının nasıl kırılabileceğini bütün ayrıntıları ile düşünmektedirler (Hale 2017, xxviii).

Bahsedilen kurum ve kuruluşların büyük veri yığınlarının depolanmasından önce söz konusu veri yığınlarına ait iş süreçlerinin yukarıda bahsedilen sürekli süreç denetimi ile kontrol altına alınması önemli bir güvenlik duvarı oluşturmaktadır; çünkü, günümüz işletmelerinde aktif hale getirilmesi üzerinde çalışılan siber güvenlik denetiminin en önemli fonksiyonlarından birisi; gerçekleştirilen faaliyetlere ilişkin BT kontrollerinin tasarlanması ve uygulamaya koyulması iken BT kontrollerinin etkin çalışması konusunda süreçlerin denetlenmesinin eksikliğidir. Bu bağlamda, iç denetimde yeni bir çağ açan *Sürekli Süreç Denetimi Modeli'nin;* kurum ya da kuruluşların gerçekleştirmiş oldukları faaliyetlerine ilişkin işlem süreçlerinin kontrol altına alınarak etkin bir şekilde denetlenmesine olanak sağlamakta ve sonucunda ise kurum çapında oluşturulan iç kontrol ağının uçtan uca değerlendirilmesine imkân vermektedir. Ayrıca süreçlerin anlık denetimini gerçekleştirmesinden dolayı herhangi bir siber saldırı ile karşılaşılması durumunda problemin hangi departmanın hangi alt faaliyetindeki hangi alt işlem sürecinde gerçekleştirildiğine dair önlem alınmasına ciddi kolaylıklar sağlayabileceği açıktır.

Yukarıda Şekil 1'de çalışmanın önceki aşamalarında bahsedilen siber güvenlik denetimi modeli üzerinde sürekli süreç denetiminin uygulama adımları entegre edilmiş ve söz konusu siber güvenliğin merkezine (işletme faaliyetlerinin iç kontrol sistemine bağlı olarak tamamına) yerleştirilerek; işletmelerin gerçekleştirmiş oldukları faaliyetlerine bağlı olarak her bir alt işlem sürecinin kontrol altına alınması, eş zamanlı denetlenmesi ve üretilen bilgilerin koruma altına alınmasına olanak sağlayabileceği bir model uyarlanmıştır. Söz konusu her iki yaklaşımın işleyiş esasları önceki başlıklarda detaylı olarak anlatılmış ve Şekil 1'de sistematize edilerek sunulmuştur. Devam eden süreçte ise siber güvenlik merkezinde sürekli süreç denetimi modelinin işleyiş mantığı ortaya koyularak konun anlaşılmasına ışık tutulmuş ve Şekil 2'de görsel olarak sunulmuştur. Ortaya koyulan yeni model ile siber güvenlik uygulamalarının denetlenmesi aşamasında ortaya çıkan 4 adım dikkate alındığında aşağıda Tablo 3'te ki şekilde sistematik bir çalışma mantığı oluşturulabilmektedir:

Tablo 3. Siber Güvenlik Denetimi Uygulama Adımları

UYGULAMA ADIMLARI	SİBER DENETİM	SÜREKLİ SÜREÇ DENETİMİ
Adım I	Siber Güvenlik Değerlendirmesi Siber Risk Profilinin Belirlenmesi	***Verilerin Elde Edilmesi*** Bilgi Edinme ve Öğrenme
Adım II	Siber BT Kontrolleri (Tasarım)	***Tüm Alt Sistemler Tarafından Denetim Kanıtlarının Tespiti*** Kanıt Değerleme ve Güvencesi, Kıyaslamanın Tanımlanması, Ölçeklenebilirlik ve Süreç Bağımsızlığı, Denetim Kuralı Uyarlama ve Oluşturma, Bilgi Erişimi, Sistem Erişim Kontrolü ve Güvenliği
Adım III	Siber BT Kontrolleri (İşletim)	
Adım IV	Yılsonu Değerlendirme	***Denetim Sonuçları ve Güvence Sağlama*** Sistem Erişim Kontrolü ve Güvenliği, Kanıt Değerleme ve Güvencesi, Sürekli Destek

