İÇ DENETİM VE BİLGİ GÜVENLİĞİ İLİŞKİSİ: BÖLGESEL BİR ARAŞTIRMA

Niyazi Kurnaz[1]
A. Kemal Dindaroğlu[2]

Özet

Şirketlerin sahip olduğu ticari varlıkların en önemlilerinden birisi de "bilgi"dir. Bilgi, sözlü, basılı veya elektronik ortamlarda bulunabilir. Günümüzdeki hızlı teknolojik gelişmeler nedeniyle sahip olunan bilginin korunması iş dünyasının stratejik önceliklerinden birisi haline gelmiştir. Şirketler bunun için günümüzde önlemler alıp ve önemli yatırımlar yapmaya başlamışlar ve yatırım yapmaya da devam edeceklerdir.

Bir şirketin kendi ürünlerine, iş süreçlerine, pazarlama stratejilerine, müşterilerine yönelik her türlü bilgi, onun rakipleriyle arasındaki farkı oluşturur. Şirketler sahip oldukları bilgiyi koruyabildikleri ve kullanabildikleri ölçüde rakiplerine göre daha başarılı sonuçlar elde edebilirler. Günümüzde şirket bilgilerinin elektronik ortamlarda tutulması zorunluluğu, bu bilgileri korumayı daha zor hale getirmiştir. Şirketler bilgi kayıpları nedeniyle para, zaman, müşteri ve pazar kayıpları, çeşitli cezai yaptırımlar ve itibar kayıpları ile karşılaşabilmektedirler. Bundan dolayı, bilgi güvenliği konusuna önem vermek durumunda kalmışlardır.

Bilgi güvenliği, kayıpların en aza indirilmesine ve ticari fırsatlardan faydalanmaya imkân sağlamaktadır. Bilginin güvenliğinin sağlanması işletme yönetiminin sorumluluğundadır. Bilgi güvenliği personeli, örgütün bilgi kaynaklarını korumak için çeşitli prosedürleri ve teknolojileri tasarlar, uygular ve yönetirler. İç denetim; bilgi güvenliğinin sağlanmasındaki riskleri değerlendirir, bu etkinliklerin iyileştirilebilmesi ve verimliliğinin artırılması için geri bildirimlerde ve önerilerde bulunur. Fakat yapılan araştırmalar bu iki fonksiyonun her zaman uyumlu bir ilişki içerisinde olmadığını gösterir. Bu çalışma, iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin doğasını etkileyen faktörlerin ortaya çıkarılması amacıyla planlanmıştır. Bu sayede şirketler kendi lehlerine çıkarımda bulunabileceklerdir. Çalışmanın verileri, ege bölgesinde faaliyette bulunan kurumlardaki iç denetçiler ile bilgi güvenliği uzmanlarıyla yapılan yarı yapılandırılmış görüşmeler sonucunda elde edilmiştir.

Anahtar Kelimeler: İç denetim, Bilgi Güvenliği, Bilgi Güvenliği Sistemleri

THE RELATIONSHIP BETWEEN INTERNAL AUDIT AND INFORMATION SECURITY: REGIONAL A RESEARCH

Abstract

One of the most important commercial properties of companies is "information". Information can be found in verbal, printed or electronic media. Today, the protection of information becomes one of the strategic priorities of business world due to the rapid technological developments. To this end, companies started to take precautions today and make significant investments and they will keep making more investments.

Any kind of information that a company owns about its products, business processes, marketing strategies and customers constitutes the difference with its competitors. Companies obtain more successful results than their competitors when they can protect their information and use it efficiently. The necessity to keep company information at electronic media makes it more difficult to protect the information. Companies may encounter the loss of money, time, customer, market, reputation and various penal sanctions due to the information loss. For that reason, they must pay attention to information security.

Information security makes it possible to minimize these losses and to get benefit from commercial opportunities. To ensure information security falls under the responsibility of company management. Information security personnel design, implement and manage various procedures and technologies so as to protect information sources of organization. Internal audit evaluates risks in information security, provides feedbacks and recommendations to improve these activities and the efficiency. However, relevant research indicates that these two functions do not necessarily have a component relationship. This study aims to reveal factors that affect the nature of the relationship between internal audit and information security. Thus, companies can make interference in their own favor. The research data were obtained by semi-structured interviews with internal auditors and information security specialists of institutions in the Aegean region.

Key Words: Internal Audit, Information Security, Information Security Systems

[1] Yrd. Doç.Dr., Dumlupınar Üniversitesi UBYO Muhasebe Bölümü, nkurnaz@gmail.com
[2] Öğr. Grv., Mersin Üniversitesi Anamur MYO, akifkemal33@hotmail.com

Giriş

Günümüzde bilgi kontrol edilmesi gereken büyük bir güç haline gelmiştir. Bilgiye sahip olan kişi, grup, şirket veya ülkeler beraberinde gelen güce de sahip durumdadırlar. Bahsi edilen güç fiziksel bir güç olmanın yanında elinde bulundurana finansal bir güç de sağlamaktadır. Çünkü günümüzde bilgi doğrudan veya dolaylı olarak nakte çevrilebilir konuma gelmiştir.

Bilginin tanımına bakacak olursak Türk Dil Kurumu bilişim sözlüğünde bilgiyi *"Kurallardan yararlanarak kişinin veriye yönelttiği anlam"* olarak tanımlamaktadır (TDK,2013). Bilgi birçok şekilde karşımıza çıkabilmektedir. Günümüzün rekabete dayanan iş ortamında, bu tür bilgiler devamlı olarak birçok kaynağın tehdidi altındadır. Bu tehditler dâhili, harici, rastlantısal veya kötü niyet şeklinde olabilir. Bilginin saklanması, iletilmesi ve alınması için yeni teknolojinin artan bir şekilde kullanılmasıyla, kurumlar kendilerini artan sayıdaki tehditlere tamamen açmış oluyorlar (http://www.bsi-turkey.com/BilgiGuvenligi/Genel-bakis/index.xalter).

Farklılık ve rekabet avantajı sağlayan varlıklar, organizasyonlar için çok değerlidir. Bir şirketin kendi ürünlerine, iş süreçlerine, pazarlama stratejilerine, müşterilerine yönelik her türlü bilgi, onun rakipleriyle arasındaki farkı oluşturur. Birçok varlığın kaybedilmesi durumunda telafisi mümkün iken kurumların yaşam deneyimlerini de yansıtan "bilgi" para karşılığı kolaylıkla yerine konamamaktadır. Şirketler bilgi kayıpları nedeniyle para, zaman, müşteri ve pazar kayıpları, çeşitli cezai yaptırımlar ve itibar kayıpları ile karşılaşabilmektedirler. Bundan dolayı, bilgiyi korumak, bilginin güvenliğini sağlamak artık bir zorunluluk haline gelmiştir (Yurtsever;2013). Çünkü bilgi güvenliği, iş sürekliliğini yani aksamaların ve durmaların yaşanmamasını sağlamaktadır. Bilgi güvenliği, kayıpların en aza indirilmesine ve ticari fırsatlardan faydalanmaya imkân sağlar (Doğantimur,2009:6).

