KÜRESEL BAKIŞ AÇILARI ve ANLAYIŞLAR

İnovasyon ve Teknoloji

KISIM I: İç Denetimin Teknoloji Güvencesindeki Rolü

KISIM II: Teknolojiyi Benimseme Sürecinde Kurumun Öncü Olması

KISIM III: İç Denetimin Teknik Yetenek Mücadelesi

Wolters Kluwer

The Institute of Internal Auditors

İçindekiler

Kısım 1: İç Denetimin Teknoloji Güvencesindeki Rolü

Uzman Hakkında

Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, TeamMate Denetim Çözümleri şirketinde kıdemli ürün yöneticisidir ve TeamMate'in sunduğu 'sınıfının en iyisi' çözüm yoluyla bir yandan stratejik içgörüler sunarken diğer yandan denetim verimliliğini sürekli olarak iyileştirmek için çalışmaktadır. Hem kamu sektöründe hem de özel sektörde 20 yılı aşkın iç denetim deneyimi bulunmaktadır.

Jim daha önce İç Denetçiler Enstitüsü'nde bir dizi liderlik görevinde bulunmuş, Palo Alto Şehri'nde Şehir Denetçisi olarak görev yapmış ve San Diego'da (CA) Denetim Şefi olarak çalışmıştır. Jim'in çok yönlü iç denetim geçmişinde California Eyalet Üniversite Sistemi, PETCO Animal Supplies, Inc., State Street Corporation ve General Electric kurumlarındaki pozisyonları da bulunmaktadır.

Giriş

Teknoloji, değişim ve iş inovasyonu için tartışmasız bir itici güç haline gelmiştir. Yaygın dijital dönüşümden yeni ortaya çıkan ve gelişen yapay zekaya kadar, yeni teknolojiler daha önce hiç olmadığı kadar çok fırsatın – ve riskin – önünü açmaktadır. Yeni teknolojilerin etkilerini anlamak amacıyla kurumlar, teknolojiyi benimsemeleri ve kullanmaları konusunda güvence almak için iç denetime güvenmektedirler. Bu özet, teknoloji güvencesinin neden her denetimin rutin bir parçası olması gerektiğini ele alacaktır. Bu özet, temel güvenlik zafiyeti alanlarını kapsayacak ve iç denetimin daha etkili teknoloji denetimleri için gereken tutarlılık ve koordinasyonun yaratılmasına öncülük eden fırsatları tartışacaktır.

Merkezi odak noktası

Teknoloji iş dünyasının her alanına nüfuz ettiğinden dolayı, teknoloji güvencesinin iç denetçiler için şimdiden merkezi bir odak noktası olması doğaldır. TeamMate Denetim Çözümleri Kıdemli Ürün Müdürü Jim Pelletier, CIA, CGAP, "Kurumların yaptığı her şeyin altında yatan bir teknoloji riski var" demiştir. Artık operasyonlar ve teknoloji arasında bir ayrım yoktur çünkü teknoloji operasyonları ve diğer birçok fonksiyonu mümkün kılmaktadır. Bu nedenle, uygun kontrollerin değerlendirilmesi ve güvence altına alınması, bir sürecin altında yatan tüm ilgili teknolojileri içermek zorundadır. Örneğin, Pelletier, iç denetçilerin bir zamanlar borç hesaplarını – ya da başka herhangi bir fonksiyonu – ve onun sistemlerini ayrı ayrı denetleyebildiklerini ancak artık fonksiyonların ve sistemlerin tamamen iç içe geçtiğini belirtmiştir. "Denetlediğiniz her şey bir dereceye kadar teknoloji güvencesi içermektedir."

Dikkate Alınması Gereken Hususlar

Üçüncü taraf riskleri ve veri yönetişimi

Anahtar tehdit alanlarını tanıma

Teknolojinin yaygınlığı nedeniyle, teknoloji güvencesi sağlarken incelenmesi gereken **birçok konu vardır.** Bu bölümde birkaç yüksek riskli alan ele alınacaktır.

Üçüncü taraf ilişkileri

Araştırmalar, dünya genelinde kurumların %98'inin, son iki yıl içinde bir ihlâl vakası yaşamış olan en az bir üçüncü taraflа tedarikçi ilişkisi olduğunu göstermiştir. Şirketler, tedarikçilerin grup içi satış bağlantılarından da etkilenebilmektedir. Kurumların toplam %50'sinin yakın zamanda ihlâl vakası yaşanmış en az 200 dördüncü taraf tedarikçiyle dolaylı ilişkisi bulunmaktadır.[1]

Kurumların üçüncü taraflara olan yoğun bağımlılığı ve bu taraflarla olan ilişkileri, özellikle de bir sorun ortaya çıktığında kritik bir risktir. Üçüncü taraf ilişkileri saldırı ve tehdide karşı özellikle açık olabilir çünkü birçok kurum, hatalı bir şekilde, bir tedarikçinin ilişkili tüm riskleri ele aldığını ve kendi çabalarının daha detaylı gözden geçirilmesine gerek olmadığını ya da daha az titiz bir gözetimin yeterli olduğunu varsaymaktadır.

Üçüncü taraf veri ihlâllerine maruz kalan şirketlere ilişkin bu örnekler, her tür kurum veya sektörün bu durumdan etkilenebileceğini göstermektedir: SolarWinds AT&T, Chick-fil-A, LinkedIn, T-Mobile, Uber, Okta ve Dollar Tree.[2]

Üçüncü taraf tedarikçilerin sunduğu teknoloji veya ilişkili hizmetler arasında web barındırma platformları ve 'hizmet olarak yazılım' (HoY), dış kaynaklı veri merkezleri veya ağ güvenliği hizmetleri yer alabilir. Her ne kadar tedarikçi sunduğu hizmetlerin sorumluluğunu üstlense de bu hizmetleri kullanan kurumlar üçüncü tarafın yükümlülüklerini yerine getirip getirmediğini tespit etmek için uygun kontrollerin ve risk yönetimi süreçlerinin mevcut olduğundan emin olmak zorundadır. "Kurumunuzun güvenliğini üçüncü tarafın işini yapacağı umuduna bağlayamazsınız," demiştir Pelletier.

İç denetçilerin, kurumlarının üçüncü tarafı ve onunla ilişkili riskleri uygun bir şekilde değerlendirip değerlendirmediğini göz önünde bulundurmaları gereklidir. İç denetim bu değerlendirmeyi kendisi yapmayabilir ancak iç denetimin, kurumun ilişkisini ve ilişkili riskleri nasıl izleyip yönettiğini ve üçüncü tarafların uygun kontrollere sahip olduğunu ve bunları takip ettiğini nasıl doğruladığını göz önünde bulundurması gereklidir. Pelletier, iç denetimin bir ihlâlden sonra da dâhil olmak üzere, gerektiğinde tedarikçi süreçlerini ve kontrollerini inceleyebilmesi için tedarikçiyle yapılan sözleşmeye bir denetleme hakkı maddesi eklenmesini tavsiye etmiştir.

Veri yönetişimi

Kurumlar hızlı bir şekilde artan hacimlerde veri toplamakta ve yapay zekâ gibi yeni gelişen teknolojilerde kullanmak üzere bu verilerden faydalanmaktadır. Veri gizliliğini korumanın önemli olması nedeniyle veriler kurumlar için kritik bir risk teşkil edebilir. Buna ilave olarak, eğer yöneticiler önemli iş kararlarını ellerindeki verilere dayanarak alacaklarsa, kurum veri bütünlüğüne güvenmek ve bu verilerin eksiksiz, doğru ve güvenilir olduğundan emin olmak zorundadır. Bu durum, özellikle de üretken yapay zekâ ile çalışıldığında veri kaynağının güvenilirliğini anlamayı da kapsamaktadır.

[1] "SecurityScorecard Araştırması, Dünya Genelinde Kurumların %98'inin İhlâl Olayı Yaşamış En Az Bir Üçüncü Tarafla İlişkisi Olduğunu Gösteriyor (SecurityScorecard Research Shows 98% of Organizations Globally Have Relationships With At Least One Breached Third-Party)," SecurityScorecard ve The Cyentia Institute tarafından yapılan bir araştırmaya dayanan SecurityScorecard basın bülteni, 1 Şubat 2022.
[2] "2023'teki En Büyük Üçüncü Taraf Veri İhlâlleri (Top Third-Party Data Breaches in 2023)," FortifyData, 4 Aralık 2023 tarihinde güncellenmiştir.

Kurumların, verilerin bilgisayar korsanlığına veya diğer uygunsuz kullanımlara karşı savunmasız olmadığını garanti etmeleri gerekecektir. "Kurumların verilerin nasıl işlendiğini ve depolandığını değerlendirmesi gerekir," demiştir Pelletier ve bunun yanı sıra, bilgi gizliliğiyle ilişkili gereklilikler gibi belirli yasal veya düzenleyici gerekliliklerin yerine getirildiğinden emin olmaları da gerekmektedir. Eğer kurum müşterilerine veya iş ortaklarına verilerinin nasıl kullanılacağı konusunda güvenceler vermişse, bu taahhüdünü yerine getirdiğinden emin olması gerekecektir. Her ne kadar veri yönetişiminden yönetim sorumlu olsa da iç denetim veri yönetişim kontrollerinin yeterli olduğu konusunda güvence sağlayabilir.

Avrupa Komisyonu'na göre veriler mümkün olan en kısa süreyle saklanmalıdır. Veri depolama maliyetli olmakla kalmaz, aynı zamanda bir ihlâl durumunda bilgisayar korsanlarının erişeceği daha fazla veri söz konusu olacaktır. Şirketlerin, bazı materyaller için daha uzun saklama sürelerini zorunlu kılan ticari, düzenleyici veya kanuni gereklilikleri göz önünde bulundurarak verilerin ne zaman gözden geçirilmesi veya silinmesi gerektiğine ilişkin uygun zaman çizelgeleri olması gereklidir. Örnek olarak, Avrupa Komisyonu'nun Genel Veri Koruma Yönetmeliği ilkeleri kapsamında, komisyon bir şirketin iş arayanların özgeçmişlerini bunları güncellemeye yönelik adımlar atmaksızın 20 yıl boyunca sakladığı bir duruma işaret etmektedir.[3] Birçok iş veya sektördeki hızlı iş değişimleri göz önüne alındığında, bu verilerin birçok durumda kısa bir süre sonra geçerliliğini yitireceği açıktır. Şirketin gelecekteki açık pozisyonlar için personel ararken bu güncel olmayan bilgi havuzuna güvenmesi durumunda, iş arayan kişi istihdam fırsatını kaçırabilir ve şirket de yetenekli kişileri kaçırabilir ya da kurumun bilgisayar korsanlarının saldırısına uğraması durumunda başvuranların kişisel verileri çalınabilir.

