TONE at the TOP®

Üst yönetime, yönetim kurullarına ve denetim komitelerine yönetişimle ilgili konularda kısa ve öz bilgiler sunar.

Sayı 120 | Aralık 2023

Yöneticilerin 2024'te Dikkate Alması Gereken Riskler

Mevcut ve ortaya çıkan riskleri belirlemeyi amaçlayan ve dünyanın geneli ile altı farklı bölgesindeki şirketler için ayrı ayrı yapılan bir ankette siber güvenlik ve beşeri sermaye en önemli riskler arasında yer almıştır. İç Denetçiler Enstitüsü (IIA) İç Denetim Vakfı tarafından yayınlanan Risk in Focus 2024, iç denetim liderlerine kurumlarındaki mevcut risk ortamı (bkz: Şekil 1) ve denetim planlarında hangi alanlara odaklandıkları konusunda bir anket düzenlemiştir. Ayrıca, önümüzdeki üç yıl içinde hangi risklerin en önemli olacağını tahmin etmelerini de istemiştir. Tone at the Top yayınının bu sayısı, liderlerin belirledikleri en önemli

risklerden bazılarını ele almaktadır. Yönetim kurullarının yeni ortaya çıkan tehditleri değerlendirmesinde iç denetim bu yönetişim çabalarının önemli bir ortağı olabilir. IIA küresel ilişkilerden sorumlu başkan yardımcısı Javier Feleato CIA, CRMA, CCSA, bu noktada şöyle demiştir:

"İç denetçiler riske proaktif bir yaklaşım benimsiyor. Şirketlerin yolculuklarında onlarla birlikte yürüyor ve doğru yola girmelerine yardımcı oluyor."

Siber Güvenlik Riskini Anlamak

Siber suçlular son yıllarda daha sofistike hale geldikçe birçok yönetim kurulu bünyesine siber güvenlik uzmanlığı eklemiştir ancak teknoloji jargonu kullanılarak tartışılan konuların iş operasyonlarına nasıl uygulanabileceğini belirlemek zor olabilir. Faleato, iç denetimin siber tehditler ve potansiyel iş riskleri arasındaki bağlantıyı kurarak bir tercüman olarak hizmet vermek için benzersiz bir konumda olduğunu belirtmiştir. İç denetim liderleri, yönetim kurullarına kurumu etkileyen siber güvenlik gelişmeleri ve olayları ile bunların risk yönetimini ve stratejik planlamayı nasıl etkilediği hakkında güncel bilgiler sağlayabilirler. İç denetim ayrıca siber güvenlikle ilgili yönetişim süreçlerinin etkinliğini de gözden geçirebilir. Faleato "İç denetimin rolü, yönetim kurullarının neyin işe yaradığını ve neyin işe yaramadığını fark etmelerini sağlamaktır," demiştir.

Bölgelere göre en yüksek riskler (%)

Kurumunuzun şu anda karşı karşıya kaldığı en önemli 5 risk nedir?

Denetim alanı	Tüm bölgelerin ortalaması	Asya Pasifik	Güney Amerika	Afrika	Kuzey Amerika	Orta Doğu	Avrupa
Siber güvenlik	%73	%66	%75	%58	%85	%70	%84
Beşeri sermaye	%51	%59	%44	%39	%65	%47	%50
İş sürekliliği	%47	%61	%47	%52	%36	%53	%35
Mevzuat değişikliği	%39	%35	%48	%32	%43	%33	%43
Dijital bozulma	%34	%30	%38	%33	%36	%32	%33
Finansal likidite	%32	%21	%33	%47	%28	%38	%26
Pazardaki değişimler	%32	%47	%26	%21	%41	%26	%30
Jeopolitik belirsizlik	%30	%28	%42	%25	%28	%16	%43
Yönetişim/kurumsal raporlama	%27	%24	%18	%36	%16	%45	%22
Tedarik zinciri ve dış kaynak kullanımı	%26	%27	%16	%19	%36	%28	%30
Kurumsal kültür	%26	%23	%26	%34	%21	%30	%20
Hile ve Suistimal	%24	%22	%30	%46	%9	%26	%13
İletişim/itibar	%21	%18	%22	%27	%21	%28	%12
İklim değişikliği	%19	%22	%22	%19	%12	%10	%31
Sağlık ve güvenlik	%11	%12	%8	%10	%17	%9	%13
Şirket birleşmeleri ve satın almaları	%6	%4	%3	%3	%8	%10	%8

Kaynak: Risk in Focus 2024

Şekil 1

Not: IIA Risk in Focus Küresel Anketi, n=4.207. Yüzde değerler, risk alanını risk düzeyi açısından ilk 5'te kimin sıraladığını göstermektedir. Koyu mavi gölgelendirme, o bölge için en yüksek riske sahip 5 risk alanını göstermektedir