Bilgi güvenliğinde temel amaç, sahip olunan bilgilerin izinsiz erişimden, kullanımdan, başkalarıyla paylaşılmasından, değiştirilmesinden, zarar verilmesinden ve yok edilmesinden korunmasıdır (Yurtsever;2013).

Şirketin bilgi güvenliği risklerini azaltmak bakımından öncelikle tutarlı bir politika geliştirmesi önemlidir. Ayrıca, şirketin sahip olduğu bilgi varlıklarının dökümü oluşturulmalı ve her bir bilgi türü için bir sorumlu atanmalıdır. Bilgi güvenliğinin şirket bünyesinde bir veya bir kaç çalışanın sorumluluğunda olan bir konu olarak değil, tüm personelin içinde bulunduğu bir yaklaşımla ele alınması gereklidir (Yurtsever,2013).

Pek çok kurumda, hem bilgi sistemleri hem de iç denetim işlevleri bilgi güvenliği kapsamında yer alır. Tüm önemli bilgiler için bilgi güvenliğinin sağlanması işletme yönetiminin sorumluluğundadır. İç denetim ise bilgi güvenliğinin sağlanmasındaki riskleri değerlendirir. İç denetim yöneticisinin bilgi güvenliği konusundaki iç ve dış riskleri analiz etmek üzere yeterli denetim kaynağına sahip olması sağlanmalıdır (Kocameşe,2010). Çünkü iç denetim, kurumlarda mali raporlama sisteminin güvenilirliği, yasa ve düzenlemelere uygunluk, faaliyetlerin ekonomikliği, etkinliği ve verimliliği, bilgi sistemlerinin güvenliği ve güvenilirliği için vazgeçilmez faaliyetlerden biri olarak kabul edilir (Uzun,2013). İç denetim ve bilgi güvenliği arasındaki ilişkinin önemi ve değerine rağmen, bu iki işlevin bir arada nasıl çalıştığını inceleyen çok az deneysel çalışma bulunmaktadır.

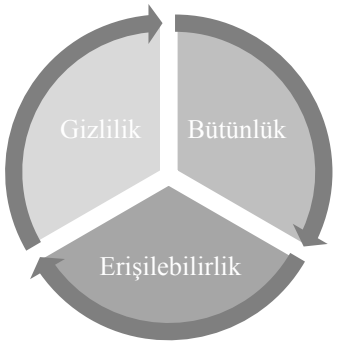
Bu nedenle çalışmamız aşağıdaki gibi tasarlanmıştır. Bilgi güvenliği ve iç denetim işlevleri kavramsal olarak irdelendikten sonra; literatür incelenerek, kurumların düşük maliyetli bilgi güvenliğini sağlamasına yardımcı olmak üzere, bu iki işlevin nasıl birlikte çalışmaları gerektiği üzerinde durulacaktır. Son bölümde yapılandırılmış görüşme sonucu katılımcılardan elde edilen

bulgular ortaya konmakta ve bunların ışığında geleceğe ilişkin bir takım önermelere yer verilmektedir.

1. Bilgi Güvenliği

Kurumların değerleri, sahip oldukları bilgi ile ölçülmektedir. Bilgi, sadece bilgi teknolojileriyle işlenen bir varlık olarak düşünülmemelidir. Bilgi bir kurum bünyesinde çok değişik yapılarda bulunabilmektedir. Dolayısıyla, bilgi güvenliğini sadece bilgi sistemlerinin güvenliği olarak değerlendirmemek gerekmektedir. Zira bilgi sadece sistemlerde bulunmamakta çeşitli ortamlarda yer almaktadır (Doğantimur,2009:6). Bilgi güvenliği yalnızca bir kurumun fiziksel kaynaklarını korumak için değil, aynı zamanda mali nitelikteki belgelerini ve raporlarının güvenilirliğini sağlamak için de gereklidir (AICPA ve CICA,2008). Kurumlar için her ortamda bulunan bir varlığın korunması ve güvenliğinin sağlanması büyük bir öneme sahiptir.

Bilgi güvenliği; En genel tanımıyla bilginin, üretim ve hizmet sürekliliğini sağlamak, parasal kayıpları en aza indirmek üzere tehlike ve tehdit alanlarından korunmasıdır (Kaya Bengshir,2008). Bilgi güvenliği; bilgi varlıklarının ortamdaki tehditlerden, zarar görmeden kullanılabilmesidir. Teknolojinin her getirdiği yenilik aynı zamanda bir zayıflık ve saldırı açığı olarak karşımıza çıkabilmektedir. Bilgi güvenliği, Bilgi Güvenliği Derneği tarafından; bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda bilginin saklanması, göndericisinden alıcısına kadar gizlilik içerisinde (mahremiyeti korunarak), bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci olarak tanımlanmaktadır (http://www.bilgiguvenligi.org.tr). Bilgi güvenliği, korunan bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sürekli olarak sağlanması şeklinde ifade edilebilir. Tanım içerisinde geçen gizlilik, bütünlük ve erişilebilirlik Şekil 1'de de gösterildiği üzere bilgi güvenliğinin temel unsurları olarak değerlendirilebilir. **Gizlilik** (Confidentiality); Bilginin yetkisiz kişilerce erişilememesidir. **Bütünlük** (Integrity); Bilginin doğruluğunun ve tamlılığının sağlanmasıdır. Bilginin içeriğinin değiştirilmemiş ve hiçbir bölümünün silinmemiş ya da yok edilmemiş olmasıdır. **Erişilebilirlik** (Availability) ise; bilginin bilgiye erişim yetkisi olanlar tarafından istenildiği anda ulaşılabilir, kullanılabilir olmasıdır (Doğantimur,2009:7).