İç denetim güvencesinin bir kurumun uygun izleme veya korumaları uygulamadaki başarısızlığını tespit edebileceği diğer teknoloji alanlarından bazıları şunlardır:

- **Erişim kontrolleri.** İç denetim, kurumun teknolojisinin iç işleyişine yalnızca meşru kullanıcıların erişebilmesini sağlamak için kullanıcı erişim gözden geçirmelerinin yapılıp yapılmadığını inceleyebilir. ISACA Journal'a göre, diğer hususların yanı sıra, bu gözden geçirmeler eski bir personelin veya departman üyesinin uygulamalara veya altyapıya yetkisiz erişimi olup olmadığını belirleyebilir. ISACA Journal'da bu durum, "Bu güvenlik açığı istismar edilebilir ve bu da kurumun mali ve/veya itibar kaybına neden olabilir," şeklinde ifade edilmiştir.[4]
- **Siber güvenlik.** Bir Forbes makalesine göre "Güvenlik yamaları, güçlü parolalar, varlık yönetimi ve personel güvenlik eğitimi, çevrimiçi ortamda güvende kalmak için uzun bir yol kat etmenizi sağlar."[5]
- **Gölge BT.** Bu terim, personelin BT departmanının bilgisi veya izni olmadan teknoloji satın aldığı ve uyguladığı durumları ifade etmektedir. Bu uygulama, uzaktan çalışma ve kişisel cihazların iş için kullanımının artması ile birlikte daha da yaygın hale gelmektedir. Riskler arasında BT ekibinin gözetimi altında olmamak veya kurumun siber güvenlik ve gizlilik protokollerine ve diğer rehberlerine uymamak yer almaktadır.
- **Üretken Yapay Zekâ ve diğer gelişmekte olan teknolojiler ile ilgili riskler.** Personelin kuruma, müşteriye veya kendisine ait verileri kamuya açık üretken bir yapay zekâ sistemine yükleme tehlikesi önemli bir endişe kaynağıdır. (İç Denetçiler Enstitüsü'nün Yapay Zekâ Denetleme Çerçevesi[6] iç denetçilerin riskleri anlamalarına ve yapay zekâ ile ilgili en iyi uygulamaları ve iç kontrolleri belirlemelerine yardımcı olmaktadır.)
- **Kültürel hususlar.** İç denetçiler, çalışanın yeterince katılım göstermemesinin ya da teknoloji rehberleri veya koruma tedbirleri konusunda iletişimin zayıf olmasının bir tehdit oluşturup oluşturmadığını değerlendirebilir.
- **Teknolojiyle ilgili mevzuat veya düzenlemelerin etkisi.** Kurumların, gelişmekte olan teknolojilerin iş dünyası ve toplum için ifade edebileceği önemli değişikliklere yanıt olarak çıkarılan yeni yasalar ve standartlar ile ilgili uyum ihtiyaçlarını izlemeleri gerekecektir.

[3] Veriler ne kadar süreyle saklanabilir ve güncellenmesi gerekli midir? (For how long can data be kept and is it necessary to update it?)" Avrupa Komisyonu.
[4] "Etkin Kullanıcı Erişimi Gözden Geçirmeleri (Effective User Access Reviews)," Sundaresan Ramaseshan, *ISACA Journal*, 21 Ağustos 2019.
[5] "Şirket Yöneticilerinin Sıklıkla Gözden Kaçırdığı Teknolojiyle İlgili 16 Risk Faktörü (16 Tech-Related Risk Factors Company Executives Often Overlook)," *Forbes*, 21 Aralık 2022.
[6] İç Denetçiler Enstitüsü'nün AI Denetleme Çerçevesi.

Koordinasyonlu Çaba ve Çalışmaların Değeri

İkinci hattaki risk uzmanlarıyla uyumlu olma

İç denetim teknoloji risk yönetiminde koordine olmaya yardımcı olabilir

Teknolojinin yaygın varlığı ve etkisinin dezavantajlarından biri, bu alanı tam olarak anlamaya ve bu alanda güvence sağlamaya çalışırken bir şeylerin gözden kaçma riskidir. "Ele alınacak çok şey olduğu için boşluklar olacaktır," demiştir Pelletier. İçerdiği birçok risk göz önünde bulundurulduğunda, teknolojinin benimsenmesi ve kullanımı konusunda bir güvence sağlayıcı olarak rolünde etkinliğini artırmak amacıyla, iç denetim mevcut kaynaklarla yüksek riskli alanları mümkün olan en iyi şekilde ele almak isteyecektir.

Pelletier'e göre bu kaynakları artırmak için, iç denetim fonksiyonunun bilgi güvenliği, iç kontroller, risk yönetimi ve uyum gibi ikinci hat güvence fonksiyonlarıyla uyum sağlama fırsatı vardır. Üst yönetime ve yönetim kuruluna risklerin tanımlandığına dair daha yüksek derecede rahatlık sağlamak amacıyla, iç denetim, teknoloji güvencesinin – ve anahtar teknoloji risklerinin – kurum genelinde nasıl ele alındığına ilişkin bütünsel bir resim elde etmek için faaliyetlerini bu fonksiyonlarla koordine edebilir.

Her ne kadar iç denetim bu ikinci hat fonksiyonlarından bağımsız kalmak zorunda olsa da bu fonksiyonlarla sağlanan koordinasyon iç denetimin hangi risklerin ne ölçüde ele alındığını belirlemesine yardımcı olabilir. "İç denetimin içine kapalı bir faaliyet göstermemesi gereklidir," demiştir Pelletier. Çaba ve çalışmaların tekrarlanmasını en aza indirmek suretiyle uyumlu olma, iç denetimin kendi kaynaklarını en önemli risklere odaklamasını sağlamaktadır. Bu çabanın bir parçası olarak iç denetim, ikinci hattaki fonksiyonların teknoloji güvencesiyle ilgili yaptığı çalışmaları değerlendirebilir.

Teknoloji iç denetçilerin en önemli konusu

Teknoloji, iç denetim liderlerinden risk, denetim planları, bütçeler, personel ve diğer önemli konular hakkında değerli kıyaslama bilgileri toplayan IIA'nın 2023 Kuzey Amerika İç Denetimin Nabzı[7] raporunun ana odak noktasıydı.

Örneğin, iç denetim yöneticilerine ellerinde olsa ilave bütçeyi nasıl harcayacakları sorulduğunda, ikinci en yaygın seçenek teknoloji olmuştur. (Kurum içi personel artışı ilk sırada yer almıştır.)

Uyuma ve operasyonlara ilişkin gözden geçirmeler geleneksel öncelikler olsa da iç denetçiler teknolojiyle ilgili konulara da büyük zaman ve çaba harcamaktadır. Nabız yoklama anketinde, katılımcılar denetim planlarının %10'unun siber güvenliğe, %9'unun ise genel olarak BT'ye odaklandığını belirtmiştir. Toplam %19'luk bu oran finansal raporlamaya (ICFR-"Finansal Raporlama ile ilgili İç Kontrol Raporu" dâhil), operasyonlara ve uyum/düzenlemelere (ICFR hariç) ayrılan ortalama denetim planı miktarından daha yüksek olmuştur. Bunların her biri denetim planlarının %15'ine konu olmuştur.

Son olarak, katılımcılardan kurumları için hangi konuların yüksek veya çok yüksek risk oluşturduğunu seçmeleri istendiğinde, ilk üç tercihlerinin hepsi teknolojiyle ilgili olmuştur:

- Siber güvenlik, %78 gibi yüksek bir oranla seçilmiştir.
- Genel olarak BT, %57 oranında.
- BT hizmetleri için sıklıkla kullanılan üçüncü taraf ilişkileri, %51 oranında.

Bu uyumluluk, aynı zamanda, çok sayıda fonksiyonun departman yöneticilerinden aynı verilerle ilgili raporlar istemesi ya da benzer gözden geçirmeler yapması durumunda ortaya çıkan "güvence yorgunluğunu" en aza indirmeye de yardımcı olabilir. İç denetim ve ikinci hattaki fonksiyonlar ihtiyaç duydukları temel bilgileri toplamak için birlikte çalışırlarsa bu durum önlenebilir.

Pelletier, iç denetimin kurum genelinde güvence faaliyetleri etrafında bu uyumluluğu koordine etmede ve var olan faaliyetleri en iyi şekilde kullanmada liderlik rolü üstlenebileceğini söylemiştir. Başlangıç olarak, iç denetçiler risk yönetimi, uyum, iç denetim ve diğer fonksiyonların her birinin riski değerlendirmek ve derecelendirmek için kendi sistemlerinin olup olmadığını tespit ederek teknoloji

[7] 2023 Kuzey Amerika İç Denetimin Nabzı (2023 North American Pulse of Internal Audit), İç Denetçiler Enstitüsü, Mart 2023.

güvence çalışmalarında daha fazla tutarlılık sağlayabilirler. Yönetim kurulu ve yönetimle yapılan görüşmelerde, fonksiyonlar arasındaki bu tutarsızlıklar kafa karıştırıcı veya belki de görünüşte noksan bir resim sunabilir. İç denetim, ortak bir risk taksonomisi (sınıflandırması) kullanarak koordineli bir çalışma önerebilir ve bu çalışmaya liderlik edebilir. İç denetim ve ikinci hattaki fonksiyonların aynı dili konuşması durumunda, yönetim kurulu ve üst yönetim ile risk hakkında kurulan iletişim daha anlaşılır olacaktır. Tüm bu fonksiyonların sonuçlarının veya değerlendirmelerinin kabul edilebilir olması gerekmez ancak kullanılan terim ve yaklaşımlar tutarlı olmalıdır.

