KÜRESEL BAKIŞ AÇILARI & ANLAYIŞLAR

Yönetişim, Risk ve Kontrol

KISIM I: Risk İştahını Finansal Olmayan Risk Perspektifinden Yeniden Düşünme

KISIM II: Finansal Olmayan Riski Ölçme

KISIM III: Dijital Dönüşüm Yönetişim, Risk ve Kontrolü (YRK) Nasıl Dönüştürüyor?

The Institute of Internal Auditors

İçindekiler

Kısım 1: Risk İştahını Finansal Olmayan Risk Perspektifinden Yeniden Düşünme

Uzman Hakkında

W. Scott Page, CIA, CCSA, CRMA, CPA, CA

Scott MDA, Ltd. şirketinde iç denetim direktörüdür. Genel merkezi Brampton, Ontario, Kanada'da bulunan MDA jeo-istihbarat, robotik ve uzay operasyonları ve uydu sistemleri sağlamaktadır. Scott'ın savunma alanında ve uzay imalatı, profesyonel hizmetler, sağlık hizmetleri, dağıtım hizmetleri ve imalat endüstrilerinde 20 yılı aşkın uzmanlığı vardır.

Giriş

Risk iştahı kavramı — bir kurumun amaçlarına ulaşmak için kabul etmeye hazır olduğu risk miktarı — tüm kurumlarda etkili yönetişim için esastır. Geçmişte, bir şirketin risk iştahı hakkında kararlar öncelikli olarak finansal risk mülahazaları doğrultusunda yönetiliyordu. Ancak, çevre, sosyal ve yönetişim (ÇSY) riskleri de dâhil olmak üzere finansal olmayan risklere ve ilişkili düzenleyici ve raporlama mülahazalarına daha fazla odaklanmasıyla birlikte bu durum değişmektedir. Kurumların çevrelerindeki dünyayla ilgili nasıl faaliyet gösterdikleriyle ilişkili risklere giderek daha fazla dikkat edilmektedir.

Risk iştahının parçası olarak bu risklerin değerlendirilmesi, iç denetçilerin anlamlı katkılarda bulunabilecekleri bir alandır. IIA'nın yönetişim, risk ve kontrol (YRK) hakkında hazırladığı üç kısımlık serinin birincisi olan bu Küresel Bilgi Özeti bu konuyu, risk iştahının finansal olmayan riskleri göz önünde bulundurarak yeniden düşünülmesinin zorluklarını ve iç denetim bu süreçteki önemli rolünü detaylı olarak incelemektedir.

Risk İştahı

Tehdit ve fırsatların dengelenmesi

Risk profilleri iştahı etkiler

IIA'nın Uluslararası Mesleki Uygulama Çerçevesi risk iştahı terimini kısaca şu şekilde tanımlamaktadır: "Kurumun kabul etmeye istekli olduğu risk seviyesi." Uygulamada risk iştahı, risk toleransı olarak da adlandırılmaktadır, inovasyonun potansiyel faydaları ile değişimin kaçınılmaz olarak getirdiği tehditler arasındaki dengeyi temsil etmektedir. Bu nedenle, risk iştahı kurumların kendisine özgüdür ve örneğin aşağıda sayılanlar gibi birçok faktöre bağlı olarak çeşitlilik göstermektedir:

Kültür — Uzun süredir mevcut olan rehberlere, tutumlara veya diğer faktörlere bağlı olarak kurumlar riske yönelik yaklaşımlarında daha fazla veya daha az agresif olabilirler.

Endüstri — Örneğin düzenleme miktarı veya uyumla ilgili diğer endişeler, kurumun riskten ne kadar kaçındığını etkileyebilir.

Pazar — Şirketin karşı karşıya olduğu rekabet seviyesi veya faaliyet gösterdiği pazarın istikrarı risk hakkında karar alma sürecini etkileyebilen faktörlerdir.

Finansal güç — Finansal konumu konusunda kendine güveni daha az olan bir şirket riskten daha fazla kaçınabilir[1].

Finansal olmayan risk nedir?

Finansal olmayan riskin risk iştahı hakkındaki tartışmaların kapsamına dâhil edilmesi, finansal olmayan riskin neleri kapsayabildiğinin anlaşılmasıyla başlamaktadır. Gerçekten de bu kategorinin altında yer alan risk sayısının fazla olması (ilgili listeye bakınız) bazılarının gözden kaçma veya yanlış anlaşılma olasılığını artırmaktadır; bu da finansal olmayan risklerin risk iştahına ilişkin tüm tartışmalara konu edilmesinin önemini vurgulamaktadır. Ancak, kurumlar finansal olmayan riskleri risk iştahıyla ilgili süreçlere sadece dâhil etmenin ötesine geçip, kurumsal seviyede farklı iş süreçleri bünyesinde riskleri ele almak için gerekli bilgileri tanımlayarak bu finansal olmayan unsurlara yönelik harekete geçmeye de hazır olmak zorundadırlar.

FİNANSAL OLMAYAN RİSKLER
(kısmi liste)

- Operasyonel
- Uyum
- Stratejik
- Üçüncü taraf
- Siber güvenlik
- Sosyal sorumluluk
- İtibar
- Veri gizliliği
- Veri bütünlüğü
- Fikri mülkiyet koruması
- Tazminat
- Personel davranışı
- İşgücü yönetimi
- Etik ve kurumsal kültür
- Halk sağlığı
- Çeşitlilik, eşitlik ve kapsayıcılık
- İnsan hakları
- İnsan kaynakları
- Çevre:
  - Sera gazı emisyonları
  - Atık yönetimi
  - Hammadde tedariki
  - Doğal kaynak erişimi/yönetimi
  - İklim değişikliği

[1] Jean-Gregoire Manoukian, "Risk İştahı ve Risk Toleransı: Fark Nedir? (Risk Appetite and Risk Tolerance: What's the Difference)?", Wolters Kluwer, 29 Eylül 2016, https://www.wolterskluwer.com/en/expert-insights/risk-appetite-and-risk-tolerance-whats-the-difference#:~:text=Risk%20Appetite%20Is%20the%20General%20Level%20of%20Risk%20You%20Accept&text=Because%20determining%20risk%20appetite%20will,risk%20you%20need%20to%20manage.

Finansal olmayan risk hakkında raporlamayla ilişkili zorluklar

Raporlama

IIA'nın *2023 İç Denetimin Nabzı, Kuzey Amerika* referansına göre, halka açık kurumlarda çalışan İDY'lerin %60'tan fazlası sürdürülebilirlik/finansal olmayan raporlama risk seviyelerinin orta, yüksek veya çok yüksek olarak değerlendirmiştir.[2] Gerçekten de birçok şirket sürdürülebilirlik/ finansal olmayan sorunları ölçmeye ve bu konular hakkında raporlama yapmaya çalışmaktadır. Örneğin, S&P 500 listesinde yer alan şirketlerin %96'sı ve Russell 1000 listesinde yer alan şirketlerin %81'i sürdürülebilirlik raporları yayınlamaktadır.[3]

Birçok finansal olmayan riski ölçmenin zor olması, kurumların bu alanda karşılaşabileceği zorluklardan biridir. Kapsayıcılık, etik davranış, kurumsal kültür ile şirketin ve onun tedarikçileri ve iş ortaklarının gerçekleştirdiği eylemlerin çevresel etkisi bunlara örnektir.[4] Kurumların finansal olmayan bilgileri toparlarken veya raporlarken doğru olmayan veya yanıltıcı göstergelere veya çerçevelere dayanması durumunda ortaya çıkabilecek potansiyel sonuçlar da bu konuyla ilişkili endişelerden biridir.

Şu anda finansal olmayan raporlama ve açıklamalar hakkında kesin ve küresel olarak benimsenmiş standartlar yoktur ve bu da tutarlı ve karşılaştırılabilir raporlamaların olmamasına sebep olabilmektedir. Bunun yerine, kurumların genelde ihtiyaçlarına bağlı olarak bir rehber ilkeler seti seçme, farklı rehberleri bir araya getirme ya da raporlamadan tamamen vazgeçme fırsatı vardır. Gerçekten de Sürdürülebilir Kurumlar Merkezi çeşitli farklı bileşenleri, performans yapılarını ve birincil ölçüm formatlarını ele alan 23 adet finansal olmayan ölçüm ve raporlama standardı ve çerçevesine ilişkin bir liste derlemiştir.[5]

Ancak, daha genel kabul görmüş raporlama standartlarından oluşan bir set de ufuktadır. Önemli gelişmelerden biri, Uluslararası Finansal Raporlama Standartları (IFRS) Vakfının Uluslararası Sürdürülebilirlik Standartları Kurulunu (ISSB) kurmasıydı. ISSB var olan Değer Raporlama Vakfı ve İklim Saydamlık Standartları Kurulunu konsolide edip ve Entegre Raporlama Çerçevesi sorumluluğunu üstlenmektedir; tüm bunlar sermaye piyasaları için kapsamlı bir küresel sürdürülebilirlik saydamlığı temeli yaratmaya yönelik çabanın parçasıdır. Şirketlerin iklim ve diğer ÇSY konuları hakkında yüksek kalitede, şeffaf, güvenilir ve karşılaştırılabilir raporlama yapmalarına yönelik talepleri karşılamayı amaçlamaktadır. ISSB, iklim ve sürdürülebilirlik raporlaması hakkında ilk standartlarının 2023 yılının 2. çeyreğinin sonuna doğru yayınlanacağını ilan etmiştir.

Düzenleme

Dünya Sürdürülebilir Kalkınma İş Konseyi (WBCSD) kurumuna göre, şu anda 70'ten fazla ülkede 2.000'den fazla zorunlu ve gönüllü ÇSY raporlama gerekliliği ve kaynağı mevcuttur. Sadece bu durum bile zorunlu ve gönüllü finansal olmayan raporlamayı ve ilişkili riskleri anlamaya çalışan kurumlar için ürkütücü bir zorluk yaratmaktadır.

Avrupa Birliği (AB), finansal olmayan riskin zorunlu olarak açıklanması konusunda öncülük etmiştir. 2014 yılından beri, Finansal Olmayan Raporlama Direktifi (NFRD) 500'den fazla çalışanı olan ve kamu yararına çalışan AB merkezli büyük şirketlerin (yaklaşık olarak 11.700 şirket) diğer konuların yanı sıra çevre konuları, sosyal konular, çalışanlara yönelik muamele, insan haklarına saygı, yolsuzluk ve rüşvet ile mücadele ve şirket kurullarında (yaş, cinsiyet, eğitim ve mesleki arka plan açısından) çeşitlilik ile ilgili bilgileri yayınlamasını şart koşmuştur.

