TONE at the TOP®

Üst yönetim, yönetim kurulları ve denetim komitelerine yönetişim ile ilgili konularda özet bilgiler.

Sayı 93 | Haziran 2019

İç Denetim, İç Denetim ile Risk Yönetimi Arasındaki İnce Çizgide Parmak Uçlarında Yürüyor

İç denetim yöneticileri öteden beri her konuda raporlama yapmaktadır ve bu böyle sürüp gidecektir. Raporlamanın kimlere yapılması gerektiği ise tartışmaya açık bir sorudur.

Bir taraftan, iç denetim yöneticilerinden daha fazlası istenmektedir. Yönetim kuruluna risklerle ilgili bilgiler aktaran güvenilir bir danışman olmaları beklenmektedir. Kurum genelinde risklerin daha iyi analiz edilmesini ve daha iyi anlaşılarak izlenmesini sağlayacak yeni teknolojilerden yararlanmalıdırlar.

Diğer taraftan, yönetim kurulları da baskı altındadır. Yasal düzenleyiciler, hissedarlar, müşteriler, iş ortakları ve diğer tüm paydaşlar riskleri daha iyi yönetmelerini, yalnızca riskleri inceleyerek tolerans seviyelerini belirlemesini değil, her zaman daha hesap verebilir olmalarını istemektedirler.

Risklerin değerlendirilmesi ve risklerin gerçekleşmesi durumları için önleyici tedbirlerin alınması sorumluluklarında daha iyi iş çıkarılması konusunda hem iç denetim yöneticisinden (İDY) hem de yönetim kurulundan daha iyi iş çıkarma beklentileri olmasının ne anlama geldiğini bir düşünün. Bu durumda kurumsal yönetişim, risk güvencesi ve iç denetim yöneticisinin görevleri hakkında tartışmalı sorular gündeme gelecektir.

Örneğin, yönetim kurulu bir risk komitesi kurmalı mıdır? Eğer kurarsa iç denetim yöneticisi (İDY) risk komitesine hangi konuları raporlamalıdır? İDY'nin bazı konuları risk komitesiyle bazılarını ise denetim komitesiyle görüşmesi akıllıca olur mu? İDY'nin rolü bölünmeli midir? Yoksa tersi mi daha doğru olur: Yeni teknolojiler iç denetim ile risk yönetimini birleştirerek daha geniş bir risk güvencesi işlevine mi dönüştürmektedir?

"Australian Broadcasting Corp"ta risk yönetimi başkanı ve Uluslararası Avustralya İç Denetçiler Enstitüsü'nün eski yönetim kurulu üyesi Tom McLeod şu yorumu yapmaktadır: "Biz, meslek mensupları olarak, alanımız konusunda bizim kadar tutkulu olmayanlara risk sahiplenmesinin faydalarını yeteri kadar iyi anlatabildiğimizden emin değilim."

Sonuç olarak da iç denetim yöneticileri kendilerini, kimsenin ummadığı biçimde hem iç denetim hem de risk yönetimi görevlerini üstlenmiş bulabilir. Bu görevlerden ilkinde zaten hep iyiydiler, yeni teknolojiler sayesinde ikincisinde de daha iyi oluyorlar ve zaten birilerinin de risk yönetimi görevlerini üstlenmesi gerekiyor.

McLeod'a göre bu "ağırlıklı olarak risk izleme ile meşgul olana kadar ağırlıklı olarak risk izleme ile meşgul olduğunu fark edemediğin, yavaş adımlarla ilerleyen bir süreçtir."

Bu, iç denetim yöneticileri için olduğu kadar yönetim kurulları için de geçerlidir. Pekâlâ, her iki grubun bu evrimi verimli bir hale getirmesi nasıl mümkün olur?

IIA Hakkında

Institute of Internal Auditors (Uluslararası İç Denetçiler Enstitüsü) 170 ülke ve bölgede 200.000'den fazla üyesi bulunan küresel bir mesleki birliktir. IIA, iç denetim mesleğinin savunucusu, uluslararası standartların düzenleyicisi, baş araştırmacı ve eğiticisidir.

The IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 USA

Ücretsiz Abonelik İçin

www.theiia.org/tone
sitesini ziyaret ediniz.

Okuyucu Görüşleri

tone@theiia.org
adresine görüş ve yorumlarınızı gönderiniz.

İçerik Danışma Kurulu

Üst yönetim ve yönetim kurullarındaki deneyimleriyle birlikte, aşağıda belirtilen saygıdeğer uzmanlar, bu yayının içeriğine doğrudan katkı sağlamaktadırlar.