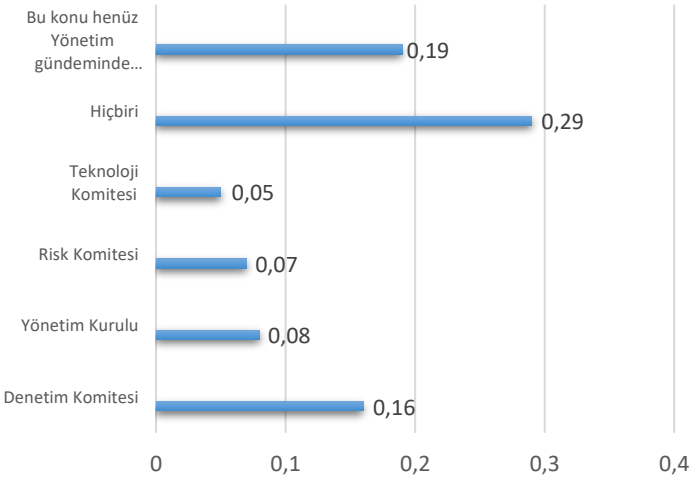
Gözünüz yapay zekada olsun

Birçok şirket hâlâ kendi yapay zekâ ve üretken yapay zekâ kullanımıyla boğuşurken iç denetçilerin yeni gelişen teknolojilere ve çalıştıkları kurumların bu teknolojileri nasıl kullandıklarına yönelik daha iyi bir gözetim sağlama fırsatı vardır.

Deloitte ve Society for Corporate Governance tarafından 2023 yılında büyük ve orta ölçekli şirketler arasında yapılan bir ankette[8], bu şirketlerin sadece %13'ünde resmiyet kazanmış bir yapay zekâ gözetim çerçevesi vardı. Sadece %9'u siber güvenlik, risk yönetimi, kayıt tutma ve diğer konularla ilgili kurumsal politikaları yapay zekâ kullanımını ele alacak şekilde revize etmişti. Bununla birlikte, Ulusal Kurumsal Yöneticiler Birliği, bir yıl önce kurumsal katılımcıların %94'ünün yapay zekanın şirketlerinin kısa vadeli başarısı için kritik öneme sahip olduğunu söylediğini belirtmiştir.[9]

Yapay zekâ ne kadar önemli olsa da yönetim kurulları bu konuyla ilgili endişelerini henüz gideremiyor gibi görünmektedir. Bu anket, katılımcıların yönetim kurullarının toplam %48'inin yapay zekayı henüz değerlendirmediğini ya da bu konuda sorumluluk atamadığını ortaya koymuştur (grafiğe bakınız). Yapay zekâ için sorumluluk atamış olanlar arasında, bu sorumluluk büyük olasılıkla denetim komitesinin gözetimi altında olmuştur ve bu komite genellikle iç denetim yöneticisinin bağlı olduğu gruptur. İç denetim, kurumların yapay zekanın önemi ile yapay zekaya verdikleri yanıt arasındaki kopukluğu fark etmelerine ve ele almalarına yardımcı olarak önemli bir değer katabilir.

Şirketin yönetim kurulunda yapay zekâ için birincil gözetim sorumluluğu kimdedir?



Kaynak: *Deloitte ve Society for Corporate Governance Yönetim Kurulu Uygulamaları Üç Aylık Dergisi: Teknolojinin geleceği: Yapay zeka (AI) (Deloitte and Society for Corporate Governance Board Practices Quarterly: Future of tech: Artificial intelligence (AI))*, Ağustos 2023.
Not: Diğer/bilmiyorum yanıtları tabloya dâhil edilmemiştir.

[8] *"Deloitte ve Society for Corporate Governance Yönetim Kurulu Uygulamaları Üç Aylık Dergisi: Teknolojinin geleceği: Yapay zeka (AI) (Deloitte and Society for Corporate Governance Board Practices Quarterly: Future of tech: Artificial intelligence (AI)),"* Ağustos 2023.
[9] "Yapay Zeka: Denetim Komiteleri için Yeni Bir Gözetim Sorumluluğu mu? (Artificial Intelligence: An Emerging Oversight Responsibility for Audit Committees?)" Brian Cassidy, Ryan Hittner ve Krista Parsons, NACD 2024 Governance Outlook.

Sonuç

Riskleri ve engelleri tanımlayan teknoloji güvencesi, iç denetimin rolüne zaten iyi bir şekilde entegre edilmiştir. İç denetim bir yandan teknolojiyle ilişkili en büyük güvenlik açıklarından bazılarına odaklanmayı sürdürürken, diğer yandan risk yöneticileri ve paydaşlar için daha eksiksiz ve daha doğru bir resim sunmak adına çabaların daha iyi koordine edilmesini de teşvik edebilir. Bu özette ana hatlarıyla belirtilen adımlar, kurumun teknoloji riskine yönelik genel yaklaşımının ve denetim planının potansiyel teknoloji risklerini yeterince ele almasını sağlamaya yardımcı olabilir.

Kısım 2: Teknolojiyi Benimseme Sürecinde Kurumun Öncü Olması

Uzmanlar Hakkında

Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, TeamMate Denetim Çözümleri şirketinde kıdemli ürün yöneticisidir ve TeamMate'in sunduğu 'sınıfının en iyisi' çözüm yoluyla bir yandan stratejik içgörüler sunarken diğer yandan denetim verimliliğini sürekli olarak iyileştirmek için çalışmaktadır. Hem kamu sektöründe hem de özel sektörde 20 yılı aşkın iç denetim deneyimi bulunmaktadır.

Jim daha önce İç Denetçiler Enstitüsü'nde bir dizi liderlik görevinde bulunmuş, Palo Alto Şehri'nde Şehir Denetçisi olarak görev yapmış ve San Diego'da (CA) Denetim Şefi olarak çalışmıştır. Jim'in çok yönlü iç denetim geçmişinde California Eyalet Üniversite Sistemi, PETCO Animal Supplies, Inc., State Street Corporation ve General Electric kurumlarındaki pozisyonları da bulunmaktadır.

Dennis Wong, CIA, CFSA

Dennis Wong, CIA, CFSA, Londra merkezli uluslararası bir bankada genel müdür olarak görev yapmaktadır. Uluslararası bankacılık ve sermaye piyasalarında 20 yılı aşkın deneyime sahip tecrübeli bir denetim ve risk uzmanıdır. Onun tutkusu, süreçlerin yeniden yapılandırılması ve teknoloji inovasyonu yoluyla değişimlere öncülük etmek ve yön vermektir. IIA New York Şubesinde gönüllü olarak çalışmakta ve küresel Sınav Geliştirme Komitesinde görev yapmaktadır.

Giriş

Teknoloji, kurumların can damarı haline gelmiş ve aslında her fonksiyonda düzenli olarak kullanılan hayati bir araç olmuştur. Bununla birlikte, PwC 2023 Küresel Risk Anketi'ne göre, iş ve risk liderlerinin %60'ı yeni bir teknoloji aracı olan üretken yapay zekayı (GenAI) bir fırsat olarak görürken %57'si yeni teknoloji yatırımlarına hazırlanmanın risk ortamını gözden geçirmek için en önemli tetikleyici faktör olduğunu belirtmektedir.[10]

Teknoloji yeni faydalar sunar ancak ona bağımlılık, teknoloji kullanımı daha kritik ve yaygın hale geldikçe artan tehditleri de beraberinde getirmektedir. Bunlar arasında teknolojinin benimsenme biçimlerine ilişkin riskler de yer almaktadır. İç denetim, kurumların riski en aza indirmek ve yeni teknolojilerin değerini artırmak için en iyi uygulama stratejilerini belirlemelerine ve uygulamalarına yardımcı olabilir. Bu özet, iç denetimin bu çabaya değer katmak için atabileceği adımları tartışmaktadır.

10 "İşletme ve Risk Liderlerinin %60'ı GenAI'yi Fırsat Olarak Görürken Bile Siber ve Dijital Teknoloji Riskleri Önemli Bir Endişe Kaynağı: PwC 2023 Küresel Risk Araştırması (Cyber and Digital Technology Risks Are a Key Concern for Businesses and Risk Leaders, Even as 60% See GenAI as an Opportunity: PwC 2023 Global Risk Survey)," PwC basın bülteni, 20 Kasım 2023.

Yeni Bir Yönetişim Çerçevesi Geliştirme

Yeni teknoloji buna nasıl uydurulacak?

İç denetim teknoloji benimseme sürecine rehberlik etmeye yardımcı olabilir

Yeni teknolojiler her zaman yeni risk hususlarını beraberinde getirmektedir. Örneğin üretken yapay zekâ (GenAI) bu dönüştürücü teknoloji için çok sayıda yenilikçi kullanıma ilham verirken, aynı zamanda gizlilik, yerleşmiş önyargı ve alınan bilgilerin şeffaflığı ve doğruluğu gibi alanlarda yeni tehlikeleri de beraberinde getirmiştir. Aynı zamanda, yeni teknolojiler iş operasyonlarında bir kurumu yeni operasyonel risklere maruz bırakan değişikliklere yol açtıkça riskler ortaya çıkabilir.

Uluslararası bankacılık ve sermaye piyasalarında 20 yılı aşkın deneyime sahip deneyimli bir denetim ve risk uzmanı olan CIA, CFSA Dennis Wong, bu nedenlerden dolayı, kurumların yeni teknolojileri benimserken bu yeni araçların işe nasıl uyum sağlayacağını, kurumsal stratejilerle nasıl uyumlu olacağını ve kurumsal hedeflere ulaşmaya nasıl yardımcı olacağını göz önünde bulunduran sağlam bir proje yönetişim çerçevesi geliştirmeleri gerektiğini ifade etmiştir. Gerçekten de PwC anketinde "risk öncüleri" olarak belirlenen şirketler arasında, daha az gelişmiş kurumların %57'sine kıyasla, %73'ünün kurum çapında bir teknoloji stratejisi ve yol haritasına sahip olması muhtemeldir. Wong, bu çerçevenin kapsamlı bir risk değerlendirmesi ve yeni risklerin yarattığı tehditleri ele alabilecek kontroller de dâhil olmak üzere riskin geniş kapsamlı bir değerlendirmesini içermesi gerektiğini söylemiştir.