İşletmelerde, kurum ya da kuruluşlarda siber güvenliğin sağlanması ve üretilen bilgilerin eş zamanlı olarak koruma altına alınarak denetlenebilir bir hale getirilmesi ve sonrasında işlem süreçlerinin anlık denetlenmesini sağlayan sürekli süreç denetimi modelinin siber güvenlik uygulamalarının merkezinde işletmenin geneline yönelik bütünleşik olarak uygulamaya geçirilmesi durumunda; (i) veri kaybının önlenmesi ve üretilen verilerin eş zamanlı olarak kayıt altına alınması, (ii) işletme faaliyetlerine ilişkin alt süreçlerin şeffaf hale gelmesinden dolayı raporlama ve karar alma noktasında isabetli ve gerçekçi sonuçlar üzerinden hareket edilmesi, (iii) iç kontrol sisteminin işletmenin daha geniş alanlarına yayarak daha fazla verinin kontrol altına alınması, (iv) öngörülebilir mutlak ve bağıl risk faktörlerinin ortaya koyulması ve sonucunda etkili bir risk yönetim planlaması, (v) siber saldırılara karşı bütünleşik olarak eş zamanlı ve her bir işlem bazında hareket takibinin şeffaf hale gelmesinden dolayı hızlı önlem alınması gibi konularda önemli bir katma değer yaratılması mümkün olabilecektir.

6. SONUÇ

Değişen ve gelişen teknoloji ile birlikte oluşan veri yığınları karşısında işletmelerin gerçekleştirmiş oldukları faaliyetlerine ilişkin alt işlem süreçlerinin sürekli olarak kontrol altına alınması ihtiyacı ortaya çıkmıştır. İlgili süreç ise iç denetim alanında yeni bir çözüm silahı olarak *Sürekli Süreç Denetimi* kavramının doğmasına zemin hazırlamıştır. Bu bağlamda gelecekte işletmelerin sürdürülebilirliklerini sağlamaları açısından; faaliyetlerine ilişkin en alt işlem süreçlerinden yola çıkılarak üretmiş oldukları veri ve bilgilerin korunması konusu siber güvenlik ve sürekli süreç denetimi konusunun kesişmesine neden olmuş ve söz konusu her iki uygulamanın yarattığı katma değer önemli merak uyandırmıştır. Bu çalışmada siber güvenlik uygulamalarının etkinleştirilmesi üzerinde sürekli süreç denetiminin etkisinin,

belirlenmesi amaçlanmıştır. Türkiye'de siber güvenlik denetimleri üzerinde daha önce çeşitli araştırmalar yapılmıştır. Fakat Sürekli Süreç Denetimi konusunun daha önce ele alınmadığı görülmüştür. Ayrıca, bu çalışmada söz konusu denetim modeli ile siber güvenlik denetimin bütünleşik olarak dikkate alınması konunun Türkiye için önemini ve diğer çalışmalardan farkını ortaya koymaktadır. Uygulamada konunun yeni olmasından dolayı çalışma teorik bir perspektiften ele alınmıştır. Çalışmanın teması kapsamında siber güvenliğin etkinleştirilmesi noktasında sürekli süreç denetiminin etkisine yönelik önemli anahtar sonuçlara ulaşılmıştır. Siber güvenlik denetiminin en önemli fonksiyonlarından birisi; gerçekleştirilen faaliyetlere ilişkin BT kontrollerinin tasarlanması ve uygulamaya koyulması iken BT kontrollerinin etkin çalışması konusunda süreçlerin denetlenmesinde açıklık ve eksiklik olmasıdır. İç denetimde yeni bir çağ açan *Sürekli Süreç Denetimi Modeli;* kurum ya da kuruluşların gerçekleştirmiş oldukları faaliyetlerine ilişkin işlem süreçlerinin kontrol altına almakta ve etkin bir şekilde denetlenmesine olanak sağlamaktadır. Sonucunda ise kurum çapında oluşturulan iç kontrol ağının uçtan uca değerlendirilmesine imkân vermektedir. Süreçlerin anlık denetimini gerçekleştirmesinden dolayı herhangi bir siber saldırı ile karşılaşılması durumunda, problemin hangi departmanın hangi alt faaliyetindeki hangi alt işlem sürecinde gerçekleştirildiğine dair hızlı bir şekilde tespit ve müdahale yapılabilmesi mümkündür. Sürekli süreç denetiminin, siber güvenliğin merkezine *(işletme faaliyetlerinin iç kontrol sistemine bağlı olarak tamamına)* yerleştirilerek; işletmelerin gerçekleştirmiş oldukları faaliyetlerine ilişkin her bir alt işlem sürecinin kontrol altına alınması mümkün olabilecektir. Ayrıca, eş zamanlı denetleme yapılmasına ve üretilen bilgilerin koruma altına alınmasına da olanak sağlanabilmektedir. Veri kaybının önlenmesi ve üretilen verilerin eş zamanlı olarak kayıt altına alınmasına olanak tanınmaktadır. Bu sayede işletme faaliyetlerine ilişkin alt süreçlerin şeffaf hale gelmesinden dolayı raporlama ve karar alma noktasında isabetli ve gerçekçi sonuçlar üzerinden hareket edilebilmektedir. Ayrıca iç kontrol sisteminin işletmenin daha geniş alanlarına yayarak daha fazla verinin kayıt ve kontrol altına alınmasına olanak tanınmaktadır. Öngörülebilir mutlak ve bağıl risk faktörlerinin ortaya koyulması ve sonucunda etkili bir risk yönetim planlaması yapılabilmektedir. Siber saldırılara karşı bütünleşik olarak eş zamanlı ve her bir işlem bazında hareket takibi mümkün hale gelebilmektedir. Ayrıca faaliyetlere ilişkin süreçler bazında denetim yapılabilmesinden dolayı süreç güvenlik anahtarlarının oluşturulabilmektedir.