İç denetim ekibi ayrıca şirketin ilgili tehditleri azaltmak için gereken her şeyi yapıp yapmadığı konusunda da içgörüler sağlayabilir. Genel olarak, bu anket iç denetim ekiplerinin denetim planlamalarında siber güvenliğe daha fazla önem verdiklerini ortaya çıkarmıştır. Siber güvenlik uzun zamandır Risk in Focus endişeler listesinin en başında yer alsa da geçmişte denetim ekipleri bu alana en fazla zaman ve çabayı ayırmıyordu. Bu yıl yapılan ankete göre bu durum değişmiş ve siber güvenlik, denetim ekiplerinin odaklandığı diğer konuların önüne geçmiştir. Yönetim kurulları, iç denetim ekiplerinin siber güvenlik konularını ele almak için yeterli kaynağa sahip olmalarını sağlayarak uygun odağı korumaya devam etmelerini güvence altına alabilirler.

Çoğu kurumdaki en büyük siber güvenlik zafiyetinin insan unsuru olduğu maalesef bir gerçektir. Çalışanlar, oltalama e-postaları veya siber suçlulara erişim sağlamak için tasarlanan ve giderek sofistike hale gelen diğer dolandırıcılık yöntemleri yoluyla hedef alınmaktadır. Yöneticilerin, siber güvenlik söz konusu olduğunda üst yönetimin tavrı ve tutumunun ne kadar önemli olduğunu ve yönetim kurullarının sahip olabileceği pozitif etkiyi unutmamaları gereklidir. Personel yönetim kurulu üyelerinin siber güvenlik çabalarının farkında olduğunu ve bu çalışmalara dâhil olduğunu gördüğünde, akıllı siber güvenlik kurallarını ihmal etme olasılıkları daha az olabilir, demiştir Faleato. Yönetim kurullarının, örneğin oltalama saldırıları hakkındaki kurumsal eğitimlerin bir parçası olmayı ve iç denetimin desteğiyle yönetim kurulu düzeyinde fidye saldırısı senaryolarına katılmayı düşünmelerini tavsiye etmiştir.

IIA Hakkında

The Institute of Internal Auditors (IIA), 230.000'den fazla küresel üyeye hizmet veren ve dünya çapında 185.000'den fazla Sertifikalı İç Denetçi (CIA) sertifikası vermiş kâr amacı gütmeyen uluslararası bir meslek birliğidir.

1941 yılında kurulan IIA, dünya çapında iç denetim mesleğinin standartlar, sertifikalar, eğitim, araştırma ve teknik rehberlik alanlarındaki lideri olarak tanınmaktadır. Daha fazla bilgi için theiia.org adresini ziyaret ediniz.

The IIA

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

Ücretsiz Abonelik

Ücretsiz abonelik kaydınızı yapmak için theiia.org/Tone adresini ziyaret ediniz.

Okuyucu Geribildirimi

Sorularınızı ve yorumlarınızı Tone@theiia.org adresine gönderiniz.

En Önemli Kurumsal Varlık için Yönetişim

Personelin yeteneği ve uzmanlığı şirketin başarısı için kritik düzeyde önemlidir. Kurumlar hem insan sermayesi, çeşitlilik, eşitlik ve kapsayıcılığın hem de yetenek yönetimi ve yeteneği kurumda tutmanın dikkate alınması gereken önemli konular olduğunun farkındadırlar ancak birçoğu bu alanlarda gösterilen çabanın anlamlı bir etkisi olup olmadığının nasıl ölçüleceğini bilmemekte veya emin olamamaktadır. Yeni nesil çalışanların değişen beklentileri ve uzaktan ve hibrit çalışma programları konusunda süregelen tartışmalardan dolayı bu konu daha da karmaşık hale gelmiştir.

Riskler ve belirsizlikler göz önüne alındığında yönetim kurullarının net bilgi ve tavsiyelere ihtiyacı vardır. İç denetim, yönetim kurullarının hangi insan sermayesi ölçütlerinin yönetim kurulu için en kıymetli olduğunu belirlemelerine yardımcı olabilir ve karmaşık anahtar performans göstergelerini (KPI) stratejik ve yönetişim perspektifinden anlaşılması kolay bir şekilde sunabilir. Örneğin, iç denetim yönetim kurulunun insan sermeyesi ve çeşitlilik stratejilerini değişen kültürel norm ve beklentilere daha uygun hale getirmek için kullanabileceği personel tatmin ölçümleri de dâhil olmak üzere çok çeşitli aydınlatıcı kurumsal bilgiye erişebilmektedir.

