Sosyal Bilimler Dergisi / The Journal of Social Sciences

Akademik Sosyal Araştırmalar Dergisi, Yıl: 6, Sayı: 41, Ekim 2019, s. 153-166
ISSN: 2149-0821 Doi Number:http://dx.doi.org/10.16990/SOBIDER.32706

Dr. Öğr. Üyesi Esin Nesrin CAN
İstanbul Aydın Üniversitesi İİBF İşletme Bölümü, esinn.can@gmail.com
Dr. Cem ÇETİN
Marmara Üniversitesi İç Denetim Birimi Başkanlığı, cem.cetin@marmara.edu.tr

COSO ERM 2017 ÇERVESİNDE KURUMSAL RİSK YÖNETİMİNDE İÇ DENETİMİN ROLÜ

Özet

Organizasyonların amaçlarına ulaşmalarında etkisi yüksek olan riskin yönetimi, zaman içinde "kurumsal risk yönetimi (KRY)" anlayışına dönüşmüştür. COSO'nun, 2004 Risk Çerçevesini revize ederek 2017'de "Strateji ve Performansla Entegre Şekilde-Kurumsal Risk Yönetimi" modeline geçmesi bu bağlamda önemli bir adımdır. Proaktif bir risk bakışı öngören yeni model, iç denetime önemli misyonlar yüklemektedir. Güvence vermenin yanı sıra özellikle dönüşüm sürecinde danışmanlık yapması beklenen süreçte iç denetçi, pozisyonuna ve standartlara uygun bir şekilde faaliyet göstermelidir. Bu bağlamda iç denetçilerin, KRY'nin kuruluşunda uyumlaştırma, tanıtım, eğitim, yönetim koçluğu vb. faaliyetleri gerçekleştirebilirler. Ancak iç denetçilerin; risk iştahı belirleme, yönetim adına risk yanıtlarını uygulama ya da sorumluluğu üstlenme gibi icraî nitelikli davranışlardan kaçınmaları gerekmektedir. KRY'nin yerleştiği organizasyonlarda ise, iç denetçiler güvence verme faaliyetine ağırlık vermelidirler.

Anahtar Kelimeler: İç Denetim, Kurumsal Risk Yönetimi, COSO KRY 2017 Çerçevesi

JEL Kodu: G32, M4, M42

THE ROLE OF INTERNAL AUDIT IN CORPORATE RISK MANAGEMENT AT THE FRAMEWORK OF COSO ERM 2017

Abstract

Risk management, which has a high impact on organizations achieving their goals, has evolved over time into the concept of "Enterprise Risk Management (ERM)". The revision of COSO in the Risk Framework in 2004 and the transition to the Corporate Enterprise Risk Management model integrated with Strategy and Performance in 2017 are an important step in this context. Providing a proactive risk perspective, the new model assigns important tasks to internal audit. In addition to providing assurance, the internal auditor should work in accordance with his / her position and standards, particularly in the process of advising during the transformation process. In this context, internal auditors are responsible for harmonization, promotion, training, management coaching, etc. in the establishment of ERM. However, internal auditors are required to refrain from any executive behavior, such as determining risk appetite, applying risk responses on behalf of management, or assuming responsibility. In organizations where ERM is established, internal auditors should focus on assurance activities.

Keywords: Internal Audit, Entreprise Risk Management, COSO ERM 2017 Framework

JEL Codes: G32, M4, M42

GİRİŞ

Amaçlara ulaşılması üzerinde etkisi olacak bir olayın meydana gelme ihtimali olarak tanımlanan risk kavramı, zaman içinde önemli bir değişim geçirmiştir. Kurumların amaçlarına ulaşmalarını engelleyen riskin yönetimi zamanla işletme risk yönetimine ve ardından da kurumsal risk yönetimi anlayışına evrilmiştir. Konu ile ilgili temel belirleyici aktörlerden olan Committee of Sponsoring Organizations of the Treadway Commission (COSO)'nun yeni risk yönetimi modelini 2017'de "Strateji Ve Performansla Entegre Şekilde-Kurumsal Risk Yönetimi" (ERM 2017) olarak belirlemesi bu bağlamda atılmış önemli bir adımdır. 2004 yılında COSO tarafından yayınlanan "Kurumsal Risk Yönetimi-Bütünleşik Çerçeve", riskin tanımlanması ve değerlendirilmesi açısından başarıyla uygulanmışsa da riskin strateji ve amaçlarla bütünleştirilmesi açısından tatminkâr olamamıştır. Bunun üzerine kuruma daha kapsayıcı şekilde bakabilmek amacıyla Enterprise Risk Management (ERM) 2017 modeline geçiş sağlanmıştır. Yeni modelle kişiye bağlı olmayan, ortak risk algısı ve proaktif bir bakış açısı mümkün olurken, daha düşük maliyet ve yüksek paydaş memnuniyeti sağlanması hedeflenmiştir. Riskler salt bir tehdit olarak değil, aynı zamanda fırsat olarak da algılanabilecek, böylelikle etkili bir stratejik bakış açısı ile iç kontrol ve iç denetim etkinliği sağlanabilecektir (Buluç 2018).

ERM 2017 modeli iç denetime önemli görevler yüklemektedir. İlk olarak güvence verme fonksiyonu bağlamında Kurumsal Risk Yönetimi (KRY) süreci denetlenmeli ve belki bundan daha önemlisi ERM 2017 geçiş sürecinde aktif bir danışmanlık faaliyeti icra edilmelidir. Danışmanlık faaliyetinde iç denetimin durması gereken yer ve kurum içi pozisyonu önemlidir. Bu bağlamda önemli olan iç denetim standartlarından taviz vermeden, icraî faaliyetlerde

bulunmadan davranabilmektir. Bu bağlamda ERM 2017 aşamalarını iç denetimin rolü bağlamında irdelemek gerekmektedir.