Ocak 2023'te, AB'nin Kurumsal Sürdürülebilirlik Raporlama Direktifi (CSRD) yürürlüğe girmiştir. Bu direktif NFRD kapsamında yer alan sosyal ve çevresel raporlama kurallarını günceller ve raporlama yapması gereken şirketlerin sayısını artırır (yaklaşık 50.000). Şirketler

---

2. *2023 North American Pulse of Internal Audit*, The IIA, 2023, https://www.theiia.org/globalassets/site/content/research/pulse/2023/2023-Pulse-of-Internal-Audit.pdf.
3. *2022 S&P 500 and Russell 1000 Sustainability Reporting in Focus*, Governance & Accountability Institute Inc., 2022, https://www.ga-institute.com/research/ga-research-directory/sustainability-reporting-trends/2022-sustainability-reporting-in-focus.html#:~:text=All%2DTime%20High%20of%20Sustainability,and%2081%25%20of%20Russell%201000.
4. *Internal Audit's Role in ESG Reporting: Independent Assurance Is Critical to Effective Sustainability Reporting*, The IIA,, May 2021, https://www.theiia.org/globalassets/documents/communications/2021/june/white-paper-internal-audits-role-in-esg-reporting.pdf.
5. "Non-Financial Measurement & Reporting Standards & Frameworks," Center for Sustainable Organizations, 2023, https://www.sustainableorganizations.org/Non-Financial-Frameworks.pdf.

yeni kuralları ilk kez 2024 mali yılında 2025 yılında yayınlanacak raporlar için uygulamak zorunda olacaktır. Bu tarihe kadar, NFRD raporlama kuralları geçerli olacaktır.[6]

ABD'de, Menkul Kıymetler ve Borsa Komisyonu (SEC) kayıtlı kurumların kayıt beyanlarına ve periyodik raporlarına iklimle ilgili ve siber güvenlikle ilgili belirli açıklamaları dahil etmelerini zorunlu kılmayı teklif etmiştir. SEC'in bu iki alandaki nihai kurallarını 2023'te ilan etmesi beklenmektedir. SEC gerekliliklerinden muaf olmalarına rağmen, özel şirketler de paydaşlarından benzer açıklamalar yapmaları yönünde baskı hissedebilirler.

Yeşil Aklama (Greenwashing)

Raporlamada karşılaştırılabilirlik ve şeffaflık unsurlarının olmamasına ilave olarak, şirketler hedefleri belirlerken aşırı iyimser varsayımlarda bulunduğunda ya da daha olumlu bir tablo sunmak için verileri çarpıttığında güvenilirlik de bir sorun haline gelebilmektedir. Avrupa'da, ulusal tüketici koruma otoriteleri şirketlerin çevre dostu iddialarının %42'sinin abartılı, yanlış veya yanıltıcı olduğuna inanacak nedenler bulmuştur. Yeşil aklama olarak bilinen bu uygulamalar kurumların itibarına zarar verebilmektedir. Bir şirkete ve onun ürün veya hizmetlerine yönelik müşteri memnuniyeti hakkında ortaya çıkan olası etkiler hisse başına kazancı ve yatırım getirisini etkileyebilir.[7]

42

ŞİRKETLERİN İDDİA ETTİKLERİ ÇEVRE DOSTU YÜZDENİN ABARTILI, YANLIŞ VEYA YANILTICI OLDUĞUNA İNANILMAKTADIR.

Kaynak: Harvard Business Review, *"Yeşil Aklama Kârlılığı Nasıl Etkiliyor? (How Greenwashing Affects the Bottom Line)"*

Buna ilave olarak, IIA'ya göre, "Sorunların net bir şekilde anlaşılması esasıyla oluşturulan mantıklı bir ÇSY risk yönetimi stratejisi olmadığında, başarısız bir şekilde uygulanan sürdürülebilirlik raporları, mevzuata uygunluğu hızla sekteye uğratabilir ve yatırımcı beklentilerini boşa çıkarabilir."[8]

Finansal olmayan verilerle ilk kez uğraşan şirketler, karar alma sürecine yönelik güvenilir bilgiler elde etmek ve üretilen ve raporlanan verilerin kaliteli olmasını sağlamak amaçlarıyla uygun politika, süreç ve iç kontrol tedbirlerinin yanı sıra yeni anahtar performans göstergeleri ve başka ölçütler geliştirmek zorunda kalacaktır.

---

6. "Kurumsal Sürdürülebilirlik Raporlaması (Corporate Sustainability Reporting)," Avrupa Komisyonu, erişim tarihi: Mart 2023, https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en.

7. Ioannis Ioannou, George Kassinis ve Giorgos Papagiannakis, "Yeşil Aklama Kârlılığı Nasıl Etkiliyor? (How Greenwashing Affects the Bottom Line)," 21 Temmuz 2022, Harvard Business Review, https://hbr.org/2022/07/how-greenwashing-affects-the-bottom-line.

8. *ÇSY Raporlamasında İç Denetimin Rolü: Etkili Sürdürülebilirlik Raporlaması için Bağımsız Güvence Kritiktir (Internal Audit's Role in ESG Reporting: Independent Assurance Is Critical to Effective Sustainability Reporting)*, The IIA, Mayıs 2021, https://www.theiia.org/globalassets/documents/communications/2021/june/white-paper-internal-audits-role-in-esg-reporting.pdf.

İç Denetimin Rolü

Güvence ve danışmanlık hizmetleri

Denetim planlamasında finansal olmayan risklerin hesaba katılması

İç denetçiler yapacakları denetimleri genel olarak kurumun risk iştahlarını ve denetlenen alanları esas alarak planlamaktadırlar. İç denetime genellikle kurumun risk iştahı çerçevesinin etkinliği konusunda bağımsız güvence sağlama sorumluluğu verilmektedir. Mevzuatın ve paydaşların sürdürülebilirliğe ve diğer finansal olmayan konulara giderek daha fazla odaklanması, iç denetim liderlerinin kurum açısından tehdit oluşturabilecek ilişkili riskleri, bunların şirketin faaliyetlerine ve stratejilerine nasıl uyduğunu anlamak ve ilişkili uygulamaların hangi departmanların gözetiminde olduğunu bilmek de dâhil olmak üzere hesaba katmalarını talep etmektedir. İç denetim liderlerinin yönetim kurulları ve icracı yönetim ile birlikte finansal olmayan risklere yönelik farkındalık yaratmaları da gereklidir.

İç denetimin anahtar rollerinden biri, finansal olmayan risklere yönelik olarak ilgili tedbirleri izleyebilen ve kurumun kötü tasarlanmış kontrol ve sistemlerden dolayı geçersiz ve yanıltıcı bilgiler raporlamasını önleyebilen uygun kontrol ortamını belirlemek olacaktır. Yetkin iç denetim fonksiyonlarında, eğitim ve danışmanlık hizmetleri de dâhil olmak üzere etkili finansal olmayan kontrol ortamlarını desteklemek için gereken beceriler ve deneyim mevcuttur. İç denetim, kurumun finansal olmayan riskleri yönetmek, hafifletmek ve muhtemelen onlar hakkında rapor vermek için kullanabileceği çerçeveler veya standartlar konusunda tavsiye verebilir. İç denetim, finansal olmayan riskleri doğru şekilde temsil eden nicel ve nitel verileri yakalamak için tasarlanan yeni göstergeler de dâhil olmak üzere en faydalı raporlama ölçütleri hakkında da tavsiyelerde bulunabilir.

Veriler, sürdürülebilirliğin ve finansal olmayan konuların yavaş yavaş iç denetimin rutinine girmeye başladıklarını göstermektedir. Nabız raporuna göre, ankete katılanların %22'si sürdürülebilirlik konularını denetimlerine genelde dâhil ettiklerini belirtmiştir. Ancak, sürdürülebilirlik/finansal olmayan raporlama konularına özgü denetimler denetim planı tahsisinde %2'lik bir bölümü oluşturmaktadır.[9]

Merkezi odağın değeri: Bir şirketin deneyimi

Doğru bir temelin oluşturulması, finansal olmayan risklerin risk iştahının kapsamına dâhil edilmesinde önemli bir faktördür.

Scott Page MDA, Ltd. kurumuna iç denetim direktörü olarak katıldığında, her iş alanının kendi risk yönetim süreci vardı ancak şirket odağını merkezileştirmek istiyordu. Bu merkezileşmeyi sağlamak için bütüncül ve entegre bir yaklaşım çok önemliydi. Bilgiyi bir araya getirmek amacıyla robotik, uydu sistemleri ve jeo-istihbarat alanlarında hizmetler sunan bu Kanada merkezli halka açık şirket değerlendirme süreci için çok yönlü bir yazılım aracı benimsedi. Aynı araç, kontrol testlerinde iç denetim ile siber ve üçüncü taraf risklerini değerlendirmede BT de dâhil olmak üzere diğer ekipler tarafından da kullanılabilir.

Dolayısıyla, risk bilgisi ve kontroller şirket genelinde paylaşılabilmektedir. Bu araç, şirketin kısa vadeli hedeflerinin yanı sıra uzun vadeli stratejik planını gerçekleştirme becerisini nasıl etkileyebileceklerini görmek için stratejiyi veya hedefleri etkileyebilen risklerim tümü hakkında detaylı bilgiler toplayabilmektedir. "Risk mülahazalarının tümünü tek bir hakikat kaynağı halinde bir araya getirmek istedik. Bu da yaptığımız işin diğer herkesle nasıl ilişki kurduğunu anlamamıza yardımcı olmaktadır," demiştir Page.

[9] *2023 İç Denetimin Nabzı, Kuzey Amerika*, The IIA.

İç kontroller, mali tablolar, operasyonlar, BT ve üçün taraflar ile ilişkili riskler güncel yaklaşımlar kullanılarak zaten iyi bir şekilde yakalanmıştır. Ancak, kurum ÇSY risklerini ve diğer finansal olmayan riskleri de hesaba katmaya başlamıştır. Page, bu ilave riskleri konsolide etmek için aynı aracı kullanmanın "diğer alanlarda neler olup bittiğinden her zaman haberdar olduğunuz" anlamına geldiğini söylemiştir.

Finansal olmayan risklerin tanımlanması, hesaba katılıp açıklanması ve denetlenmesi karmaşık olabilirken MDA'nın merkezi odağı ona sağlam bir başlangıç noktası sağlamıştır. Bu şirket, diğer endişelerin yanı sıra, ÇSY konusunu bir silo olarak ayırmak istememektedir çünkü ilişkili finansal olmayan riskler birçok alana dokunmaktadır.

Page, merkezileştirme şirket genelinde ve paydaşlar tarafından anlaşılabilen ortak bir dil kullanılmasına olanak tanır demiştir. Page, kurumsal risk yönetimi (KRY) grubundaki liderlerle birlikte riskleri ve bu risklerin 1 ilâ 5 aralığında bir ölçek üzerinden nasıl değerlendirilmesi gerektiğini tanımlar. Risk bilgisi bir kez toplanabilir ve kurum genelinde kullanılabilir; bu da versiyon kontrolü sağlamanın yanı sıra iç denetimde ve başka alanlarda verimliliği artırabilir. Ortak dil kullanılmasıyla birlikte, icracı yönetim ve yönetim kurulu iç denetim veya diğer ekipler bir riski daha az acil bir önceliğe -Kategori 1- kıyasla en yüksek öncelik -Kategori 5- olarak belirlediğinde bunun ne demek olduğunu kolayca anlayabilirler.

