İletişim Teknolojilerindeki Gelişmeler, Riskler ve İç Denetimin Rolü

Batuhan F. MOLLAOĞULLARI[*] Burak ÖZDOĞAN[**]

ÖZ

Gelişen bilgi teknolojileri işletmenin tüm fonksiyonlarıyla birlikte iç denetimi de önemli ölçüde etkilemiştir. İç denetimin görevi; işletmeye değer katmak ve işletme bünyesinde bağımsız olarak danışmanlık hizmeti sunmaktır. İç denetim, işletmenin karşılaşabileceği riskleri önceden belirleyerek üst yönetimin tedbir almasını sağlamalıdır. Bilgi teknolojilerindeki değişimin ortaya çıkardığı yeni riskler işletmenin kurumsal yapısını, güvenliğini ve veri gizliliğini tehdit etmektedir. Bütün bu gelişmeler çerçevesinde, yeni risklere karşı iç denetim fonksiyonu da yapısı değiştirirken, riskleri etkin şekilde yönetmek için gelişen bilgi teknolojilerine uyumlu çalışması gerekmektedir.

Sosyal medya, mobil cihazlar, büyük veri ve bulut bilişim teknolojilerinin işletme sistemlerine entegre olması, işletmelere sistem verimliliği açısından önemli katkı sağlamakla birlikte yeni nesil risklerin ortaya çıkmasına neden olmuştur. Nitekim ortaya çıkan bu durum, işletmeleri riskleri yönetme konusunda zorlamaktadır. Bu çerçevede iç denetim, gelişen risklerin yönetiminde bilgi teknolojilerinden yararlanarak işletmeyi koruma altına alabilecektir.

Bilgi güvenliği artık, tüm iç denetçilerin çalışmalarında önem vermeleri gereken bir risk haline gelmiş ve işletmelerin geleceği tehdit etmektedir. Bu çalışmada gelişen bilgi teknolojisinin işletmelere getirdiği risklerin neler olduğu tartışılmış ve iç denetimin bu riskleri nasıl yöneteceği ve yeni duruma nasıl adapte olması gerektiği değerlendirilmiştir. Sonuç olarak iç denetim biriminin sürekli olarak gelişen teknolojilerle uyumlu biçimde faaliyet göstermesi, yeni teknolojilerin olası etkilerine yönelik analizleri yapması ve bu analizlerin sonuçları doğrultusunda proaktif şekilde riskleri yönetebilecek önlemleri alması gerekmektedir.

Anahtar Kelimeler: *Bilgi teknolojileri, iç denetim, risk yönetimi*

Jel Kod: *M42*

Developments in Communication Technologies, Risks and Role of Internal Audit

ABSTRACT

Emerging information Technologies has affected internal auditing significantly as well as other functions of enterprises. The role of internal audit is to add value to and service as an independent advisor to the enterprise. Internal audit should define the risks that enterprise would face with in the future and should take precautions. New risks emerged with the changes in information Technologies are threatening the corporate structure, security and data privacy of business. Within the scope of those developments, while changing the structure of internal audit function to cope with emerging risks, it should work in accordance with developing information technologies for an effective risk management.

Integrating social media, mobile devices, big data and cloud computing technologies into business systems have significant contribution for efficiency, however they give rise of new risks. Hence, this situation forces businesses to manage those risks. In this context, internal audit can put

[*] Arş.Gör. Manisa Celal Bayar Üniversitesi İ.İ.B.F, Muhasebe- Finansman Anabilim Dalı, b.mollaogullari@cbu.edu.tr

[**] Dr.Öğr.Üyesi Manisa Celal Bayar Üniversitesi İ.İ.B.F, Muhasebe- Finansman Anabilim Dalı, burak.ozdogan@cbu.edu.tr

(Makale Gönderim Tarihi: 01.11.2018 / Yayına Kabul Tarihi: 19.12.2018)

Doi Number: 10.18657/yonveek.477585

the enterprise under protection in terms of managing the developing risks by benefiting from information technologies.

Information security has become a risk which should be given weight that threatens the future of businesses. In this study, the emerging risks that arouse from developing information Technologies were discussed and how the internal audit should manage these risks and how it should adopt into this new position were assessed. As conclusion, internal audit unit should continuously operate in a manner consistent with developing technologies, perform analysis of the potential effects of new technologies and take the necessary actions in order to manage those risks proactively.

Key Words: *Communication technologies, internal audit, risk management*
Jel Classification:*M42*

GİRİŞ

3Com'un kurucusu Robert Metcalfe 1995 yılın da "internet yakın zamanda bir süpernova gibi patlayacak ve 1996 yılında da korkunç bir biçimde çökecektir" ifadesinden bu tarafa 22 yıl geçmiş ve Robert Metcalfe'nin öngörüsünün gerçekleşmesi bir tarafa internet, insanlar için zaruri bir ihtiyaç haline dönüşmüştür. Yapay zeka teknolojisinin ilerlemesi, verilerin bulut depolama araçlarında saklanması ve büyük veri gibi bilgi teknolojisindeki gelişmeler, işletmelerin kendi sistemlerini, fonksiyonlarını ve kontrol yapılarını yeni duruma entegre etmeleri gerekliliğini beraberinde getirmiştir.

Bilgi teknolojileri ve makineleşme eş anlı biçimde gelişirken bugün insanlar tarafından yapılan birçok işi gelecekte makinelerin yapması öngörülmektedir. IFR 'nin (International Federation of Robotics) "2018 World Robotic" raporuna göre toplam küresel robot satışları 2020 yılında yaklaşık 520.900 adede ulaşması beklenmektedir. 2017-2020 arasında dünyanın dört bir yanındaki fabrikalarda 1,7 milyondan fazla yeni sanayi robotunun kurulacağı tahmin ediliyor (IFR,2017;23). Bu durumun denetim mesleğini, denetimin yapısını ve kullandığı araçları etkilemesi kaçınılmaz bir durumdur. Birleşik Devletler İş İstatistikleri Bürosunun, İstihdamın Geleceği araştırmasına göre, muhasebeci ve denetçi olarak sınıflandırılmış mesleğin gelecek 20 yıl içerisinde bilgisayar ve robotlar tarafından yapılma ihtimali %94 olarak tahmin edilmektedir. (Uzun ve Usluer, 2017;18) Dolaysıyla günümüz denetim süreçlerinin evraklı, belgelemeye dayalı yerinde incelemeye dayalı geleneksel yapısı, bilgi teknolojilerinin öneminin artması ile birlikte evraksız, elektronik sürekli denetim yaklaşımına doğru evrilmektedir. Özellikle büyük bağımsız denetim şirketleri bu teknolojik dönüşümde öncü rol oynamakta ve dev veri setlerini dijital analiz yöntemleriyle denetleyebilmektedir.[1] Bu kapsamda iç denetim fonksiyonu, bilgi teknolojileri ile gelen bu dönüşümün bir parçası olmak durumundadır.