1. COSO ERM 2017 ÇERÇEVESİ

COSO, hileli finansal raporlamaların önlenmesi, risk yönetimi, iç kontrol, kurumsal yönetim ve suiistimal önleme ile ilgili konularda rehberler hazırlamak ve bu bağlamda fikri önderlik yapmak amacıyla beş kuruluşun (Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü, Amerikan Muhasebe Birliği, Finansal Yöneticiler Enstitüsü, İç Denetçiler Enstitüsü, Yönetim Muhasebecileri Enstitüsü) desteğiyle 1985'te kurulmuştur (COSO, coso.org 2017)

Genel misyonuna uygun olarak, COSO ilk olarak 2004 Kurumsal Risk Yönetimi - Bütünleşik Çerçeve'yi yayımlamış; bu çerçeve, kuruluşların riski yönetme çabalarında geniş kabul görmüştür. Bununla birlikte, finansal krizler ve skandalların yaşanmasının sonucu olarak, risk kavramının karmaşıklaşması, rekabetin globalleşmesi, dijital dönüşüm vb. yeni risklerin ortaya çıkması, kurumsal risk yönetimi konusundaki farkındalık düzeyinin artması üzerine çerçevenin köklü biçimde güncellenme ihtiyacı ortaya çıkmıştır. Bunun sonucunda da Çerçeve, Haziran 2017'de "COSO Kurumsal Risk Yönetimi Çerçevesi-Strateji ve Performansla Entegre Şekilde" haline gelmiştir. Kısaca bu güncelleme ile aşağıdaki hususların sağlanması hedeflenir (COSO, Enterprise Risk Management Integrating with Strategy and Performance-Executive Summary 2017, iii):

- Strateji oluştururken ve uygularken kurumsal risk yönetiminin değeri hakkında daha fazla bilgi sağlar.
- Performans hedeflerinin belirlenmesini geliştirmek ve riskin performans üzerindeki etkisini anlamak için performans ile kurumsal risk yönetimi arasındaki uyumu arttırır.
- Yönetişim ve gözetim için beklentileri karşılar.
- Piyasaların ve operasyonların küreselleşmesini ve coğrafyalara özel, ortak bir yaklaşım uygulamanın gerekliliğini kabul eder.
- İş karmaşıklığı bağlamında hedefler koyma ve gerçekleştirme riskini görmenin yeni yollarını sunar.
- Daha fazla paydaş şeffaflığı beklentilerini karşılamak için raporlamayı genişletir.
- Karar vermeyi desteklemek için gelişen teknolojilere ve verilerin ve analitiklerin çoğalmasına yardımcı olur.
- Kurumsal risk yönetimi uygulamalarının tasarlanması, uygulanması ve yürütülmesinde yer alan tüm yönetim düzeyleri için temel tanımları, bileşenleri ve ilkeleri belirler ve stratejileri ve karar vermeyi geliştirir.

ERM'de yer alan faaliyetler genel olarak aşağıdaki gibi sıralanabilir (Florea ve Florea 2016, 76-77):

- Organizasyonun amaçlarını ifade etmek ve iletmek,
- Organizasyonun risk iştahını belirlemek,
- Bir risk yönetimi çerçevesi dâhil olmak üzere uygun bir iç ortamı oluşturmak,
- Hedeflerin gerçekleştirilmesine yönelik olası tehditleri belirlemek,
- Riski (ortaya çıkan tehdidin etkisi ve olasılığını) değerlendirmek,
- Risklere verilen yanıtları seçmek ve uygulamak,
- Kontrol ve diğer müdahale faaliyetlerini üstlenmek,
- Organizasyonun her seviyesine risklerle ilgili bilgileri tutarlı bir şekilde iletmek,

- Risk yönetimi süreçlerini ve sonuçlarını merkezi olarak izlemek ve koordine etmek,
- Risklerin yönetiminin etkinliği hakkında güvence sağlamak.

2. ERM 2017'DE İÇ DENETİMİN ROLÜ

Risk yönetiminde üçlü savunma hattı olgusunun iç denetime verdiği rol ERM 2017'de çok daha belirgin olarak işlerlik kazanmıştır. Böylelikle iç denetimin süreçteki asli görevleri, belli şartlarda üstlenebileceği ve üstlenmemesi gereken görevler net olarak ortaya konulmuştur.

İç denetçilerden bazıları organizasyonların ERM yaklaşımında inisiyatif alırlarken, bazıları uyumlaştırıcı rol üstlenirler. Bir kısım iç denetçi ise risk yönetiminin tasarımı ve ERM'nin uygulanması ile ilgili değerlendirmeler yapmakla yetinir. The Institute of Internal Auditors (IIA) Pozisyon Raporu, iç denetimin ERM 2017 ile ilgili faaliyetleri ve bu faaliyetlerin sınırları konusunda yararlı bir rehber niteliğindedir (Anderson 2017, 38-43). Uyumlaştırma, eğitim vb. yoluyla ERM'de daha fazla rol sahibi olan iç denetçiler, IIA Pozisyon Raporu sayesinde yeni COSO ERM çerçevesi ile rol aşımı olmadan faaliyet gösterebileceklerdir (Anderson 2017, 41).

2.1. İç Denetimin Risk Yönetimi Algısı

İç denetim, organizasyonlar için değer oluşturmaya çalıştığından, ilk olarak risk yönetiminin ilkelerini iyi anlamak ve bunları iç denetim uygulamasına dâhil etmek durumundadır. Bu bağlamda her iç denetçi için önerilen bazı adımlar şu şekilde sıralanabilir:

Birincisi, iç denetçiler çerçevenin temellerini tanımak zorundadırlar. İç denetçilerin çoğu iç kontrollerin yeterliliğine odaklanırlar ve iç kontrol sistemini bir risk azaltma yöntemi olarak görürler. Buna karşılık ERM 2017'de "risk" merkezi ve ilk sırada yer almaktadır. İç denetçiler, risk kavramını tanımlayarak, değerlendirmeli; ardından analize tabii tutarak cevaplandırmalı ve son olarak cevaplarını gözden geçirirerek raporlamalıdır. Bu bağlam olmaksızın, iç kontrolleri etkin bir şekilde ele almak mümkün değildir. İkinci olarak, denetçiler iç kontrollerin yeterliliği üzerinde daha az buna karşılık risk üzerinde daha fazla durmak suretiyle yönetimin hedef belirleme ve bunları başarma noktasındaki risklerini azaltabilirler. Ne kadar fazla iç denetçi, bu şekilde davranırsa ve performansı etkileyebilecek olaylar hakkında görüş bildirirse, üst yönetim iç denetimin değer katma fonksiyonunu o kadar iyi anlayacaktır. Yalnız bu noktada dikkat edilmesi gereken iç denetçilerin icrai bir tutum içinde olmamaları ve yalnızca yönetimin hedeflerine ulaşmasına yardımcı olmak için çaba harcadıkları bilincini gözden uzak tutmamalarıdır. Bu rol denetçilerin risk, potansiyel etki ve tepki konuları üzerinde daha fazla yoğunlaşmasını gerektirir. Üçüncüsü, iç denetçiler sadece iç kontrolleri değil, aynı zamanda yönetimin risk tepkilerini de değerlendirmelidir. İç kontroller potansiyel risk yanıtlarından yalnızca birine cevap verir. Dolayısıyla iç denetçilerin, yönetimin bir riski ele almak için en uygun yöntemi seçip seçmediğini değerlendirirken, sadece iç kontrolleri değil, kapsamlı bir risk cevabını dikkate almaları gerekir. Dördüncüsü, iç denetçiler her zaman körü körüne riski azaltmaya odaklanmamalıdır. Risk tepkileri aynı zamanda, performansı artırmak için tasarlanmalıdır. Bu, risklerin tehdit olduğu kadar fırsatta olabileceği gerçeğini içerir. İç denetçiler herhangi bir yönetim kararındaki riskin performansı olumlu etkilediğinden hareketle daha fazla riskin uygun olduğu sonucuna varabilir (Anderson 2017, 43).