Bahsedilen sonuçlardan hareketle siber güvenlik mekanizmalarının işletmelerde oluşturulmasına yönelik iç kontrol sistemlerinin; özellikle, kontrol ortamının yeniden tanımlanması gerektiği büyük önem taşımaktadır; çünkü, işletmelerin kimlikleri üzerinde siber saldırıların yarattığı zararın çıkış noktasının bilgi güvenliği zafiyeti olmasından dolayı iç kontrol sistemlerinin bilgi güvenliği merkezli yeniden yapılandırılması, iç denetim faaliyetlerini güçlendirebilecektir. Bu bağlamda, iç kontrol sistemlerinin bilgi güvenliğinin siber sistemler aracılığı ile sağlanması iç denetçilerin sahip olması gereken mesleki yeterliliklerin de genişlemesine neden olabilecektir. Öncelikle uluslararası profesyonel

meslek örgütlerinin sertifikasyon süreçlerinin yeniden yapılandırılması gerekliliği ortaya çıkmaktadır. Diğer taraftan, sürekli süreç denetiminin uygulamada siber güvenlik merkezli hayata geçirilmesi işletmelerin kurumsal yönetim yapılarında yeni bir reform yaratacaktır. Bu doğrultuda kurumsal yönetim anlayışı yeniden ve farklı bir boyutta disipline edilebilecektir. Ayrıca söz konusu uygulamaların öncelikle ülkeler arasındaki uluslararası hukuk kuralları bağlamında; yasal bir statüye ve zemine kavuşturulması öncelikli ihtiyaç olarak ortaya çıkmaktadır. Gelecekte siber güvenlik merkezinde sürekli süreç denetimi uygulamasının hayata geçirilebilmesi bakımından; siber güvenlik ağlarının oluşturulmasında büyük ölçekli işletmelerin kurumsal yönetim anlayışlarının araştırılmasının yararlı olacağı düşünülmektedir. Ayrıca, işletmelerin içinde bulunmuş olduğu toplumun ekonomik ve sosyo-kültürel temel özelliklerinin tespit edilmesi gerekmektedir. Böylelikle siber güvenlik denetimi ve sürekli süreç denetimi uygulamalarına adaptasyon sağlanmasında önemli bir yol haritası çıkarılması mümkün olabilecektir.

YAZARIN BEYANI

Bu çalışmada, Araştırma ve Yayın Etiğine uyulmuştur, çıkar çatışması bulunmamaktadır ve de finansal destek alınmamıştır.

AUTHOR'S DECLARATION

This paper complies with Research and Publication Ethics, has no conflict of interest to declare, and has received no financial support.

KAYNAKÇA

Alles, M., Kogan, A. ve Vasarhelyi, M. 2008. "Audit Automation for Implementing Continuous Auditing: Principles and Problems", Rutgers Business School, 1–24. https://www.researchgate.net/publication/228530458_Audit_Automation_for_Implementing_Continuous_Auditing_Principles_and_Problems#fullTextFileContent (Erişim Tarihi: 01.02.2021)

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

BSI. 2008. "Information Security Audit (IS audit): A Guideline for IS Audits Based on IT-Grundschutz", German Federal Office for Information Security. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ISRevision/guideline-isrevision_pdf.pdf?__blob=publicationFile&v=1 (Erişim Tarihi: 03.01.2021)

Can, Ö. ve Ünalır, M. O. 2010. "Ontoloji Tabanlı Erişim Denetimi", Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, 16(2), 197-206.