İç denetim biriminin, gelişen bilgi teknolojileri ile birlikte kendini kurum için güvenilir bir danışman olarak konumlandırması gerekmektedir. İç denetim birimi bu anlamda birim yöneticisi ve iç denetçiler de dâhil olmak üzere, bilgi teknolojileri alanında kendilerini geliştirmek ve bu doğrultuda yeni yetenekler

[1] Bknz: KPMG tarafından geliştirilen Clara yazılımı: https://home.kpmg.com/au/en/home/services/audit/kpmg-clara.html , E&Y tarafından geliştirilen EY CANVAS yazılımı: https://www.ey.com/en_gl/audit/technology/canvas

kazanmak durumunadırlar. Nitekim teknolojinin gelişmesi ile artan bilgi güvenliği sorunları, işletmenin fikri mülkiyet haklarını koruyamamasına ve temel faaliyetlerini yürütememesine sebep olacaktır. Bu sebeple iç denetim yöneticileri bilgi güvenliği meselesini şirket içi toplantılarda sıkça dile getirerek gündemde tutmalı, aynı zamanda bilgi güvenliği ile ilgili yürütülecek sürece dâhil olmalıdır. KPMG (2017) tarafından gerçekleştirilen ve 200 CFO (Chief Financial Officer-Finansal İşler Başkanı), iç denetim birim yöneticisi ve denetim komitesi üyelerini içeren araştırma sonuçlarına göre; katılımcıların %80'i denetçilerin daha büyük örneklemler ve daha sofistike veri toplama ve analiz teknikleri kullanmaları gerektiğini vurgulamaktadır.

Bilgi teknolojilerine verilen önem işletmenin iş yapış süreçleri ve denetim süreçlerindeki hataları minimize edecek şekilde katkı sağlarken, bu teknolojiler kötü niyetli kişiler tarafından kullanıldığında aynı oranda hile, bilgi hırsızlığı ve yolsuzluklarda artışlara da sebep olmaktadır. Dolayısıyla işletme üst yönetimi işletmenin marka ve finansal değerlerinde derin yaralar açabilecek bu tür bilgi teknolojileri kaynaklı hırsızlıklara karşı dikkatli davranmalı ve gerekli önlemleri almalıdır. Yine KPMG (2018) tarafından 2.200 üst düzey yöneticiyle yapılan bir araştırma sonuçlarına göre CEO'ların %65'i kendi örgütlerinin kullandığı veri analiz yöntemlerine güvenmemektedir. Üst yönetimin bu kapsam dâhilinde şirket içi en etkin yardımcısı, hile ve yolsuzluklara karşı gelişen bilgi teknolojilerine hâkim şekilde oluşturulmuş veya yenilenmiş bir iç denetim yapısı olacaktır. Bu şekilde oluşturulmuş iç denetim yapısı ortaya çıkabilecek sorunlara proaktif yaklaşarak işletme değerindeki kayıplar önlenebilecektir.

Bu çalışma ile, gelişen bilgi teknolojisinin işletmelere getirdiği risklerin neler olduğu tanımlandıktan sonra iç denetimin bu risklerle mücadelesi ve yeni duruma nasıl adapte olması gerektiği ele alınacaktır. Aynı zamanda siber güvenlik, bulut bilişim, sosyal medya vb. bilgi teknolojilerinin iç denetim üzerindeki etkileri tartışılacaktır.

I. TEKNOLOJİNİN İÇ DENETİM SÜREÇLERİNE ETKİSİ

İleri teknolojilere dayalı bilgi, iletişim sistemlerinin işletmelerde kullanılmasıyla birlikte, denetim sürecinin bu teknolojilerle uyumlu bir yapıya kavuşturulması önemli bir konu haline gelmiştir. Bu doğrultuda, denetim süreçlerine bilgi teknolojilerinin yerleştirilerek otomasyon sağlanması, böylece denetim kalitesinin ve etkinliğinin arttırılması son derece önem kazanmıştır (Ertaş ve Güven,2008;51). Bu duruma ek olarak sosyal medya, mobil cihazlar, bulut bilişim ve büyük veri teknolojilerinin işletme sistemlerine dâhil olması ile iç denetimin genel alanı ve kapsamı değişirken, denetim sürecinde kullanılan tekniklerde değişikler söz konusu olmuştur (Kim, vd.2009; White ve Bond, 2014).

Son yıllarda sosyal medyanın, mobil cihazların, bulut bilişimin, giderek artan kullanımı işletmeleri güvenlik ihlalleri, müşteri verilerinin çalınması, itibar kaybı gibi çok tehlikeli risklerle karşı karşıya getirmiştir. Bu çerçevede işletmeler gelişen teknoloji ile ortaya çıkan risklerle mücadele edebilmek amacıyla iç denetim birimlerinden yardım istemektedir (Steinbart vd. 2015). Ortaya çıkan bu yeni durum denetim sürecinde iç denetçileri de yetkinliklerini geliştirmeleri ve bu

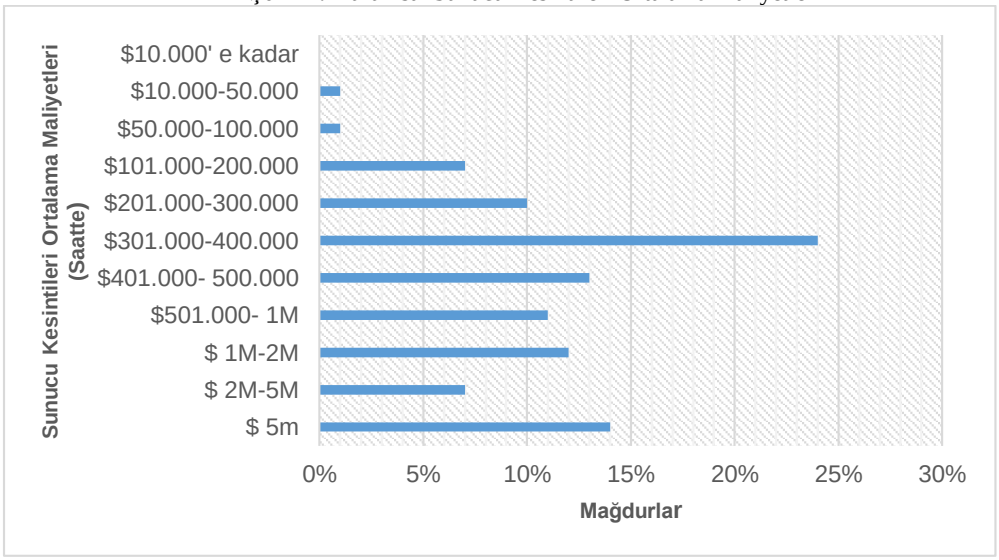
yetkinliklere yenilerini eklemeleri, geleneksel yöntemleri terk etmeleri konusunda mecbur bırakmıştır.