Martin M. Coyne II
Michele J. Hooper
Kenton J. Sicchitano

Yönetim Kurulu Üzerindeki Baskılardan Başlayın

2018 yılında EY Yönetim Kurulu Konuları Merkezi tarafından yapılan ve Harvard Hukuk Okulunun Kurumsal Yönetişim ve Finansal Düzenleme Forumunda yayımlanan bir araştırmaya göre, S&P 500 firmalarının yönetim kurullarının yalnızca %11'inde bir risk komitesi vardır. Bunların içinde de çoğunluğu, %74'ünde risk komitesi bulunan, finans sektöründeki firmalar oluşturmaktadır. Finans sektörü dışındaki firmalar olan tüketim malları, sanayi, teknoloji ve hizmet sektörleri için ise risk komitesi bulunanların oranı adeta bir serbest düşüşle %4 seviyesinde bulunmaktadır.

Fakat bu sayılar hikayenin tümünü anlatmakta yetersizdir. Örneğin, Federal Reserve (Amerikan Merkez Bankaları Sistemi) aktif büyüklüğü 10 milyar Amerikan Doları veya daha büyük tutarda aktifi olan halka açık bankaların risk komitesi kurmasını zorunlu tutmaktadır ki finans sektöründeki firmaların çoğunda risk komitesi olması bu bakımdan şaşırtıcı değildir.

Bu arada, aynı EY araştırmasının sonuçlarına göre, tüketim ürünleri sektöründeki firmalarının %14'ünde kamu politikası komitesi, %38'inde ise kurumsal sorumluluk komitesi bulunmaktadır. Sağlık sektörü firmalarının ise %21'inde yasal yasal işler komitesi ve %18'inde de teknoloji komitesi bulunmaktadır.

Bu rakamlar akla uygundur. Tüketim ürünleri firmaları iyi birer kurumsal vatandaş olarak algılanmak istediklerinden, pek çoğunda kurumsal sosyal sorumluluk komitesi bulunmaktadır. Sağlık sektöründeki firmalar, özellikle kişisel sağlık bilgileri konusunda, yoğun yasal düzenlemelerle karşı karşıya olduğundan, pek çoğunda yasal düzenleme ve teknoloji komiteleri bulunmaktadır. Firma için önemli olan riskleri takip eden herhangi bir komite bulunuyorsa, bu komitenin isminin ne olduğu ne farkeder ki?

E*TRADE firmasının risk komitesi başkanlığını üstlenen ve uzun yıllar risk yönetimi danışmanlığı yapmış olan James Lam'a göre: "yıllık cirosu 1 milyar Amerikan Dolarından çok olan her firma risk komitesi kurmayı değerlendirmelidir."

Lam'a göre bu komite yasal uyumdan sürdürülebilirliğe, bilgi güvenliğinden para aklamanın önlenmesine kadar herhangi alandaki ve dikkate alınması gereken diğer tüm alanlardaki teknik tüm riskleri en ince ayrıntısına kadar ele almalıdır. Burada öncelikli amaç, yönetim kurulunun iş yoğunluğunu azaltmak ve özellikle stratejik risklere odaklanabilmesini sağlamaktır.

Lam, "eğer yönetim kurulu tüm bu işlerin hepsini birden yapabilirse sorun yok, ancak hepsi birden aşırı yoğun bir gündem oluşturacaktır" diye ekler.

McLeod, 2010'ların başında iç denetim yöneticisi olarak görev aldığı Rio Tinto madencilik firmasından bir örnekte şunları aktarır: Yönetim kuruluna bağlı sürdürülebilirlik komitesi, arazi hakları, su kullanımı ve diğer çevre konularıyla meşgul olurken, "en derin, temel risk konuları nadiren gündeme gelir ya da değerlendirilirdi."

Yayımcı The Institute of Internal Auditors

McLeod Rio Tinto'dayken hem denetim komitesine hem de risk komitesine raporlama yapıyordu. Ancak her iki komite ile de konuşması gereken konuların neler olduğunu biliyordu. Hem risk hem de denetim komitesi ikisi aynı anda bulunduğunda, McLeod'un ifadeleriyle "aradaki sınırlar net bir biçimde anlaşılamamaktadır."

Bu anlatılanların en önemli sebebi, diğer her şey bir yana, risk yönetişimi hakkında yetersiz kavrayış olabilir. Denetim komiteleri onlarca yıldır var olan bir organizasyonel yapıdır ve güçlü mali raporlama ile ilgili sorumlulukları da 2002 yılında yasalaşan Sarbanes Oxley Act ile (Sarbanes Oxley Yasası, kısaca SOX, ABD'de kanun, ÇN) net bir biçimde belirlenmiştir. Yani insanların denetim komitelerinden anladığı ile denetim komitelerinin görev tanımları aynıdır.