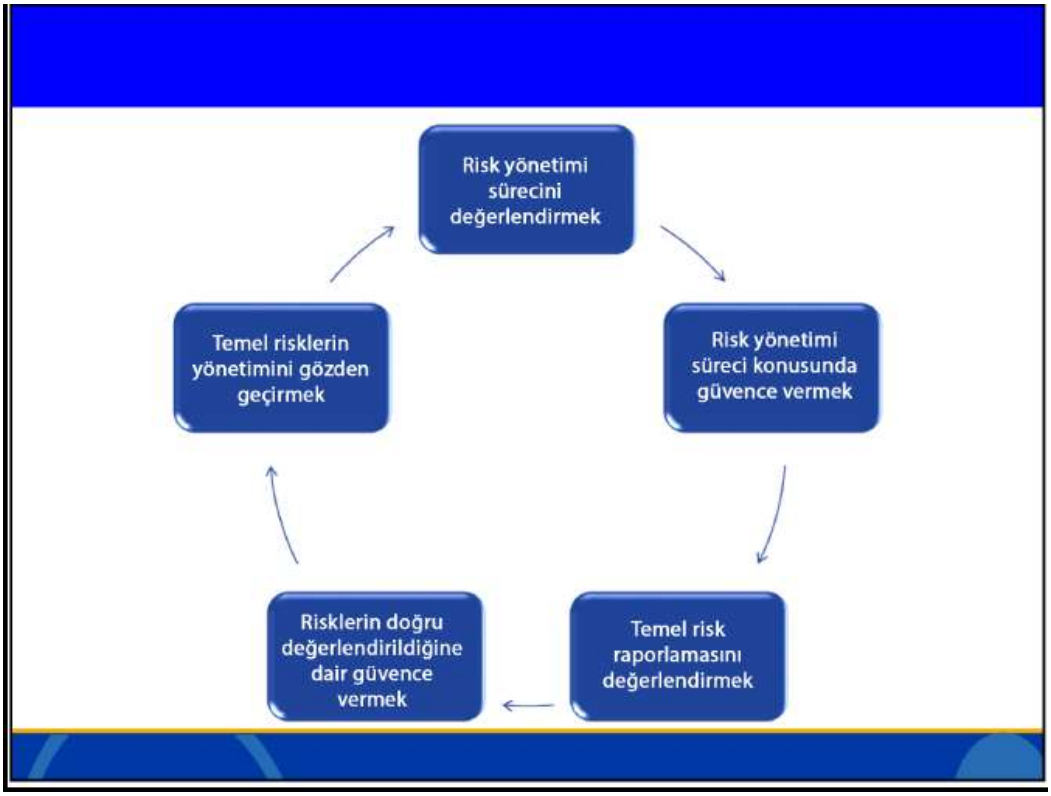
ERM, organizasyonun hedeflerine ulaşılmasını etkileyen fırsat ve tehditleri tespit etmek, değerlendirmek, karar vermek ve raporlamak için tüm kurum genelinde yapılandırılmış, tutarlı ve sürekli bir süreçtir. Bağımsız, objektif bir güvence ve danışmanlık faaliyeti olan iç denetimin

ERM ile ilgili temel rolü, yönetim kuruluna risk yönetiminin etkinliği konusunda nesnel bir güvence sağlamaktır. İç denetimin kuruma değer sağladığı en önemli iki yol, ana iş risklerinin uygun bir şekilde yönetildiğine dair objektif bir güvence sağlamak ve risk yönetimi ile iç kontrol çerçevesinin etkin bir şekilde çalıştığına dair güvence sağlamaktır (Florea ve Florea 2016, 76).

2.2. Uluslararası İç Denetçiler Enstitüsünün Risk Yönetimine Yaklaşımı

Uluslararsı İç Denetçiler Enstitüsünün (IIA) risk yönetimi sürecinde iç denetçiler için biçtiği esas görevler aşağıdaki gibi açıklanabilir (ISACA 2017, 25):

