KÜRESEL BAKIŞ AÇILARI & ANLAYIŞLAR

SUİİSTİMAL

BÖLÜM I: Kripto Dünyasında Suiistimal

BÖLÜM 2: İç Denetçiler ve Suiistimal İnceleme Uzmanları: Değerli Bir Ortaklık

BÖLÜM 3: Hangover: COVID-Sonrası Dönemde Suiistimal

The Institute of Internal Auditors

İçindekiler Tablosu

Bölüm 1

Kripto Dünyasında Suiistimal

Uzmanlar Hakkında

Dana Lawrence, CIA, CRMA, CFSA, CAMS, CRVPM

Dana Lawrence, Fideseo'nun Baş Uyum Görevlisidir. Lawrence, karmaşık uyum, kurumsal risk yönetimi (ERM), iç denetim ve yönetişim programı yapma, ölçeklendirme ve iyileştirme konularında tanınmış bir uzman ve liderdir. Lawrence'in teknoloji ve finans hizmetleri alanındaki kariyeri, ipotek karşılığı krediler, topluluk bankacılığı, büyük A.B.D. bankaları ve global bankalar, açık bankacılık ortakları, finans teknolojisi ve kripto alanlarını da kapsamaktadır. Lawrence, bankacılık düzenleyici otoriteleriyle ve iç/dış denetçilerle doğrudan çalışan üst liderlik rolleri üstlenmiş bulunmaktadır. Kendisi 40.000'e kadar çıkabilen katılımcıyla düzenlenen yerel, ulusal ve global etkinliklerde konuşmalar yapan popüler bir konuşmacı ve etkinlik evsahibidir. IIA gibi çeşitli farklı gruplara da hizmet eden, kendini adamış bir gönüllü ve fikir lideridir.

Lourdes Miranda, CAMS, CCE, CCFI, CEIC, CFE, CRC, FIS, MS

Lourdes Miranda, bir blok zincir teknoloji şirketi olan SendCrypto'da Baş Uyum Görevlisidir. Miranda, 20 yılı aşkın bir devlet ve kurumsal hizmet deneyimine sahip olan ve özellikle global düzeyde mali suç soruşturmaları, istihbarat toplama ve analizi konularında uzmanlaşmış bir eski CIA Görevlisi ve FBI Analistidir. Miranda, karapara aklayanları ve terörizmi finanse edenleri hedefleyen kapsamlı ve ileri düzeyde saha deneyimine sahiptir. Miranda, 2017 yılından beri, Finansal Teknoloji firmaları için bir kıdemli kripto soruşturmacısı, kıdemli uyum görevlisi ve risk müdürü olarak görev yapmakta ve uyum, soruşturma, kripto ve istihbarat ekipleri inşa etmekte ve eğitim programları düzenlemektedir. Aynı zamanda bu konuda çalışan bir yazar ve eğitmendir ve bir konu uzmanı olarak çok sayıda çevrimiçi kursa da katkıda bulunmaktadır. Buna ek olarak, Miranda, Kanada merkezli Toronto Compliance & AML Enterprise (TCAE) firmasında bir Danışma Kurulu Üyesidir.

Giriş

Global konuşmalarda kripto ve suiistimal

Kripto para borsası FTX'in karizmatik kurucusu **Sam Bankman-Fried** bir zamanlar tahminen 26,5 milyar $'lık bir servete sahipti. Kripto pazarındaki en büyük üçüncü borsanın bir noktada lideri olarak, Bankman-Fried ve FTX'in ikisi de BlackRock gibi çok farklı yüksek profilli yatırımcıların ve NFL oyuncusu Tom Brady'nin sevgilileriydiler. Tüm bunlara rağmen, Bankman-Fried, modern tarihin en dramatik şirket iflaslarından biri neticesinde bir gecede tüm servetini kaybetti.