İç denetim, bu proje yönetişimi ve onun ne kadar iyi işlediği konusunda güvence sağlayabilir ve genel olarak teknolojinin benimsenmesi konusunda tavsiye verebilir. Başlangıçta, iç denetim, teknolojinin uygunluğunun yanı sıra ilgili riskleri ve kontrollerdeki değişiklikleri de dikkate alan bir uygulama öncesi gözden geçirme yürütebilir. Wong'a göre, yeni araçlar kullanılmaya başlandıktan sonra, iç denetim teknoloji benimseme sürecinin nasıl işlediği ve yeni araçların kurum genelinde yarattığı etki hakkında geri bildirim de sağlayabilir. Uygulamadan sonra, iç denetim, teknolojinin öngörüldüğü gibi işleyip işlemediği, eğer işlemiyorsa neden işlemediği ve beklenen faydaların elde edilip edilmediği konularında görüş bildirebilir.

İç denetim, benimsemeyi sekteye uğratabilecek engelleri de tespit edebilir. Büyük ölçüde bölümlere ayrılmış şirketler, farklı fonksiyonlarda çalışan uzmanların diğer faaliyet alanlarında neler olup bittiğinden habersiz olduğu içe dönük ve iletişimsiz bir bilgi sistemine maruz kalabilir. Bir faaliyet alanı, başka bir grubun aynı teknolojiyi araştırdığını ancak bunun için farklı kullanımlar keşfettiğini ya da üçüncü bir fonksiyonun teknolojiyle ilgili bazı başarısızlıklarla karşılaştığını ancak değerli dersler çıkardığını bilmeyebilir. Wong'a göre "Uyumlu ve ortak bir güç ararken bu durum ikilik yaratabilir." İç denetim kuruma bütüncül bir bakış açısıyla baktığından, bu içe dönük ve iletişime kapalı sistemleri yıkmak ve çaba ve çalışmaların tekrarlanmasını önleyen uçtan uca içgörüler sunmak için eşsiz bir konumdadır. "Kurumsal bilgi birikimi sayesinde iç denetim, teknolojinin daha değerli bir şekilde kullanılmasını sağlayacak yeni bir bakış açısı getirebilir," demiştir Wong. Ayrıca, operasyonel kontrollerin uygun şekilde işleyip işlemediği ve güvenli ve emniyetli teknoloji kullanımının sağlanıp sağlanmadığı konusunda da güvence sunabilir. Wong, yatırım için ayrılan sermaye her zaman kıt olduğundan, kurumların teknoloji harcamalarının en iyi şekilde kullanılıp kullanılmadığına ilişkin tavsiyelere değer vereceğini belirtmiştir.

Kurumların stratejik ve operasyonel riskler ile bunların altında yatan teknoloji arasındaki karşılıklı ilişkiyi ele almaları gerekecektir. "Biri diğerini etkiler," demiştir Wong. Yeni teknoloji kurumun çalışma şeklini değiştirmektedir ve bu yeni riskleri beraberinde getirmektedir. Bu da operasyonlarda ilave risklere yol açabilecek değişimlere neden olabilmektedir. Önemli olan, kurumun hedeflerini, bu hedeflerin nasıl etkilendiğini veya yeni riskler taşıdığını ve hangi kontrollerin bu endişeleri giderebileceğini net bir şekilde anlamaktır.

Yeni teknolojinin getirdiği değişimler göz önüne alındığında, kurumlar güçlü bir risk kültüründen de fayda sağlayacaktır. Wong, kurumun sağlam bir kontrol zihniyetine ve kontrol çerçevesine sahip olduğu durumlarda bile, kontrolleri uygulamak veya onların yokluğunda doğru adımları atmak için yine kişilere bağlı olması gerektiğini ve bu nedenle güçlü risk disiplini ve yeni teknoloji riskinin uygun bir şekilde anlaşılmasının kritik önem taşıdığını belirtmiştir. Şirket kültürü, yeni araçların potansiyel tehditlerini ve bu araçların kullanımına ilişkin kurumsal beklentileri tanımlamalı ve herkese açık olacak şekilde iletmelidir.

Ölçülü Adımları Dikkate Alın

Hız ve güvenlik arasında denge kurma

Yeni teknolojinin ne zaman benimsenmesi gerektiği konusunda danışmanlık yapma

Yeni bir teknoloji ortaya çıktığında genelde uygulama konusunda bir aciliyet söz konusudur; bunun en yakın örneği de üretken yapay zekâ (GenAI)'yı uygulamaya koyma konusundaki aceledir. Wong, yeni araçlarla ilişkili potansiyel riskler nedeniyle "kurumların hız ve güvenlik arasında doğru dengeyi bulmaları gerektiğini" söylemiştir. Wong, ilk piyasaya sürüldüklerinde emniyet kemeri bulunmayan ancak daha hızlı hareket etmeye başladıkça yıllar içinde daha fazla güvenlik özelliği eklenen otomobillere dikkat çekmiştir. Teknolojideki mevcut değişim hızı ve içerdiği sistemlerin karmaşıklığı göz önüne alındığında, iç denetim yönetimin uygun güvenlik özelliklerini – veya kontrollerini – uygulayıp uygulamadığının incelenmesine yardımcı olabilir. “Risk, tanımlanmış olsun ya da olmasın, ilk günden başlar,” demiştir Wong. “Bu risk hemen bir kayıp veya tehdide dönüşmeyebilir ancak bir teknolojiyi kullanmaya başladığınızda zaten riske maruz kalırsınız.”

Örnek olarak, GenAI, karmaşıklık katmanları olan sofistike bir araçtır; kötü niyetli aktörlerin onu kötü amaçlarla kullanması kolaydır. Ek olarak, GenAI riskleri konusunda uygun şekilde eğitilmemiş bir personel farkında olmadan gizli veya hassas verileri yükleyebilir ve bu veriler programın eğitimine dâhil edilerek yabancıların erişimine açılabilir.

Kurumlar, pazara ilk giren olma ve beklenmedik kaynaklardan gelen risklerle ve potansiyel iş veya itibar hasarıyla yüzleşme ile başkalarının deneyim ve hatalarından ders almak için hızlı bir takipçi stratejisi benimseme seçeneklerini değerlendirmelidir.

Teknolojik Borcu Anlama

Altyapı, personel ve kültür son teknolojiye vakıf olamayabilir

Teknolojik borcu ve düzeltme adımlarını tanımlama

Kurumların var olan altyapılarının yeni teknoloji araçlarını kaldırıp kaldıramayacağını da tespit etmeleri gerekecektir. Teknoloji benimsendiğinde, zaman baskısı, maliyetle ilgili hususlar veya diğer engeller genelde kurumları son teslim tarihine yetişmek için işin kolayına kaçmaya zorlar ya da diğer zorluklar kurumların optimum uygulamaya ulaşamamalarına neden olabilir. TeamMate Denetim Çözümleri kıdemli ürün müdürü Jim Pelletier, CIA, CGAP, kurumun yeni yazılım sürümlerine veya yeni donanımlara yükseltme yapmaması, yamaları uygulamaması veya diğer önemli bakım adımlarını atmaması durumunda bu teknik borcun zaman içinde birikebileceğini ifade etmiştir. Kurum, sistemi devam ettirmek için sürekli yeni geçici çözümler benimsedikçe teknik çevikliği daha da geride kalmaktadır.

Pelletier, teknik borcun, kurumun var olan yazılımdan en iyi şekilde yararlanmasını engelleyebileceğini ya da hatta yeni teknolojilerin etkin bir şekilde benimsenmesini imkânsız hale getirebileceğini ifade etmiştir. BT ekibinin sorunun farkında olmaması, sistemin hatalarını tartışmaya isteksiz olması ya da teknolojinin teknoloji uzmanı olmayan kişilere açıklanamayacak kadar karmaşık olduğunu düşünmesi nedeniyle, sorun BT ekibince iyi bir şekilde aktarılamayabilir. Bunun sonucunda, iç denetçiler bu teknik borcun veya onun kurumun yeni teknolojiyi benimseme yeteneği üzerindeki etkisinin farkında olmayabilirler.

Yeni Teknoloji Hakkında Sorulacak Sorular

İç denetimin güvence veya danışmanlık sağlarken sorabileceği sorulardan bazıları şunlardır:

- Riskler, faydalar ve yeni fırsatlar da dâhil olmak üzere yeni teknolojinin kurum ve onun iş süreçleri üzerinde nasıl bir etkisi olacak?
- Teknoloji, kurumun kurumsal risk yönetimi ve yönetişim, risk ve uyum yaklaşımlarına nasıl uyum sağlar?
- Teknoloji mevcut kontrollerle nasıl entegre olmalıdır? İç kontroller üzerindeki etkiye ilişkin bir değerlendirme yapılmış mı? Eğer yapılmışsa, kontrollerde ve süreçlerde ne gibi değişiklikler yapılmalıdır? İç denetim, iş birimlerinin risk ve kontrollerini yeniden değerlendirmek ve yeni risk ve kontrolleri belgelendirmeye hazırlanmak için her bir iş birimiyle birlikte çalışması gerekir mi?
- Teknolojiyi yükseltmemiz, iş süreçlerinde değişiklik yapmamız veya personelimizin becerilerini geliştirmemiz gerekir mi?
- Gizlilik, müşteri verileri, özel bilgiler ve diğer konulara yönelik tehditler de dâhil olmak üzere ne tür yeni riskler doğurur?
- Yeni sistem nerede ve kimler tarafından kullanılmaktadır?
- Teknolojinin topladığı veya ürettiği verilere ne oluyor? Bu veriler nerede depolanıyor ve nasıl korunuyor?
- Kurum artık paylaşmaması gereken verileri mi paylaşacak yoksa kendini yeni veri gizliliği risklerine mi maruz bırakacak?