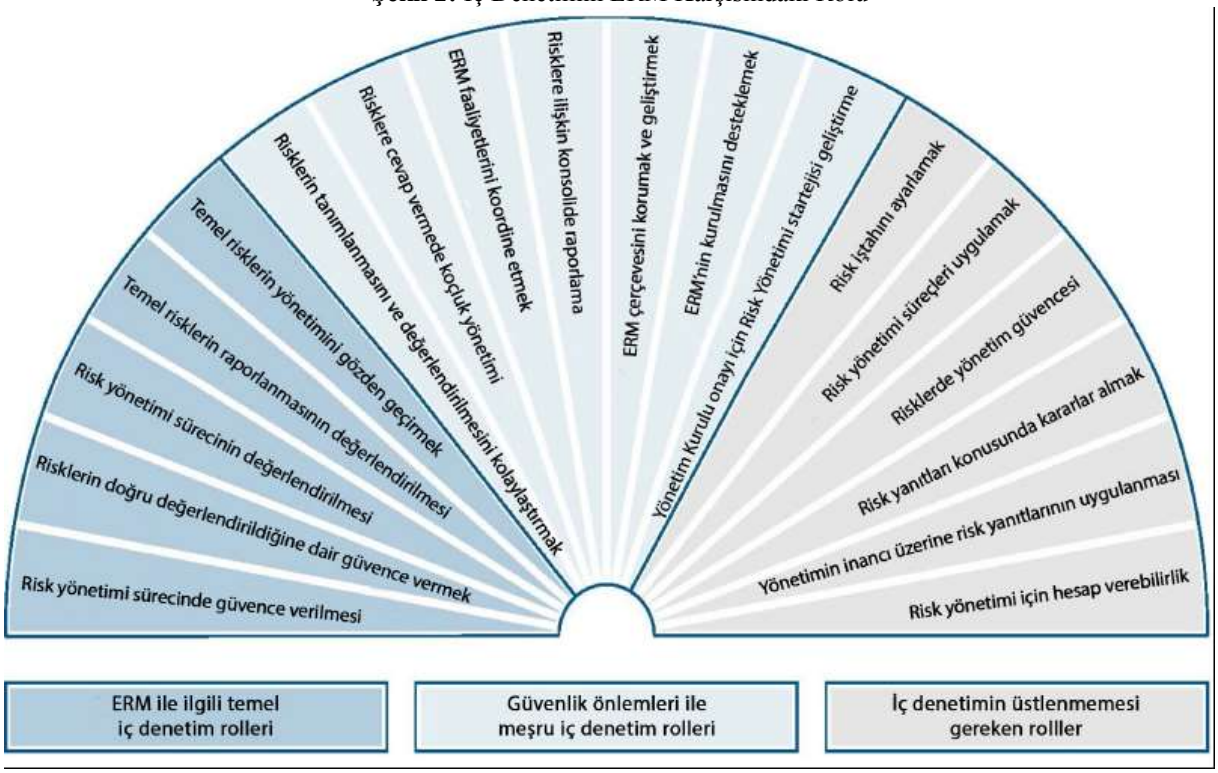
Şekil1: İç Denetimin Çekirdek Rolleri



Kaynak: ISACA, 2017 ERM and Audit-Charlotte-Handout.pdf.

- Risk yönetimi proseslerini değerlendirmek,
- Risk yönetimi prosesi için güvence vermek,
- Temel risklerin raporlanmasını değerlendirmek,
- Risklerin doğru olarak değerlendirildiği ile ilgili güvence vermek,
- Temel risklerin değerlendirilmesini gözden geçirmek

Şekil 2: İç Denetimin ERM Karşısındaki Rolü



Kaynak: Timothy Kimathi, Role of Auditors in Risk Management, 6th July 2017, "Role of Auditors in Risk Management", Management Audit Consulting Ltd., 12.

İç denetçi risk yönetimine üç alanda güvence sağlar. Bunlar:

- Risk yönetimi süreçlerinin tasarımlarının ve etkililiklerinin değerlendirilmesi,
- Kontrollerin etkinliği ve "kilit" olarak sınıflandırılan risklerin yönetimi,
- Risklerin güvenilirlik ve uygunluğunun değerlendirilmesi; risk ve kontrol durumunun raporlanması (Kimathi 2017, 13).

İç denetçiler bir kuruluşun hedeflerine ulaşmasına yalnızca "süreç veya kontrol temelli" bilgisi ile değil aynı zamanda "risk temelli" bilgisini kullanarak da yardımcı olabilir. Ayrıca, risk değerlendirme sürecinde yönetimin kolaylaştırılmasında, kuruluşun karşılaştığı kilit riskleri konsolide etmede, ERM'nin değerlendirilmesi ve iç kontrol sistemlerinin iyileştirilmesinde iç denetim kurum için değer sağlayabilir (Lo 2016, 47).

Koruma önlemleri bağlamında iç denetçinin rolleri aşağıda sıralanmıştır (Kimathi 2017, 15):

- Risklerin tanımlanmasının ve değerlendirilmesinin kolaylaştırılması,
- Risklere cevap vermede koçluk yönetimi,
- ERM faaliyetlerini koordine etmek,
- Risk yönetimi üzerinde konsolide raporlama,
- Kurul onayı için risk yönetimi stratejisi hazırlanması,
- ERM kurulumunun desteklenmesi

İç Denetçiler, mesleki kapasitelerine göre, risk yönetimi konusunda danışmanlık hizmeti sağlayabilirler. Ancak risk yönetiminden sorumlu olamazlar. Yönetişim sürecini gözden geçirebilirler, ancak muhasebe işlerine dâhil olamazlar. İç denetçi, yönetim işlevlerinden sorumlu olmamalıdır; bu, esas olarak, yönetim kurulunda oturamayacakları veya şirketin hissedarları olamayacakları anlamına gelir. Bunu yaparlarsa, bu bir öz değerlendirme tehdidi niteliği kazanır ve bağımsızlıkları zedelenebilir. İç denetimin rolü, risklerin tanımlanması ve yönetilmesi sürecini kolaylaştırmaktır. Örneğin iç denetçiler, #wannacry (bir tür teknolojik saldırı) gibi bir şey olduğunda ve iş operasyonlarını tehdit ettiğinde ortaya çıkan riskleri tanımlamaya ve değerlendirmeye yardımcı olabilir. Ayrıca, riske en iyi nasıl yanıt verebilecekleri konusunda yönetim koçluğu yapabilir ve risk yönetimi süreçlerini kolaylaştırmak veya iyileştirmek için danışmanlık sağlayabilirler (Williams 2017).

İç denetçinin dahil omaması gereken durumlar ise aşağıda sıralanmıştır (Lo 2016, 47)**:**

- Risk iştahını ayarlamak,
- Risk yönetimi süreci uygulamak,
- Yönetimin risklerle ilgili güvencesi,
- Risk yanıtları konusunda karar vermek,
- Yönetim adına risk yanıtlarını uygulamak ve
- Risk yönetiminin sorumluluğu üstlenmek.

Risk yönetiminden yönetim sorumludur. İç denetçinin sorumluluklarının niteliği İç Denetim Yönergesinde belgelenmelidir. Güvence faaliyetlerinin dışındaki herhangi bir çalışma, danışmanlık olarak kabul edilmeli ve danışmanlıkla ilgili uygulama standartlarına uyulmalıdır. Ayrıca iç denetim, değer katma bağlamında aşağıdaki rolleri de üstlenmelidir (Kimathi 2017, 17-18):

- Risk ve risk yönetimi kavramları hakkında denetim komiteleri ve yönetimi eğitmek,
- Risk yönetimi programını yöneten kişiyi desteklemek için daha fazla risk yönetimi danışmanlığı hizmeti yapma fırsatları aramak

Sınırın nerede olduğu, iç denetçilerin değer katabileceği ve sorumluluklarının nerede başlayacağı ve sona ereceği konusunda net olmak gerekir. Roller konusunda belirsizlik yaşayan veya iç denetçilerin sınırları aştığından şüphelenilen organizasyonlar, daha fazla güvence için dış kaynaklı iç denetim danışmanlığı alabilirler. Organizasyonun iç denetçilerin riskleri yönettiğinden ve rol tanımlarının açık olduğundan emin olmak için, iç denetim işlevine yönelik bir kalite güvencesi gözden geçirme (QAR) gerçekleştirmek yararlıdır. Bu birçok önde gelen kuruluş tarafından yürütülen ve işe yaradığı kanıtlanan güvenilir bir süreçtir (Williams 2017).