Bununla birlikte risk yönetimi bulanık bir alandır. Bankacılık sektörü dışında, risk komitesinin sorumlulukları hakkında yürürlükte olan yasal düzenlemelere de çok karşılaşılmaz. Riski anlamak yaratıcılık ve hayal gücü gerektirir ve bu yetenekler genellikle denetim komitesi üyeleri için zorunlu değildir.

Lam'ın ifadeleriyle, "Kurumsal duyurular, mali raporlama kuralları ve SOX kontrolleri dünyasında denetim komitesinin süreçlere 'geleneksel bir çerçeveden bakması' yeterlidir. Net bir biçimde belirli özel kurallar, iç kontrol gereksinimleri ve SOX kontrolleri mevcuttur."

Ancak, risk komitesi ise süreçlere 'daha geniş bir çerçeveden' bakmak zorundadır. Dolayısıyla kurumun faaliyetlerini denetim komitesinden daha farklı bir bakış açısıyla izleyecektir. Risk komitesi, çalışmalarına rehberlik etmesi için, denetim komitesinin ihtiyaç duyduğundan daha farklı ve daha çok bilgiye ihtiyaç duyacaktır.

Farkı Ayırt Ederken Karşılaşılan Sorunlar

Bir dakika. İç denetim yöneticileri yönetim kuruluna raporlar. Dolayısıyla, eğer yönetim kurulu ayrı ayrı hem denetim komitesi hem de risk komitesi kurmuş ise, İDY her ikisine de raporlayabilir mi?

McLeod öyle olabileceğini düşünmektedir. Kendisi de Rio Tinto'dayken böyle yapmıştı. Yelpazenin diğer ucunda ise Londra'daki Pay.UK firmasının risk komitesi başkanı ve denetim komitesi üyesi Richard Anderson gibi isimler bulunuyor. Anderson'a göre, risk yönetimi "kurumun karşılaşabileceği birden fazla olası gelecek ile mücadele etmektir" ve bu nedenle de denetim işlevinden oldukça farklıdır.

Bu soruyu çetrefilli hale getiren şey gelişmekte olan yeni teknolojilerdir. Evet, iyi haber, yapay zekâ, robotik süreç otomasyonu ve veri görselleştirme iç denetim yöneticilerine daha önce hiç mümkün olmadığı biçimde risklerin tespit edilerek iç kontrollerin test edilmesi için yardımcı olmuştur.

Ne var ki, iç denetim bu yeni nesil risk analiz araçlarının kurulumunu bir kez tamamladığında, bu araçlar anında, diğer departmanların faaliyetlerini gerçekleştirirken kullanabileceği risk yönetimi araçlarına dönüşmektedir.

Örneğin, gerekli algoritmaları geliştirerek, rıza alınmadan

Eylem Listesi

Komitelerin yönetmeliklerini gözden geçirin. Denetim komiteleri çeşitli sorunları ele alır. Yasal uyum, bilgi güvenliği, kurumsal kültür ve diğer pek çok konu ele alınıyor olsa da en öncelikli rutin sorumlulukları mali raporlama ve iç kontrollerin denetlenmesidir. Mali olmayan raporlama riskleri konularının bu konulara hakettiği özeni gösteren bir risk komitesi tarafından daya iyi ele alınıp alınamayacağını anlamak için yönetim kurulu komitelerinin yönetmeliklerini yeniden inceleyin.

Risk güvence görevlerini inceleyin. Kurumun savunma hatlarındaki risk güvence görevlerini inceleyerek bir risk yöneticisi (RY) görevinin ihdas edilmesinin gerekli olup olmadığını değerlendirin. Büyük ihtimalle birinci ve ikinci savunma hatlarında, muntazam ve disiplini bir yaklaşımla gerçekleştiriliyor olmasa da, bazı risk yönetimi faaliyetleri gerçekleştirilmektedir. Eğer öyleyse, bir RY bu faaliyetlere bir disiplin gelmesine yardımcı olabilecek midir? Ya da, nispeten küçük kurumlarda, risk yönetimi için standart bir metodoloji kullanarak RY'den beklenen fayda sağlanabilecek midir?