Şekil 1: Bilgi Güvenliğinin Temel Unsurları

Bu üç temel unsur birbirinden bağımsız olarak düşünülemez. Bilginin gizliliğinin sağlanması o bilginin erişilebilirliğini engellememelidir. Aynı zamanda erişilebilen bilginin bütünlüğünün de sağlanması önemlidir. Eğer bir bilgi için sadece gizlilik sağlanılıyor ve bilgiye erişim engelleniyor ise kullanılamaz durumda olan bu bilgi bir değer ifade etmeyecektir. Eğer erişimi sağlanıyor ancak bütünlüğü sağlanmıyor ise kurumlar ve kişiler için yanlış veya eksik bilgi söz

konusu olacak ve olumsuz sonuçlara neden olabilecektir. Dolayısıyla tam olarak bir bilgi güvenliği kavramından bahsedilebilmesi içinbu üç unsurun bir arada sağlanması gerekmektedir (Doğantimur,2009:7). Bu unsurlara ek olarak bilgi güvenliği prensipleri arasında güncellik, açıklanabilirlik, süreklilik, izlenebilirlik, kimlik sınaması, inkâr edememe ve güvenilirlik gibi özellikleri de yer almaktadır (Kaya Bengshir,2008).

COBIT; uygun maliyetli bir bilgi güvenliği programı oluşturma ve uygulamanın yönetimin sorumluluklarından biri olduğunu vurgulamaktadır (ITGI 2007). Literatürde bilgi güvenliği yönetimi ve boyutları üzerine pek çok araştırma yapılmıştır.

Bunları özetleyeci bir biçimde incelediğimizde Dlamini ve arkadaşları, çalışmalarında bilgi güvenliğinin dünü, bugünü ve geleceği hakkında bilgi verirken, bilgi güvenliğinin geleceğinin stratejik yönetişim seviyesine çıkarılmasını önermişlerdir (Dlamini ve diğerleri,2009:1-10). Posthumus, bilgi güvenliği ile kurumsal yönetişimin bilgi güvenliği yönetişim çerçevesi aracılığıyla birleştirilmesini önermiştir (Posthumus,2004:638-646). Solms, bilgi güvenliği konusunda COBIT ve ISO 17799 metodolojilerini karşılaştırmış, her iki metodolojinin birbirlerini tamamlayan yönlerini göstermiştir (Solms,2005:99-104). Solms diğer bir çalışmasında, bilgi güvenliğinin operasyonel yönetimi ve bilgi güvenliği uygunluk yönetimi adlı iki boyutundan söz etmektedir (Solms,2005:443-446). Yine Solms'un, bilgi güvenliği yönetişim modeli üzerine yaptıkları çalışmada, tüm organizasyonel seviyelerde yönlendir, yürüt ve kontrol et işlevleri için yapılması gerekenler belirtilmiştir (Solms ve Solms,2006:408-412).

Bilgi güvenliği özetle; bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, üçüncü kişiler tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi sürecidir. Kurumsal bilgi güvenliği ise, kurumların bilgi varlıklarının tespit edilerek zaafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınmasıdır (Vural ve Sağıroğlu, 2008).

Kurumsal bilgi güvenliği insan faktörü, eğitim, teknoloji gibi birçok faktörün etki ettiği tek bir çatı altında yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır. Literatür incelemesinde de görülüyorki yapılan çalışmaların pek çoğu bilgi güvenliğindeki yatırımların değerini ölçmeye odaklanmıştır. Bunun dışında bilgi güvenliği girişimleri ve meseleleri ve borsa tepkisinin analizi ile nihai kullanıcının, kurumun bilgi güvenliği politikalarına uyumunu geliştirme yolları incelenmiştir (Gordon ve diğerleri, 2002/2003/2010; Çavusoglu ve diğerleri, 2004a/2004b; Iheagwara, 2004;Bodin ve diğerleri, 2005/2008; Campbell ve diğerleri, 2003; D'Arcy ve diğerleri, 2009;Bulgurcu ve diğerleri, 2010;Johnston ve Warkentin, 2010;Siponen ve Vance, 2010; Spears ve Barki, 2010;Kumar ve diğerleri,2008; Ito ve diğerleri,2010).

Mishra ve Dhillon'un yaptığı bir çalışmada; bilgi güvenliği konusunda yapılan çalışmalarda ve yapılan tanımlarda "bireysel aktörlerin ve insanların yönetimiyle ilgili konuların kurum içerisindeki rolü"nün ihmal edildiğini belirtmişlerdir (Mishra ve Dhillon,2006). Özellikle, Uluslararası İç Denetim Enstitüsü tarafından yapılan araştırmalar da, iç denetim ve bilgi güvenliği uygulamalarının ortaklık yaklaşımı içinde ele alınması gerekliliği açıkça ortaya konmaktadır (Phelps ve Milne, 2008). Yapılan araştırmaların geneli incelendiğinde iç denetim ile bilgi güvenliği arasındaki ilişkiye gereken önemin verilmediği ve bu konularda yapılan çalışmaların yetersizliği açıkça görülmektedir.

2. İç Denetim

Uluslararası İç Denetçiler Enstitüsü tarafından yapılan tanımıyla iç denetim; bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. İç denetim, kurumun risk yönetim, kontrol ve kurumsal yönetim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur (The IIA,2013).

İç denetim; risk ve kontrol değerleme faaliyetlerine destek sağlar, işletme faaliyetlerini izler, faaliyetlere ilişkin risk ve kontrol faaliyetleri ile ilgili önerilerde bulunur, kontrollerin uygunluğunu ve etkinliğini test eder. Bu işlev ve kapsam özellikleri ile iç denetim; şirket ve kurumlarda mali raporlama sisteminin güvenilirliği, yasa ve düzenlemelere uygunluk, faaliyetlerin ekonomikliği, etkinliği ve verimliliği, bilgi sistemlerinin güvenliği ve güvenilirliği için vazgeçilmez, olmazsa olmaz faaliyetlerden biri olarak kabul edilir. İç denetim, kurumlarda yönetsel hesap verebilirliğin yerleşmesine çok büyük katkı sağlamaktadır. Risk yönetiminin bir parçası olarak önleyici niteliği bulunmaktadır. Kurumsal yönetim kalitesini geliştirir, kurumsal değeri yükseltir. Pay ve menfaat sahipleri için güvence sağlar. (Uzun,2013).

Uluslararası iç denetim standartlarına göre; iç denetim faaliyeti bağımsız olmalı ve iç denetçiler görevlerini yaparken tarafsız davranmalıdırlar. İç denetçilerin daha önce sorumlusu olduğu faaliyetlere ilişkin en az bir yıl süre geçmeden değerlendirme yapmaması tarafsızlığının bir gereğidir. İç denetçiler, çalışmalarını serbest ve tarafsız bir şekilde yapabildiklerinde bağımsız sayılırlar. İç denetçiler her türlü bilgi ve belgeye erişebilmeli, inceleyebilmeli ve her seviyede çalışan ile görüşebilmelidir. İç denetim yöneticisinin, kurum içinde, iç denetim faaliyetinin sorumluluklarını yerine getirmesine imkân sağlayan bir yönetim kademesine bağlı olması ve bu kademe tarafından desteklenmesi gerekir (Uzun,2013).