2.3. İç Denetimin ERM'nin Kuruluşu Aşamasındaki Rolü

İç denetim aşağıdaki durumlara uygun soruları yönelterek ERM'in kurulması sürecinde yardımcı olur (ISACA 2017, 53):

<u>Genel Anlamda Stratejik Risklerin Değerlendirilmesi</u>

- Yönetim stratejik riskler tespit etti mi?
- Yönetim, bu riskleri hafifletmek için sağlam yöntemler geliştirdi mi?
- Yönetim, bir felaketten önce stratejik riskleri tespit etmek için izleme yaptı mı?

<u>Stratejik Risklerin "Gemiyi Batırıyor Olması" Halinde</u>

- İç denetimin strateji incelemesinde oynayabileceği rol nedir?

- Risk yönetimi, stratejide yer aldı mı?

Verilerin Paylaşımı Noktasında

- Denetim raporları ve yıllık risk değerlendirmesi yapılması.
- İş birimlerinden elde edilen bilgilerin değerlendirilmesi

"Kuruluş aşamasında denetim ne yapabilir?" sorusu irdelenecek olunursa (ISACA 2017, 56)**:**

Eğitmen: İç denetim başkanı, üst düzey yöneticilerin ERM'yi anlamalarına yardımcı olabilir.

Kolaylaştırıcı: Risk değerlendirmeleri gereklidir ve iç denetçi bunu sürekli yapar.

Koordinatör: Kuruluş genelindeki iş/görev dağıtımının tutarlılığnı değerlendirir.

Entegratör: Risk verilerinin toplanması, maruziyet ve denetim sonuçlarının raporlanmasına yardımcı olur.

Değerlendirici: ERM'nin etkinliğini gözden geçirir.

İç Denetimin ERM'nin kuruluş sürecindeki rollerine ilişki yol haritası aşağıdaki gibi olabilir (KPMG, 20 key risks to consider by Internal Audit before 2020 - KPMG 2017)**:**

- Bütünleşik ve organizasyon çapında risk değerlendirmesini kolaylaştırmak için ikinci savunma hattına yardımcı olun.
- Ortak risk dilinin tutarlı kullanımına ve kurumsal kilit risklerin anlaşılmasının kolaylaştırılmasına yönelik eğitim yapın.
- Büyük stratejik girişimlerle ilgili olarak organizasyonun, risk değerlendirme süreçlerini ve bu girişimlerle ilgili değişimi nasıl yönettiğini değerlendirin.
- Faydaları görünür kılmak amacıyla küçük risk alt grupları için sürekli risk değerlendirmeleri yapın.

"Üç Savunma Hattının" mevcut kurgusunu, iç denetimin ikinci savunma hattı içerisinde varlığını artıp artıramayacağını ve ortaya çıkan riskin belirlenmesine yardımcı olup olmadığını değerlendirin (KPMG, 20 key risks to consider by Internal Audit before 2020 - KPMG 2017, 22).

Yönetimden gelen yeni taleplerle birlikte bir iç denetçinin rolü, kontrol odağı danışmanlığından, örgüt hedeflerini destekleyen, riskleri izleyen ve iç kontrol çerçevesinin etkinliğini sağlayarak değer üreten bir danışmanlığa dönüşür. Bu bağlamda iç denetçiler, söz konusu faaliyetlerin bağımsızlıklarını ve tarafsızlıklarını etkileyip etkilemeyeceğini değerlendirmelidirler (Lo 2016, 46).

Bu bağlamda bir danışmanlık yapabilmek için iç denetçinin aşağıdaki donanımlara sahip olması gerekir (KPMG, 20 key risks to consider by Internal Audit before 2020 - KPMG 2017, 22**:**

- Risk yönetimi çerçeveleri uzman bilgisi (COSO ERM Integrated Framework, ISO 31000 vb.).
- Kuruluşun risk iştahı ve risk yönetimi süreçlerini iyi anlamak.

- Risk yönetim sistemlerini gözden geçirme de dâhil olmak üzere kurumsal risk yönetimi çerçevesinin bağımsız değerlendirmesinde en üst düzeyde çaba harcama.
- Kilit risklerin kurum tarafından etkili bir şekilde yönetilip yönetilmediğini ve hafifletici kontrollerin uygulanmasının gerçekleştirilip gerçekleştirilemeyeceğini değerlendirebilme.

Risk kültürü farkındalık seviyesini değerlendirebilme (KPMG, 20 key risks to consider by Internal Audit before 2020 - KPMG 2017, 22).

ERM'nin organizasyona tanıtılması sürecinin ilk aşamalarında, iç denetçiler yönetişim ve risk yönetimi süreçlerine ilişkin danışmanlıklarını bir proje yöneticisi rolüyle verebilirler. Buna karşılık organizsyonda risk yönetim anlayışının yerleşmesinin ardından iç denetçiler güvence rollerine geri dönmelidir. Güvence ve danışmanlık faaliyetlerinin tamamı için şu hususların her zaman gözününe alınması gerekir (Lo 2016, 47):

- Yönetim, risk yönetim sisteminden sorumlu olmaya devam eder,
- İç denetçinin sorumlulukları, çalışma planı ve sorumlu ekipler uygun şekilde belgelendirilmelidir,
- İç denetim, yönetim adına riskleri yönetmemeli, bunun yerine yönetime karar vermesinde öneride bulunmalı ve tavsiyede bulunmalıdır,
- İç denetim, sorumlu olduğu ERM çerçevesinin herhangi bir kısmı hakkında güvence veremez.

IIA Pozisyon belgesinde danışmanlık faaliyetleri "risk yönetimi konusunda güvence verme hedefinin bir parçası" olarak belirtilmiştir. Uluslararası İç Denetim Mesleki Uygulama Standartlarına uygun bir iç denetimin bu faaliyetlerin en azından bir kısmını gerçekleştirmesi gerekir. Buna karşılık iç denetim faaliyetlerinin çoğunun bu şiddetle tavsiye edilen rehberlikten mahrum kaldığı anlaşılmaktadır (Florea ve Florea 2016, 76-77).

İç denetçinin ERM'deki danışmanlığının kapsamı, kuruluşun risk olgunluk seviyesine bağlı olacaktır ve zaman içinde değişmesi muhtemeldir. İç denetçinin, riskleri değerlendirme, riskler ve yönetişim ve kolaylaştırma arasındaki bağlantıları anlama konusundaki uzmanlığı, özellikle risk yönetiminin ilk aşamalarında; onu ERM destekçisi ve hatta proje yöneticisi olarak hareket etmeye yöneltebilir. Kuruluşun risk olgunluk seviyesine arttıkça ve risk yönetimi işletme faaliyetlerine daha fazla dahil edildikçe, iç denetimin ERM'yi desteklemedeki rolü azalabilir. Benzer şekilde, eğer bir kuruluş bir risk yönetimi uzmanı veya fonksiyonunun hizmeti satın alıyorsa, iç denetimin, danışmanlık faaliyetinde bulunmak yerine, güvence rolüne odaklanarak değer vermesi daha olasıdır. Bununla birlikte, iç denetim henüz güvence faaliyetleri ile temsil edilen riske dayalı yaklaşımı benimsemediyse, danışmanlık faaliyetlerinde bulunmak için donanımlı olması muhtemel değildir (Florea ve Florea 2016, 76-77).