Finansal olmayan bilginin denetlenebilirliği süregelen bir hususdur çünkü daha önce de tartışıldığı üzere, genel olarak benimsenen raporlama standartları mevcut değildir. Bu durum değişene kadar, iç denetim kurumun hangi kontrol, süreç ve bilgilere hazırlıklı olması gerekeceği konusunda tavsiyeler verebilir.

Rakamları ölçmek de başka bir zorluktur çünkü veriler mevcut olmayabilir ve karşılaştırılabilir verileri elde etmek zor olabilir. Örneğin, MDA yaygın bir ÇSY endişesi olan sera gazı emisyonları konusunda pek bir şey yapmamaktadır. Ancak, birçok dış tedarikçi ve danışmanla çalışmaktadır ve bu üçüncü taraflar emisyon üretebilir ya da MDA'nın dikkate alması gerekecek başka adımlar atabilir. MDA, finansal olmayan risk programının temellerini geliştirirken söz konusu üçüncü tarafları tanımlayarak her türlü ilişkili riskin nasıl ölçüleceğini hesaba katmakta, bu üçüncü tarafların en iyi nasıl denetleneceğine karar vermekte ve ardından, üçüncü tarafın ve diğer finansal olmayan risklerin şirket için ne anlama geldiğine ilişkin daha kapsamlı bir anlayış oluşturmaktadır.

IIA'nın Nabız anketine göre, üçüncü taraf ilişkileri üçüncü en yüksek riskli alandır (siber güvenlik ve BT'den sonra gelir) ve üçüncü taraf ilişkilerine yönelik denetim sıklığı risk seviyesine kıyasla oldukça düşüktür.

MDA potansiyel finansal olmayan risk alanlarını tanımlamanın ilk aşamalarında olmasına rağmen, şu ana kadarki süreç şirketin stratejilerini gerçekleştirme kabiliyetinin yanı sıra kamunun şirkete ilişkin algısı üzerinde ne kadar etkili olabileceklerinin de altını çizmiştir. Page, bu süreç icracı yönetime ve kamuya karar alma sürecinde daha fazla bilgi de sağlayacaktır, demiştir. "Hem finansal ve de finansal olmayan riskler hakkında hem de onları nasıl kontrol etmemiz gerektiği konusunda daha kapsamlı bir anlayışımız var" belirtti.

En başından dâhil olmak

İç denetçilerin, özellikle finansal olmayan risk gibi yeni bir kavramı ele alırken iç denetimin sürece ve faaliyetlere dâhil edilmesinin değeri konusunda yönetimi ve yönetim kurullarını en başından itibaren uyarmaları gereklidir. Page şöyle demiştir: "Eğer iç denetim önceden dâhil edilirse ileride başarı şansı o kadar yüksek olur. "Bir şirket neden ÇSY veya finansal olmayan plan veya süreçlerini uygulamaya koyduktan sonra iç denetimin gelip bunlarla ilgili tüm sorunlara dikkat çekmesini istesin ki?" Page demiştir.

İç denetim bağımsızlığını koruyabilmek için şirket açısından karar verme konumunda bulunamaz ancak finansal olmayan riskleri hesaba katmaya başlamak için en iyi yolu ve hangi yaklaşımların işe yarayıp yaramayacağı konusunda içgörüler sunabilir. Page "Katma değerli bir iş ortağı olabiliriz," demiştir.

Page, kurum genelinde temaslarda bulunmanın ekibinin denetleyeceği alanları daha iyi anlamak için iyi bir yol olduğunu keşfetmiştir. Page, önemli iş fonksiyonlarında yer alan kişilerle düzenli olarak iletişime geçerek kahve eşliğinde 15 dakikalık toplantılar yapmayı

istemektedir ve personelini de aynısını yapması yönünde teşvik etmektedir. Page “Hiç kimse hayır demedi. “Herkes tutkulu ve yaptığı işi seviyor,” demiştir.

Page “Denetim fonksiyonunun başkanı olarak beni endişelendiren şey şu: Neyi bilmiyorum? Soruyu cevaplamanın tek yolu insanlarla konuşmak,” diye eklemiştir. Page’in ekibinin yürüttüğü denetimler denetlenen alanın personeliyle görüşmeler yapmayı içermektedir. Ayrıca, iç denetimin kendi bağımsız risk değerlendirme süreci olmasına rağmen kurumsal KRY ekibinin çalışmalarını da güncel olarak takip etmektedir.

Page’in endüstrideki veya mesleki komitelerdeki meslektaşlarıyla iletişimde olması da risk yönetimi yaklaşımının güncel ve olabildiğince kapsamlı olup olmadığının belirlenmesine yardımcı olmaktadır. Bu arka plan bilgi birikimi, finansal olmayan bilgiler veya ÇSY bilgileri için özellikle önemli olacaktır çünkü bu riskler gelişmeye devam etmektedir.

Page ve ekibi diğerleriyle yaptıkları sohbetler sonucunda daha iyi bir anlayış elde etmiş ve bundan dolayı bir alanı denetleme zamanı geldiğinde daha iyi konumlanmış olurlar; bu da finansal olmayan verilerin yeni sınırlarını anlamada özellikle faydalı olacaktır. MDA üç ayrı iş alanını kapsamaktadır; dolayısıyla iç denetim diğer ekiplerin kullandığı başarılı uygulamaları paylaşabilir ve gereçsiz çaba ve çalışmaları tekrarını tespit edebilir. Page “İş zekâsı çok daha büyük başarılara götürür,” demiştir. İç denetçiler statükoya meydan okuyarak, var olan uygulamaları sorgulayarak ve finansal olmayan bilgilerin daha iyi anlaşılmasını ve tanımlanmasını sağlamak için kılavuzlar geliştirerek de değer sağlayabilirler.

Risk in Focus 2023 raporundan pratik yönlendirme

Avrupa İç Denetim Enstitüleri Konfederasyonu (ECIIA) üyelerinin hazırladığı en son yıllık risk raporu olan *Risk in Focus 2023*, makroekonomik ve jeopolitik riskler de dâhil olmak üzere çeşitli finansal olmayan risk alanlarını ele almıştır. İç denetim liderlerinin yuvarlak masa toplantısına katılanlar, özellikle Ukrayna'daki çatışmanın küresel enerji sistemlerinin stabilitesi de dâhil olmak üzere çeşitli alanlarda riskleri etkilemesi nedeniyle küresel riskin yeniden değerlendirilmesini masaya yatırmışlardır. Yuvarlak masa katılımcılarından biri olan Ken Marnoch (Shell International'da iç denetim ve soruşturmalardan sorumlu başkan yardımcısı) kendisinin ve ekibinin "risk iştahı konusunda daha güçlü görüşmeler" yaptığını söylemiştir.

Risk in Focus 2023 raporundan:

> "[Marnoch] her bir işletmenin spesifik alanlarda ne kadar risk alabileceğine ilişkin net bir anlayışa sahip olmanın en faydalı olacağı zamanlardan biri, tüm seçeneklerin potansiyel artı ve eksi yönlerinin olabileceği bir ikilemdir. Ardından, farklı seçeneklerle ilişkili olan risklere yönelik iştahın netleştirilmesi sorun karşısında yol gösterici olabilir.
>
> Geçmişte, Shell iç denetimi operasyon, kültür ve davranış temelli risklere odaklanmıştı. İç denetim grubu artık stratejik hedeflerin gerçekleştirilmesiyle ilişkili risk ve kontrol çerçevesine odaklanmak için özel bir ekip oluşturmuştur.
>
> 'Stratejik hedefleri ölçülebilir amaçlara, ilgili risklere, açık kontrollere ve iş liderlerinin kontrollerin işleyip işlemediğini nasıl bileceğine ilişkin bir anlayışa ayırmanız durumunda iç denetim için kapsamınız var demektir,' der Marnoch. 'Yeni ekibin rolünün bir kısmı, dünyada bu kadar çok şey dramatik şekilde değişirken insanların bir projenin veya stratejinin başlangıcında yaptıkları varsayımların doğruluğuna ilişkin sabit düşüncelerden uzaklaşmalarına yardımcı olmaktır. Belirsiz bir geleceğe doğru ilerlerken etkin şekilde sorgulayıcı olmak, inançları test eden bilgiler bulmak ve mevcut gerçeklik hakkında hızlı geribildirim almak gerekmektedir.
>
> 'Haklı olma ihtiyacını bir kenara bırakır ve bu kararın o zamanki en iyi bilgilerle verilmiş karar olduğunu kabul ederseniz, kendi görüş ve düşüncelerinize meydan okuyan bilgileri aramaya daha açık olursunuz. Bu da stratejik hedeflerinizin gerçekleştirilmesinde önemli olan bir riskin yönetilmesinde çok daha fazla güç sağlar.'"[10]

Risk in Focus 2023, iç denetçilerin kurumsal riski değerlendirirken kullanabilecekleri soruların bir listesini içermektedir:

1. İç denetim görevlerinde harcanan zaman ve efor açısından, iç denetim jeopolitik risk ve iklim değişikliğini içerenler de dâhil olmak üzere kurumun stratejik hedefleriyle nasıl uyumlu hale getirilmiştir?
2. Strateji ve kriz yönetimi gibi alanlarda iç denetim faaliyetlerine verilen destek ne kadar güçlüdür ve eksik olduğu yerlerde bu desteği artırmak için neler yapılabilir?
3. İç denetim uygun kapsamı sağlamak ve çaba ve çalışmaların gereksiz yere tekrarlanmasını en aza indirmek için diğer birimlerin kaynaklarından ne ölçüde yararlanabilmektedir?
4. Kurumun (ve iç denetim biriminin) anahtar risk alanlarının doğası hakkında yaptığı varsayımların bugün hâlâ geçerli olup olmadığını ve 2023'te ortaya çıkması muhtemel koşullara uyup uymadığını nasıl bilebilirsiniz?
5. Kurumun yaptırım riski için güncel risk değerlendirmeleri ve üçüncü taraf sahiplik ve şirket hissedarlarının taranması için sağlam kontrolleri var mıdır?
6. Kurum, anahtar riskleri modellemek ve " eğer..." senaryolarını uygulamak için dijital araçlardan ne kadar yararlanmaktadır?
7. Amaca uygun olduklarından emin olmak için kurumun iş sürekliliği, kriz yönetimi ve risk yönetimi ekipleri arasındaki ilişkiyi yeniden değerlendirdiniz mi?
8. Kurum, riskleri değerlendirirken eleştirel sesleri ve dış uzmanların görüşlerini ciddi anlamda dikkate almakta mıdır?