A. Bulut Bilişim ve İç Denetim

ABD Ticaret Bakanlığı'na bağlı Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) bulut bilişimi, çok az yönetim çabası veya servis sağlayıcı etkileşimi ile hızlı bir şekilde hazırlanabilen ve piyasaya sürülebilen, yapılandırılabilir bir kaynak havuzuna her yerde, uygun, isteğe bağlı ağ erişimini sağlayan bir model olarak tanımlamaktadır. Bulut bilişim teknolojisinin, diğer iletişim teknolojilerinde olduğu gibi maliyetlerinin aşağı çekilmesi, geleneksel teknolojilere alternatif olarak hızla ivme kazanmasını sağlamıştır. Bulut tabanlı bu tür dış kaynaklı depolama hizmetleri, işletmelere müşterilerin verilerini yönetmek için karşılaştırılabilir şekilde düşük maliyetli, ölçeklenebilir ve konumdan bağımsız bir platform sağlayarak çeşitli avantajları beraberinde getirmiştir. Bulut depolama servisi (CSS) depolama yönetimi ve bakım yükünü hafifletir. Ancak, eğer böyle önemli bir hizmet, saldırılara veya başarısızlıklara karşı savunmasız ise, veri veya arşivleri işletmelerin dışındaki belirsiz bir depolama havuzunda depolandığından, kullanıcılara geri dönüşü olmayan kayıplar getirecektir (Zhu vd, 2012;1083).

Bulut bilişimin, zaman veya mekan ile sınırlı olmaması ve işletmelerin internet bağlantıları olduğu sürece, müşteri sorgularına açık durumda olması bu teknolojiyi işletmeler açısından vazgeçilmez hale getirmektedir. Ancak avantajlarının yanında, bulut bilişim teknolojisi büyük miktarda elektronik verilerin işlenmesinde hâlâ çözülmemiş problemleri beraberinde getirmektedir. Bu problemler arasında bulut bilişim sisteminin arızası, veri kaybı veya hırsızlık gibi güvenlik sorunları sayılabilir.

Şekil 2: Kurumsal Sunucu Kesintileri Ortalama Maliyetleri



Kaynak: Information Technology Intelligence Consulting, 2018
https://www.statista.com/statistics/753938/worldwide-enterprise-server-hourly-downtime-cost/

Şekil 2'de 750'den fazla şirketin katıldığı araştırma ile 2017 yılında yaşanan sunucu kesintilerinin ortalama maliyetleri belirtilmiştir. Araştırmaya katılanların %24'ü, sunucu kesintisinin saatlik maliyetinin ortalama 301 bin $ ile 400 bin $ arasında gerçekleştiğini belirtmiştir.

Bu nedenle bulut bilişim hizmetlerini benimsemeden önce, bulut bilgi işlem güvenliği dikkate alınmalıdır. Müşteri bilgilerinin korunması, yüksek bilgi güvenliği uygulamaları gerektirmektedir. "Bilgi sızıntıya açık mı? Eğer bilgi diğer departmanlarda depolanırsa veya başka şirketlerle sunucu paylaşıyorsa, bu durum tehlikeye girer mi? Bulut bilişim iletimi, uygulaması ve kullanılabilirliği ne kadar verimli?" gibi sorulara yanıt verilmesi gerekmektedir. (Hu vd., 2016;3) İşletmelerin; kullanıcılar, kullanıcı ve hizmet sağlayıcıların yasal rolleri ve sorumlulukları, yerel yasa ve yönetmeliklere uyum, veri koruma, somut güvenlik, mahremiyet ve kullanılabilirlik dahil olmak üzere, uygulamadan önce bu riskleri anlamaları gerekmektedir (Chou, 2015; 137).

Bulut bilişim teknolojisi yukarıda bahsedilen güvenlikle ilgili risk içeren yönlerinin yanında işletmelere maliyetler açısından önemli faydalar sağlamaktadır. Bunlar (Chou, 2015;73);

- Bulut bilişim teknolojisi kullanıcıları yalnızca kullandıkları depolama alanı karşılığında ödeme yaptıkları için depolama maliyetlerini azaltır.
- İşletme bünyelerinde donanım, yazılım, ağ oluşturma ve bilgi teknolojisi uzmanları istihdam etme zorunluluğu bulunmaması beraberinde tasarrufu getirmektedir.
- Bulut bilişim teknolojisi esnek bir yapıya sahiptir, iş yükü değişikliklerinde işletmenin ihtiyaçlarına hızlı bir şekilde karşılık verebilir.
- İşletme çalışanları internetin olduğu her yerden veriye ve yazılıma kolayca ulaşabilir.

Bulut teknolojisi, bilgi işlem denetimlerinin açık bir şekilde incelenmesi açısından denetçilere pratik, aktif bir rehberlik hizmeti sağlayarak denetim alanına katkıda bulunabilir (Chou, 2015; 137). Bu çerçevede düşünüldüğünde, iç denetimin de bilgi teknolojilerini kullanan firmalarda ortaya çıkabilecek risklerin, iş süreçlerinin değerlendirilmesinde ve yönetilmesinde işletmelere yardımcı olması beklenmektedir. İç denetimin bu değerlendirmeleri yaparken aşağıda belirtilen noktalara dikkat etmesi gerekmektedir.(PWC, 2015;7):

- **Sözleşme Yönetimi:** İç denetim, bulut hizmetini sunan firmanın sorumluluklarından, yapılan sözleşmenin yerel ve uluslararası normlarla uyumu gibi önemli noktaların yapılan sözleşmede olup olmadığından emin olmalıdır ve bunun kontrolünü gerçekleştirmelidir.
- **Yetkilendirme:** İç denetim, bulut teknolojisinin sağlayıcısı firmadaki "bilgi güvenliği açısından" şirket bilgilerine ulaşabilecek kişilerin geçmişlerini araştırmalı ve sonuçlara göre değişiklik

istemelidir. Bu anlamda bulut sağlayıcısından gerekli yönetsel kontrollerin yapılmasını talep etmelidir.

- **Sertifikasyon ve hizmet sağlayıcı denetimleri:** Bulut teknolojisini işletmeye sağlayan firma ve faaliyetleri bağımsız olarak denetlenip denetlenmediği iç denetim birimince kontrol edilmelidir.
- **Yedekleme, kurtarma ve verilerin imhası:** Bulut hizmeti sağlayıcısının acil durumlarda " yedekleme, kurtarma verilerin imhası vb" işletme beklentilerini güvenli şekilde, tam olarak karşılayabilecek alt yapısının var olup olmaması durumunun kontrolü yine iç denetim birim tarafından gerçekleştirilmelidir.
- **Taşınabilirlik:** İç denetim birimi, ihtiyaç halinde işletme verilerinin başka bir bulut sağlayıcısına transferini ve bu anlamda firmanın teknolojik kısıtlarını dikkate almalıdır.