Öte yandan ERM'nin bizzat kendisinin de, her şeyin risk yönetimi anlayışından hiçbir şeyin risk yönetimine dönüşme, teknik araçların yetersizliği ve aşırı kavramsallaşma risklerinin varlığı gibi bazı riskleri barındırdığı yönündeki eleştiriler söz konusudur (Kıral 2018, 9-11). Bu noktada iç denetçi orgaznizasyon içinde kavram birliği sağlamak ve ERM'nin tanıtımını yapmak suretiyle önemli danışmanlık görevi üstlenebilecektir.

2.4. İç Denetimin ERM'nin İşleyişi Aşamasındaki Rolü

Risk yönetiminden sorumlu yönetim kurulu ve üst düzey yönetimin görevi çeşitli risk yanıtları, süreçleri ve yapıları geliştirmesidir. İç denetimin işlevi ise, kontrollerin yeterli ve etkili olup olmadığına karar vermek amacıyla iç kontrolleri gözden geçirmektir. İç denetçiler risk yönetimi sorumlu olamaz. Yönetim kurulu ve üst düzey yönetim, devredilemeyen bir sorumluluk olan risk yönetimi sürecinin uygulanmasından sorumludur. Viljoen ve Barac, Güney Afrika Hesap Verebilirlik ve Denetim Araştırmaları Dergisi'nde "Risk yönetimi: İç denetim ne yapmalı?" başlıklı makalesinde doğrudan bu konuyu ele almaktadır. Bu bağlamda bir iç denetçinin iki tür rolü vardır: Çekirdek roller ve meşru roller. Çekirdek roller güvence faaliyetleri ile ilgilidir. Kontrollerin çalışıp çalışmadığına, risk yönetimi ve yönetişim süreçleri ilişkin denetim komitesine ve yönetime güvence sağlarlar. Viljoen ve Barac'e göre iç denetim risklerin doğru değerlendirilip değerlendirilmediğinin belirlenmesi ile ilgilir. Bunun için risk yönetimi süreçlerini ve kilit risklerin raporlanmasını değerlendirir (Williams 2017).

Kurum genelinde risk olgunluk düzeyini değerlendirebilmek için iç denetim tarafından geliştirilen denetim programları güncellenmeli ve geliştirilmelidir. Bu bağlamda denetim programları aşağıdakileri içerebilir (PWC 2017, 11):

- ERM liderliğini değerlendirmek,
- Yönetim tarzının etkinliğini; hesap verebilirliği ve yetkilileri değerlendirmek,
- Risk yönetimiyle ilgili kararların performans yönetimiyle ilişkilendirmek,
- Karar verme sürecini gözden geçirerek, riskin sürece gömülü olduğundan emin olmak,
- Risk iştahını belirleme sürecini analize etmek,
- Kurum genelinde risk farkındalığı etkinliklerini gözden geçirmek. İç denetim, kuruma, geleneksel finansal güvenceden örgütsel risk yönetimi modellerine kadar geniş bir katma değerli hizmet yelpazesi sağlayabilir (PWC 2017, 11).

İç Denetim, kurum içinde etkililiğini korumak adına ortaya çıkan iş sorunlarını ve eğilimleri proaktif olarak belirlemelidir. Ortaya çıkan iş trendleri yeni riskler taşır. İç denetçinin bu riskleri ve organizasyon üzerindeki potansiyel etkilerini sürekli izlemesi gerekir. En yüksek katma değeri sağlamak için iç denetçi, ortaya çıkan risklerle karşı karşıya kaldığında hızlı davranmalı ve riski azaltmak, kontrolleri iyileştirmek ve kurum genelinde verimlilik ve maliyet avantajlarını gerçekleştirmek için statükoya meydan okuma fırsatlarını değerlendirilmelidir. Mevcut sorunların ve temel risklerin yönetimi, iç denetçinin katma değer yaratma ve kuruluştaki etkisini en üst düzeye çıkarma yeteneğini artıracaktır (KPMG, The New Head of Internal Audit 2017, 1-19).

İç denetçinin güvence verme görevleri arasında; organizasyonun risk yönetim sürecine ilişkin değerlendirmelerde bulunmak, risklerin tam ve doğru olarak belirlenmesi ve önceliklendirilmesine yönelik güvence vermek; risklere karşı uygulanan kontrol eylemlerinin etkinliği ile risk izleme ve raporlama süreçlerinin yeterliliğini değerlendirmek bulunmaktadır (Ilgar ve Erdoğdu 2018, 73).

ERM'nin etkili olup olmadığının değerlendirilmesinde, iç denetçi aşağıdaki kriterleri baz alır (Lo 2016, 46):

- Organizasyonel hedefler örgütün misyonunu destekler ve bunlarla uyum sağlar,
- Önemli riskler tanımlanır ve değerlendirilir,
- Riskleri, kurumun risk iştahı ile uyumlu hale getiren uygun risk yanıtları seçilir ve

- İlgili risk bilgileri kurum genelinde, personelin, yönetimin ve yönetim kurulunun sorumluluklarını yerine getirmesini sağlayacak şekilde uygun zamanda iletilir

İç denetçi tarafından sağlanan güvencelerin yanı sıra, yönetim, dış denetçi ve hukuk danışmanları gibi diğer kaynaklardan da güvence almalıdır. Kurumsal Yönetişim Kodu altında, yönetim kuruluna risk yönetimi ve iç kontrol sistemlerinin etkinliği konusunda bir onay sağlanmalıdır.

ERM'de meşru iç denetim rolleri genellikle iç denetimin risk yönetimine sağladığı değeri büyük ölçüde artırabilecek danışmanlık faaliyetleri olarak kabul edilir. Konuyla ilgili yapılan anket, iç denetim faaliyetlerinin çoğunun bu değerli rolleri yerine getirmediğini göstermektedir. Sağdaki altı alan, iç denetimin ERM'de üstlenmemesi gereken rollerdir. Çünkü bunlar iç denetim faaliyetinin tarafsızlığını açıkça olumsuz yönde etkileyebilecek yönetim sorumluluklarıdır. Ankete katılanlar için, bu tür rollerde az sayıda iç denetim faaliyetinin ortaya çıkması olumludur (Florea ve Florea 2016, 77).