Pelletier, iç denetim kurumun teknoloji ekibiyle aynı uzmanlığa ihtiyaç duymamasına rağmen, iç denetim personelinin BT ekibiyle kurumun sistemlerinin mevcut durumunu ortaya çıkarabilecek verimli diyaloglar kurmak için yeterli becerilere sahip olmasını sağlayacak adımlar atarak teknik borç sorununu ele alabileceğini ifade etmiştir. Bu bilgiyle donatılan iç denetim ekibi üyeleri, BT ekibi üyelerinin zamanına ve uzmanlığına saygı duyan verimli görüşmeler yapabilirler.

Diğer durumlarda, bir kurumun teknoloji altyapısı yeterli olsa bile teknoloji şirketin ve personelinin önüne geçebilir. Bu durum, kurumlar iş güçlerini veya iş süreçlerini güncel hale getirmeden teknolojilerini modernleştirdiklerinde ortaya çıkabilir. Şirket, verimliliği artırmak için teknolojiyi uyguluyor olabilir ancak süreçlerin nasıl etkileneceğini veya nasıl değişmesi gerektiğini anlamak ve buna uyum sağlamak için zaman ayıramamaktadır. “İnsanlar teknolojiyi nasıl kullanacaklarını bilmiyor ve bu da zaman, enerji ve para kaybına

neden oluyor," demiştir Pelletier. "Önemli iyileştirmeler yapma konusunda kaçırılan bir fırsat var." Bir kez daha iç denetim, teknoloji ile işletme hedef ve varlıklarının eşit derecede örtüşmesini sağlamak adına doğru soruları sormak için gereken kurumsal bilgiye sahiptir.

Son olarak, Wong, teknoloji ilerledikçe insan dokunuşunun değerini unutmanın kolay olabileceğini ancak insan gözden geçirmesi ve değerlendirmesi süreç için kritik öneme sahip olmaya devam edeceğini not etmiştir. GenAI gibi bir araç müşteri veya diğer insan etkileşimlerinde kullanıldığında, bazen sadece hata yapmakla veya bir şeyler uydurmakla kalmaz, aynı zamanda bir kişinin anlayacağı sinyalleri kaçırabilir veya müşteriyi tanıyan bir insanın uygunsuz olduğunu bileceği işe yaramaz cevaplar verebilir.

Bazı GenAI Sınırlamalarını Ele Alma

GenAI ilk tanıtıldığında büyük bir coşkuyla karşılanmıştı ancak bu raporda tartışıldığı üzere eksiklikleri endişe yarattı. Doğru kullanıldığı takdirde, bir kurumda teknolojinin benimsenmesini ele almada değerli bir araç olabilir. Jim Pelletier, GenAI kullanımını geliştirmek isteyen iç denetçiler için iki seçenek tanımlamaktadır:

- Bazı durumlarda, GenAI bir sorguya cevap veremezse cevaplar uydurur veya halüsinasyon görür ya da sadece eğitildiği şeyleri bildiği için hatalar yapar. Bu sorunu ele almak için, Geri Alım-Artırılmış Üretim (Retrieval-Augmented Generation - RAG), GenAI sistemindekileri güçlendirmek için doğru ve güncel veri sağlayan bir tekniktir. RAG, bir yanıt oluşturulmadan önce GenAI'ın eğitim veri kaynaklarının dışındaki güvenilir bir bilgi tabanına başvurarak GenAI gibi büyük dil modellerinin çıktılarını optimize etmektedir. Ayrıca, GenAI kaynakları şeffaf olmazken, RAG kaynak materyallerin tanımlanmasını mümkün kılmaktadır.
- GenAI'dan en iyi çıktıyı almak, kısmen istemler (prompts) olarak bilinen doğru talimatları vermeye bağlıdır. İstemlerin, yanıtın ne kadar uzun olması gerektiği, başkalarıyla paylaşılacaksa hangi kitleye hitap edeceği, üslup ve tarz gibi ayrıntıları belirtmelidir. Pelletier şöyle bir örnek veriyor:

  Finansal hizmetler sektöründe teknoloji risk yönetimi konusunda uzmanlığı olan deneyimli bir iç denetim yöneticisisiniz. Teknoloji riskini, iş operasyonları üzerindeki etkisine ve riskin gerçekleşme olasılığına göre değerlendiriyorsunuz.
  - Büyük bir bankada yeni teknolojinin benimsenmesiyle ilgili en önemli 10 riski tablo formatında tanımlayınız.
  - Riskin neden öncelikli olduğunu açıklayan Risk Adı, Risk Tanımı ve Gerekçe sütunlarını ekleyiniz.
  - Tablonun satırlarını yüksek riskten düşük riske doğru önceliklendiriniz.

Sonuç

Yeni teknolojileri benimsemek riskler doğurabilir, bununla birlikte yeni araçları takip etmemenin yaratacağı tehlikeleri de unutmamak gerekir. Böyle davranmanın birçok dezavantajı vardır:

- Yeni teknolojinin sunabileceği faydaları kaçırmak.
- Rakiplerin dijital dönüşümden elde ettikleri avantajları nedeniyle rakiplere ayak uyduramamak.
- Geliştirilmiş verimlilik ve üretkenlikten mahrum kalmak veya yeni ürün ve hizmetlerde inovasyon yapamamak.
- Teknolojik açıdan daha gelişmiş kurumlarla çalışmayı tercih eden potansiyel veya mevcut müşterileri, değerli iş ortaklarını veya yetenekli personeli kaybetmek.

Pelletier "Teknoloji her gün yaptığımız her şeyin temelini oluşturuyor," demiştir. İç denetim, yeni araçların maksimum olumlu etkiye sahip olmasını sağlamak konusunda rol oynayabilir.

Kısım 3: İç Denetimin Teknolojiye Hâkim Yeteneklerle Mücadelesi

Uzmanlar Hakkında

Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, TeamMate Denetim Çözümleri şirketinde kıdemli ürün yöneticisidir ve TeamMate'in sunduğu sınıfının en iyisi çözüm yoluyla bir yandan stratejik içgörüler sunarken diğer yandan denetim verimliliğini sürekli olarak iyileştirmek için çalışmaktadır. Hem kamu sektöründe hem de özel sektörde 20 yılı aşkın iç denetim deneyimi bulunmaktadır.

Jim daha önce İç Denetçiler Enstitüsü'nde bir dizi liderlik görevinde bulunmuş, Palo Alto Şehri'nde Şehir Denetçisi olarak görev yapmış ve San Diego'da (CA) Denetim Şefi olarak çalışmıştır. Jim'in çok yönlü iç denetim geçmişinde California Eyalet Üniversite Sistemi, PETCO Animal Supplies, Inc., State Street Corporation ve General Electric kurumlarındaki pozisyonları da bulunmaktadır.

Dennis Wong, CIA, CFSA

Dennis Wong, CIA, CFSA, Londra merkezli uluslararası bir bankada genel müdür olarak görev yapmaktadır. Uluslararası bankacılık ve sermaye piyasalarında 20 yılı aşkın deneyime sahip tecrübeli bir denetim ve risk uzmanıdır. Onun tutkusu, süreçlerin yeniden yapılandırılması ve teknoloji inovasyonu yoluyla değişimlere öncülük etmek ve yön vermektir. IIA New York Şubesinde gönüllü olarak çalışmakta ve küresel Sınav Geliştirme Komitesinde görev yapmaktadır.

Nisha Nair, CIA, FCCA, UAECA, CFE, ACMA, CGMA

Nisha Nair, Birleşik Arap Emirlikleri'ndeki Federal Nükleer Düzenleme Kurumu'nda iç denetim uzmanı olarak çalışmaktadır. '4 Büyük' danışmanlık firmasının birinde risk danışmanlığı da içeren finansal ve ticari risk danışmanlığı uzmanı olarak 10 yıldan fazla deneyime sahiptir. Nair, çeşitli mesleki yeterlilik kurumlarının üyesidir ve iç denetim mesleğinin gerçek değerini ortaya çıkarma ve tanıtma konusunda tutkuludur. Bunlara ilave olarak, risk yönetimi, veri analitiği, yönetişim, suistimal risk yönetimi, etik ve dış denetim de dâhil olmak üzere iç denetimle ilgili çeşitli konularda sahip olduğu uzmanlıkla IIA Global için Küresel Mesleki Bilgi Grubu'nda konu uzmanı olarak görev almaktadır.

Giriş

İç denetimin zırhındaki çatlak

2024 Kuzey Amerika İç Denetimin Nabzı yayınına göre, katılımcıların sırasıyla %78 ve %58'inin yüksek veya çok yüksek risk olarak değerlendirdiği siber güvenlik ve BT, iç denetim liderleri tarafından kurumlarındaki en yüksek iki risk alanı olarak seçilmiştir. Bu durum sürpriz olmamalı; gerçekten de teknoloji son birkaç yıldır risk ortamını domine etmektedir. Bununla birlikte, her geçen yıl, iç denetimin bu alanda ciddi zorluklarla karşı karşıya olduğu ve ele alınmadığı takdirde daha da kötüleşeceği daha görünür hale gelmektedir.

Çoğunluğu Kuzey Amerikalı denetim liderlerinden oluşan Nabız anketi katılımcılarına göre, siber güvenlik ve BT çalışmalarının toplamı denetim planlarının yaklaşık %20'sini oluşturmaktadır. Bu ikisi birlikte diğer risk alanları arasında en yüksek yüzdeyi oluşturmaktadır ancak Nabız verileri aynı zamanda hem siber güvenlik ve veri güvenliği hem de BT alanlarının en çok dış veya ortak kaynak kullanılan alanlar olduğunu göstermektedir. Bunlara ilave olarak, her 10 katılımcıdan 2'si teknolojinin en önemli öncelik olacağını belirtse de denetim fonksiyonlarının neredeyse yarısı kurum içi personel artışına öncelik vermektedir. Bu durum, denetim birimlerinin işe alım konusunda çeşitli sorunlarla karşılaşmaya devam etmesine rağmen geçerlidir ve Nabız katılımcılarının %29'u ücret beklentilerini en önemli zorluk olarak belirtirken, %17'si iş adaylarının gerekli yetkinliklere sahip olmadığını belirtmektedir.