B. Büyük Veri (Big Data) ve İç Denetim

"Büyük veri" terimi, 1997'de Michael Cox ve David Ellsworth tarafından IEEE konferansında sunulan çalışmada, verilerin görselleştirilmesini ve bilgisayar sistemleri için yarattığı zorlukları açıklamak amacıyla ilk kez kullanılmıştır. 1990'lı yılların sonunda, hızlı gelişen bilgi teknolojileri birçok yeniliği beraberinde getirmiş bu da büyük miktarda veri üretilmesini sağlamıştır. Fakat üretilen bu bilgi karşılaştırılabilir anlamda bir özelliğe sahip değildi (Wang vd., 2018;2). 2001 ile 2008 arasındaki dönem, büyük veri gelişimi için evrimsel bir aşama olmuştur. Büyük veri ilk olarak 2001 yılında Laney tarafından 3V (Volume, Velocity Variety,) hacim, hız ve çeşitlilik cinsinden tanımlanmıştır. Bu tanımdan sonra 3V'ler büyük verileri tanımlamak için ortak bir çerçeve haline gelmiştir (Gandomi ve Haider, 2015;138). Kavramlar çerçevesinde düşünüldüğünde büyük veri analizlerinin ilk ve en önemli avantajı özelliklerinde de bahsedildiği üzere karmaşık büyük verileri öz bir şekilde güncel olarak kullanıcının hizmetine sunmasıdır.

Büyük veri, Gartner Inc[2] tarafından gelişmiş iç görü ve karar alma için maliyet-etkin, yenilikçi bilgi işleme biçimleri talep eden yüksek hacimli, yüksek hızlı ve çok çeşitli bilgi varlıkları şeklinde tanımlanmaktadır. Büyük veri, benzer şekilde TechAmerica Vakfı (TechAmerica Foundation, 2012;10) tarafından ise yakalama, depolama ve veri aktarımı için gelişmiş teknikler ve teknolojiler gerektiren yüksek hızlı, karmaşık ve değişken büyük hacimleri tanımlayan bir terim olarak tanımlanmıştır. Diğer bir deyişle bilginin dağıtımı, yönetimi ve analizidir.

Günümüzün giderek karmaşıklaşan iş ortamında, veri odaklı risk yönetimi ve kontrolleri kritik önem taşımaktadır. Operasyonel değişimin, anlamlı ve kabul edilebilir olabilmesi için üst yönetim organlarından gelmesi gerekmektedir. Yönetim organları daha iyi kararlar almak için doğru soruları sormalı ve daha sonra bunların cevaplarını verilerde aramalıdır. Bu anlamda büyük veri ve analitiğin denetim ile bütünleştirilmesi, işletmenin uyumluluk ve itibar risklerini azaltmasına yardımcı olmakta, aynı zamanda, stratejik değer yaratarak örgütte daha iyi kararlar

[2] http://www.gartner.com/it-glossary/big-data/

verilmesini sağlamaktadır. Bu da dolaylı olarak finansal raporlamanın kalitesini artırabilir (E&Y,2015;2).

Büyük veri, işletmelerin denetiminde önemli bir rol oynayacaktır. Büyük verinin geleneksel kanıtları yeterli, güvenilir ve ilgili bilgilerle verilerle tamamlaması denetçilerin müşteri verilerine bağımlılığını azaltırken, denetçilerin iç denetim kanıtlarını değerlendirmesinde bağımsız bir kıyaslama imkânına kavuşmasını beraberinde getirecektir. Bununla birlikte büyük veriyi geleneksel denetim kanıtlarıyla bütünleştirmek, müşteriler arasında bilgi aktarımı ve bilgi gizliliği sorunlarını da ortaya çıkaracaktır (Yoon vd.,2015;436). Yoon ve arkadaşları (2015), işletmelerin büyük veriden kaynaklı bilgi aktarımı sorununu müşterilerin toplantı tutanakları ve web sitesi trafiği gibi dahili verilerin kullanımıyla ilgili olarak işletmeyle, denetçiler vasıtasıyla resmi sözleşme yaparak çözebileceğini ifade etmektedir. Bu anlamda bir müşterinin dahili verileri başka bir müşterinin denetim görevi için kullanılıyorsa, anahtar tanımlama bilgileri silinmeli veya gizlenmelidir. Genel olarak denetçiler, diğer denetim görevleri için yalnızca büyük veriden yüksek düzeyde sentezlenmiş bilgileri kullanmalı ve orijinal işlenmemiş verilere erişimi sınırlandırmalıdır. Diğer bir sorun olan bilgi güvenliği endişeleri gidermek için ise, denetim firmaları müşterileri ile işbirliği yapmalı ve iş ile ilgili tüm veri kaynaklarının denetim amacıyla kullanılabileceğini önceden bildirmelidir. Ayrıca çalışanlarla ve işle ilgili verilerin sadece belirli bir denetim hedefi için kullanılacağını bildirmelidirler. Hile tespit edilmedikçe bilgiler anonim hale getirilmeyeceğinin garantisini vermelidir. İç denetim birimi bütün bu riskleri bertaraf etmek ve işletmenin bilgi güvenliğini sağlamak adına bağımsız denetim ile sıkı bir işbirliği yapmalıdır. Ayrıca bağımsız denetim firması ile yapılan sözleşmelerin (bilgi aktarımı ve bilgi güvenliği) içeriğinin denetim firması tarafından tam olarak yerine getirilip getirmediğinin kontrolünü sağlamadır. Bu çerçevede oluşabilecek bilgi aktarımı ve bilgi güvenliği riskleri için yönetimi bilgilendirmelidir.

İç denetim, risk değerlendirme ve denetim planlamasının bir parçası olarak organizasyonlar içindeki büyük verilerin rolünü dikkate almalıdır. Riskler önemliyse, iç denetim, büyük veriden kaynaklı riskleri ve kontrollerinin kapsamını sağlamak için uygun bir plan belirlemelidir. İç denetim birimi bu kapsamda ortaya çıkan riskler, fırsatlar ve bunun getireceği faydalar hakkında yönetimi bilgilendirmelidir (IIA,2017;22). Ayrıca iç denetçiler, veri toplama, depolama, analiz, güvenlik ve gizlilik açısından riskleri daha iyi anlamak için işletmenin bilgi işlem birimi ve diğer kilit liderlerle işbirliği halinde olmalıdır.

C. Sosyal Medya, Riskler ve İç Denetim

2000'li yıllardan itibaren internetin cebe girmesi, uygulamaların ve web sitelerin fazlalaşmasıyla internetin sosyal yaşamda etkinliğinin artmasına neden olmuştur. Ardından kullanıcıların düşünce, ilgi ve bilgi paylaşımlarına olanak sağlayan karşılıklı etkileşime izin veren web sitelerinin yani sosyal medya uygulamalarının yaygınlaşması, yeni iletişim ortamlarının oluşmasını beraberinde getirmiştir (Sayımer, 2008:123). Geleneksel medyadan farklı olarak nitelendirilen sosyal medya, sosyal ağlar vasıtasıyla insanların görüşlerini interaktif olarak

sınırsız bir şekilde birbirleriyle paylaşabildikleri yeni içerikler oluşturabildikleri hayatın işleyişini değiştirebilecekleri bir olgu olarak karşımıza çıkmaktadır.