---

[10] *Risk in Focus 2023: Önümüzde Daha Riskli, Belirsiz ve Dalgalı Zamanlar Var (Risk in Focus 2023: More Risky, Uncertain, and Volatile Times Ahead),* Avrupa İç Denetim Enstitüleri Konfederasyonu, 2022, https://www.eciia.eu/2022/09/risk-in-focus-2023-more-risky-uncertain-and-volatile-times-ahead/.

Varılan Sonuçlar

Kapsamlı bir anlayış

Finansal olmayan risklerin kurumun üzerinde, KRY çaba ve çalışmaları da dâhil olmak üzere anlamlı bir finansal etkisi olabildiğini anlamak önemlidir. Liderlerin finansal olmayan riskleri anlamasına ve onlarla mücadele etmesine yardımcı olmak amacıyla, iç denetim liderleri bu riskler hakkında değerli içgörüler sağlamanın yanı sıra kurumun risk iştahının belirlenmesine yardımcı olurken bu riskleri de uygun şekilde hesaba katmak ve ele almak için kurumun birçok yönü -ve karşı karşıya olduğu tehditler- hakkında sahip oldukları kapsamlı anlayışı kullanabilirler.

Kısım 2: Finansal Olmayan Riskin Ölçülmesi

Uzman Hakkında

Anishka Collie, CIA, CPA

Anishka Collie (CIA, CPA) Bahamalar'ın Nassau kentinde bulunan ATC Financial Advisors & Consultants kurumunun CEO'su ve baş danışmanıdır. Dış denetim, iç denetim ve kurumsal yönetim, kurumsal risk yönetimi ve iç kontrollerin yanı sıra finansal planlama, danışmanlık, finansal süreçlerin iyileştirilmesi ve iş süreçlerinin gözden geçirilmesi alanlarında 20 yılı aşkın deneyime sahiptir. Finansal hizmetler sektöründeki müşterilere odaklanmaktadır ve çok sayıda muhasebe ve denetim eğitim seminerinde sunum yapmıştır.

Hassan NK Khayal, CIA, MBA, CRMA, CFE

Hassan NK Khayal (CIA, MBA, CRMA, CFE) Dubai'de Scope Investment kurumunda iç denetim yöneticisidir. İç Denetçiler Enstitüsü'nün küresel yayını Internal Audito'da iç denetim mesleğinin gelecek vaat eden yıldızı olarak 30 yaş altı 15 küresel Yükselen Liderden biri olarak gösterilmiştir. İspanya'nın Murcia kentinde Katolik Üniversitesinde işletme alanında doktorasını tamamlamaktadır. Derecelerine ve mesleki sertifikalarına ek olarak robotik süreç otomasyonu, kalite yönetimi, sağlık ve güvenlik, çevre yönetimi ve risk yönetimi alanlarında da mesleki sertifikaları vardır.

Jason Minard, CIA, CISA, CPA (inaktif)

Jason Minard (CIA, CISA, CPA (inaktif) St. Louis, Missouri, ABD'de bulunan Wells Fargo Advisors kurumunda kıdemli başkan yardımcısı ve Gözetimsel Kontroller ve Analitik kıdemli yöneticisidir. Menkul kıymetler sektöründe ve denetiminde 25 yılı aşkın deneyimi ile yatırım satışı, mevzuata uygunluk, menkul kıymet işlemleri, yatırım bankacılığı, varlık yönetimi, tröst yönetimi ve finans gibi alanlarda denetimler yapmış ve yönetmiştir. St. Louis Üniversitesi'nden işletme alanında lisans derecesine sahiptir ve genel menkul kıymetler temsilciliği ve genel satış süpervizörlüğü ruhsatları vardır.

GİRİŞ

Yönetim gurusu Peter Drucker'ın "[sadece] ölçülen şey yönetilir" sözü sık sık alıntılanmaktadır. Gerçekten de şirketler finansal riskleri ölçmenin ne kadar önemli olduğunun uzun zamandır farkındadırlar. Son yıllarda çevre, sosyal ve yönetişim (ÇSY) de dâhil olmak üzere finansal olmayan risklere ve bunlarla ilişkili düzenleme ve raporlama mülahazalarına artan bir ilgi söz konusudur. Buradaki zorluk, genelde kolayca tanımlanabilen bir parasal değeri olmayan şeylerin nasıl ölçüleceğidir. Kurumlar bu zorluğu aşmak zorundadırlar çünkü finansal olmayan risklerin finansal etkisinin olabileceği kesindir.

Yönetişim, risk ve kontrol (YRK) hakkındaki üç kısımlık serinin ikincisi olan bu Küresel Bilgi Özeti iç denetimin bu alanda anlayışın geliştirilmesinde oynayabileceği rolün yanı sıra, finansal olmayan riskleri ölçmenin zorluklarını ve şirketlerin bu riskleri nasıl ele aldığını incelemektedir.

FİNANSAL OLMAYAN RİSKLERİN ANLAŞILMASI

Sayısız potansiyel tehdit

Tanımayı ve Ölçmeyi Öğrenme

Genel kural olarak, finansal olmayan riskler bir kurumun dünya üzerindeki etkisinden ve buna karşılık, dünyanın kurum üzerindeki etkisinden kaynaklanan risklerdir. Kısmi liste (yan kutuya bakınız) kurumların karşılaşabileceği çok çeşitli finansal olmayan risklerin hepsini olmasa da birçoğunu yansıtmaktadır. Bu risklerin tanımları genellikle tutarsız veya belirsizdir; bu da onları tanıma ve ölçmeyi daha zor hale getirmektedir.

Ancak, finansal olmayan riskler basit finansal işlemlerde de mevcuttur. Örneğin, Örneğin, 50.000$'lık bir kredinin kredi riski göz önüne alındığında, kredi değeri ve olası ilk kayıp bellidir. Diğer yandan, dış kaynaklı risk ve iç denetim danışmanlık hizmetleri sunan ATC Financial Advisors & Consultants (Nassau, Bahama Adaları) kurumunda CIA, CPA, CEO ve baş danışman olan Anishka Collie'nin de not ettiği üzere bu işlem için finansal olmayan risk olası bir kredi temerrüdüyle başa çıkmak için harcanan zaman ve çaba gibi hususları içermektedir. Kredi tutarının yüksek olması ya da batık kredi modelinin bir parçası olması halinde, kurumun kurumsal kültürün, mevcut dokümantasyonun ve iç kontrollerin ya da mevcut eğitim seviyesinin kredi riskini azaltmak ve iyi kredi kararları alınmasını sağlamak için uygun olup olmadığını anlamak amacıyla daha derine inmesi ve kapsamlı araştırmalar yapması gerekebilir.

Finansal olmayan risklerin ölçülmesi zor olabileceği için, kurumun finansal olmayan risklere ilişkin rapor ve açıklamalarının güvenilir olmama ihtimali de bununla ilgili risklerden biridir. Örneğin, belirli bazı sürdürülebilirlik hedeflerinin gerçekleştirilmesi kasıtlı olarak şişirilmiş görülebilir ya da bu hedeflere ulaşma sürecinde karşılaşılan sorunlar küçümsenmektedir -ki ÇSY konularıyla ilgili olduğunda yeşil aklama olarak bilinen uygulama tam da budur. Avrupa İç Denetim Enstitüleri Konfederasyonu (ECIIA) tarafından düzenlenen yuvarlak masa toplantısında bir iç denetim yöneticisinin not ettiğine göre, yeşil aklama kasıtlı olabilir ya da basit bir şekilde finansal olmayan raporlama standartlarında şu anda mevcut olan olgunluk seviyesinin nispeten düşük olmasından kaynaklanabilir.[11] Şu anda, raporlama tutarsız olabilir ya da karşılaştırılması zor olabilir çünkü finansal olmayan rapor ve açıklamalar konusunda küresel olarak benimsenmiş standartlar yoktur. Çeşitli çerçeveler veya standartlar da mevcuttur; bu da özellikle başka bir standart veya çerçevedeki kurallarla birlikte veya kısmen kullanılabildiklerinden dolayı şirketlerin hangi rehberleri takip edeceğini ve onları nasıl uygulayacağını belirlemesini potansiyel olarak zorlaştırmaktadır. Sürdürülebilir Kurumlar

Finansal Olmayan Riskler
(kısmi liste)

- Operasyonel
- Uyum
- Stratejik
- Üçüncü taraf
- Siber güvenlik
- Sosyal sorumluluk
- İtibar
- Veri gizliliği
- Veri bütünlüğü
- Fikri mülkiyet koruması
- Tazminat
- Personel davranışı
- İşgücü yönetimi
- Etik ve kurumsal kültür
- Halk sağlığı
- Çeşitlilik, eşitlik ve kapsayıcılık
- İnsan hakları
- İnsan kaynakları
- Çevre:
  - Sera gazı emisyonları
  - Atık yönetimi
  - Hammadde tedariki
  - Doğal kaynak erişimi/yönetimi
  - İklim değişikliği

[11] *Risk in Focus 2023: İç Denetçiler için Önemli Konular*, Avrupa İç Denetim Enstitüleri Konfederasyonu, 2023.

Merkezi, birçok farklı performans ölçütüne dayanan ve farklı kurum türlerine yönelik olan 23 adet finansal olmayan ölçüm ve raporlama standartlarından oluşan bir liste derlemiştir.[12]

Sahne Hazırlığı

Kurumların finansal olmayan riskin nasıl ölçüleceğini düşünürken proaktif olması gereklidir ancak birçok kurum böyle hareket etmemektedir. Finansal riskle uğraşmak bir kurumun temel amacıyla, yani hissedarların servetini ve refahını en üst düzeye çıkarmak ve geliri artırmak ile ilişkilidir. Finansal olmayan riskleri ele alırken kurumlardan değeri zor anlaşılabilen ve gelire hemen katkıda bulunmayan çaba ve çalışmalara para harcaması istenmektedir. PwC'ye göre "Riskin etkisini ölçüp finansal bir rakam ortaya koyana kadar bu riskin ele alınması için gerekli yönetim katılımını sağlamanız pek olası değildir."[13]

Finansal olmayan risklere yönelik kontrol fonksiyonlarının kurum genelinde silo halinde olabilmesi başka bir engeldir. Bu riskler çok çeşitli olduğundan dolayı genelde çok çeşitli ekiplerin gözetimi altındadırlar. Her ekibin finansal olmayan risklerle ilgili kendi risk tanıma süreci, raporlama yapısı ve hatta farklı BT sistemleri vardır. Scope Investment (Dubai) kurumunda iç denetim yöneticisi olan Hassan NK Khayal (CIA, MBA, CRMA, CFE) "İç denetim, uyum veya başka bir alan olsun aynı prosedürü tekrar tekrar yapmaları isteniyor," demiştir. Çaba ve çalışmaların bu şekilde tekrarlanmasının ek gideri, yönetimin bilgi toplama ve ölçme çalışmalarına yapılan yatırımları geri çekme olasılığını artırmaktadır.