Yönetim, iç denetimi bilgi güvenliğine yönelen mevcut tehditler konusunda uygun şekilde bilgilendirmelidir. İç denetim, geçmiş ve gelecekteki saldırılara karşı etkinliği ölçerek değerlendirmelidir. Konuyla ilgili yönetici birimler uygun şekilde bilgilendirilmelidir. İç denetçiler aynı zamanda bilgi güvenliği uygulamalarını belirli aralıklarla değerlendirmelidirler. Bu değerlendirmelere istinaden yeni veya geliştirilmiş kontroller önerilir ve denetim sonuçlarıyla ilgili raporlar düzenlenir (Kocameşe,2010).

İşletme yönetimi bilgi güvenliği altyapısını oluşturarak ve gözlemleyerek kişisel bilgilerin güvenliğinin sağlanmasından birinci derece sorumludur. İç denetçiler mevcut yapıyı değerlendirir, riskleri tanımlar ve düzeltici öneriler geliştirir. Bunu yaparken iç denetçilerin kanunları, düzenlemeleri, uygulamaları, hukuk biriminin görüşlerini ve IT bölümünün güvenlik uygulamalarını değerlendirmesi gerekir. İç denetçinin bu süreçteki rolü, programın yürütülmesi, risklerin ortaya konması ve denetim çalışmalarını kapsayabilir. Ancak faaliyetle ilgili sorumluluk yüklenilmesi bağımsızlığa zarar verebilir (Kocameşe,2010).

İç denetim ve bilgi güvenliği arasındaki işbirliği seviyesi, kurumun bilgi teknolojileri ile ilgili iç kontrol gereksinimlerine uygunluk seviyesiyle yakından ilgilidir (Wallace ve diğ, 2011:185-212). Yapılan araştırmalara bakıldığında dikkati çeken bir konu ise İç denetim ve bilgi güvenliği arasındaki ilişkiyi konu alan araştırma sayısının nerdeyse hiç denecek kadar az olmasıdır.

3. Kurumsal Bilgi Güvenliği ve İç Denetim İlişkisi

Kurumsal bilgi güvenliği, bilginin üretildiği, işlendiği ve saklandığı her ortamda sağlanmak zorundadır. Bunun için mevcut yazılımlar, donanımlar, ortamlar ve insan kaynakları dikkate

alınmalıdır (Barrett,2003:56-58). Yapılan çalışmalarda bilgi güvenliğinin henüz doğru olarak anlaşılmadığı, gereken önemin verilmediği ve bilinçlenmenin gereken seviyede olmadığı görülmektedir (Barrett,2003:Arce,2003:Dodge ve diğerleri,2007).

Kurumlar, bilgi güvenliğinde istenen düzeye ulaşmak için pek çok araç ve yöntem kullanmaktadır. Bilgi güvenliğine yönelik önlemleri Şekil 2'de de gösterildiği gibi üç ana başlık altında toplamak mümkündür (Doğantimur,2007:22; Kaya Bensghir,2008).

Şekil 2: Bilgi Güvenliğine Yönelik Önlemler

a.Yönetsel Önlemler: Güvenlik yönetimi ile ilgili bir dizi kuralın ortaya koyulması ve uygulanması şeklinde özetlenebilir. Bilgi güvenliğinin yönetiminde başarı; iyi bir planlama ve üst düzey politikaların doğru ve tutarlı bir şekilde belirlenmesi ile elde edilebilir. Üst yönetimin desteği olmadan, kurumsal tabanda bir işi gerçekleştirmek zordur. Bu nedenle üst yönetim ile güvenlik yönetimi arasında açık bir iletişim kanalı kurulmalı ve çift taraflı, kusursuz bir bilgi akışı sağlanmalıdır. Böylece, yürütülen güvenlik yönetim programı üst yönetimden ihtiyacı olan desteği alır, üst yönetim de gerektiğinde devreye girerek gerekli stratejik kararları verir. Yönetsel önlemler kapsamında yapılması gereken temel işlemler aşağıdaki başlıklar altında toplanabilir (Bilişim Güvenliği, 2003):

a) Risk Yönetimi
b) Güvenlik Politikaları
c) Standartlar, Yönergeler ve Prosedürler
d) Güvenlik Denetimleri

b. Teknolojik Uygulamalar: Bilgi güvenliğine ilişkin kurumsal bir politika oluştururken bilgi ve iletişim teknolojilerinde gözlenen gelişmelerin ne olduğunu ve ne yönde olacağını doğru anlamak ve içeriğini doğru belirlemek ve takibini yapmak son derece önemlidir. Elektronik ortamdaki bilgilerin saklanması kurumsal bilgi güvenliğinin önemli bir kısmını oluşturmaktadır. Elektronik ortamdaki bilgilerin korunabilmesi için gerekli teknolojik önlemlerin alınması şarttır (Doğantimur,2007:32). Elektronik ortamdaki bilgilerin korunabilmesi için kullanılabilecek bazı teknolojik önlemler şunlardır (Kaya Bensghir,2008);

a) Kriptografi
b) Sayısal İmza
c) PKI (Açık Anahtar Altyapısı)
d) Ağ Bölümlendirmesi
e) Güvenlik Duvarları
f) Yedekleme
g) Saldırı Tespiti
h) Erişim Denetimi
i) Anti-Virüs Sistemleri

c. Eğitim ve Farkındalık Oluşturma: Bilgi güvenliğini sağlamaya çalışırken alınacak önlemler ne olursa olsun, eğer insan faktörü göz ardı edilirse alınan hiçbir önlem istenilen sonucu vermeyecektir. Çünkü bilgi güvenliği bilinci ve farkındalığı olmayan insanlar bu güvenlik sürecini aksatacaktır. Bilgi güvenliğini sağlamak için çalışanların, bilgi güvenliği konusunda eğitimi şarttır. Bu eğitimle, bilginin, nasıl korunacağı ve neden korunması gerektiğini

öğretmelidir. Çalışanlar tarafından, hatalı davranışlarının kurum bilgi güvenliği üzerinde yaratabileceği etki iyice anlaşılmalıdır. Eğitimin temel amacı, çalışanları kurumsal bilgi güvenliği hususundaki görev ve sorumlulukları hakkında bilinçlendirmek, güvenlik ve güvenlik kontrollerinin önemi hakkında kollektif bir bilinç oluşturmak olmalıdır. Çalışanların bilgiyi ve bilgi kaynaklarını koruma konusunda üzerlerine düşen sorumlulukları anlaması kritik öneme sahiptir (Doğantimur, 2007:40).