Sosyal medya; insanlara, kişi veya kurumlara istedikleri anda istek ve şikâyetlerini iletebilme imkânı sağlarken, işletmelere de müşterilerinin görüş, öneri, istek ve şikâyetlerine hızlı bir şekilde cevap verme olanağı sağlamaktadır. Bu çerçevede düşünüldüğünde işletmelerin müşterileriyle sosyal medya üzerinden etkileşimleri hız ve yeni müşteri kazanma konusunda ve marka bilinirliliği anlamında birçok fayda sağlarken beraberinde belli riskleri de getirebilmektedir. Sosyal medyanın ve internetin gücünü kanıksamış işletmeler, genellikle bünyelerinde kurdukları sosyal medya birimleri eliyle pazar ile güçlü bağlar kurabilmektedirler. Bazen de işletmeler sosyal medyada yaşadıkları iş kazaları ile marka imajına büyük zararlar verebilmektedirler.

We Are Social ve Hootsuite tarafından yayınlanan "Digital in 2018 Global Overview" raporu internet, mobil ve sosyal medya kullanıcı istatistikleri konusunda dikkat çekici bilgiler ortaya koymaktadır. Araştırmaya göre dünyadaki 7,6 milyar nüfusun üçte ikisi artık bir cep telefonuna sahip ve dünya genelinde web trafiğinin % 50 den fazlası cep telefonları ile gerçekleştirilmektedir. Raporun Türkiye kısmında ise internet ve sosyal medya kullanımı ile ilgili rakamlara yer verilmektedir. Rapora göre Türkiye'de ise 54 milyonu aşkın internet kullanıcısı varken, çoklu hesap kullanımları da hesaba katıldığında 51 milyon sosyal medya kullanıcı sayısı söz konusudur. Ayrıca bunlara ek olarak raporda, Türkiye'de sosyal medyaya mobilden bağlanan kullanıcı sayısını ise 44 milyon olduğu ortaya koyulmuştur.

Bütün bu istatistiki bilgiler çerçevesinde, görüldüğü üzere internet ve sosyal medya; iç denetim ile ilgili güncel gelişme ve mesleki çalışmaların, iç ve dış paydaşlar ile paylaşılması ve aynı şekilde kendilerinin beklenti ve sorularının en etkin ve hızlı şekilde takip edilip cevaplandığı interaktif bir iletişim aracı ve kurumsal itibar yönetiminin de en önemli unsurlarından biridir (TİDE,2017;1). Çalışanların sosyal medya kullanımını ve şirketlerin ilgili riskleri ve fırsatları nasıl etkin bir şekilde yönetebileceğine daha spesifik bir bakış getiren Scott ve Jacka (2013) işletmelerin sosyal medya kaynaklı riskleri ve bu risklerin nasıl yönetilmesi ile ilgili görüşlerini 7 maddede özetlemiştir. Bunlar;

- Sosyal medya riskleri değerlendirilmeli: Sosyal medya risklerinin (marka ve itibar kaybı, veri güvenliği, veri sızması virüsler, kötü amaçlı yazılımlar) etkili bir şekilde yönetilmesi iş stratejilerinde iyileştirmeleri ve itibar kaybı riskinin azalmasını beraberinde getirecektir.
- Hangi çalışanların sosyal medya kullandığını belirlenmelidir.
- Bir sosyal medya politikası geliştirilmeli; açık öz ve kullanışlı kurallar belirlenmeli ve bu politika belli aralıklarla güncellenmelidir.
- Çalışanlar ve yöneticiler eğitilmeli; CEO veya yönetim kurulu üyesi olarak kişisel sosyal medya kullanımı diye bir şey söz konusu

değildir. Çünkü yöneticilerin sosyal medyada yaptıkları her şeyin şirketin imajını etkileme potansiyeli vardır. Bu anlamda İç denetçiler, şirket liderlerinin sosyal medya risklerini anlamalarına yardımcı olabilir.

- Şirket için kimin konuşacağını ve kimin konuşmayacağını belirlenmelidir.
- İnternette, sosyal medyada şirketin içindeki ve dışındaki insanların şirketin adı altında neler söylediği takip edilmelidir.
- Yöneticiler, sosyal medya kullanımı ile ilgili olarak çalışanlarına iyi bir model olmalıdır. Çünkü çalışanlar liderlerini takip etme eğilimindedir.

Değinilen bu riskler değerlendirildiğinde, işletmeler için en büyük risk herhangi bir şekilde sosyal medyada yer almamaktır. Çalışanlar da dahil olmak üzere tüm paydaşların (müşteriler, satıcılar, hissedarlar) şirket hakkında konuşurken ve yorum yaparken, şirketin bu alanda temsil edilememesi ve görüşlerini açıklamaması temel olarak bu durumun şirket tarafından önemsenmediği şeklinde anlaşılması olasıdır (IIA,2013;2). İç denetim biriminin bütün bu durumlar karşısında işletme sosyal medya stratejisi sınırları içerisinde sosyal medya kontrolüne imkân sağlayacak gerekli alt yapının kullanılması sağlayarak olası kriz durumlarında ne gibi önlemlerin alınacağını planlarını yapması gerekmektedir.

II. İLETİŞİM TEKNOLOJİLERİ KAPSAMINDA SİBER GÜVENLİK VE İÇ DENETİMİN ROLÜ

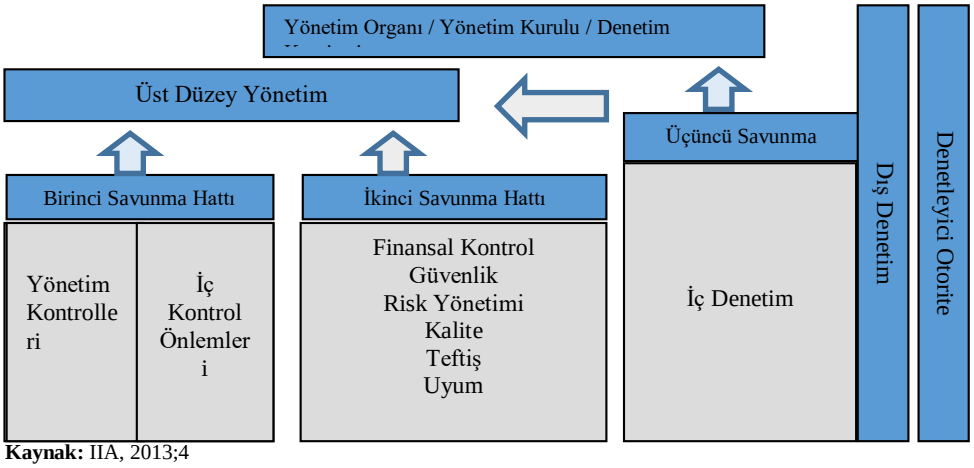
Siber güvenlik terimi, bilgi varlıklarını korumak için kullanılan işlevini ve teknoloji araçlarını ifade etmektedir. Fakat Solms ve Niekerk (2013), siber güvenliğin sadece bilgi kaynaklarının korunmasını değil, aynı zamanda kişinin kendisi de dahil olmak üzere diğer varlıkların korunmasını da içerecek şekilde geleneksel bilgi güvenliğinin sınırlarının ötesine geçtiğini ileri sürmektedir. Yazarlar, insanların siber saldırıların potansiyel hedefleri arasında olduğunu ve hatta insanların bilmeden bir siber saldırıya katılabildiklerini ifade etmişlerdir.