City of Vancouver. 2016. "Internal audit summary report" http://vancouver.ca/files/cov/internal-audit-cyber-security.pdf (Erişim Tarihi: 04.01.2021)

COSO. 2015. COSO in the Cyber Age: Report Offers Guidance on Using Frameworks to Assess Cyber Risks. https://global.theiia.org/standards-guidance/Public%20Documents/COSO-in-the-Cyber-Age.pdf (Erişim Tarihi: 31.12.2020)

Coşkunçay, A. ve Demirörs, O. 2014. İş Süreç Modellerinden Ontolojiye Dönüşüm: Bir Durum Çalışması. 223-244. https://www.researchgate.net/publication/266614042 (Erişim Tarihi: 12.01.2021)

De Cesare, S., Juric, D. ve Lycett, M. (2017). Toward The Automation Of Business Process Ontology Generation. Proc. - 16th IEEE Conf. Bus. Informatics, CBI 2014. 1, 70–77. https://ieeexplore.ieee.org/document/6904139 (Erişim Tarihi: 02.02.2020)

Efe, A. 2018. Siber Güvenlik Denetimi. Ş. Sağıroğlu ve M. Alkan icinde, Siber Güvenlik ve Savunma-Farkındalık ve Caydırma (ss. 349-370), Grafiker Yayıncılık, Ankara

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

Forgy, C. 1982. "Rete: A Fast Algorithm for The Many Pattern - Many Object Pattern Match Problem", Artificial Intelligence, 19(1), 17–37.

Gruber, T. 1995. "Toward Principles for The Design Of Ontologies Used For Knowledge Sharing", Int'l Journal of Human-Computer Studies, 43(4-5), 907–928.

Gürbüz, Ö. ve Demirörs, O. 2016. Süreç Ontolojisi Oluşturma Yöntemi: Durum Çalışması, http://ceur-ws.org/Vol-1721/UYMS16_paper_124.pdf (Erişim Tarihi: 06.01.2021)

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

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

IIA. 2018. Global Bakış Açıları ve Anlayışlar: 2018 Global Risk Raporu-İç Denetim Yöneticilerinin Karşılaştığı En Büyük Riskler. The Institute Of Internal Auditing. https://global.theiia.org/translations/PublicDocuments/GPI-2018-Top-Risks-Faced-by-CAES-Turkish.pdf (Erişim Tarihi: 17.01.2021)

IIA. 2017. Küresel Bakış Açıları ve Anlayışlar Yapay Zekâ – İç Denetim Mesleğine İlişkin Dikkate Alınması Gerekenler. The Institute of Internal Auditors. https://global.theiia.org/translations/PublicDocuments/GPI-Artificial-Intelligence-Part-I-Turkish.pdf (Erişim Tarihi: 11.01.2021)

IIA. 2016. Global Perspektifler ve Anlayışlar: Güvenilir Bir Siber Danışman Olarak İç Denetim. The Institute of Internal Auditors. https://global.theiia.org/translations/PublicDocuments/GPI-Emerging-Trends-Turkish.pdf (Erişim Tarihi: 08.02.2021)

ISACA. 2017. Auditing: Cyber Security Evaluating Risk and Auditing Controls. https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2017/isaca-expands-cyber-security-resources-for-auditors (Erişim Tarihi: 02.01.2021)

ISACA. 2004. Information Systems Audit and Control Association. Cyber security audit. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.124.6737&rep=rep1&type=pdf (Erişim Tarihi: 03.01.2021)

ITU-T X.1208, 2014. Series X: Data Networks, Open System Communıcations and Security: Cyberspace Security – Cybersecurity, International Telecommunication Union. https://www.itu.int/rec/T-REC-X.1208/en (Erişim Tarihi: 07.01.2021)

Jiang, X. ve Tan, A. 2010. CRCTOL: A Semantic-Based Domain Ontology Learning System. 61, 150–168. http://cobweb.cs.uga.edu/~kochut/teaching/8350/Papers/Ontologies/CRCTOL.pdf (Erişim Tarihi: 09.01.2021)