Teknolojinin risk yönetimine nasıl katkıda bulunabileceğini göz önünde bulundurun. Veri analitiği, grafik ve görselleştirme uygulamaları ve yapay zekâ; bu teknolojilerin her biri kolaylıkla çeşitli amaçlar için kullanılabilecek teknolojilerdir ve iç denetime kontrollerin test edilmesinde ve diğer departmanlara da risklerin yönetilmesinde katkı sağlayabilir. Kurumunuzda üst düzey yönetim ve yönetim kurulunuzun daha iyi karar vermesinde rehberlik ederek yardımcı olmak için bu teknolojileri yönetebilecek bir bilgi teknolojileri stratejisi mevcut mudur?

derlenen kişisel verileri bulmak ya da üçüncü kişi özel denetimleri gerçekleştirilmeden üçüncü kişilerle imzalanan sözleşmeleri tespit etmek denetim ekibi için zor olmayacaktır. Sonrasında ise pazarlama veya satış ekipleri de bu algoritmaları kendi risklerini yönetmek için kullanabilir. Kişisel verilerin korunması veya rüşvet gibi konularda hassas olan uluslararası şirketler için bu alanlar risk komitelerinin göz önünde bulundurmak isteyeceği alanlardır.

Veri analitiği tarafından yön verilen günümüz dünyasında – ki hatırlayınız, herkes tarafından iç denetimin kucak açması gerektiği söylenen bir dünyadır – denetim nerede sona erer ve operasyonel risk yönetimi nerede başlar?

Anderson, iç denetim tarafından kurumlarının risk yönetimi için kullanabileceği algoritmalar geliştirilmesi beklentisi konusunda görüşlerini ifade ederken sözünü sakınmıyor: "İç denetim, herhangi bir algoritma geliştirme ya da kullanılması işine hiç girmemelidir." Kurumlar kendi algoritma modellerini geliştirmelidir, sonrasında ise iç denetim bu modellerin etkinliğini test edebilir.

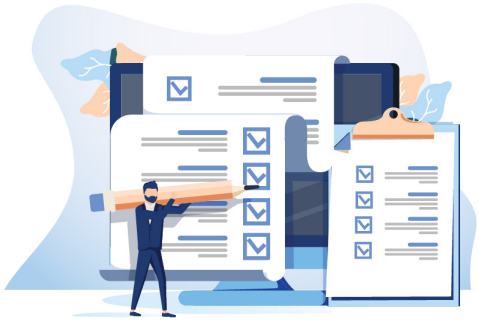
Ancak, öyle ya da böyle, çoğu kurum bu yolu tercih etmiyor. Genelde veri analitiği güdümlü risk yönetimi işlerine girişiyorlar ve mali işlemler ve gider kontrolü gibi alanlardaki bugüne kadar kazanmış oldukları veri analitiği deneyimi nedeniyle de iç denetimin bu girişime öncülük etmesini istiyorlar.

Bu sürece başından sonuna şöyle bir bakarsak: Yönetim kurulu daha iyi risk yönetimi için acil bir başlangıç yapar, ancak hangi komitenin bu işler için ne yapacağını belirlemez. Bunun yerine iç denetime "İç denetim, bu işlerde yardımınızı rica ederiz." der.

Bu hızla başlayan işler denetimin ve risk yönetiminin önünde sonunda McLeod'un bahsettiği "güvence yöneticisi" rolünde birleşmesine yol açabilecektir. Olması gerektiği gibi ayrıştırılmadığı için birleşmiş, geleceğin rolü."

Ancak, McLeod'a göre, "bu yolda bağımsızlık feda edilmiş olacaktır."

Ve nihayet, yönetim kurullarının iç denetimin sunduğu hizmetlerin eşsizliğini ve bağımsız bir iç denetimin sunduğu değeri anlaması gerekir.



Hızlı Anket Sorusu

İç denetim, Risk Komitesine ne sıklıkla raporlama yapmaktadır?

- ❑ Düzenli olarak raporlama yapılıyor
- ❑ Belirli dönemlerde belirli konularda raporlama yapılıyor
- ❑ Yalnız talep edildiğinde raporlama yapılıyor
- ❑ Hususi bir Risk Komitesi mevcut değildir

Cevaplamak ve diğer cevapları da görmek için **www.theiia.org/tone** sayfasını ziyaret ediniz.

HIZLI ANKET SONUÇLARI:

İç denetim birimi, yönetim kuruluna doğru ve tam bilgi sunulmasına yönelik süreçlerin ne kadar içinde yeralmaktadır?

- %12 Her yönüyle içinde yeralıyor
- %19 Çok içinde yeralıyor
- %17 Orta düzeyde içinde yeralıyor
- %27 Biraz içinde yeralıyor
- %25 Hiç içinde yeralmıyor

Kaynak: Tone at the Top Nisan 2019 anketi.

İşbu belge Türkiye İç Denetim Enstitüsü tarafından çevrilmiştir.

Tone at the Top Haziran 2019 bülteni Sayın Tuğrul Bozbey tarafından Türkçe'ye tercüme edilmiş, Sayın Alp Buluç tarafından gözden geçirilmiş ve "edit" edilmiştir.