Siber güvenlik, bilgi teknolojisinin çok ötesine geçen stratejik bir kurumsal risktir. Ürün bütünlüğünü, müşteri deneyimini, yatırımcı güvenini, operasyonları, mevzuata uygunluğu, marka itibarını ve daha fazlasını etkileyebilecek işletme güvenliği sorunudur. Dolayısıyla kurumlar, siber güvenlik risklerine ve siber güvenlik tehditlerine nasıl cevap vereceklerine karar vermelidir (KPMG,2017;1). Bu anlamda sorumluluk makamında oturan yöneticilerin işletme ve paydaşlarını koruyacak güvenlik önlemlerini almaları gerekmektedir. İç denetim birimi ile ortak olarak belirlenebilecek risk haritaları ve savunma stratejileri yöneticilerin işlerini bir hayli kolaylaştıracaktır.

FERMA (The Federation of European Risk Management Associations - Avrupa Risk Yönetimi Kuruluşları Federasyonu**)** ve ECIIA (European Confederation of Institutes of Internal Auditing-Avrupa İç Denetim Enstitüleri Konfederasyonu) tarafından ortaya koyulan ve siber saldırılara karşı bütüncül bir savunma yaklaşımı olan Üç Kademeli Savunma Hattı Modeli, temel rolleri ve

görevleri açıklığa kavuşturmak suretiyle risk yönetimi ve kontrolü konusundaki iletişimi geliştirmek için basit ve etkili bir yol sağlamaktadır. Bu model, risk yönetimi girişimlerinin sürmekte olan başarısını garantilemeye yardımcı olan operasyonlara yeni bir bakış sağlamakta ve büyüklük veya karmaşıklık gözetmeksizin tüm örgütlere uygulanabilmektedir. Resmi bir risk yönetimi çerçevesinin veya sisteminin bulunmadığı organizasyonlarda bile, Üç Kademeli Savunma Hattı modeli, risk ve kontrollere ilişkin netliği artırabilecek ve risk yönetim sistemlerinin etkinliğini artırmaya yardımcı olabilecektir (IIA,2013;2).

Şekil 3: Üç Kademeli Savunma Hattı Modeli



Kaynak: IIA, 2013;4

Etkin risk yönetimi, çoklu risk savunma katmanlarının ürünüdür. FERMA ve ECIIA işletmelerin üç sıra savunma modeli kurmaları ve bunun sürekliliğini sağlamaları gerektiğini belirmektedir. Buna göre Üç Kademeli Savunma Hattı Modeli aşağıdaki şekilde detaylandırılmaktadır (FERMA,2011;7);

1. Savunma Hattı Yönetim Kontrolü: Bilgi güvenliği risklerini yönetmede iyi olan şirketler, genellikle güvenlik politikaları için kurumun en üst düzeylerine sorumluluk yükler. Yönetim; riskleri değerlendirmek, kontrol etmek ve hafifletmek için sahipliğe, sorumluluğa ve hesap verebilirliğe sahiptir (Deloitte,2015;4). Yönetim, işletme süreçlerindeki kontrol eksikliklerini gidermek için düzeltici eylemlerin uygulanmasından sorumludur.

Yönetim etkin iç kontrolü korumak için gün gün risk ve kontrol prosedürlerini yürütmekten sorumludur. Yönetim doğal olarak ilk savunma hattı görevi görür. Çünkü kontroller, yönetimin rehberliği altındaki sistemlere ve süreçlere göre tasarlanır. Bu çerçevede yetersiz süreçler ve beklenmedik olayları vurgulamak için yeterli yönetimsel ve denetleyici kontroller olmalıdır (IIA,2013;3).

2. Savunma Hattı; Risk yönetimi ve Uyumluluk Fonksiyonları: Yönetim, ilk savunma hattı kontrollerinin oluşturulmasına ve izlenmesine yardımcı olacak çeşitli risk yönetimi ve uyum fonksiyonlarını oluşturmaktadır. İkinci savunma hattı, finansal kontrol, risk yönetimi, güvenlik, kalite, teftiş ve mevzuata

uyum başlıklarından oluşur. Söz konusu hatta yer alanlar, riskin gözetimi ve kontrolü fonksiyonlarını bir nevi yarı bağımsız olarak yerine getirseler de etkili risk yönetimi politikalarının sağlıklı uygulanmasına ve işletme içerisinde doğru bilgi üretimine katkıda bulunurlar (Uzel vd.,2016;204). Bu anlamda ikinci savunma hattının fonksiyonlarını aşağıdaki gibi özetlemek mümkündür (IIA,2013;4):

- Yönetim politikalarını desteklemek, rolleri ve sorumlulukları tanımlamak ve uygulama için hedefler belirlemek.
- Risk yönetimi çerçeveleri oluşturmak.
- Bilinen ve olası riskleri belirleme.
- İşletmenin örtülü risk iştahındaki değişimleri belirleme.
- Risklerin ve sorunların yönetilmesi için süreçlerin ve kontrollerin geliştirilmesine yardımcı olmak.
- Risk yönetim süreçleri hakkında rehberlik ve eğitim sağlamak
- Yönetim ile etkin risk yönetimi uygulamalarını izlenmek.
- Yönetimi, ortaya çıkan sorunlara yeni risk senaryolarına ve değişen mevzuata karşı uyarmak.
- İç kontrolün yeterliliğini ve etkinliğini, raporlamanın doğru yapılıp yapılmadığını, hazırlanan raporun yasa ve yönetmeliklere uyumunun sağlanmasını izlemek.

3. Savunma Hattı; İç Denetim: Üçüncü savunma hattı iç denetimdir. Dolayısıyla iç denetim, yönetim kurulu ve üst yönetimin beklentileri ile tutarlı olarak hem birinci hem de ikinci hatların çabaları üzerinde üst yönetime ve yönetim kuruluna güvence sağlar (Anderson ve Eubanks,2015;3). İç denetim birimi, işletme üst yönetimine ve diğer paydaşlara işletmenin yönetim sisteminin işletmenin faaliyet gösterdiği hukuki ve ekonomik çevreye tam uyumlu olarak risk unsurlarını dikkate alarak etkin ve verimli bir şekilde çalıştığı konusunda bağımsız ve objektif çalışmalara dayanan bilgi güvencesi sunmaktadır. Sonuç olarak, iç denetim biriminin yaptığı bu değerlendirmeler içerisinde birinci ve ikinci savunma hatlarının performans seviyeleri de yer almaktadır (Uzel vd, 2016;205).

Bağımsız ve etkin bir iç denetim biriminin oluşturulması ölçeği fark etmeksizin tüm işletmeler açısından son derece önemlidir ve iyi bir kurumsal yönetimin temelini oluşturmaktadır. İç denetim birimi, üst yönetime, bağımsız ve tarafsızlığı sağlandığı takdirde en üst düzeyde güvence sağlayacaktır.