Ancak, önleyici tedbirler almak iyileştirme maliyetlerini düşürmekte ve şirketin markasını ve iş ilişkilerini korumaktadır. Khayal, çoğu kurumda risk raporlama yöntemlerinin henüz yönetim için ikna edici bir durum oluşturacak kadar karmaşık veya kesin olmadığını söylemiştir. Ama uygun şekilde seçilmesi halinde doğru göstergeler finansal olmayan riskleri yakalayıp doğru şekilde ölçebilir ve yönetimin bunların potansiyel etkilerini kavraması için uygun bağlamı sağlayabilir.

Potansiyel finansal olmayan tehditleri gerçekleşmeden proaktif olarak tanımlamak onları anlamayı ve ölçmeyi kolaylaştırmaktadır. Örneğin, yiyecek ve içecek endüstrisinde, belirli miktarda gıda bozulduğunda finansal riski ölçmek kolaydır. Ancak, Khayal ilişkili sağlık ve güvenlik maliyet ve risklerini hesaplamanın daha zor olduğunu not etmiştir. Bir kurum bu riskleri hesaba katarak, örneğin bir restoranı daha cazip kılmak ve müşterilerin hastalanma olasılığını azaltmak amacıyla temizliği artırmak gibi proaktif, hazırlık niteliğinde adımlar atabilir. Benzer şekilde, inşaat endüstrisinde, iş güvenliği mühendisleri sağlık ve güvenlik kurallarının izlenmesi ve uygulanması konusunda daha sıkı davrandıklarında kazaların sayısı genelde düşmektedir.

İster olayla ve ilişkili herhangi bir yaralanmayla ilgilenmenin doğrudan maliyeti, isterse ilişkili gecikmelerin masrafı olsun "Her olayın kendine özgü maliyeti vardır," demiştir Khayal. "Risk meydana geldiği anda artık çok geçtir," diye de not etmiştir ve kurumun itibarı ve ilişkileri belki de kalıcı veya önemli etkileri olacak şekilde zarar görmüştür. Ama, kurumlar potansiyel risk olaylarının maliyetlerini değerlendirdiklerinde, önleyici tedbirler almanın değerini görme olasılıkları daha yüksektir.

Khayal, finansal olmayan risklerin finansal risklerden daha büyük etkilerinin olabileceğini düşünmektedir. Finansal olmayan risklerin etkisi, itibar kaybı meydana geldiğinde, örneğin hissedarlar, çalışanlar ve müşteriler gibi paydaşların şirketin iş modelini veya uygulamalarını sorgulamasına sebep olabilir. Khayal "Tüm bunlar, kurumlar üzerinde finansal olmayan riskleri yönetme konusunda önemli bir baskı oluşturmaktadır," demiştir.

Ölçmeye Yönelik Çalışma

Finansal olmayan riskler doğrudan parasal değer taşımasa da bu risklere sayısal değerler atamak mümkündür. Önemli olan riskleri ve neleri kapsadıklarını tanımlamak ve ardından onları ölçmek için somut mülahazalar bulmaktır. Örneğin, müşteri riskini ele alırken

[12] https://www.sustainableorganizations.org/Non-Financial-Frameworks.pdf
[13] "Kontrolü Ele Alma: Finansal Olmayan Risklerin Üstesinden Nasıl Gelebiliriz? (Taking Control: How to Get on top of Non-Financial Risks)," Christopher Eaton and David O'Brien, PwC Channel Islands, 9 Mart 2021.

müşteri şikayetlerinin sayısı, ilgili yerler veya durumlar, ilişkili müşteri kayıpları, yeni müşterilerde düşüş ve bu verilerin zaman içerisinde hangi eğilimleri ortaya çıkardığı gibi faktörleri belirlemek mümkündür.

Ölçüm için hiçbir somut kriter olmadığında seçeneklerden biri riskleri, örneğin yüksek, orta veya düşük seviyelerde olup olmadıkları gibi mümkün olduğunca açıklayıcı ve anlamlı şekilde kategorize etmektir. Örneğin, uyum ve mevzuat riski söz konusu olduğunda, kurumlar her bir risk kategorisinde bir düzenleyicinin potansiyel bulgularının aralığını belirleyerek riski ölçmeye çalışabilirler. Bulguların bu şekilde kategorize edilmesi, şirketlere her riski değerlendirmek ve öncelikleri belirlemek için çerçeve sağlamaktadır.

Organize bir derecelendirme çerçevesi, bir dizi finansal olmayan riske ilişkin bulguları yakalamayı mümkün kılan bir başka seçenektir. İç denetim ekipleri, iç denetimin ve hafifletilmemiş riskleri tanımlayan ve izleyen, onları raporlayan veya düzelten uyum, risk, bilgi güvenliği veya hukuk gibi diğer ekiplerin gözlemleri derecelendiren bir derecelendirme çerçevesi kullanabilir. Bu çerçeve finansal olmayan risklerin etkisini değerlendirmek ve onların ölçülmesini desteklemek için kullanılabilir. Sorumlu Yatırım Değeri Sürücü Modeli için Birleşmiş Milletler Küresel Sözleşmesi ve İlkeleri şirketlerin sürdürülebilirlik tedbirlerinin finansal etkisini daha iyi anlamak ve raporlamak için kullanabileceği bu tip çerçeveye bir örnek olarak gösterilebilir.

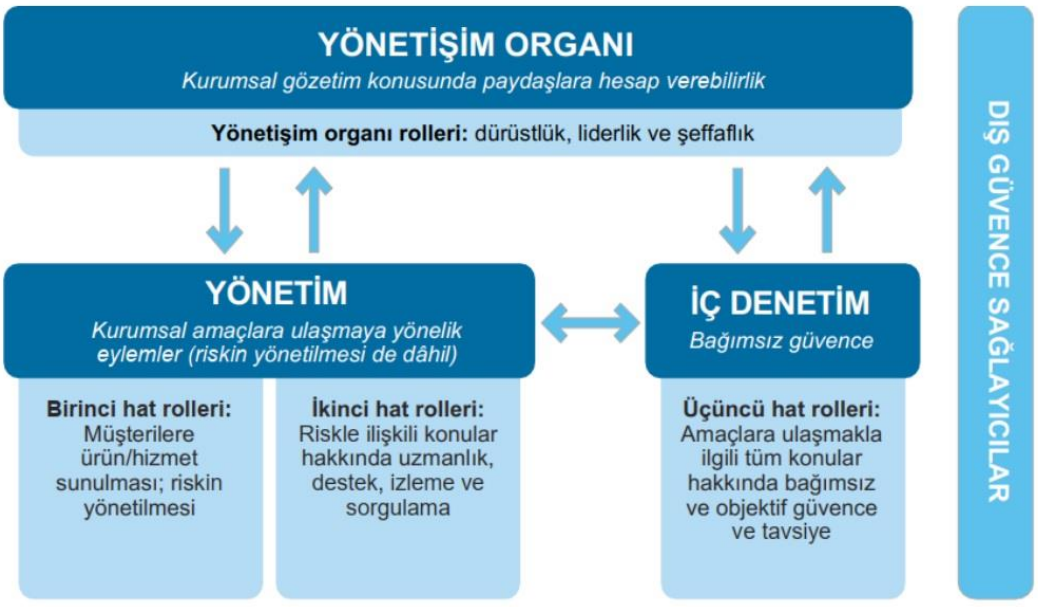
İÇ DENETİMİN ROLÜ

Finansal Olmayan Risk "Öncüleri"

Geleceğe Odaklı Kalma ve Kontrolleri İzleme

Şirketler nicel olarak ölçme konusunu ele almaya çalışırken iç denetimin rolü, IIA'nın Üçlü Hat Modelinde (bakınız: Şekil 1) tarif edildiği gibi stratejik olmak ve değer katmanın en iyi yollarına odaklanmaktır. Khayal, bu hedefi gerçekleştirmek için iç denetçilerin kendilerini tabloları ve finansal riskleri analiz etmekle sınırlamamaları gerektiğini, bunun yerine risk temelli bir yaklaşım izlemek ve her zaman geleceği düşünmek suretiyle finansal olmayan riskleri ele almada öncü olmaları gerektiğini söylemiştir. "İdeal olarak, kurumda geleceğe daha fazla odaklanan departmanlardan biri olmamız gerekir. Gelecekteki risklere, günlük etkilere odaklanan yönetim daha bu risklerin farkına varmadan odaklanmamız gerekli," demiştir Khayal. İç denetim, bağımsızlığını korumak ve sürdürmek için, kurumun kullandığı risk kategorilerini veya tanımlarını belirlemez ancak finansal olmayan risk politikalarına ve bu politikaların genel risk değerlendirme süreci doğrultusunda nasıl uygulandığına meydan okur.

Şekil 1: Üçlü Hat Modeli



Danışman olarak Collie'nin rolü iç denetçinin rolüne çok benzerdir ve finansal olmayan riskler söz konusu olduğunda denetçilerin izleyebileceği bir roldür. Başlangıçta, CEO ve CFO'nun yanı sıra uyum, risk ve iç denetim birimlerinin müdürleri de dâhil olmak üzere kurum liderleriyle görüşmektedir. Bu görüşmelerde liderlerin kurumları için risk tanımlarını, riskleri nasıl tanımladıklarını, hangi detay seviyesinde tanımladıklarını ve hangi kontrollerin mevcut olduğunu anlamayı amaçlamaktadır. Collie, bu görüşmeler sırasında katılımcıların genelde risk ve riskin etkisi hakkında yeni bir anlayış kazandıklarını söylemiştir.

Bu ilk görüşmeler, kurumun etkili faaliyet göstermesi için gerekenleri anlamak amacıyla yapılan üst düzey görüşmelerdir. Sonraki adım, günlük operasyonlar ve risklerin meydana gelebileceği alanlar hakkında daha fazla bilgi almak için departmanların yöneticileri veya müdürleriyle görüşmektir. Bu anlayışla birlikte denetçi, hangi risk yönetim adımlarının halihazırda başarılı veya başarısız olduğunu ve nerelerde risk yönetim zafiyetinin olduğunu anlamak için bu seviyede çalışanlarla beyin fırtınası yapabilir. Tıpkı danışmanların çeşitli kurumlarda deneyim sunabilmeleri gibi iç denetçiler de kurumun birçok alanı hakkında bütüncül bilgiye sahiptirler. Collie "Bu ekiplerin aklına gelmemiş olabilecek konuları gün yüzüne çıkarabilirsiniz," demiştir.