Bu bulgular birlikte ele alındığında, iç denetimin kendisinin, dış ve ortak kaynak kullanımı yoluyla teknoloji risklerini elinden geldiğince ele alırken, genel olarak kurum içinde teknoloji yetkinlikleri kazandırmak için ideal bir konumda olmadığını gösteren bir tablo ortaya çıkmaktadır. Uzun vadede bu yaklaşımın sadece risk kapsamı açısından değil, aynı zamanda denetim fonksiyonlarının kendi rollerinin tüm yönlerini geliştirmek üzere teknolojiden yararlanma yetenekleri açısından da önemli yansımaları olabilir.

TeamMate kurumunun sponsor olduğu inovasyon ve teknoloji konulu bu üç kısımlık serinin son kısmı olan bu bilgi notu, teknoloji meraklısı ekipler oluşturmanın zorluğu gibi iç denetimin "teknoloji mücadelesi" olarak adlandırılabilecek pek çok yönünü incelemektedir. Ayrıca, seçkin sektör uzmanlarının katkılarıyla, sektör, bütçe veya fonksiyon büyüklüğünden bağımsız olarak ekiplerin, teknolojinin hızlanan ve durmak bilmeyen ilerleyişine ayak uydurabilecek güvence ve danışmanlık hizmetleri sağlamak için kullanabilecekleri bazı en iyi uygulamaları ve stratejileri de sunacaktır.

Teknolojiye Hâkim Ekip Oluşturma

Teknolojik Geleceğe Şimdiden Hazırlanın

Finansman sorunu

İç denetim, teknoloji okuryazarı yetenekleri kazanma yarışında yalnız değildir. Gerçekten de her sektördeki her kurumun neredeyse her departmanı aynı zorluğu yaşamaktadır ve bu da zaten sınırlı olan personel havuzundan işe alım yapma konusunda kıyasıya bir rekabet yaratmaktadır. COVID-19 pandemisi sırasında teknoloji sektörlerinde yaşanan toplu işten çıkarmaların ardından, birçok analist iş arayan yaklaşık 20.000 teknoloji sektörü çalışanının bu ihtiyacı bir şekilde karşılamasını bekliyordu. Ancak, teknolojinin hızlı gelişiminin bir göstergesi olarak, ihtiyaç duyulan pozisyonlar ile yeterli beceriye sahip kişiler arasındaki uçurum genişlemiştir ve işe alınabilecek yetenekler de ucuz değildir. Nabız Anketi verilerine göre, denetim fonksiyonlarının %51'inin bütçelerinin bir önceki yıla göre yaklaşık olarak aynı kaldığı göz önüne alındığında, teknolojiye hâkim personel istihdam havuzuna girmek isteyen her denetim fonksiyonunun önünde zorlu bir mücadele olduğu açıktır.

Birleşik Arap Emirlikleri'nde Federal Nükleer Düzenleme Kurumu'nda iç denetim uzmanı olan Nisha Nair, "Çeşitli iç denetim liderleri teknolojinin yaygınlaştırılmasındaki zorluklardan bahsederken en sık tekrarlanan konu yeterli finansman ihtiyacıdır" demiştir. "Bu durum BT araçları için finansmanı, iç denetim personeline yönelik teknoloji eğitimi için finansmanı ve ekip bünyesinde doğru teknoloji kaynaklarının işe alınması için finansmanı içermektedir. Çoğu zaman, örneğin siber sektör gibi belirli bir alandan bir kişiyi işe almaya çalıştığınızda, bu kişilerin ücret paketi açısından beklentileri tipik iç denetim ücret paketinden çok daha yüksek olacaktır; ayrıca, bu kişilerin çoğu genel bir iç denetim rolünde istihdam edilmek yerine daha fazla ödeme yapan niş uzmanlık alanlarında çalışmayı ve büyümeyi tercih etmektedir."

Bu acı gerçekle yüzleşen iç denetim, teknoloji odaklı risk ortamına en azından ayak uydurabilmek amacıyla bu gerekli beceri boşluklarını doldurma konusunda yaratıcı olmak zorunda kalmıştır. HSBC'nin mali suç risk denetimi genel müdürü ve küresel başkanı Dennis Wong, "Beceri seti stratejisi, her duruma uyan tek strateji değildir," demiştir. "Doğru karışım her denetim departmanı için farklıdır. Bu, organik olarak büyüme/yetiştirme, danışmanlık şirketleriyle ortak kaynak kullanımı ve mümkün olduğunda dışarıdan işe alımın bir kombinasyonudur."

Bu üç yönlü stratejinin her bir unsuru tartışmaya değerdir:

Dışarıdan işe alma

Daha önce de belirtildiği üzere, mevcut bütçe seviyeleri ve ek finansman eksikliği göz önüne alındığında, bu stratejinin uygulanması gerçekçi olmayan bir düşünce olarak görülebilir ve hatta tamamen göz ardı edilebilir. Ancak, kesinlikle bir zorluk olsa da bu alanda ilerleme kaydetmek mümkündür ve bu da denetim komitesiyle başlar.

Yönetim Kurulu ve/veya Denetim Komitesi, iç denetimin yıllık bütçesinin onaylanmasında güçlü bir role sahip olduğundan, bir iç denetim liderinin hedefi, teknolojinin yayılması ve inovasyon doğrultusunda teknik personel istihdamı için ek finansmanın neden gerekli olduğuna ilişkin güçlü bir iş gerekçesi oluşturmak olmalıdır. Nair, bunun verilerden alıntı yapmanın ötesine geçtiğini, daha ziyade reddedilmesi zor "ilgi çekici bir hikâye sunmayı" hedeflemek gerektiğini belirtmiştir. "İç denetim liderleri, Denetim Komitesinin ve Üst Yönetimin iç denetim departmanında teknolojiye hâkim yeteneklere duyulan ihtiyaç ve bu yeteneklerin kuruma sağlayacağı değer konusunda onayını almalı ve bu yetenekleri iç denetim departmanına çekmek için uygun ücretlendirme paketi ve kariyer yolunun gerekliliğini açıklamalıdır," demiştir Nair.

Nair, “Denetim komitesinin desteğini almalı ve bu tür yeteneklerin niş olduğunu ve iç denetim ekibi için geçerli olan ücret paketinin siber alandaki biri için aslında yeterli olmayabileceğini fark etmelerini sağlamalıyız,” demiştir.

Bu durum, denetim komitesinin iç denetim ekiplerinin günümüzün risk ortamı için ne kadar etkin yapılandırıldığını yeniden gözden geçirmesini de gerektirebilir. Denetim personelinden günümüzde beklenenler, 15 yıl öncesinden bile çok farklıdır. “Büyük resme baktığımızda, ekiplerimizin neye benzemesi gerektiğini düşünmemiz gerekiyor,” demiştir TeamMate Denetim Çözümleri kurumunda kıdemli ürün müdürü olan Jim Pelletier. “Günümüzde geleneksel bir iç denetçi değil, bir siber güvenlik uzmanı işe alıyorsunuz ve belki de sahip olmanız gereken rol budur. Denetim liderlerinin komitelerine iç denetim ücretlerini teklif edemeyeceklerini, çünkü bir iç denetçi işe almadıklarını açıklamaları gerekiyor. Bu kişilerin iş unvanlarında ‘denetim’ kelimesi bile olmayabilir.”

Bu çerçevede, böyle bir siber güvenlik uzmanının açıkça iç denetim için ayrılmış olması gerekmez. “Bu uzmanlar becerilerinin uygun olduğu her yerde kullanılabilirler,” demiştir Pelletier. “Bir siber güvenlik denetimi yaptığımda, bu denetimi kapsamlı bir şekilde yaparım ancak bunu sürekli olarak yapmam gerekmeyebilir; bu nedenle belki yılda birkaç kez siber güvenlik becerilerine ihtiyaç duyabilirim. İç denetimin yaratıcı olma zamanı geldi. Bir siber uzmanı ekibime tam zamanlı olarak almam gerekmeyebilir ancak normalde ikinci hatta çalışan bir siber uzmanını gerektiğinde denetçi olarak kullanabiliyorsam, bu durum bağımsızlık ve objektiflik ile ilgili endişeleri yönetebildiğim sürece son derece değerli ve verimli olacaktır.”

Bu tür konuşmalar Denetim Komitesi veya Yönetim Kurulu ile sınırlı kalmamalıdır; bununla birlikte, iç denetim liderinin yetenekli teknoloji uzmanlarının değerini anlatmak için güvenilir bir danışman olarak konumunu kullanması gereklidir. “Denetim departmanındaki liderler değişimin taşıyıcıları haline gelebilirler,” diye devam etmektedir Nair. “Yönetim ekibiyle teknoloji odaklı iletişim kurmaları ve tüm kurumun daha teknoloji destekli bir geleceğe doğru yol almasını kolaylaştırmaları gerekir.” Üst düzey yöneticiler düzeyinde böyle bir iletişimin kurulmasının, kurum bünyesinde diğer departmanlara da yansıyacağını söylemektedir Nair. Bu, ortak bir hedefe ulaşmak için teknolojik çözümler geliştirmek veya mümkün kılmak üzere iş birliğini teşvik eden bir ortam yaratılmasına yardımcı olacaktır. Yeterli kurumsal katılım ve destek sağlandığında, finansman da kaçınılmaz olarak bunu takip edecektir.