2.5. ERM'nin İç Denetimin İşleyişine Katkısı

ERM ile iç denetim rasaında iki yönlü bir etkileşim söz konusudur. ERM iç denetime aşağıda belirtilen hususlarda yardımcı olur (ISACA 2017, 55).

- Organizasyonların yüksek riskli alanlarını ele almak için çalışma planını daha iyi şekillendirmek,
- Genel organizasyon riski önceliklerine ilişkin tavsiyelerde bulunmak,
- Planlarındaki boşluklar ("Ya eğer" senaryoları, karşılıklı bağımlılıklar / çapraz örgütsel riskler) konusunda veri sağlamak.

Bu iki yönlü süreçten faydalanabilmek ve iç denetimin, genel ERM'ye dâhil edilmesi için öncelikle kendi "denetim riskini" değerlendirmesi gerekmektedir. Bu bağlamda;

- ERM ile kapsamlı iletişim kurulması,
- Risk Azaltma / Niceleme çalışmalarının tamamlanması,
- Denetim Planının güncellenmesi,

adımları atılmalıdır.

ERM denetimin planlanması sürecine, senkronizasyonu temin etmek suretiyle, çok önemli bir katkı sağlar. İç denetim, mevcut yıl yürütülen risk değerlendirmesi sonucunda organizasyonun gelecek yılı için bir iç denetim planı oluşturur. Ancak, bu durum, organizasyon genelinde sürekli olarak gelişen diğer risk izleme işlevlerini gözardı eder. Bu nedenle organizasyonlar koordineli bir risk tanımlama çalışmasını içeren ve giderek entegre olmuş bir risk anlayışına yönelmişlerdir.

Koordine edilmiş bir çaba sağlamak için, aşağıdaki bileşenlere ihtiyaç vardır (KPMG, 20 key risks to consider by Internal Audit before 2020 - KPMG 2017, 22)**:**

- Problem derecelendirmeyi de içeren ortak bir risk dili,
- Çabaların tekrarlanmasını en aza indiren toplu risk değerlendirme programı,
- Diğer risk ve kontrol fonksiyonlarının katılımına izin veren bir denetim süreci ve
- Uyumlaştırılmış ve tutarlı bir risk raporlama anlayışı.

Bu yaklaşımı, kilit risk ve performans göstergelerini toplamak için teknik yetenekle birleştiren bir iç denetçi, daha dinamik bir planlama kabiliyetine kavuşur. Sürekli bir risk değerlendirme süreci (örneğin, veri kalitesi, veri kullanılabilirliği vb.) bazı zorluklar sunabilir.

Ancak, iç denetimin ve diğer risk ve kontrol gözetim işlevlerinin değerini önemli ölçüde arttırma fırsatı sağlar. Yöneticilerin genel riskleri iyileştirmek, farkındalığı ve çevreyi kontrol etmek ve de bu yaklaşımı kendi uygulamalarına entegre etmeleri için bir fırsatı vardır. Bu sağlandığında iç denetim daha gelişmiş bir izleme seviyesine ve sürekli risk değerlendirme anlayışına evrilebilecektir (KPMG, 20 key risks to consider by Internal Audit before 2020 - KPMG 2017, 22)**.**

Denetim planı sürecinde olduğu gibi sürekli izleme süreci üzerinde de ERM'nin kolaylaştırıcı etkisi vardır. Bu sayede (KPMG, The New Head of Internal Audit 2017, 7-9);

- Bir organizasyon içindeki tüm ilgili fonksiyonları içeren entegre bir risk değerlendirmesini kolaylaştırır.
- Küçük bir risk grubu için sürekli risk değerlendirmesinin faydalarını analiz eder.
- Şirketin risk yönetimi konusundaki yaklaşımını, kurumsal risk değerlendirme sonucu ışığında değerlendirir.
- Stratejik iç denetim planını belirlemek için risk yönetimini kullanmak, kurum genelinde risk yönetimini içine alan ve ortaya çıkan riski proaktif olarak belirleyen ve daha sonra uygun şekilde azaltılabilen etkin bir ERM programı oluşturmaya olanak tanır.

3. MEVCUT DURUM

"Kamu İç Denetim Reform Uygulamalarının Derinleştirilmesi Projesi Kapsamlı Değerlendirme Raporu" KRY'nin mevcut durumuna ilişkin önemli veriler içermektedir. Çalışma kapsamında gerçekleştirilen anket uygulamasına 506 kamu iç denetçisi (toplam kamu iç denetçisinin %56'sı) katılmıştır. Buna göre "iç denetçilerin %61'i kurumlarındaki risk değerlendirme faaliyetlerinin olgunluk seviyesini Düşük/Çok Düşük olarak değerlendirirken; %70'i, kurumlarında yürütülen risk yönetimi çalışmalarını yeterli bulmadıklarını belirtmiştir. Aynı şekilde araştırma kapsamında yer alan iç denetçilerin yalnızca %22'si risk yönetimi süreçlerinin kurulumunda, %25'i de geliştirilmesinde danışmanlık hizmeti vermişler. Araştırma kapsamındaki odak grup toplantılarında ise, mali hizmetler birimi temsilcileri, iç kontrol ve risk yönetimi sistemlerinin geliştirilmesi çalışmalarında iç denetim birimleri ile daha fazla işbirliği geliştirmek istediklerini belirtmişlerdir (İDKK 2018, 4, 5, 22, 29).

Konuyla ilgili değerlendimelerde bulunabileceğimiz bir başka çalışma IIA tarafından gerçekleştirilen North American Pulse 2019 raporudur. Bu çalışma için hazırlanan çevrimiçi anket 500'ün üzerinde kişiye uygulanmıştır. Katılımcıların %85'i Amerika Birleşik Devletleri'nde, % 10'u ise Kanada'da görev yapan iç denetim yöneticileri olup; %31'i halka açık şirketerde, % 19'u ise kamu sektöründe çalışmaktadır. Çalışma sonuçlarına göre; genel olarak iç denetim planınlarının %22,8'i kurumsal risk yönetimi, hile denetimi ve soruşturması, üçüncü taraf ilişkileri, yönetişim ve kültür gibi önemli risk alanlarına ayrılmıştır. Sektörel olarak bakıldığında ise kurumsal risk yönetimine halka açık şirketlerde ait iç denetim planlarında % 4,5; kamu sektörüne ait iç denetim planlarında % 6 oranında süre ayrılmıştır (IIA, 2019 North American Pulse Of Internal Audit - Defining Alignment İn A Dynamic Risk Landscape 2019, 32-35).