Denetçilerin süreci kolaylaştırmak için yeni becerilere ihtiyacı olacaktır. Geleneksel iç denetim yaklaşımları riskin kontroller, veriler ve dokümanlarla ilgili olarak tanımlanmasını içermektedir. Collie, finansal olmayan riskleri tanımlamak ve anlamak amaçlarıyla müşterilerle birlikte çalışmanın mülakatlarla veya betin fırtınası oturumunun kolaylaştırılmasıyla ilgili ilave beceriler ve sürekli eğitim gerektirdiğini söylemiştir. "Aslında müşterilerin risk belirleme sürecinden geçmelerine yardımcı olmak tamamen farklı bir çalışmadır," demiştir. Liderler, kurumun etkili ve verimli performans göstermesini sağlamak için bu eğitime yatırım yapmak zorunda kalacaktırlar.

İç denetim, özel olarak finansal olmayan riskler için geliştirilen yeni ölçümlerin ve ilişkili kontrol ve risk yönetim süreçlerinin yanı sıra var olan anahtar performans göstergeleri ve ölçütlerinin finansal olamayan risklere uygulandığındaki değeri ve güvenilirliğini de değerlendirebilir. ECIIA'ya göre, iç denetim yeşil aklama suçlamalarını önlemek için paydaşlarla paylaşılan verilerin kurumsal çaba ve çalışmaların adil ve doğru bir tablo çizilmesini sağlayabilir.[14]

Khayal, denetim planını ve risk değerlendirmesini kurumun hem finansal hem de finansal olmayan stratejisini gerçekleştirme becerisini etkileyebilecek birçok risk unsuru etrafında oluşturmaktadır. Örneğin, eğer kurumsal strateji ve değer yaratma titiz tedarik zinciri uygulamalarına dayanıyorsa satın alma her zaman önemli bir konu olacaktır demiştir. Risklerin ve özellikle de finansal olmayan risklerin haritalanması müşteri kredibilitesi sorunları, tedarik zinciri sorunları ve siber güvenlik zorlukları gibi tehditleri ortaya çıkarabilir.

Kurumlar kendi çerçevelerini oluşturdukça ve kullandıkları tanımları iyileştirdikçe finansal olmayan riskler hakkında ortak bir dil yaratmaktadır. Bu da birinci, ikinci ve üçüncü hatlar arasında risk hakkındaki iletişimi geliştirir; her hat için sorumluluklara açıklık getirir ve her birinin paylaşılan tanımlara kendi iyileştirmelerini eklemesine olanak tanır.

Geleceğe Yönelik Sorumluluklar

Khayal'ın çalıştığı kurumda, kontroller ve risk öz-değerlendirmesinde yer alan herkes finansal olmayan riskleri içeren detaylı bir risk eğitimi kursu almak zorundadır. Khayal, ayrıca personelini aşağıdaki üç anahtar göreve odaklanmaları için teşvik etmektedir:

- **Güncel kalma**. İç denetçiler, şu anda ya da kısa veya uzun vadede riski etkileyebilecek olaylara ilişkin daha iyi bir anlayış kazanmak için dünyada ve bulundukları bölgede meydana gelen son olaylardan haberdar olmak zorundadırlar.
- **Gelişmekte olan teknolojileri takip etme.** Khayal, geleceğin denetçilerinin ve çalıştıkları kurumların BT konusunda bilgili olmak zorunda olduklarına inanmaktadır. Denetçiler artık sadece geleneksel yöntemlere itimat edemezler, çalışmalarına teknoloji araçlarını da dâhil etmek zorundadırlar. "Dünya çok daha hızlı değişiyor," demiştir Khayal. Güçlü teknoloji olmadan "özellikle de karşılaştığımız giderek daha fazla makroekonomik faktörün finansal olmayan faktörler olmasından dolayı kurumlar ayak uyduramayacaklardır."
- **Kurumsal strateji, misyon ve vizyon ile uyumlu kalma.** Denetim planları hangi risklerin en önemli olduğunu ve bu risklerin en iyi nasıl ölçüleceğini düşünmek zorundadır. Kurumlar genelde karşı karşıya kalabilecekleri her risk tipini ele alamadığı için denetçiler önemi ve etkisi en büyük olabilecek riskleri tanımlamak ve ölçmeye çalışmak amaçlarıyla çeşitli faktörleri dikkate almak zorundadırlar.

[14] *Risk in Focus 2023: Risk in Focus 2023: İç Denetçiler için Önemli Konular*, Avrupa İç Denetim Enstitüleri Konfederasyonu, 2023.

VARILAN SONUÇLAR

Kurumun güvenilir danışmanları olarak iç denetçiler finansal olmayan risklerin daha iyi anlaşılmasını ve tanınmasını sağlamak için benzersiz bir konumdadırlar. İş ve işletme ile ilgili var olan kapsamlı bilgilerinden yararlanarak, yeni yetkinlikler ekleyerek ve finansal olmayan riskin en iyi nasıl ölçüleceğini belirleyen kurumsal bakış açısında bir değişikliği savunarak bunu yapabilirler.

Kısım 3: Dijital Dönüşüm GRC'yi Nasıl Dönüştürüyor?

Uzmanlar Hakkında

Sarah Kuhn, CIA, CCSA, CRMA

Sarah Kuhn, iç denetim alanında oldukça deneyimli bir profesyoneldir. İç Denetçiler Enstitüsü'nde (IIA) 20 yılı aşkın üyeliği ve Tulsa Şubesinin eski başkanlığı sayesinde, analitiğe ve otomasyona odaklanan bir denetim ekibine liderlik etmeni yanı sıra departman eğitimi, raporlama ve standartlara uyum konularındaki deneyimiyle sektöre bağlılığını göstermiştir. Sarah, ayrıca şu anda IIA Houston Şubesinde çalışmaktadır.

Audra Nariunaite, CIA, CISA, CFE, CHC, CHPC

Audra Nariunaite, birden fazla sektörde deneyimi olan ve stratejik girişimler ve süreçlerin yeniden yapılandırılması yoluyla büyüme ve mükemmeliyet sağlama konusunda kendini kanıtlamış bir uyum ve denetim uzmanıdır. Şu anda IIA Kuzeydoğu Florida Şubesi'nin yönetim kurulunda görev yapmaktadır ve IIA-Litvanya üyesidir. Audra, şu anda küresel istihdam platformu olan Oyster HR kurumunda uyum direktörüdür.

Giriş

Muhtemelen, hiçbir trend yönetişim, risk ve uyum (GRC) ortamını teknolojilerin günlük iş operasyonlarındaki yükselişinden daha önemli ölçüde etkilemiyor ve bunun nedenini anlamak çok kolay. Dijital dönüşümün faydaları küçümsenemez ve bu trendden doğan araçlar şu anda neredeyse tüm büyük endüstrilerde süreçleri otomatikleştirmek ve hızlandırmak için kullanılıyor; bu da GRC ve güvenlik operasyonlarının potansiyel risk ve sorunları hızlı tanımlayıp onlara yanıt vermesine olanak tanıyor.

Örneğin, e-postalardan sosyal medya akışlarına kadar yapılandırılmamış veri kaynaklarını analiz etme kabiliyeti olan yapay zekâ destekli doğal dil işleme, beşerî GRC ekiplerinin beceri ve deneyimleriyle birleştirilerek sadece bir nesil önce hayal bile edilemeyecek bir karmaşıklık ve gelişmişlik düzeyinde risk ve uyum yönetimi kaynakları sağlayabilir.

Böylesine radikal bir dijital dönüşüm geçirme ihtiyacı bir zamanlar lüks olarak görülmüş olmasına rağmen, günümüzde söz konusu olan risk ortamı kurumlara bu dönümü geciktirmek için çok az alan tanımaktadır. Siber tehditlerin hacmi ve karmaşıklığı gün geçtikçe artmaktadır; üretilen, toplanan ve işlenen verilerin ham hacmi şaşırtıcı bir oranda artmaya devam ederek sürekli artan veri gizliliği riskleri yaratmaktadır ve düzenleyici ortam günümüz risklerinin hızına ayak uyduracak şekilde hızlı gelişip değişmeye devam etmektedir. Gerçekten de dijital dönüşümün sağladığı avantajlar olmadan, günümüz dünyasında GRC fonksiyonları pekâlâ yitirilebilir.

IIA'nın GRC hakkındaki Küresel Bilgi Özeti serisinin 3. Kısmı olan bu son bölüm, dijital dönüşümü benimsemenin ne gibi doğal riskler içerdiğinin yanı sıra GRC sistemlerinin yeni teknolojilerin eklenmesi sayesinde nasıl geliştiğini de ele almaktadır. Bu özet, iç denetimin bu tartışmanın neresinde bulunduğunu ve bu kritik yolculuğa devam ederken kurumlara en iyi nasıl yardım edebileceği konularını da ele almaktadır.

2023 Dijital Dönüşüm Konusu

Yüklü riski anlama

Dijital dönüşümün kapsamı

COVID-19 salgını sırasında görülen dijital dönüşüm patlaması şiddetlenmeye devam etmektedir ve bazı açılardan evrimi hız kazanmaktadır. Bu durum sadece pazarda rekabet üstünlüğü elde etmek için kâr ve verimliliği artırma arzusundan değil, aynı zamanda son yıllarda ortaya çıkan kapsamlı risklerden oluşan listeye ayak uydurma (veya ideal olarak bunların önüne geçme) dürtüsünden kaynaklanmaktadır. Enflasyon, Ukrayna çatışması ve Çin-Tayvan çekişmesi gibi jeopolitik gerilimler, çok sayıda büyük ölçekli bankacılık kurumunun aniden kapanması gibi olaylardan kaynaklanan geniş kapsamlı ekonomik belirsizlik, ÇSY risklerine ve düzenleyici ortamda yapılan ilişkili değişikliklere ilişkin sürekli devam eden tartışmalar, tedarik zinciri aksaklıkları ve eksiklikleri — bunlar riskin 2023 yılında aldığı formlardan sadece birkaçıdır. Bu risklere karşı bir nevi güvence sağlayıp sürdürmekle görevli kurumların perspektifinden bakıldığında, dijital dönüşümün geniş ölçekte benimsenmesi etkili bir merhem gibi görünmektedir. Gerçekten de Gartner tarafından hazırlanan yakın tarihli bir rapora göre, yönetim kurulu üyelerinin sadece %35'i dijital dönüşüm hedeflerine ulaştığını ya da ulaşma yolunda ilerlediğini belirtmesine rağmen %89'u dijital işin tüm ticari büyüme stratejilerinin bünyesine dâhil edildiğini söylemektedir.