Kurumsal bilgi güvenliği yönetim, teknoloji ve eğitim üçgeninde devamlılık gerektiren ve yönetilmesi zorunlu olan canlı bir süreçtir. Bu üç unsur arasında tamamlayıcılık olmadığı sürece etkin bir güvenlikten bahsedebilmenin mümkün olamayacağı kaçınılmaz bir gerçektir. (Vural,2007).

Yukarıda bahsedilen önlemlerin alınması tek başına yeterli değildir. Bu üç önlem türünün her biri, başarıya ulaşmak için diğer iki önlem türü ile tam ve eksiksiz çalışmalıdır. Bu üç önlem türü birbirileri ile ayrılmaz ve sıkı bağlara sahiptir. Bir kurumun bilgi güvenliği bu üç önlem türünün birlikte çalışmasıyla sağlanabilmektedir. Her kurum bir güvenlik politikası oluşturmalı, bunu yazılı olarak raporlayarak, çalışanlarına, paydaşlarına aktarmalıdır. BIT Standartları benimsenmeli ve tüm uygulanmalar bu standartlar çerçevesinde yapılmalıdır (Yıldız,2014:62). Mali bilgiler ve raporlama açısından bakıldığında; Ratliff'in çalışmasında da belirttiği üzere, Muhasebe meslek mensupları ve denetçiler kontrolleri temelde üçe ayırmaktadır (Ratliff ve Diğerleri, 1996). Bunlar;

a) ***Önleyici Kontroller:*** Güvenlik duvarları, internet güvenlik sistemleri, saldırı önleme sistemleri, fiziksel ve mantıksal erişim kontrolü, cihaz konfigürasyonu ve şifreleme istenmeyen durumları önlemede en sık kullanılan yöntemlerdir
b) ***Belirleyici Kontroller***: Saldırı tespit sistemleri, zafiyet taraması, penetrasyon testleri ve kayıtlar olası sorun ve güvenlik olaylarını belirlemek için tasarlanmış kontrollere örnek olarak gösterilebilir.
c) ***Doğrulayıcı/Sorunların Çözümüne Yönelik Kontroller***: Acil durum merkezleri, iş sürekliliği yönetimi, yama yönetimi sistemleri ise belirlenen sorunların çözümü için geliştirilen kontrollerin en yaygın kullanılan örneklerindendir.

Bilgi güvenliğiyle ilgili kontrollerini sınıflandırırken Ransbotham ve Mitra yukarıdaki sınıflandırmalara alternatif olarak aşağıdaki yaklaşımı kullanmıştır (Ransbotham ve Mitra ,2009).

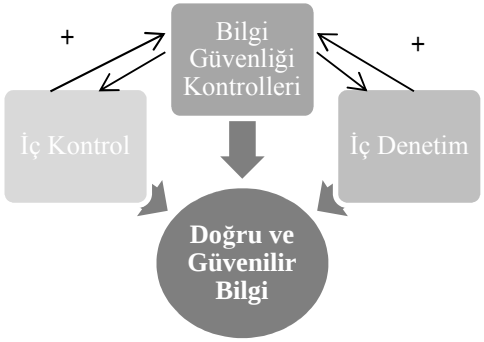
a) ***Konfigürasyon Kontrolleri***, zafiyet taraması, yama yönetim sistemleri gibi saldırganların tespit edip faydalanabileceği zayıf noktaları azaltan yöntemlerin kullanımını kapsar.
b) ***Erişim Kontrolleri*** güvenlik duvarı, saldırı önleme sistemleri, fiziksel erişim kontrolleri, kimlik doğrulama ve erişim izni usulleri gibi saldırganların sisteme izinsiz erişim olasılığını azaltmakta kullanılan araçları kapsar.
c) ***İzleme Kontrolleri***, iyileştirme için gerekli bilgi sağlayan ve problemleri tespit eden belgelendirme ve kayıt analizini kapsar.

Bu kontrollerin uygulanmasında bilgi sistemleri güvenlik işlevinin rolüne vurgu yapmaktadır. Ancak, kurumun iç denetim işlevi bilgi sistemleri güvenliğini de kapsayan iç kontrollerinin etkinliğini periyodik olarak değerlendirmelidir (IIA, 2005 ve ITGI, 2007: CoBiT DS 5.5 ve ME2). Bir şirketi güçlü kılacak en önemli konu sağlam bir bilgi güvenliği alt yapısıdır. Bilgi güvenliği ve sistemleri, işletmelerde kuvvetli bir iç kontrol ortamıyla oluşmaktadır (https://www.kpmg.com/TR/tr/hizmetlerimiz/Audit/irm/Documents/ITGC-yeni.PDF). Bilgi güvenliği kontrollerinin izlenmesi genellikle bilgi işlem departmanları tarafından yerine getirilse

de, iç denetçi tarafından yapılacak inceleme ve gözlemler kuruma ekstra faydalar sağlayabilir (Wallace ve diğerleri, 2011).

Birçok kuruluşta kullanılan geleneksel bilgi güvenlik kontrolleri saldırganları durdurmak için güçlü sınırlar oluşturmayı hedefler. Ancak bu kontroller; ortaklar ve tedarikçilerle karmaşık ilişkiler, sosyal medya ve mobil erişimdeki aşırı artış karşısında yetersiz kalabilir. (http://www.pwc.com.tr/tr_TR/tr/risk-surec-teknoloji-hizmetleri/ic-denetim-ve-kontrol-hizmetleri-yayinlari/ic-denetimin-gelisen-teknolojideki-yeni-rolu-web.pdf).

İç denetimden alınan geribildirimler sayesinde bilgi güvenliği işlemlerinin etkinliği ve etkililiği arttırılabilir. Bilgi güvenliği yöneticileri ile iç denetçiler arasındaki iletişim yeteneği, ilişkinin kalitesini ve ilişkinin sürekliliğini olumlu yönde etkileyecektir. İç denetim ve bilgi güvenliği yöneticileri arasındaki iletişim kopukluğu bu işlevler arasındaki ilişkide olumsuz bir etkiye neden olabilir. Bilgi Teknolojisi sistemlerinin, denetçinin risk konusundaki görüşünü etkileyebilecek ya da farklı bir denetim yaklaşımını benimsemesini gerektirebilecek özellikleri vardır. (http://www.sayistay.gov.tr/yayin/ yayinicerik/75.k5biltekort.pdf). İletişim sorunları; yöneticiler arasında yaşanan anlaşmazlıklardan kaynaklanabileceği gibi, departmanın büyüklüğü, kültürü, kaynakları ve birim başkanının davranışlarındaki farklılıklar örgütsel birimler arasındaki sorunlardan da kaynaklanabilir. Son olarak, üst yönetime erişimdeki farklılıklar da iç denetim ve bilgi güvenliği arasındaki ilişkiyi etkileyebilir. İşletmelerde, iç denetim bölümü önemli görevler üstlenmektedir. Bu bölüm yönetim kuruluna bağlı olarak faaliyet gösterirken iç denetimden gelecek raporlar, üst yönetimin özellikle iç kontrole ilişkin kararlarını etkileyecektir. Örneğin, iç denetim, kullanılmakta olan bilgisayar sisteminin, donanım ve yazılım düzeyinde iç kontrol etkinliğini sağlamada yetersiz kaldığını saptayarak, bunu üst yönetime raporlayabilir. İç denetim tarafından güvenilir bilgi sağlama ihtiyacı karşılanır, iç denetim etkinliği bir anlamda iç kontrol sisteminin etkinliği ile direkt olarak ilişkilidir. İşletmede etkin bir iç kontrol ortamı mevcutsa iç denetimde etkin olacaktır. Böylece işletme hakkında bilgi edinmek isteyen tarafların güvenilir ve doğru bilgiye ulaşmaları kolaylaşacaktır (www.tide.org.tr/uploads/UMUC_2013.doc). Dolayısıyla iç denetimin içinde yer almadığı bir bilgi güvenliği önlemler silsilesi sorunların çözümünde tek başına yetersiz kalacaktır.