Mümkün olduğunda, havuzu genişletmek için her türlü olanaktan yararlanmak, kurum dışı yetenek arayışlarında aynı derecede önemli olan bir husustur. Bu birkaç yolla gerçekleştirilebilir. Örneğin, çeşitlilik, eşitlik ve kapsayıcılık (DEI) girişimlerine odaklanmayı sürdürmek departman ve kurum bünyesinde bilişsel zekayı teşvik etmekle kalmaz, aynı zamanda kurumları daha genç nesil yetenekler için daha cazip hale getirir. Buna ilave olarak, boş pozisyon ilanı veren departmanların, bu havuzu uzaktan çalışma seçeneklerini de kapsayacak şekilde genişletmeyi kuvvetle düşünmeleri gerekir. Nabız Anketine göre, Y kuşağı (1981-1996) iç denetim liderlerinin %95'i uzaktan çalışma seviyelerinin aynı kalmasını beklemektedir; bu da gelecekte işe alınacak kişilerin bu tür seçeneklere yöneleceği beklentisi olduğunu göstermektedir.

Son olarak, işe alım yaparken, teknolojinin çok hızlı ilerlediğinin ve bu nedenle bir iş tanımında yer alan birçok yetkinliğin birkaç yıl, hatta birkaç ay içinde güncelliğini yitirebileceğinin farkında olmalısınız. Bundan dolayı, işe alım yöneticilerinin, adayların beceri seti kutucuklarını işaretleme konusunda çok katı olmamaları gereklidir. Önemli olan, kişinin belirli bir teknoloji becerisini ne kadar iyi bildiği değil, sürekli olarak yeni beceriler geliştirme yeteneğidir. “Belirli bir teknoloji için bir kişiyi işe almanızı değil, yeni teknolojiyi kolayca kavrayabilecek birini işe almanızı öneriyoruz,” demiştir Nair. “İç denetim fonksiyonları, yeni becerileri bir sünger gibi emebilme açısından uyum sağlayabilen kişilere ihtiyaç duymaktadır.”

Bu tür kişiliğe sahip olanlar, kendilerini öğrenmeye ve başarılı olmaya hazır konuma getiren ekip eşleştirmelerinden en fazla fayda sağlayacak kişilerdir. “Risk, iş bilgisi, denetim, veri bilimi ve teknoloji becerilerinin tümüne 'tek başına' sahip olan benzersiz bir kişi bulmak çok nadirdir. İmkânsız değil ama nadiren olur,” demiştir Wong. “Dolayısıyla öncelik, denetim süreci boyunca öğrenebilen ve gelişebilen iç denetçilerle birlikte çalışan veri bilimcileri gibi kolektif olarak birlikte çalışan insanlardan oluşan bir ekibin oluşturulmasıyla ilgili olmalıdır”.

Beceri Kazandırma için Dış ve Ortak Kaynak Kullanma

Daha önce belirtildiği üzere, günümüzde birçok denetim fonksiyonu siber ve BT denetim sorumluluklarını dış ve ortak kaynaklardan temin etmeyi tercih etmektedir. Bu eğilim, işe alma konusundaki zorluklar ve kısıtlamalar göz önüne alındığında bir gereklilikten kaynaklandığı açıktır, ancak özellikle siber güvenlik gibi teknoloji alanlarında bu aynı zamanda bir zorunluluktur.

"Kurum içinde, en son ve en iyi teknoloji hakkında bilgi edinmek çok zordur," demiştir Wong. "Bu uzmanlığı aramak için şirketinizin dışına çıkmanız gerekir. İşte bu noktada danışmanlar ve uzmanlar devreye girer."

Bununla birlikte, bu dış firmalara iş verirken, dış kaynak kullanılarak temin edilen yeteneklerin denetim fonksiyonu üzerinde sözleşmelerinin süresinin ötesinde nasıl bir etkiye sahip olabileceği bazen göz ardı edilebilmektedir.

"İç denetim departmanlarının mevcut iç denetim tedarikçilerini, iç denetim ortaklarını ve/veya danışmanlık firmalarını kendi departmanlarındaki iç denetim personelinin becerilerini artırmak için kullanması ve dış/ortak kaynaktan temin edilen yeteneklerin öngörülen denetim işini yürütmesi gerçekten işe yarayan bir durumdur," demiştir Nair. "Görev yürütülürken bilgi aktarımını sağlamak için dış/ortak kaynaktan temin edilen kurum dışı yetenekleri/ortakları/danışmanları kurum içi iç denetim personeliyle eşleştirmek iyi olacaktır. İş başında öğrenmenin kesinlikle daha etkili olduğu kanıtlanmıştır."

Pelletier de aynı fikirdedir.

"Dış veya ortak kaynak kullanıyorsak bu sorun değil ama gelişme sağlıyor musunuz?" diye soruyor Pelletier. "Personelinizi, öğrenmeleri için onların projelerine dâhil ediyor musunuz? Kurum içi beceri setlerinizi biraz daha geliştirmek için sahip olduğunuz zamandan tam olarak yararlanıyor musunuz?"

Dış ve ortak kaynaktan temin edilen yeteneklerin temel teknoloji yetkinliklerini daha yapılandırılmış bir şekilde yaymak da faydalı bir fikirdir. Bu, tüm departmanlardan kişilerin teknolojinin olanaklarını ilk elden görebilecekleri ve daha sonra yeni keşfedilen bilgileri kendi alanlarına geri getirebilecekleri atölye çalışmaları veya grup oturumları şeklinde olabilir.

Bununla birlikte, ekibin becerileri geliştirildikten veya tam zamanlı uzmanlık kazandırıldıktan sonra, ortak kaynak kullanımı bir kurumun beceri seti stratejisinin her zaman bir parçası olmalıdır. "Yüksek nitelikli yetenekler tam zamanlı personel olarak işe alındığında, kaçınılmaz olarak üstünlüklerini kaybederler," demiştir Wong. "Örneğin, siber güvenlik alanında, sızma testi gibi işleri yapması için son teknoloji uzmanlığına sahip bir beyaz şapkalı bilgisayar korsanını işe aldığınızı varsayalım. Ancak eğer bundan böyle 'bilgisayar korsanlığı' yapmayacaklarsa, artık bu alandaki en ileri noktada olmayacaklardır. Dolayısıyla, kurum içi ekibin beceri düzeyi ne olursa olsun, her zaman bir dereceye kadar harici bir firma tutmak isteyeceksiniz çünkü onlar en son güvenlik açıklarını her zaman bileceklerdir."

İçten Dışa Beceri Geliştirme

Teknolojiyle ilgili tartışmaların büyük bir kısmı yeteneklerin kuruma kazandırılması etrafında dönse de halihazırda kurum içinde bulunan yetenekleri göz ardı etmemek çok önemlidir. İç denetim, üst yönetim ve BT ekibi arasındaki olumlu ilişkiler ve iş birliği aracılığıyla, iç denetimin diğer departmanların sahip olduğu beceriler ve araçlar hakkında net bir anlayış geliştirmek için çalışması gereklidir. Örneğin, veri analitiği veya sürekli izleme yazılımı, küçük bir eğitimle denetim görevlerine sorunsuz bir şekilde uyum sağlayabilecek geniş uygulamalara sahip olabilir.

"Diğer ekiplerle birlikte çalışmalı ve iş birliği yapabileceğiniz çeşitli yolları keşfetmelisiniz ve eğer kurduğunuz bu ilişki iyiyse, 'Tamam, elimizde bu araçlar var; neden bunları iç denetim amacıyla kullanmıyoruz?' gibi şeyler söyleyebilirler" demiştir Wong.

Bu durum üst yönetim için de geçerlidir. Üst yönetim, ikinci hat olarak veri analitiği araçlarına, sürekli denetim sürekli izleme (CACM) araçlarına ve ISO standartları ve prosedürlerle ilgilenen araçlara erişebilir ve bunların hepsi iç denetim bağlamında faydalı olabilir.

Elbette, beceri geliştirme ihtiyacı sadece iç denetimin çok ötesine geçmektedir. Şüphesiz, kurum genelinde temel teknoloji yetkinliklerini artırma çabasının günümüz ortamında her zaman ve her yerde mevcut olması gerekir. İç denetim liderlerinin, bir kez daha, değişimin öncüsü rollerinden yararlanarak tüm departman etkileşimlerinde güncel teknoloji trendleri ve teknikleri konusunda

zorunlu eğitim verilmesini savunmaları gereklidir. “İç denetim yetkinlik çerçevesindeki her bir pozisyon için ilerleme/uzmanlık seviyeleriyle birlikte teknoloji veya veri ile ilişkili bilgi ve beceriler için minimum seviyeyi tanımlamak etkili bir yaklaşım olacaktır,” demiştir Nair. “Her bir iç denetim uzmanını, işteki pozisyonları için en azından temel BT becerilerini öğrenmek ve bu konuda ilerlemek üzere gerekli minimum eğitimi almaya teşvik etmeliyiz.”

Wong da benzer bir duyguyu dile getirmektedir. “Tüm rollerde sürekli olarak beceri geliştirme ihtiyacı var,” demiştir Wong. “Güncel kalmak ve piyasalara ayak uydurmak için bu bir zorunluluktur. Her zaman haberdar olunması gereken yeni araçlar ve teknikler vardır.”

Bu tür becerileri edinmek için her zaman eğitim bütçelerini artırmak gerekmez. Bu becerilerin çoğu, ücretsiz çevrimiçi kurslar veya departmanlar arası bilgi paylaşım oturumları – ki ideal olan her ikisini de uygulamaktır – aracılığıyla bireysel olarak öğrenilebilir. “Çoğu zaman teknik konulara hâkim olmayan kişiler internette teknik makaleler okuduklarında teknik jargon onları soğutur,” demiştir Nair. “Departman veya kurum bünyesinde iç denetim personelinin bu tür teknik ve teknolojik jargonları ve kavramları anlamasına yardımcı olacak kişilerin bulunması, teknolojinin çeşitli yönlerini keşfetme arzusu yaratma açısından oldukça faydalıdır.”

Bununla birlikte, “minimum çıta” bir kez belirlendikten sonra, bu çıtanın kısa sürede yükseltilmesi gerekeceğini unutmayın. Bir denetim aracılığıyla bu çerçeveleri değerlendirirken, iç denetçilerin sadece becerilerin öğretilip öğretilmediğine değil, aynı zamanda bu becerilerin sürekli ve etkili bir şekilde nasıl uygulandığına ve bilgi tabanı büyüdükçe nasıl geliştirildiğine de odaklanmaları gerekir.