Yeni Ortaya Çıkan Risklere Hazırlanmak

Risk in Focus 2024, iç denetim liderlerinden kurumlarının günümüzden itibaren karşılaşabileceği riskleri derecelendirmelerini istemiştir (bkz: Şekil 2). Siber güvenliğin listenin başında kalmaya devam etmesi şaşırtıcı değildir. Bununla birlikte, dijital bozulma beşinci sıradan ikinci sıraya ilerlemiş ve iklim değişikliği on dördüncü sıradan beşinci sıraya sıçramıştır. İşte yöneticilerin her alanda dikkate alması gerekenler şunlardır:

3 yıl içinde beklenen risk değişimi

Kurumunuzun şu anda karşı karşıya olduğu en önemli 5 risk nedir?		Kurumunuzun 3 yıl sonra karşı karşıya olacağı en önemli 5 risk nedir?	
1. Siber güvenlik	%73	1. Siber güvenlik	%67
2. Beşeri sermaye	%51	2. Dijital bozulma	%55
3. İş sürekliliği	%47	3. İnsan sermayesi	%46
4. Mevzuat değişikliği	%39	4. İş sürekliliği	%41
5. Dijital bozulma	%34	5. İklim değişikliği	%39
6. Finansal likidite	%32	6. Mevzuat değişikliği	%39
7. Pazar değişimleri	%32	7. Coğrafi belirsizlik	%34
8. Coğrafi belirsizlik	%30	8. Pazar değişimleri	%33
9. Yönetişim/kurumsal raporlama	%27	9. Tedarik zinciri ve dış kaynak kullanımı	%25
10. Tedarik zinciri ve dış kaynak kullanımı	%26	10. Finansal likidite	%23
11. Kurumsal kültür	%26	11. Kurumsal kültür	%21
12. Suistimal	%24	12. Yönetişim/kurumsal raporlama	%20
13. İletişim/itibar	%21	13. Suistimal	%20
14. İklim değişikliği	%19	14. İletişim/itibar	%15
15. Sağlık ve güvenlik	%11	15. Sağlık ve güvenlik	%11
16. Şirket birleşmeleri ve satın almalar	%6	16. Şirket birleşmeleri ve satın almalar	%11

Şekil 2

Kaynak: Risk in Focus 2024
IIA Risk in Focus Küresel Anketi, n=4.207. Yüzde değerler, risk alanını en yüksek ilk 5'te sıralayanları göstermektedir.

Dijital bozulma. Yakın dönemde hangi yeni teknolojilerin en fazla etkiye sahip olacağını bilmek zordur ancak üretken yapay zekanın (YZ) bunlardan biri olması muhtemeldir. Üretken YZ'nin ilk iyi bilinen örneği, yani ChatGPT piyasaya sürüldüğü tarihten itibaren birkaç ay içinde tahmini 100 milyon kullanıcıya ulaşmıştır.[i] Genel olarak YZ ve özel olarak üretken YZ işletmelerin çalışma şeklini değiştirmeye başlamıştır. Faleato, YZ'nin sunabileceği büyük fırsatları ve ayrıca önemli riskleri anlamada iç denetimin yönetim kurullarına yardımcı olabileceğini belirtmiştir. Üretken YZ'nin kamuoyunda coşkuyla karşılanmasının ardından, konuyla ilgili etik ve yasal kaygılar hakkında birçok soru ortaya çıkmıştır. Mahremiyet ve gizlilik ile ilgili riskler, kaynak malzemenin şeffaf olmaması, fikri mülkiyetle ilgili konular ve bilgi doğruluğu bunlar arasındadır. Teknoloji geliştikçe ve kullanım arttıkça iç denetim risk ve faydalar konusunda yönetim kurulunu uyarabilir ve bunların yönetilmesi konusunda danışmanlık sunabilir.

İklim değişikliği. Bu alanda kurumsal raporlama çok uzun zamandır gönüllü olarak yapılmaktadır ancak bu durum düzenleyicilerin yeni düzenlemeler yayınlaması veya önermesiyle hızlı bir şekilde değişmektedir. Avrupa Sürdürülebilirlik Raporlama Standartları, ABD Menkul Kıymetler ve Borsa Komisyonu'nun iklim değişikliğiyle ilgili açıklamalara ilişkin teklifi ve Uluslararası Sürdürülebilirlik Standartları Kurulunun yeni kılavuzunun yanı sıra Avustralya, Kanada, Hindistan, Brezilya, Singapur ve diğer ülkelerdeki ulusal düzenlemeler bunlar arasında yer almaktadır. İç denetim, yönetim kurullarına, bu alana dâhil olan yeni kavramlardan bazıları hakkında güncel bilgiler sunabilir. Örneğin, kurumlar finansal risk söz konusu olduğunda önemlilik kavramını uzun zamandır anlamış olsalar da artık çifte önemlilik kavramına aşina olmaları gerekecektir.