Şekil 3: İç Denetim - Bilgi Güvenliği Kontrolleri ilişkisi

4. Araştırmanın Yöntemi

Bu çalışmada, Kurumun bilgi güvenliği ve iç denetim işlevleri arasındaki ideal işbirliği gelişimini engelleyebilecek ya da geliştirebilecek diğer olası unsurları ortaya çıkarmak için Ege Bölgesinde bulunan 2 devlet üniversitesi, 1 özel ve 1 vakıf üniversitesi, 2 yerel yönetim, 2 KİT ve 2 özel şirket olmak üzere toplam 10 kurumda; ortalama beş yıllık deneyime sahip, iç denetim, enformatik, bilgi işlem departmanları (sistemleri) ve güvenliği departmanlarında 20 yönetici

personel ile görüşülmüştür. Görüşmeler hem iç denetim hem de bilgi sistemleri ve güvenliği işlevlerinden sorumlu temsilcilerle gerçekleştirilmiştir. Katılımcılara, bilgi teknolojileri güvenliği ve iç denetim arasındaki ilişkiyi daha iyi anlamaları için görüşme öncesinde çalışmanın amacı hakkında bilgi verilmiştir. Çalışma soruları Paul John Steinbart ve arkadaşlarının 2012 yılında yapmış oldukları "*The relationship between internal audit and information security: An exploratory investigation*" isimli çalışmadan yararlanılarak hazırlanmıştır. Görüşmede kullanılan soru başlıkları özet halinde aşağıdaki gibidir.

Sorular;

- Üst yönetimin güvenliğe karşı tutumu.
- Güvenlikten sorumlu kişi ve Ünvanı, Raporların kime sunduğu.
- Güvenlikte harcanan zaman yüzdesi, Kullanılan güvenlik/BT çerçeveleri
- Yürütmede etken olan yönetmelikler
- BT demografik özellikler, BT personeli sayısı, Güvenlikle ilgilenen BT personeli sayısı, Eğitim düzeyi, Güvenlik sertifikası olan personel sayısı, BT bütçesi, BT güvenlik bütçesi.
- Katılımcıların BT güvenlik personeli ve iç denetim; BT güvenliği personeli ve diğer BT çalışanları arasındaki ilişkiyi nasıl tanımladığı.
- İç denetimçilerin sahip olduğu BT bilgisi seviyesi.
- Denetçinin demografik özellikleri, İç denetimin büyüklüğü, Sahip olunan sertifikalar, İç denetim bütçesi, Denetim bütçesinden BT/BS denetimine ayrılan yüzde.

5. Görüşme Bulguları

Bu bölümde görüşme bulguları, farklı görüşmeler olmasına rağmen elde edilen verilerin ortak olması nedeniyle özetlenerek düzenli bir şekilde verilecektir bu ise bundan sonra yapılacak çalışmalara bir projeksiyon vermesi açısından önemlidir.

Yapılan görüşmelerin sonucuna bakıldığında iç denetçiler ile bilgi güvenliğinden sorumlu uzmanlar arasındaki ilişkiyi etkileyen unsurları katılımcılar; iç denetçinin sahip olduğu kişisel ve mesleki özelliklerin (*teknik bilgi seviyesi, iletişim becerileri ve denetçinin tavrı…gibi*) iç denetim ve bilgi sistemleri güvenliği işlevleri arasındaki ilişkiyi etkilediğini söylemişlerdir. Bu Sonuç daha önce yapılan benzer çalışmaların sonuçları ile örtüşmektedir. Elde edilen bazı sonuçlar aşağıdaki gibidir.

Hem iç denetçiler hem de bilgi sistemleri güvenlik uzmanları, iç denetçinin sahip olduğu yetersiz BT bilgi düzeyinin aralarındaki ilişkiyi olumsuz yönde etkilediğini belirtmişlerdir.

Katılımcılar kişilerin takındıkları tavrın ve iletişim becerilerinin aralarındaki ilişkiyi etkilediğini belirtilmiştir. Yine katılımcılar örgüt yapısının yanında iç denetim ve bilgi işlem departmanlarının fiziksel konumlarının (yakınlık ve uzaklıklarının) iletişimin kalitesini ve sıklığını etkilediğini belirtmişlerdir. Ayrıca daha önce dış kaynak yoluyla iç denetim yaptıran bir özel şirket bilgi işlem yöneticisi, aralarındaki ilişkiyi daha formal ve sadece iş ilişkisi olarak tanımlamıştır.

Hem KİT hemde devlet üniversitesinde çalışan bilgi işlem uzmanları; iç denetçilerin denetim işini teftişe çevirdikleri ve bunun psikolojik baskı oluşturduğunu ve suçlanıp ihbar edileceklerini düşündüklerinden bilgi saklama yoluna gittiklerinden bahsetmişlerdir.

Tüm bunlar, iç denetimin işletme içinde üstlendiği rolün tam olarak diğer departmanlar tarafından anlaşılmadığı takdir de aradaki ilişkinin ve elde edilen bilginin kalitesini daha çok denetçinin özelliklerinin ve denetçinin takınacağı tavrın belirleyeceğini bize göstermektedir.