Gartner kurumunda başkan yardımcısı ve uzman analist olan Jorge Lopez bu raporda "Yönetim kurulları, dijital iş stratejisi ve genel iş stratejisinin bir ve aynı şey olduğu noktaya ulaştılar," demiştir. "CIO'lar operasyonel mükemmeliyet için teknolojiden yararlanmada önemli ilerleme kaydetmiş olmasına rağmen, bu ilerleme [yönetim kurullarının] dijital yatırımlardan beklediği stratejik iş faydalarını gerçekleştirmek için yeterli değildir."[15]

Dijital dönüşümün nasıl göründüğü bölge den bölgeye, endüstriden endüstriye ve kurumdan kuruma çeşitlilik göstermektedir. Bir kurumun etkili veya hatta ulaşılabilir gördüğü başka bir kurum için ideal olmayabilir. Buna rağmen, dijital dönüşümün bir formunu benimseyen kurumlar arasında birtakım temel benzerlikler vardır. Brainvire kurumunun CEO'su ve kurucusu olan ve Forbes için yazılar yazan Chintan Shah "[Dijital dönüşüm] teknolojiden daha fazlasıdır. Kurumların iş model ve süreçlerini ortaya çıkan yeni teknolojilerin doğurduğu fırsatlardan faydalanacak şekilde yeniden tasarlamalarını sağlayan zihniyet değişimidir," demiştir.[16]

Lopez de benzer bir görüşü dile getirmiştir. "İşletmeler sürekli kesintilerin söz konusu olduğu bir dünyada giderek daha fazla faaliyet gösterirken geleceği en iyi kavrayan yönetim kurulları çalkantı ve risklerin nasıl bir fırsat kaynağı olabileceğini düşünmektedir. Teknoloji iş başarısını artırma konusunda kapsamı sürekli genişleyen bir rol oynadıkça CEO'ların ve CIO'ların da bu zihniyeti benimsemeleri gerekecektir."

Bu tür bir yeniden tasarlama, aşağıda sayılanlar da dâhil ancak bunlarla sınırlı kalmaksızın birçok farklı şekilde olabilir:

- Yapay zekâ (AI), makine öğrenimi ve doğal dil işlemenin benimsenmesi.

15. "Gartner, Yönetim Kurulu Üyelerinin %89'unun Dijitalin Tüm İş Büyüme Stratejilerinin Bünyesine Dâhil Edildiğini Söylediğini Belirtmiştir (Gartner Says 89% of Board Directors Say Digital Is Embedded in All Business Growth Strategies)," basın bülteni, Gartner, 29 Ekim 2022, https://www.gartner.com/en/newsroom/press-releases/2022-10-19-gartner-says-89-percent-of-board-directors-say-digital-is-embedded-in-all-business-growth-strategies.

16. Chintan Shah, "İşletmelerin 2023 yılında Bu Dijital Dönüşüm Trendlerini İzlemesi Gerekiyor (Businesses Need to Watch these Digital Transformation Trends in 2023)," Forbes, 27 Ocak 2023, https://www.forbes.com/sites/forbestechcouncil/2023/01/27/businesses-need-to-watch-these-digital-transformation-trends-in-2023/?sh=7147b04a185d.

- Robotik süreç otomasyonu (RPA).
- Siber güvenlik ve veri gizliliği odağı.
- Buluta geçiş.
- Veri analitiği.
- 5G'ye geçiş ve dijital optimizasyon.
- Blok zincir.
- Sanal iş birliği.
- Tüketici veri platformları.

Dijital dönüşümün GRC üzerindeki etkisi

Pek çok çağrışımı ve uygulaması olan dijital dönüşümün GRC fonksiyonları üzerinde önemli bir etkisi olduğu açıktır ve çoğu durumda kurumlar teknoloji ortamındaki değişiklikler hızlı şekilde devam ederken GRC kapsamını yeterli düzeyde tutmakta zorlanmaktadırlar. Risk.net kurumunun IBM iş birliğiyle finansal hizmetler sektöründe çalışan GRC profesyonelleri arasında yaptığı yeni bir anket, aşağıdakiler de dâhil olmak üzere bazı endişe verici eğilimleri ortaya çıkarmıştır:

- Katılımcıların %62'si, dijital dönüşümün var olan GRC süreçlerindeki boşlukları ortaya çıkardığına inanmaktadır ve katılımcıların neredeyse yarısı (%45) kurumlarının şu anda "arayı kapatmak için çok çalıştığını" düşünmektedir. Sadece %37'si, geçişten önce dijital dönüşümlerine zaman ve kaynak yatırımı yaptıklarını söylemiştir.
- Katılımcıların %77'si, dijital kanallara daha fazla bağlı hale geldikçe firmalarının karşı karşıya olduğu risklerin arttığına inanmaktadır.[17]

Buna ilave olarak, aynı çalışmada, dijital dönüşüm trendlerinin sonucunda kurumlarında hangi risklerin daha fazla önem kazandığı sorulduğunda katılımcıların %56'sı bilgi/veri güvenliği, %48'i siber güvenlik ihlâlleri, %32'si üçüncü taraf/tedarik zinciri riski ve %31'i uyum riski demiştir.

GRC fonksiyonları, etkin kalabilmek için, dijital dönüşümü benimsemek üzere kesin adımlar atarak modernize olmak ya da kurumlarını önemli risklere maruz bırakma riskini almak zorundadır. Bu tür adımlar aşağıda sayılanları içermektedir:

- Yeni kaynaklar tahsis etmek veya edinmek.
- Gelişmiş veri analitiği kullanımları için bir tür hibrid bulut veri depolama modelini benimsemek.
- Güncel GRC araçlarını ve kapasitelerini güncellemek.
- AI ile ilişkili araçlar ve otomasyon sistemleri de dâhil olmak üzere ileri teknoloji kullanmak.

Bu eylemlerden bazıları biraz aşikâr görünmesine rağmen güncek risk ortamının değişip gelişme hızı onları böyle olmaktan çıkarıyor. Örneğin, geçmişte kurumlar GRC fonksiyonunu başarıya ulaştıran kanıtlanmış kontrol ve süreçlerden oluşan bir temel oluşturmak amacıyla belirli bir rehbere veya standartlardan, sertifikalardan ve/veya düzenlemelerden oluşan bir çerçeveye uymaya itimat etmişlerdir.

Ancak, günümüzde, bu tür bir yaklaşım hızlı şekilde karmaşık hale gelebilir. Bu durum aşağıdakilerden kaynaklanabilir:

17. "Dijital Dönüşüm ve GRC'nin Geleceği (Digital Transformation and the Future of GRC)," Risk.net, IBM, Şubat 2022, https://www.ibm.com/downloads/cas/WWQXRPLG.

- Hızlı uyum gerektiren yeni veya güncellenmiş çerçevelerin süratle geliştirilmesi. AB'de dijital stratejiyle ilgili olarak Veri Uyum Yasası, Dijital Piyasalar Yasası, Dijital Hizmetler Yasası, Veri Yasası ve Yapay Zekâ Yasası da dâhil olmak üzere, 2023 yılının sonuna kadar onaylanması beklenen çeşitli düzenleyici girişimlerin hızlı şekilde ortaya konulması örnekler arasında yer almaktadır ya da
- Mevcut çerçevelerin netlik veya rehberlik sağlamaması, kurumları — en azından bir süre boyunca — kendi başlarının çaresine bakmak zorunda bırakmaktadır.

Meslekte yirmi yılı aşan deneyimi ve hizmetiyle tanınan bir iç denetim lideri olan Sarah Kuhn "ChatGPT ve Bing Chat gibi sistemler piyasaya sürülmüşken ve CoPilot şu anda piyasaya sürülmeye hazırlanırken birçok kurumun hızlı hareket etmesi gerekiyor çünkü çalışanlar görevleri tamamlamak için bu teknolojilerden bazılarını zaten kullanıyor," demiştir. "Bazı kurumlar bunları tamamen engellerken, teknolojileri anlamak için daha donanımlı ekiplerin bulunduğu diğer kurumlar bunların nasıl ve ne zaman kullanılması gerektiği konusunda daha detaylı dâhili rehberler hazırlayacaktır."

Bu tür rehberler oluşturmaya yönelik stratejiler geliştirmekle görevlendirilen bu ekiplerin yapısı kuruma göre çeşitlilik gösterecektir ama dijital konulardan ve bilgiden sorumlu genel müdür yardımcısı, BT ve risk yönetim ekipleri, hukuk ve finans grupları gibi tarafları içerebilir. Ancak, oluşturulduktan sonra bu rehberlerin iletilmesi ve uygulanmasına yönelik stratejiler de aynı düzeyde kritiktir. Kuhn "Şirketler bir dereceye kadar onur sistemiyle faaliyet gösterebilir ancak değişip gelişen rehber ilkeleri iletmek için daha resmi önlemler gereklidir. Örneğin, bir çalışan belirli bir adresi girdiğinde tarayıcısında şirket rehber ilkelerini hatırlatan bir banner açılmasını sağlayacak programlar uygulanabilir," demiştir.

Kuhn, bu tür başarıları böyle sorunsuz şekilde gerçekleştirmek için ChatGPT gibi yeni teknolojiler kurumun risk ortamına girmeden önce çevik, uyarlanabilir bir GRC fonksiyonunun mevcut olması gerektiğini belirtmiştir. Kaynakların kısıtlı olması, eldeki verilerin sınırlı veya kalitesinin düşük olması, başka konulara öncelik verilmesi ya da basit bir ihmal nedeniyle tüm kurumlarda böyle bir öngörü olmayacaktır. Sebebi ne olursa olsun, iç denetimin bu yeni dönemde başarılı olmak için GRC fonksiyonlarını hızlı bir şekilde uygun konuma getirmek üzere inisiyatif almaya hazır olması gereklidir.

GRC Tartışmasında İç Denetim

Dijital dönüşüm bağlamında GRC'nin iyileştirilmesi

Masada yer tutma

İç denetim, özellikle GRC fonksiyonlarını güncelleme hedeflerinde geri kaldığı düşünülen kurumlarda etkili GRC'yi birden fazla önemli yolla destekleyebilir.

İlk olarak, takip etmeye değer çok az değişiklik belirli bir yatırım olmadan gerçekleştirilebilir. Ancak, kurumun en tepesinden GRC fonksiyonundaki her bir münferit paydaşa kadar her seviyeden katkı ve destek olmadan bu tür yatırımları yapmak zor olabilir. Dijital dönüşüm konusunda katkı ve destek yoksa sağlayacağı faydaların uygun şekilde iletilmemiş olma ihtimali vardır. Bu bakımdan, iç denetim sadece masada yer tutarak bu tür bilgileri aktarmak için benzersiz bir konumdadır.

Kuhn "Masadaki yerimiz sayesinde, yönetim ve yönetim kurulunun ortaya çıkan her yeni trend doğrultusunda bilgiye dayalı kararlar almasını sağlayabiliriz," demiştir.

Gerçekten de iç denetçilerin görevlerini yetkilerine uygun olarak ifa etmesi için masada yerinin olması her zaman kritik düzeyde önemli olmalıdır. İç denetim, paydaşlarla düzenli ve bilgiye dayalı iletişim yoluyla, risk güvencesi ve uyum etrafında güçlü bir kurumsal kültürü destekleme ve teşvik etmede değerli bir rol oynamaktadır. İç denetim iletişim kanallarından tam potansiyelinde yararlanıldığında GRC'nin asla akıldan çıkmaması gereklidir.