SONUÇ

Risk yönetimi, kurumsal yönetimin temel bir unsurudur. Yönetim, risk yönetimi çerçevesinin oluşturulmasından ve işletilmesinden sorumludur. İç denetim ise süreçte güvence vermek ve danışmanlık yapmak suretiye yer alır. Risk yönetiminde üçlü savunma hattı olgusunun iç denetime verdiği rol ERM 2017'de çok daha belirgin olarak işlerlik kazanmıştır. Böylelikle iç denetimin süreçteki asli görevleri, belli şartlarda üstlenebileceği ve üstlenmemesi gereken görevler net olarak ortaya konulmuştur. İç denetçilerden bazıları organizasyonlarının ERM kuruluş sürecinde aktif rol üstlenirken bazıları uyumlaştırıcı olmaya karar verebilirler. Yine bazı iç denetçiler ise risk yönetiminin tasarımı ve ERM'nin uygulanması ile ilgili değerlendirmeler yapmakla yetinirler. IIA Pozisyon Raporu, iç denetimin ERM 2017 ile ilgili faaliyetleri ve bu faaliyetlerin sınırları konusunda yararlı bir rehber niteliğinedir. Uyumlaştırma, eğitim vb. yoluyla ERM'de daha fazla rol sahibi olan iç denetçiler, bu rehber sayesinde yeni COSO ERM çerçevesi ile rol aşımı olmadan faaliyet gösterebileceklerdir. Bununla birlikte, her iç denetçinin farklılık gösteren uygulamalar sergileyecekleri de tartışmasızdır.

Kurumsal çapta risk yönetimi, yapılandırılmış, tutarlı ve koordineli yaklaşımı sayesinde birçok fayda sağlar. İç denetçinin ERM ile ilgili temel rolü, yönetime ve yönetim kuruluna risk yönetiminin etkinliği konusunda güvence sağlamak olmalıdır. İç denetim bu temel rolün ötesine danışmanlık rolü icra edebilir. Bu şekilde, iç denetim bağımsızlığını ve güvence hizmetlerinin nesnelliğini koruyacaktır. Bu sınırlamalar içinde iç denetim, ERM profilinin yükseltilmesine ve iç denetimin etkinliğinin arttırılmasına yardımcı olabilir (Florea ve Florea 2016, 77).

KAYNAKLAR

Anderson, J. Doug. «COSO ERM Getting Risk Management Right.» *Internal Auditor*, 2017: 38-43.

Buluç, Alp. *Haziran 2017 COSO Kurumsal Risk Yönetimi Çerçevesi, Strateji ve Performansla Entegre Şekilde.* 8 Ocak 2018. http://teolupus.com/teo/haziran-2017-coso-kurumsal-risk-yonetimi-cercevesi-strateji-ve-performansla-entegre-sekilde/ (erişildi: Mart 3, 2019).

Florea, Radu, ve Ramona FLOREA. «Internal Audit and Risk Management. ISO 31000 and Erm Approaches.» *Economy Transdisciplinarity Cognition* 19, no. 1 (2016): 72-77.

Ilgar, Tuğçe, ve Görkem ERDOĞDU. «Kurumsal Risk Yönetimi Türk Kamu Yönetimine Nasıl Entegre Edilebilir?» *Denetişim* 8, no. 18 (Eylül/Aralık 2018): 63-76.

İDKK. *Kamu İç Denetim Reform Uygulamalarının Derinleştirilmesi Projesi Kapsamlı Değerlendirme Raporu.* Ankara: İç Denetim Koordinasyon Kurulu, 2018.

Kimathi, Timothy. *Role of Auditors in Risk Management, Management Audit Consulting Ltd., ss.1-19.* 6 7 2017.

Kıral, Halis. «Kurumsal Risk Yönetiminin Riskleri.» *Denetişim* 8, no. 18 (Eylül/Aralık 2018): 5-14.

Lo, Roy. «The Role of Internal Auditors in Enterprise Risk Management.» *Source Risk Manengment*, 7 2016: 46-47.

Williams, George. «Internal Auditors. Where the Boundaries Lie With Enterprise Risk Management, 30 May 2017.» 30 Mayıs 2017. https://www.bdo.co.za/en-za/insights/2017/audit/internal-auditors-where-the-boundaries-lie-with-enterprise-risk-management (erişildi: May 19, 2019).

İnternet Kaynakları

KPMG. «20 key risks to consider by Internal Audit before 2020 - KPMG.» *kpmg.com.* 2017. https://home.kpmg/ch/en/blogs/home/posts/2018/10/20-key-risks-to-consider-by-internal-audit-before-2020.html (erişildi: Mayıs 18, 2019).

—. «The New Head of Internal Audit.» *kpmg.com.* 2017. https://home.kpmg/xx/en/home/services/advisory/risk-consulting/internal-audit-risk.html (erişildi: Mayıs 19, 2019).

ISACA. «2017 ERM and Audit-Charlotte-Handout.» 2017. http://www.isaca.org/chapters3/Charlotte/Events/Documents/Event%20Presentations/04192017/2017%20ERM%20and%20Audit%20-%20Charlotte%20-%20Handout.pdf (erişildi: Mayıs 20, 2019).

COSO. *coso.org.* 2017. https://www.coso.org/Pages/aboutus.aspx (erişildi: Mayıs 25, 2019).

—. «Enterprise Risk Management Integrating with Strategy and Performance-Executive Summary.» *coso.org.* June 2017. https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf (erişildi: Mayıs 26, 2019).

IIA. «2019 North American Pulse Of Internal Audit - Defining Alignment İn A Dynamic Risk Landscape.» *global.theiia.org.* 2019. https://www.theiia.org/centers/aec/Pages/2019-Pulse-of-Internal-Audit.aspx (erişildi: Haziran 1, 2019).

—. «IIA Position Paper – Role of Internal Audit in ERM.» *na.theiia.org.* 2009. https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf (erişildi: Haziran 2, 2019).

—. «The Instıtute of Internal Auditors International Conference, Dubai, UAE, 6-9 May 2018, COSO ERM 2017 – Emerging Trends in Auditing ERM.» *global.theiia.org.* tarih yok. https://global.theiia.org/news/press-releases/Pages/IIAs-2018-International-Conference-in-Dubai-To-Address-Importance-of-Controls-Risk-Management.aspx (erişildi: Haziran 3, 2019).

PWC. «How and When Should You Leverage Internal Audit.» *assets.hcca-info.org.* 28 March 2017. https://assets.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2017/508print2.pdf (erişildi: Haziran 5, 2019).