İç denetimin 3. Savunma hattı çerçevesinde üst yönetime ve paydaşlara sağladığı güvencenin kapsamı ve odaklanması gereken noktalar genellikle şunlardan oluşmaktadır (PWC,2015;9 ve IIA,2013;5):

- Alınan güvenlik önlemlerinin müşteri veri güvenliği açısından durumu tespit etmek,
- Sürekli kontrol ve aksaklıklarla ilgili gerekli düzenlemelerin yapılıp yapılmadığının tespiti,
- Önemli şirket bilgilerinin tespiti ve bu bilgilere erişim izinlerinin denetimi yapmak,

- İşletme verilerinin korunması ve yedeklemesinin yapılması sağlamak,
- Siber güvenlik ile ilgili önleyici tedbirlerin bağımsız olarak değerlendirilmesini sağlamak,
- Sorunlu web siteleri, zararlı yazılımlar ve veri sızması gibi durumların işletme verilerine zarar vermemesi için işletme verilerine ayrıcalıklı erişime sahip kullanıcıların yeterliliklerini denetleme,
- Raporlama süreçlerinin güvenilirliği ve bütünlüğü ve yasalara, yönetmeliklere, politikalara, prosedürlere ve sözleşmelere uygunluğunu denetlemek.

Üst yönetimin ve yönetim kurulunun öncelikleri arasına giren siber güvenlik konusu, sadece iç denetim birimlerinin değil, işletmenin bütününde bilinçlenme ve teknik yeterliliğe ihtiyaç duymaktadır. Bilgi güvenliği artık sadece bilişim denetçilerinin yapacağı çalışmaların konusu olmaktan çıkmış, tüm iç denetçilerin çalışmalarında dikkat etmeleri gereken bir risk haline dönüşmüştür. Dolayısıyla, denetçiler dışında tüm çalışanların siber güvenlik konusunu dikkate alması gerekmektedir (Uzun ve Usluer, 2017;14).

SONUÇ

Geleneksel anlamda iç denetim uygulamaları, teknolojinin ulaştığı gelişmişlik seviyesi ile bu gelişmişliğin ortaya çıkardığı yeni riskler ile mücadele ederken yetersiz kalmakta ve beklentileri karşılayamaya bilmektedir. Her geçen gün değişen risk unsurları ortaya sistematik olarak yönetilemeyen ve denetlenemeyen işletme yapılarını çıkarmaktadır. Bu anlamda işletme yönetimleri, geleneksel risklerle mücadele araçlarını terk ederek teknolojinin (bulut bilişim, siber güvenlik, büyük veri, sosyal medya) ortaya çıkardığı yeni riskler ile mücadele planları ortaya koymalılar. Bu çerçevede yönetimler, yeni nesil iç denetim birimi rehberliğine ihtiyaç duyacaktır.

İç denetim birimi ile bulut teknolojisi arasındaki ilişki ilk olarak işletme tarafından bulut teknolojisi hizmeti sağlayıcısının seçiminde ortaya çıkmaktadır. İç denetim birimi, hizmet sağlayıcısının seçiminde işletme dinamiklerini dikkate alarak ve firmanın güvenlik anlamında referanslarını, alt yapısını dikkate alarak araştırmalarını gerçekleştirmelidir. Çünkü yaşanabilecek herhangi bir güvenlik açığı işletme ve müşteri bilgilerinin çalınmasına ve dönülemez zararların ortaya çıkmasına neden olabilecektir. Ayrıca iç denetim birimi, bulut teknolojisinin sürekliliğini ve güvenliğini proaktif şekilde izleyerek, yönetimi bu konuda bilgilendirmeli, güncel tutmalıdır. Bulut bilişim, doğal olarak teknolojik alt yapısı gereği tehditleri de beraberinde getirmektedir. Fakat işletmelerin bu teknolojiyi kullanmamalarının fırsat maliyeti, kaybettikleri esneklik ve hızdan kaynaklı olarak son derece yüksek olabilecektir.

Hataların ve sorunların temel nedenlerini gerçek zamanlı olarak belirleyebilme yeteneğini işletmelere kazandıran büyük veri analizi, işletmelerin büyük çaplı verileri işleyerek daha isabetli iş kararları vermelerine yardımcı

olacaktır. Dolayısıyla iç denetçiler ilk olarak, son derece büyük ve karmaşık veri kümelerini ifade eden bu kavram hakkında yeterli ölçüde bilgi edinmeli ve kendilerini devamlı güncelleyebilmelidir. Bilgi güvenliğinin ve gizliliğin son derece önem kazandığı günümüzde, iç denetim birimleri bilgi sızmalarına karşı gerekli alt yapının oluşması için yönetimle ve ilgili birimlerle sürekli temas halinde olmalı yani işletme bilgilerinin başka bir büyük veri kullanıcısının girdisi olmasına engel olmalıdır.

Herhangi bir konu hakkındaki olumsuz fikrin, olumlu görüşlerden daha hızlı yayıldığı sosyal medya platformlarında, işletmeler son derece planlı ve tedbirli olmalıdır. Kurumsal sosyal medya hesaplarının yanı sıra özellikle üst düzey yöneticilerin bireysel hesapları da işletme imajı açısından önemli riskler taşımaktadır. Bu sebeple iç denetim biriminin bu ve benzeri risklere yönelik olarak iç iletişim kanallarını kullanarak işletme çalışanlarını bilgilendirmesi ve olası eylem planlarının hazırlanmasında ilgili birimlere destek olması gerekmektedir. Ayrıca iç denetim birimi tarafından devamlı kontrol edilebilen bir sosyal medya yönetim alanı da oluşturulmalıdır.

Siber güvenlik konusu işletmenin tüm birimlerince ve bütüncül bir bakış açısıyla, sistemli bir biçimde dikkatle ele alınmalıdır. Çünkü bir işletmenin siber güvenliği sağlayamaması en temel fonksiyonlarını bile yerine getirememesine ve işletme itibarının büyük zarar görmesine ve marka değerinin alt üst olmasına yol açabilecektir. Dolayısıyla siber güvenlik risklerini anlayan iç denetim liderleri, siber güvenlik konusunu sürekli olarak işletmenin gündeminde tutmalı ve işletmenin zayıf yönlerini gidermek için çaba sarf etmelidir. Bu sebeple iç denetim yöneticileri bilgi güvenliği meselesini şirket içi toplantılarda sıkça dile getirerek gündemde tutmalı, aynı zamanda bilgi güvenliği ile ilgili yürütülecek sürece dâhil olmalıdır.

Araştırmacılar gelecekteki çalışmalarda; iç denetim birimlerinin büyük veri, bulut bilişim ve mobil teknolojilere uyumu, iç denetçilerin bu teknolojileri kabullenme düzeylerinin ölçülmesini inceleme konusu yapabilirler. Araştırmacılar bu bağlamda, işletmelerin iç denetim birimlerinin geleceğe hazır olma düzeylerini ortaya koyacak çalışmalar yürütebilir ve konu hakkında modelleme çalışması yaparak, işletmelere klavuz özelliği taşıyacak daha derin bulgular sunabilirler.