Bu kavram, kurumsal açıklamaların hem bir kurumun finansal değerine olası etkileri hem de bir kurumun genel olarak dünya üzerindeki etkisi açısından nasıl önemli olabileceğini açıklamaktadır. "Çifte önemlilik fikri, bir şirketin finansın ötesinde dünya üzerindeki etkisinin, bir firmanın kâr hanesi üzerindeki etkisinden başka nedenlerle de önemli ve dolayısıyla açıklanmaya ve şeffaf davranmaya değer olabileceğinin kabul edilmesinden kaynaklanmaktadır."[ii]

"Yönetim kurulu, çifte önemlilik raporlaması hakkında kararların arkasında yatan varsayımlar konusunda güvence sağlamada güvenebileceği insanlara ihtiyaç duyacaktır," demiştir Faleato. Kurum, kurumun işi ve süreçleri hakkında derin bilgi sahibi olan iç denetçiler kapsamlı ve güvenilir güvence sunabilirler.

"Yeşil yıkama" yönetim kurullarının aşina olması gereken bir başka kavramdır. Bu kavram Kurumun iklim değişikliği politikaları veya eylemleri hakkında şişirilmiş veya yanlış iddialarda bulunmayı ifade etmektedir. Özellikle çevresel raporlamada daha fazla şeffaflık talep eden geniş ve çeşitli paydaş grupları göz önüne alındığında, yeşil yıkamayla suçlanmak bir kurumun itibarı üzerinde önemli bir etkiye sahip olabilir. İç denetim, kurumların iklimle ilgili raporladığı bilgiler hakkında güvence sağlayarak bu bilgilere duyulan güveni artırabilir. İç denetim, tüm bu konuları yönetim kurulu masasına getirebilir ve yöneticilerin bunları ele almak için ihtiyaç duydukları bağlamı sunabilir.

Risklerin Birbiriyle Bağlantısı

Faleato, Risk in Focus 2024 yayınının, ayrıca, risklerin birbiriyle bağlantısına, yani bir riskin başka risklere sebep olma ve hatta onların etkisini artırma şekline vurgu yaptığını not etmiştir. Örneğin, bir siber güvenlik olayı genelde BT ekibi veya olaydan doğrudan doğruya etkilenen her türlü personel için sadece baş ağrısına sebep olmaz. Diğer olumsuz etkilerinin yanı sıra, müşterilerin, iş ortaklarının veya diğer paydaşların dâhil olması durumunda kurumun markası veya tedarik zinciri ilişkileri üzerinde sıklıkla olumsuz bir etkisi olabilir. "Risklere izole olaylar olarak bakamazsınız," demiştir Faleato.

İç denetim, yönetim kurullarına, olaylar arasında bağlantı kuran ve karşılaştıkları görünüşte alakasız çok çeşitli riskleri anlamlandıran bir bakış açısı sunabilir. Faleato, yönetim kurullarının veya denetim komitelerinin risk yönetimini, uyumla ilgili endişeleri, iş fırsatlarını ve süreç verimliliklerini tartışmak için iç denetim liderleriyle düzenli olarak toplantı yapmalarını tavsiye etmektedir. "Bu alanların tümünde iş ortağı olabiliriz," demiştir Faleato. "Yönetim kurulları için en büyük değerimiz budur."

YÖNETİM KURULU ÜYELERİ İÇİN SORULAR

- Yönetim kurulu çevresel, toplumsal ve yönetişim bilgilerinin açıklanmasına ilişkin düzenlemelere nasıl hazırlanıyor?
- Hangi düzenlemelerin kurum üzerinde etkisi var veya olması bekleniyor?
- İş ortaklarımıza veya değer zincirimizin diğer üyelerine ÇTY bilgileri sağlamamız beklenecek mi?
- Kurum stratejik karar alma süreçlerinde kullanılmak üzere güvenilir ÇTY bilgileri elde edebiliyor mu?

i"ChatGPT en hızlı büyüyen kullanıcı tabanı rekorunu kırdı - analist notu (ChatGPT sets record for fastest-growing user base - analyst note)," Hu, K., Reuters, 2 Şubat 2023

ii"Çifte önemlilik: Yeni yasal kavramın SEC'in iklim planına ilişkin tartışmalarda rol oynaması muhtemel (Double materiality': New legal concept likely to play in debate over SEC's climate plan)," ," Engler, H., Reuters, 12 Nisan 2022.