Üst yönetimin iç denetim ile bilgi güvenliği arasındaki ilişkideki rolüne bakıldığında; yapılan görüşme sonuçları, daha önce yapılan benzer çalışmaların sonuçları ile örtüşmektedir. Özellikli olarak; KİT'lerde, yerel yönetimlerde ve Devlet Üniversitelerinde çalışan bilgi işlem uzmanları ve iç denetçiler; üst yönetimin prensipte bilgi güvenliğini desteklediklerini düşünmediklerini, yapılan yatırımı çok yüksek bulduklarını ve yeterli bütçe ayırmadıklarını belirtmişlerdir. Buna karşın, özel üniversite ve özel şirkette çalışan hem bilgi işlem yöneticileri hem de iç denetçiler, üst yönetim tarafından bilgi güvenliği için gerekli bütçe desteğinin sağlandığını düşünmekte ve bu konuda teşvik edildiklerini söylemektedirler.

İç denetim ve bilgi güvenliği arasında kurulacak yakın ilişkinin kurumlara önemli yararlar sağlayacağı tüm katılımcılar tarafından belirtmişlerdir. Bilgi işlem tarafından bakıldığında iç denetçinin teknik bilgi düzeyinin artırılması şartıyla birlikte iç denetimden elde edilecek geri bildirimlerle bilgi güvenliği uygulamalarının etkinliği ve kalitesinin arttırılabileceği bir gerçektir. İç denetçiler açısından bakıldığında ise iç denetimin rolünün ve sağlayacağı faydaların tüm personel tarafından iyi algılanması ve benimsenmesi halinde bilgi güvenliği için istenilen sonuçlara ulaşılabilecektir.

6. Sonuç

İç denetim ve bilgi güvenliğinden sorumlu departmanlar arasında kurulacak iyi ilişkilerin doğru ve güvenilir bilginin elde edilmesinde önemli bir araç olduğu kesindir. İç denetim sonucunda elde edilecek geribildirimlerin kurumun tüm bilgi sistemleri güvenliğinin etkinliğini arttıracaktır. İç denetim açışından bakıldığında, bilgi güvenliğinden sorumlu departmanlar arasında kurulan iyi ilişkilerin işletmede risk yönetiminin geliştirileceğinden iç denetimin etkinliğini arttıracaktır. Tüm bunların yanında iç denetim standartlarında belirtildiği gibi iç denetimin işlevini etkili bir şekilde yerine getirebilmesi için kurulacak ilişkilerde bağımsızlığın ve tarafsızlığın koruması şarttır. Bilgi güvenliği kontrollerinin düzenli bir şekilde izlenmesi ve sonuçlarının geri bildirimi kurumun bilgi güvenliği etkinliğini arttıracaktır. Bilgi güvenliği kontrollerinin izlenmesi genellikle bilgi işlem departmanları tarafından yerine getirilse de, iç denetçi tarafından yapılacak inceleme ve gözlemler kuruma ekstra faydalar sağlayabilir (Wallace ve diğerleri, 2011).

İç denetim ve bilgi güvenliği arasındaki ilişkinin unsurları tam olarak yerine getirildiğinde işletmelere sağlayacağı faydalar görüşme sonuçlarında da açıkça görülmektedir. Tehdit ve risklerin belirlenerek etkin bir risk yönetiminin sağlanması, kurumsal saygınlığın korunması ve artışı, iş sürekliliğinin sağlanması, bilgi kaynaklarına erişimin denetlenmesi, ilgili tarafların güvenlik konusunda farkındalık düzeyinin yükseltilmesi ve bilgilendirilmesi, bilgi varlıklarının bütünlüğünün ve doğruluğunun sağlanması, personelin bilgi sistemleri kaynaklarını kötü amaçlı olarak kullanma ve/veya kaynakları suistimal etmelerinin engellenmesi, bilgi varlıklarının gizliliğinin korunması, personelin, dış kaynaklı suistimal ve tacizlere karşı zan altında kalmasının engellenmesi ... gibi faydalar bunların arasında sayılabilir. İç denetim ve bilgi güvenliği arasındaki etkileşimin sonucunda yüzde yüz güvenlik ulaşılabilir bir sonuç değildir. İç denetim ve bilgi güvenliği işlevi arasında kurulacak iyi ilişkilerin yanında pek çok faktör bu sonucu etkileyecektir. Kurumsal bilgi güvenliği bir kez gerçekleştirilen bir çalışma olarak değil, bir süreç olarak ele alınmalı ve oluşturulan kurumsal güvenlik politikalarına uygunluk sürekli denetim altında tutulmalıdır (www.erzincan.edu.tr/userfiles/file/stratejidb/guvenlik.ppt). Bundan sonra

yapılacak çalışmalarda iç denetim ve bilgi güvenliği işlevleri arasındaki işbirliğinin farklı düzeyleriyle ele alınması ve bundan elde edilecek sonuçlar bize farklı bir bakış açısı kazandıracaktır.

Kaynakça

AICPA ve CICA, Trust Services Principles And Criteria. American Institute Of Certified Public Accountants And Canadian Institute Of Chartered Accountants, 2008.

Arce, I., The weakest link revisited, IEEE Security & Privacy Magazine, 1(2):72-74, 2003.

Barrett, N., Penetration testing and social engineering: Hacking the weakest link, Information Security Technical Report, 8(4):56-58, 2003.

Bodin, L. D., Gordon, L. A., ve Loeb, M. P., Evaluating Information Security Investments Using The Analytical Hierarchy Process, Communications Of The ACM 2005.

Bodin, L. D., Gordon, L. A., ve Loeb, M. P., Information Security And Risk Management, Communications Of The ACM 2008.

Bulgurcu, B., Çavuşoğlu, H., ve Benbasat, I., Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness, MIS Quarterly 2010.

Campbell, K., Gordon, L. A., Loeb, M. P., ve Zhou, L., The Economic Cost Of Publicly Announced Information Security Breaches: Empirical Evidence From The Stock Market, Journal Of Computer Security 2003.

COSO, Enterprise Risk Management – Integrated Framework: Executive Summary, 2004.

Çavuşoğlu, H., Mishra, B., ve Raghunathan, S., A Model For Evaluating IT Security Investments, Communications Of The ACM 2004a.

Çavuşoğlu, H., Mishra, B., ve Raghunathan, S., The Effect Of Internet Security Breach Announcements On Market Value: Capital Market Reactions For Breached Firms And Internet Security Developers, International Journal Of Electronic Commerce 2004b.

D'Arcy, J., Hovav, A., ve Galletta, D., User Awareness Of Security Countermeasures And Its Impact On Information Systems Misuse: A Deterrence Approach, Information Systems Research 2009.

Dhillon, G., Tejay, G., ve Hong, W., Identifying Governance Dimensions To Evaluate Information Systems Security in Organizations, Proceedings Of The 40th Hawaii International Conference On Systems Sciences, 2007.

Dlamini, M.T., Eloff, J.H.P, Eloff, M.M, Information Security : The Moving Target, Computer & Security, 2009.