KPMG. 2016. Denetim Komiteleri İçin Siber Güvenlik. https://assets.kpmg/content/dam/kpmg/pdf/2016/07/tr-denetim-komiteleri-icin-siber-guvenlik.pdf (Erişim Tarihi: 11.01.2021)

KPMG. 2016. GRC Gündemi: Yönetişim, Risk ve Uyumluluğu Anlamak. https://home.kpmg/tr/tr/home/gorusler/2016/03/grc-gundemi.html (Erişim Tarihi: 12.01.2021)

KPMG. 2019. Siber Güvenlik ve Denetim. https://home.kpmg/tr/tr/home/hizmetlerimiz/danismanlik/teknoloji-danismanligi/siber-guvenlik.html (Erişim Tarihi: 13.01.2021)

Kumar, V., Srivastava, J., ve Lazarevic, A. 2005. Manager Cyber Threats Issues, Approaches and Challenges, Springer, Berlin.

Kestane, A. 2020. Kurumsal Yönetim ve Kurumsal Kaynak Planlaması Uygulamaları Işığında İç Denetim, Gazi Kitabevi, Ankara.

Kurnaz, N. ve Kestane, A. 2020. Denetimde Seçme Konular 4 İç Denetim İç Kontrol Sektörle Uygulamalar, Aslan, Ü ve Bozkuş Kahyaoğlu, S. içinde Blokzincir Teknolojisi ve İç Denetim (ss. 1-34), Gazi Kitabevi, Ankara.

Kurnaz, N. ve Dindaroğlu, A. K. 2015. "İç Denetim ve Bilgi Güvenliği İlişkisi: Bölgesel Bir Araştırma", Bilgi Ekonomisi ve Yönetim Dergisi, X (1), 52-63.

Li K. C., Chen X. ve Susilo W. 2019. Foreword I-II". Kuan-Ching, L. Xiaofen, C. ve Willy, S. (Eds.) Advances in Cyber Security: Principles, Techniques, and Applications, Springer Nature Singapore Pte Ltd., Singapore.

Mccarthy T. 2017. Cybersecurity Risk Management: A Practical Guide for Businesses. https://www.mccarthy.ca/en/insights/blogs/techlex/cybersecurity-risk-management-practical-guide-businesses (Erişim Tarihi: 17.01.2021)

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. https://www.pwc.com/gx/en/news-room/docs/pwc-global-economic-crime-survey-report.pdf (Erişim Tarihi: 22.01.2021)

Poonia, A.S. 2014. "Audit Tools for Cyber Crime Investigation", International Journal of Enhanced Research in Science Technology & Engineering, 3(12), 16-20.

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

Selimoğlu, Kardeş S. ve Altunel, M. 2019. "Siber Güvenlik Risklerinden Korunmada Köprü ve Katalizör Olarak İç Denetim", Denetişim Dergisi, 9(19), 5-16.

SPK. (2018). Bilgi Sistemleri Yönetimi Tebliği. Sermaye Piyasası Kurulu, www.spk.gov.tr (Erişim Tarihi: 01.01.2021)

Subhani, N. ve Kent D. R. (2015). Continuous Process Auditing (CPA): an Audit Rule Ontology Based Approach to Audit-as-a-Service. Erişim adresi: https://www.semanticscholar.org/paper/Continuous-Process-Auditing-(CPA)%3A-an-Audit-Rule-to-Subhani/6317f72b351a85168e778522fdaf2021edbafe38 (Erişim Tarihi: 01.02.2021)

Subhani, N. ve Kent, R. 2014. Novel Design Approach to Build Audit Rule Ontology For Healthcare Decision Support Systems. EEE,133–138. http://worldcomp-proceedings.com/proc/p2014/EEE2631.pdf (Erişim Tarihi: 23.01.2021)

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

The Institute of Risk Management. 2014. Cyber Risk Executive Summary. https://www.theirm.org/media/8635/irm-cyber-risk-exec-summ-a5-low-res.pdf (Erişim Tarihi: 29.01.2021)

Ünalır, M.O., Can, Ö. ve Ünalır, E. 2010. "Ontoloji Tabanlı Bilgi Sistemlerinde Erişim Denetimi: Ulusal Aşı Bilgi Sistemi İçin Durum Çalışması", Tübav Bilim Dergisi, 3(3), 238-249.

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