KAYNAKÇA

Anderson, D. J., & Eubanks, G. (2015). Leveraging COSO across the three lines of defense. COSO, https://www.coso.org/ Documents/COSO-2015-3LOD.pdf

Chou, D. C. (2015a). Cloud computing risk and audit issues. Computer Standards & Interfaces, 42, 137-142. Doi: 10.1016/j.csi.2015.06.005

Chou, D. C. (2015b). Cloud computing: A value creation model. Computer Standards & Interfaces, 38, 72-77. https://doi.org/ 10.1016/j.csi.2014.10.001

Cox, M., & Ellsworth, D. (1997, October). Application-controlled demand paging for out-of-core visualization. In Visualization'97., Proceedings (pp. 235-244). IEEE. https://www.nas.nasa.gov/assets/pdf/techreports/1997/nas-97-010.pdf

Deloitte (2015) "Cybersecurity: The changing role of audit committee and internal audit" https://www2.deloitte.com/content/dam/ Deloitte/sg/Documents/risk/sea-risk-cyber-security-changing-role-in-audit-noexp.pdf

E&Y (2015) "Big data and analytics in the audit process", BoardMatters Quarterly Volume 9, https://www.ey.com/Publication/ vwLUAssets/ey-big-data-and-analytics-in-the-audit-process/$FILE/ey-big-data-and-analytics-in-the-audit-process.pdf

Executive Summary World Robotics 2018, Industrial Robots, https://www.ifr.org/downloads/press2018/Executive_Summary_ WR_2018_Industrial_Robots.pdf

FERMA, E. Guidance on the 8th EU Company Law Directive, article 41-2b. http://www.eciia.eu/wp-content/uploads/2013/09/Blog-4.4-Avoid-reg-part-2.pdf

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management, 35(2), 137-144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Gartner IT Glossary (n.d.). Retrieved from http://www.gartner.com/it-glossary/big-data/ https://assets.kpmg.com/content/dam/kpmg/bh/pdf/cyber-security-and-the-role-of-internal-auditors.pdf

https://wearesocial.com/blog/2018/01/global-digital-report-2018

Hu, K. H., Chen, F. H., & We, W. J. (2016). Exploring the key risk factors for application of cloud computing in auditing. Entropy, 18(8), 401. Doi:10.3390/e18080401

IIA, (2013) "7 Tips For Governing Social Media," Tone at the Top, Sayı:64,https://global.theiia.org/knowledge/Public %20Documents/TaT_October_2013.pdf

IIA, (2016) "Global Perspektiflerve Anlayışlar: Güvenilir Siber Danışman olarak İç Denetim," https://www.theiia. org/gpi

IIA, (2017) " GTAG / Understanding and Auditing Big Data"

Institute of Internal Auditors. (2013). The three lines of defense in effective risk management and control. Position paper. https://na.theiia.org/standardsguidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

Kim, H. J., Mannino, M., & Nieschwietz, R. J. (2009). Information technology acceptance in the internal audit profession: Impact of technology features and complexity. International Journal of Accounting Information Systems, 10(4), 214-228. Doi:10.1016/j.accinf.2009.09.001

KPMG (2017), "The Future is Now", Forbes Insights, https://i.forbesimg.com/forbesinsights/kpmg_audit2025/KPMG_ Audit_2025.pdf, Erişim Tarihi:22.10.2018

KPMG (2018), "Guardians of Trust, Who is Responsible for Trusted Analytics in the Digital Age?", https://assets.kpmg.com/content /dam/kpmg/xx/pdf/2018/02/guardians-of-trust.pdf, Erişim Tarihi:22.10.2018

PWC, (2015). İç Denetimin Gelişen Teknolojideki Yeni Rolü, https://www.pwc.com.tr/tr/risk-surec-teknoloji-hizmetleri/ic-denetim-ve-kontrol-hizmetleri-yayinlari/ic-denetimin-gelisen-teknolojideki-yeni-rolu-web.pdf

Sayımer İ. (2008). Sanal Ortamda Halkla İlişkiler, Beta Yayınları, İstanbul.

Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. N. (2015). The Influence of Internal Audit on Information System Effectiveness: Perceptions of Internal Auditors. https://doi.org/10.1016/j.aos.2018.04.005

TechAmerica Foundation's Federal Big Data Commission. (2012). Demystifying bigdata: A practical guide to transforming the business of Government. https://bigdatawg.nist.gov/_uploadfiles/M0068_v1_3903747095.pdf

Uzel, M. N., Hasanefendioglu, B., & Durmus, C. N. (2016). 3'LÜ SAVUNMA Hattının Coso İç Kontrol Sisteminin Etkinliğinin Arttırılmasında Kaldıraç Etkisi. Mali Çözüm Dergisi, 26, 199. http://archive.ismmmo.org.tr/docs/malicozum / 136malicozum/16 .pdf

Uzun, A.K, Usluer, T. (2017). İç Denetimde Dönüşüm ve 2017 Yılında Öne Çıkan Konuların Değerlendirilmesi. TIDE http://www.tide.org.tr/uploads/Muhasebe EgititimSempozyumBildirisi TIDE2017.pdf.2

Wang, Y., Kung, L., & Byrd, T. A. (2018). Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. Technological Forecasting and Social Change, 126, 3-13. https://doi.org/10.1016/j.techfore.2015.12.019

White, N., & Bond, R. (2014). Analytics refresher: internal audit can be a catalyst for expanding the use of analytics through the company to provide greater, more holistic business insights. Internal Auditor, 71(5), 19-21.

Yoon, K., Hoogduin, L., & Zhang, L. (2015). Big Data as complementary audit evidence. Accounting Horizons, 29(2), 431-438 https://doi.org/10.2308/acch-51076

Zhu, Y., Hu, H., Ahn, G. J., & Yau, S. S. (2012). Efficient audit service outsourcing for data integrity in clouds. Journal of Systems and Software, 85(5), 1083-1095. Doi: 10.1016/j.jss.2011.12.024

SUMMARY

After the rapid integration of information technologies into the existing operations of the enterprises, it has become mandatory for employees of the Internal Audit unit to develop themselves in this field and adapt to the use of developing technologies. This integration can lead to increased data security issues and risks that may affect the core functions of the enterprise. Under these conditions, expectations for the role of internal auditing within the enterprise have changed and the validity of the existing audit methods has become questionable.

Since the information security and confidentiality are extremely important in today; communication technologies such as social media, mobile devices, big data and cloud computing are making businesses to face with new risks. Important weaknesses can occur in businesses that cannot manage communication technologies correctly and cannot take precautions by analyzing those risks. In this context, enterprises must review the roles and responsibilities of internal audit units and transform them into structures that are in contact with all units and that can coordinate risk management processes.

As a result, the compliance of the internal audit unit with emerging information technologies will enable an effective internal audit by preventing leaks that could jeopardize the continuity of business, protecting brand value and corporate reputation and identfying potential risks arising in various departments of business.