Dodge, C. R., Carver, C., Ferguson, J. A., Phishing for User Security Awareness, Computers & Security, 26(1): 73, 2007.

Doğantimur, F., ISO 27001 Standardı Çerçevesinde Kurumsaş Bilgi Güvenliği, TC Maliye Bakanlığı Strateji Geliştirme Başkanlığı Mesleki Yeterlilik Tezi, Ankara 2009.

Gordon, L. A., Loeb, M. P., ve Lucyshyn, W., Information Security Expenditures And Real Options: A Wait And See Approach, Computer Security Journal 2003;XIX: 1-7.

Gordon, L. A., Loeb, M. P., ve Sohail, T., Market Value Of Voluntary Disclosures Concerning Information Security, MIS Quarterly 2010.

Gordon, L. A., ve Loeb, M. P., The Economics Of Security Investment, ACM Transactions On Information And System Security 2002.

http://www.bilgiguvenligi.org.tr

http://www.bsi-turkey.com/BilgiGuvenligi/Genel-bakis/index.xalter

http://www.erzincan.edu.tr/userfiles/file/stratejidb/guvenlik.ppt

http://www.pwc.com.tr/tr_TR/tr/risk-surec-teknoloji-hizmetleri/ic-denetim-ve-kontrol-hizmetleri-yayinlari/ic-denetimin-gelisen-teknolojideki-yeni-rolu-web.pdf

http://www.sayistay.gov.tr/yayin/yayinicerik/75.k5biltekort.pdf

http://www.tdk.gov.tr

https://www.kpmg.com/TR/tr/hizmetlerimiz/Audit/irm/Documents/ITGC-yeni.PDF

https://www.theiia.org

Iheagwara, C., The Effect Of Intrusion Detection Management Methods On The Return On Investment, Computers & Security 2004.

ITGI COBIT 4.1, Control Objectives For Information And Related Technology, IT Governance Institute: Rolling Meadows, IL., 2007.

Ito, K., Kagaya, T., ve Kim, H., Information Security Governance To Enhance Corporate Value, NRI Secure Technologies 2010.

Johnston, A. C., ve Warkentin, M. Fear Appeals And Information Security Behaviors: An Empirical Study. MIS Quarterly 2010.

Kaya Bensghir T., Kurumsal Bilgi Güvenliği Yönetim Süreci, TODAİ Mart 2008.

Kocameşe M., İç Denetim ve Bilgi Güvenliği, http://denetimforumu.blogspot.com/2010/10/ic-denetim-ve-bilgi-guvenligi.html

Kumar, R. L., Park, S., ve Subramaniam, C., Understanding The Value Of Countermeasure Portfolios İn İnformation Security, Journal Of Management Information Systems 2008.

Kurnaz N. Ve Çetinoğlu T., İç Denetim- Güncel Yaklaşımlar, Umuttepe, 2010.

Mishra, S., And Dhillon, G., Information Systems Security Governance Research: A Behavioral Perspective in 1st Annual Symposium On Information Assurance, Academic Track Of 9th Annual NYS Cyber Securityconference, New York, USA , 18-26, 2006.

Phelps, D. And Milne, K., Leveraging IT Controls To Improve IT Operating Performance, The Institute Of Internal Auditors Research Foundation, 2008.

Posthumus, Shaun, A Framework for the Governance of Information Security, Computer & Security,vol 23, 2004.

Ransbotham, S., & Mitra, S., Choice ve Chance: A Conceptual Model Of Paths To Information Security Compromise, Information Systems Research 2009.

Ratliff, R.L., W.A. Wallace, G.E. Sumners, W.G. Mcfarland, ve J.K. Loebbecke, Internal Auditing: Principles And Techniques, 2nd Edition. Altamonte Springs: Institute Of Internal Auditors, 1996.

Siponen, M. ve Vance, A, Neutralization: New Insights into The Problem Of Employee Information Systems Security Policy Violations, MIS Quarterly 2010.

Spears, J. L., ve Barki, H., User Participation in Information Systems Security Risk Management, MIS Quarterly 2010.

Steinbart, P.,J., Raschke, R., L., Gal, G. Ve Dilla, W., N., The relationship between internal audit and information security: An exploratory investigation, International Journal of Accounting Information Systems, Volume 13, Issue 3, September 2012.

Uzun, Ali Kamil, Değer Yaratan Denetim, http://www.denetimnet.com

Uzun, Ali Kamil, İşletmelerde İç Denetim Faaliyetinin Başlatılmasında Başarı Faktörleri, http://www.denetimnet.com

Uzun, Ali Kamil, İşletmelerde İç Denetim Faaliyetinin Rolü ve Katma Değeri, http://www.denetimnet.com

Uzun, Ali Kamil, İşletmelerde İç Kontrol Sistemi, http://www.denetimnet.com

Uzun, Ali Kamil, Kriz Yönetiminde İç Denetim'in Rolü, http://www.icdenetim.net/makaleler/62-kriz-yonetiminde

Uzun, Ali Kamil, Kurumsal Yönetim ve İç Denetimin Rolü, Referans Gazetesi

Uzun, Ali Kamil, Organizasyonlarda İç Denetim Fonksiyonu ve Önemi, Active Bankacılık ve Finans Dergisi, Yıl:1, Sayı:6, Nisan-Mayıs 1999

Von Solms, Basie, Information Security Governance: COBIT or ISO 17799 or Both?, Computer & Security,vol 24, 2005.

Von Solms, Rossouw ve Von Solms, S.H. Bassie, Information Security Governance a Model Based on the Direct-control Cycle, Computer & Security, vol 25, 2006.

Von Solms, S.H. Basie, Corporate Governance and Information Security, Computers & Security, vol 20, 2001.

Von Solms, S.H.Basie, Information Security Governance – Compliance Management vs Operational Management, Computer & Security, vol 24, 2005.

Vural Y., Sağıroğlu Ş., Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir Inceleme, Gazi Üniv. MMF Dergisi, Cilt :23 No: 2, 2008.

Vural, Y., Kurumsal Bilgi Güvenliği ve Sızma Testleri, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 2007.

Wallace, L., Lin, H., And Cefaratti, M. A., Information Security And Sarbanes-Oxley Compliance: An Exploratory Study, Journal Of Information Systems 2011.

Williams, Patricia A.H., In a 'trusting' Environment, Everyone is Responsible for Information Security, Information Security Technical Report, Vol 13, 2008.

Yıldız, Mithat, Siber Suçlar ve Kurum Güvenliği, Denizcilik Uzmanlık Tezi, Kasım 2014.

Yurtsever, G., Bilgi güvenliği İçin Ne Yapmalı? Turcomoney Dergisi, Ocak 2013.