“Etkili bir beceri geliştirme stratejisinin ‘dijital uygunluk’ ölçümünü de içermesi gereklidir” demiştir Nair. “Departman performans ölçümlerinin teknolojinin uygulanmasıyla sınırlı kalmaması ve aynı zamanda departmanın söz konusu teknolojinin kullanımı açısından sürekli olarak nasıl gelişme gösterdiğini ölçen anahtar performans göstergelerini (KPI) de içermesi gereklidir. Bu nedenle, iç denetim liderlerinin, departmanların sadece belirli bir teknolojiyi uygulamak yerine nasıl dönüştüğünü gösteren KPI'ların geliştirilmesini savunmaları gerekir. Sürekli gelişim veya dönüşüm olmadan herkes durağan kalma riskiyle karşı karşıyadır.”

Pelletier şunları ekliyor: “Teknoloji yaptığımız her şeye entegre olmuş durumda ve dolayısıyla, bu çıtanın yükseltilmesini sürekli olarak savunmamız gerekiyor. Teknoloji sürekli değişiyor ve bu yüzden biz de aslında hep arayı kapatma modundayız. Eğer harekete geçmezsek, aradaki fark giderek açılmaya devam edecek. Bir denetim lideri olarak hedefiniz, sizin ve yönetim kurulunuzun bu farkın ne kadar geniş veya dar olmasını istediğinizi yönetmektir.”

Çok Yaşa Kral Veri!

Tüm Teknolojik İlerlemenin Temeli

Kaliteli veriyi bulma ve anlama

"Veri kraldır" derler ve bu deyiş gün geçtikçe daha gerçekçi bir hal alıyor. Etkili dijital ekipler oluşturmak için kullanılan strateji ne olursa olsun, kaliteli veriye erişim olmadıkça bunların hiçbir etkisi olmayacaktır.

"Veri, özellikle de sistematik ve otomatik hale getirilmiş kontrollerin kullanımının yaygınlaşmasıyla birlikte denetim çalışmaları için zorunlu hale gelmiştir," demiştir Wong. "Günümüzde veri bolluğu göz önüne alındığında, verinin nasıl kullanılacağının bilinmesi şartıyla, iç denetimde bu veriden faydalanma fırsatları oldukça fazladır ve bu da veri eksikliğini daha da sorunlu hale getirmektedir."

Veri eksikliğinin sorunlu olduğunu kabul etmekle birlikte, bugün bile kaliteli veriye erişim söz konusu değildir. Nair'e göre, iç denetim departmanlarının veri elde etmedeki yetersizlik algılarını, iç denetim faaliyetlerinde teknolojinin yaygınlaştırılması yönünde ilerlememek için bir bahane olarak kullanmaları da aynı derecede endişe vericidir. Böyle bir durum söz konusu olamaz. Bunun yerine, veri elde etme ve veriden yararlanma yolculuğu, iç denetimin teknolojik ilerlemeye yönelik iş gerekçesinin kritik bir parçası olarak kullanılmalıdır. "Veri bütünlüğü söz konusu olduğunda, iç denetim fonksiyonlarının kendilerini sadece verilerin iyi veya kötü olarak tanımlanması veya kategorize edilmesiyle sınırlandırmaması gerekir," demiştir Nair. "Bunun yerine, iç denetim fonksiyonlarının bu fırsatı değerlendirerek konuyu üst yönetimin dikkatine sunması, veri kalitesinin iyileştirilmesine yönelik tavsiyelerde bulunması ve sürece önayak olması gereklidir. Bu tür endişeler nedeniyle denetimlerde teknoloji kullanımının durdurulması, iç denetim fonksiyonlarının teknoloji çalışmalarında asla ilerleyememesine neden olabilir."

Böyle bir durum söz konusu olamaz. Aksine, veri elde etme ve veriden yararlanma yolculuğu, iç denetimin teknolojik ilerlemeye yönelik iş gerekçesinin kritik bir parçası olarak kullanılmalıdır. "Görüyoruz ki kendimizi her zaman sadece verinin iyi mi kötü mü olduğunu belirlemekle sınırlamamamız gerekiyor," demiştir Nair. "Bunun yerine, aslında ilerlemeli, bunu vurgulamalı ve iyileştirme alanlarını tanımlamak, yönetimle iletişim kurmak ve sürece önayak olmak için bir yol olarak kullanmalıyız. Çünkü herhangi bir noktada durursak, bu sonsuza kadar yerinde sayma riski taşır."

Veri, toplanabilmesi için mutlaka yatırım gerektirmez. Çoğunlukla, mesele sadece halihazırda elde bulunan verilerden yararlanacak bilgiye sahip olmak olabilir. Bir Excel tablosunda izlenen bilgiler bile duruma bağlı olarak kaliteli veri olarak kabul edilebilir. Bunu çözmenin yolları basittir: Fark etmek, vurgulamak ve kullanmak için doğru beceri ve böyle bir becerinin gelişmesini teşvik edecek doğru kültür. Başka bir deyişle, yetenekli kişinin beslendiği ve geliştirildiği her yerde veri de onu takip eder.

Doğru ortamda, verilerin değerli sayılabilmesi için mükemmel düzeyde ideal olması bile gerekmez. "Bence verinin olması, hiç veri olmamasından her zaman daha iyidir," demiştir Wong. "Eksik veri seti bile hiç veri olmamasından daha iyidir. Aslında elinizde olandan her türlü veri analitiği fırsatını elde etme zihniyetine sahip olmak ise verinin eksiksiz olmasından daha önemlidir. Diyelim ki size 10 dolar veriyorum ama bunu bozukluk olarak veriyorum. Biraz külfetli olsa bile, yine de 10 dolar olduğunu düşünerek kabul edeceksiniz."

Bununla birlikte, iç denetim verilerin nasıl kullanıldığını anlamaktan daha fazlasını yapmak zorundadır. Pelletier'e göre, veri bilgisi şu dört soruyu yanıtlamaya dayanmaktadır:

- Veri nereden geliyor?
- Veri nerede depolanıyor?
- Veriyle ne yapılıyor?

- Veri nasıl imha ediliyor?

Çoğu zaman, bu soruları yanıtlamak özellikle yüksek düzeyde teknik bilgi gerektirmez.

“Veri yönetişimi, bence her denetçinin uzman olması gereken bir konudur,” demiştir Pelletier. “Bazı hususlar daha derin teknik bilgi gerektirebilir ancak her denetçinin zorlu sorular sorabilecek, altta yatan süreçleri anlayabilecek ve sadece ihtiyaç duyduğu kısımlarda teknik uzmanlığı devreye sokabilecek donanıma sahip olması gereklidir.”

Sonuç

Teknoloji kayıp değil fırsattır

Teknolojinin getirebileceği inanılmaz faydalar hakkında yapılan tüm konuşmalara rağmen, teknoloji bir o kadar da endişe getirebilir. Bu durumu bunaltıcı görmek doğaldır; öyle ki, kişi kendi iş güvenliğini bile sorgulamaya başlayabileceği bir noktaya gelebilir. Teknoloji geliştikçe bir noktadan sonra insan emeğine ihtiyaç duyulacak mı?

Bu anlaşılabilir bir kaygıdır ancak yanlış kurumsal kültürden kaynaklanan bir kaygıdır. Teknolojinin bir rakip ya da tehdit olarak görülmemesi gerekir — daha fazlasını başarmak, kuruma daha fazla değer sağlamak ve hatta her çalışanın günlük yaşamını iyileştirmek için bir fırsat olarak coşkuyla karşılanmalıdır.

"Çoğunluk olmasa da otomasyonun işlerini ellerinden alacağına inanan ya da davranışsal olarak denetimleri yürütmede sabit yöntemlerini sürdürmeye, örneğin eski güzel elektronik tabloları kullanarak rahat ettiği şeyi yapmaya meyilli olan bazı insanlar olabilir," demiştir Nair. "İç denetim liderlerinin, öğrenme zihniyetini ve teknolojinin potansiyel faydalarını benimsemek yoluyla teknoloji odaklı bu dinamik çağda çevik kalma ihtiyacı hakkındaki tartışmaları, özellikle de denetçilerin yerini alacak bir araçtan ziyade, departmanın iş yükünü azaltacak veya verimliliği artıracak bir araç çerçevesinde ele alınan tartışmaları teşvik etmeleridir."

İç denetim, kurum bünyesinde teknolojinin en büyük savunucusu olabilir ve olmalıdır. İç denetim değişimin yüklenicisi, işbirlikçisi, müjdeleyicisidir. Teknoloji mücadelesi devam ettikçe kurumlar birden fazla teknolojiden faydalanabilir.

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 alanlarındaki lideri olarak tanınmaktadır. Daha fazla bilgi için, lütfen **theiia.org** adresini ziyaret ediniz.

Wolters Kluwer TeamMate Hakkında

Wolters Kluwer TeamMate Denetim Yönetimi Çözümleri, 25 yılı aşkın süredir kurumsal, ticari ve kamu sektörü denetçilerini geliştirmeye adamış, dünya lideri bir iç denetim ve güvence uzmanı çözümüdür. İç denetim ekipleri daha derin içgörü ve daha fazla risk güvencesi sağlamak ve verimliliği artırmak için gelişirken, amaca yönelik ve geleceğe hazır çözümlere ihtiyaç duymaktadırlar. TeamMate, iç denetçilerin kurumlarına değer katmak için güvendikleri uzman çözümler sunmaktadır. Daha fazla bilgi için, lütfen https://www.wolterskluwer.com/en/solutions/teammate 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 bu nedenle sadece bir rehber olarak kullanılması amaçlanmaktadır. IIA, herhangi bir spesifik durumla doğrudan ilgili konularda bağımsız uzman tavsiyesi almanızı önerir. IIA, herhangi bir kimsenin bu rehberi tek referans kaynağı olarak kullanması durumunda hiçbir sorumluluk kabul etmez.

Telif Hakkı

Mayıs 2024

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