GRC araçlarının yayılma riski

Uygulamaya hazır tüm kontroller başarılı bir GRC odaklı kültür için elverişli olmayacaktır. Örneğin, kurumsal süreçlerin dijitalleşmesiyle birlikte, GRC modüllerini eklenti olarak sunan birçok veri analitiği aracı vardır. Münferit GRC fonksiyonlarının kendilerine yardımcı olacak ayrı araçlar kullanmayı tercih etmeleri durumunda, iç denetim paydaşlara GRC'ye ilişkin kapsamlı bir bakış iletme konusunda önemli bir engelle karşılaşabilir.

Otomatikleştirilmiş istihdam platformu sağlayıcısı olan Oyster kurumunda uyum direktörü olan Audra Nariunaite "Veri analitiği araçlarını ve sundukları %100 test olanaklarını seviyorum ancak şu anda GRC'yi bir değer teklifi olarak bünyesine ekleyen birçok başka araç vardır. Yakın zamanda incelediğim bir araç, hangi sözleşmelerin yenilenmeye yakın olduğunu ve vergilerde yapılabilecek potansiyel tasarrufları göstermek için diğer SaaS araçlarını bir araya getiriyor ancak aynı zamanda SaaS araçlarının işlediği bilgilere dayanarak risk panosunun bir çeşidini de sunuyor. Bu tür bir aracı satın alma amacımız GRC'den farklı bir şey için olsaydı bu araçtan haberim bile olmazdı," demiştir.

"Birdenbire, tedarikçilerin özel bilgilerimizi işlemesi nedeniyle tümünün yüksek risk teşkil ettiği bileşenleri olan bir düzine SaaS aracına sahip olduğum bir durumda olabilirdim," diye devam etmiştir Nariunaite. "Şu anda, ekosistemimizde 100'den fazla SaaS aracı var. Bu araçların küçük bir yüzdesi GRC'nin çok spesifik süreçlerine yönelik bir versiyonunu sunmasına rağmen yönetmesi zorlaşıyor. Bu durum insanlar risk değerlendirmesi yaptıklarına inandıkları münferit boşluklar yaratıyor ancak bu risk değerlendirmelerini bütüncül ve raporlanabilir şekilde entegre edilmiş tarzda yapmıyorlar."

Bu tür bir riske karşı koyabilmek için, GRC paydaşlarının benimseyebileceği stratejilerden biri GRC yaklaşımını düzene koymak ve iç denetim için açık bir iletişim yolu yaratmak amaçlarıyla münferit süreç sahipleri atamaktır. Nariunaite "Herkes doğru olanı yapmak istiyor. Şu anda genel riski yönetmeye yönelik bir baskı var ve bu harika. Ancak, öncelik ve kapsamların uyumlu hale getirilmesi için görev ayrılığı ve bunun nasıl yapılması gerektiği tartışılmalıdır," demiştir.

Kuhn, kurumların paylaşılan sorumluluk ve yukarıdan aşağıya kontrol arasında kurması gereken dengeyi vurgulayarak benzer bir görüş ifade etmiştir. "İç denetimin, GRC hedef ve süreçlerini mümkün olduğunda paydaşların yönlendirmesine izin vermeye çalışması ve ardından, iş birliği ve şeffaflığı teşvik edip destekleyen bir bağlamda yaklaşması gereklidir. İç denetim bu muhabbetin bir parçası olmak zorundadır; böylece bir sorun gördüğümüzde kırmızı bayrak çekmek için orada olabiliriz. Çoğu insan risk ve kontrolü kendi rolleriyle ilgili olarak anlar. Aslında bizim müdahale etmemize ihtiyaçları yok ama yeterli gözetim için daha kapsamlı hedefleri ve sorumlulukların nerede konumlandırıldığını anlamamız gerekiyor."

Tartışmayı yönlendirmeye ve teşvik etmeye yönelik stratejiler

Mümkün olduğunda, iç denetim dijital dönüşümün faydalarını öngörüp teşvik ederek fonksiyonunun etkinliği yoluyla örnek olmak zorundadır. İç denetim bünyesinde dijital dönüşümün bazı yönlerinin bütçe serbestisi gerektirdiği açık olsa da temel otomasyon gibi diğer yönleri, muhtemelen kurumda zaten mevcut olan ya da en azından minimum maliyetle satın alınabilen, örneğin Excel, Power BI ve diğer Microsoft üretkenlik araçları gibi programlar aracılığıyla gerçekleştirilebilir.

Örnek olmak, GRC fonksiyonlarında kritik yetkinliklerin bulunmadığı yerlere dikkat çekmek de dâhil olmak üzere bilginin paylaşılması için de geçerlidir. Hem iç denetim fonksiyonu bünyesinde hem de diğer departmanlarda, iç denetim bir yandan işgücünün yeni ortaya çıkan teknolojilerle çalışmasıyla ilgili bilgi, eğitim veya deneyim eksikliklerini vurgularken diğer yandan uygun düzeltici tedbirleri teşvik ederek yapıcı bir rol oynayabilir. Konferanslarda ortak eğitim, personeli eğitmek ve onlara beceri kazandırmak için harici tarafların istihdam edilmesi ya da ücretsiz veya makul ücretli çevrimiçi kaynaklar aracılığıyla beceri temelli eğitimin iş rollerine dâhil edilmesi bu tür tedbirler arasında yer alabilir.

Bazı durumlarda, kurumlar becerilerin diğer departmanlarla etkileşim ve iş birliği yoluyla kurum içinde kazanılması ve geliştirilmesini teşvik etmek üzere çalışabilir. Kuhn "Gördüğüm stratejilerden biri, kurumdaki herkesin kendi inovasyon fikirlerini paylaşabileceği ve sonrasında şirkette görmek istediklerine oy verebilecekleri veya yorum yapabilecekleri bir internet sitesi oluşturmaktır. Bu, bilgi ve fikirlerin kontrollü şekilde paylaşılması için bir yol olabilir ve böylece, herkes yetkinlik kazanmak ve geliştirmek için binlerce farklı şey yapmak zorunda kalmaz," demiştir.

Bu tür bir tartışmanın her zaman resmi olması şart değildir; toplu bir sohbet gibi basit bir iletişim bile benzer sonuçlar doğurabilir. Nariunaite "Bizim kurumumuzda herkesin katılabileceği birden fazla Slack kanalı var. Örneğin, son zamanlarda mühendislik mizah kanalında takılıyorum. Uyum departmanının başında olduğumu anlıyorlar ama bana arkadaşları gibi davranıyorlar. Hepimizin dijital dönüşüm hareketinin fiilen ön saflarında yer alan ekiplerle gayri resmi bağlantılar kurabilmesini seviyorum," demiştir.

Ancak, tartışmanın katkıda bulunan parçalarından biri olabilmek için, iç denetimin bu teknolojiler hakkında bilgi sahibi olmasına yönelik ilave bir itici güç olması gereklidir.

Gerçekten de bu tür bilgileri edinmek iç denetimin sunduğu kurumsal değere katkıda bulunması için kıymetli bir fırsat olabilir. Nariunaite "Paydaşlarla, örneğin AI veya veri analitiği ile ilgili görüşmek istediğimizde, eğer bunlar hakkında önemli ölçüde bilgi sahibi değilsek, onlarla yapılan tartışmalara anlamlı şekilde dâhil olabileceğimizi sanmıyorum. GRC'de dijital dönüşümün birçok yönü, bunların sahipliğini üstlenecek taraflar açısından hâlâ belirsizliğini koruyor. Neden iç denetim olmasın ki? Meraklıyız, açık fikirliyiz ve müşterilerimizle birlikte daima öğreniyoruz; bu nedenle tartışmalara katılabiliriz. Uyum alanında AI uygulaması gibi bir konuda danışmanlık sağlayanlar biz olsaydık ne olurdu?" demiştir.

Varılan Sonuçlar

İç denetim topluluğunun aktif üyesi olmak

Dijital dönüşümden geriye dönüş yoktur ve kurumlar için seçenekler basittir: benimse veya geride kal. Bu görüş gerçekten de tepe pozisyon ve yönetim kurulu toplantı odasından GRC, operasyon ve iç denetime kadar kurumun her unsuruna yayılmaktadır.

Buna ilave olarak, özellikle de giderek birbirine bağlanan ve küreselleşen dünyada, bu görüşün endüstriler ve coğrafi sınırlar boyunca yayılması gereklidir. Bu da sadece kurumun sınırları içerisindeki görevleri ifa etmek değil, bunun ötesine geçerek küresel denetim tartışmalarında aktif bir katılımcı olmak anlamına gelmektedir. IIA internet seminerlerine ve konferanslarına düzenli katılmak gibi yerel IIA şubelerine dâhil olmak da bu tür bağlantılar kurmak için uygun bir ortam olabilir.

Nariunaite "Alabileceğiniz en iyi iç denetim eğitimi, diğer fonksiyonların deneyimlerini ilk elden duymaktır. Twitter'da diğer profesyonellerle güncel denetim konuları ve teknoloji trendleri üzerine 'kafa yorarken' çok şey öğreniyorum. Mesleğe başladığımdan beri çok şey değişti; bu sektör bağlantılarını sürdürmek ve başkalarının sizin karşılaştığınız zorluklarla nasıl başarılı şekilde başa çıktığının nabzını tutmak çok önemlidir," demiştir.

Teknoloji çok ilerlemiş — ve ilerlemeye devam edecek — olmasına rağmen, mesleki bir rolde öğrenme ve büyüme söz konusu olduğunda, gerçek insan ilişkisinin yerini hâlâ hiçbir şeyin tutamadığını bilmenin verdiği bir rahatlık vardır. Bu amansız değişim karşısında bunu hatırlamak önemli olacaktır.

IIA Hakkında

İç Denetçiler Enstitüsü (IIA) 235.000'den fazla küresel üyeye hizmet veren ve dünya çapında 190.000'den fazla Sertifikalı İç Denetçi (CIA) sertifikası vermiş olan, kâr amacı gütmeyen uluslararası bir meslek kuruluşudur. 1941 yılında kurulan IIA, dünya çapında iç denetim mesleğinin standartlar, sertifikalar, eğitim, araştırma ve teknik rehberlik alanlarında lideri olarak tanınmaktadır. Daha fazla bilgi için, lütfen theiia.org adresini ziyaret ediniz.

Sorumluluğun Reddi Beyanı

IIA bu dokümanı bilgi ve eğitim amaçlı yayımlamaktadır. Bu materyalin spesifik münferit koşullara kesin ve nihai cevaplar vermesi beklenmemelidir ve sadece bir rehber olarak kullanılması amaçlanmıştır. IIA, herhangi bir spesifik durumla doğrudan ilgili konularda daima bağımsız uzman tavsiyesi almanızı önerir. IIA, herhangi bir kimsenin bu rehberi tek referans kaynağı olarak kullanması durumunda hiçbir sorumluluk kabul etmez.

Telif Hakkı

Haziran 2023

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101