Bankman-Fried, 13 Aralık 2022 günü Bahamalar'da tutuklandı. Kamuya yapılan açıklamalara göre, elektronik dolandırıcılık, elektronik dolandırıcılık için kumpas kurmak, menkul kıymetler dolandırıcılığı, menkul kıymetler dolandırıcılığı için kumpas kurmak ve kara para aklamak da dâhil çeşitli farklı suçlamalarla karşı karşıya.

Bu kadar inanılmız bir çöküşün yarattığı büyük gösteriye insanların gösterdiği yaygın ilgiye ek olarak, bu olay, aynı zamanda dijital varlıklar hakkında daha da büyük soruları gündeme getirdi. Tornado Cash ve Bitzlato gibi skandallara benzer şekilde, FTX'in iflas etmesi ve bu iflasın onun temsil ettiği sektöre yaptığı etkiler, en azından A.B.D. Menkul Kıymetler ve Borsa Komisyonu Başkanı Gary Gensler'in "Vahşi Batı" olarak tarif ettiği mevcut haliyle kripto varlıkların uzun vadeli yaşama gücü ve kapasitesi hakkında pek çok sorunun sorulmasına yol açtı.

Kripto varlıkları ve bilgileri korumanın en güvenli ve emin yollarından biri olan blok zincir teknolojisi üzerine inşa edilmesine rağmen, dünyanın en önde gelen kripto para borsalarından birinin çok göz önünde olan başkanı bile bu kadar büyük ölçekli suiistimal ve dolandırıcılık eylemleri yapabiliyorsa, bu sektörde belirli bir kapasiteyle faaliyet gösteren şirketlerin karşılaşabileceği başka hangi kırılganlıklar vardır bu alanda? Kripto varlıkların meteorik yükselişiyle birlikte risk ortamı nasıl ve ne yönde değişmiştir ve bazı kurumlar ve onların iç denetim bölümleri bu değişikliklere nasıl başarıyla cevap verebiliyorlar?

Suiistimalle ilgili bu üç-bölümlük kitapçığın 1. Bölümü, bir kripto varlık dünyasının erken aşamalarında tanık olunan yaygın suiistimal tertiplerini inceleyerek bu soruları ele alacaktır. Bu konu hakkında daha fazla bilgi verebilmek için, IIA, bu brifingde isimleri anılan konu uzmanlarının katılacağı bir canlı Soru & Cevap oturumuyla birlikte, yakın zamanda gerçekleştirilen "Suiistimal perspektifleri: Blok Zincir, Kripto ve KYC" başlıklı bir webinarın tekrar gösterimini gerçekleştirecektir.

Kripto Dünyasında Belirsizlikler

Heyecan verici, fakat riskli bir gelecek

Kuruluşlar artık dikkatli davranıyorlar

Etki ve sonuçları çok büyük olmasına ve aslında tamamen bir devrim niteliğinde olmasına rağmen, blok zincir teknolojisini kavramsal anlamda sanal ortamda ve ağ yapısında paylaşılabilen ve saklanabilen dijital varlık işlemlerinin kesintisiz ve sürekli büyüyen bir günlüğünden başka bir şey olmayan bir teknoloji olarak anlamak nispeten kolaydır. Onu ayırt eden özellik, her yeni işlemle birlikte bloğu kesintisiz olarak şifreleyen ve böylece daha da güvenli ve emin hale getiren doğrulama metodolojileri kullanmasıdır.

"Teknolojinin kendisi son derece komplike ve karmaşıktır ve onu analiz edebilmek için yıllarca eğitim ve öğretim almak gerekir, fakat ben blok zincirin kendisini bir mali tablo olarak görüyor ve düşünüyorum," diyor bir blok zincir teknolojisi şirketi olan SendCrypto'nun baş uyum görevlisi Lourdes Miranda. "Blok zincir, varlıkları kimin gönderdiğine, varlıkların nerede depo edildiğine, herhangi bir varlık çekme işlemi yapılıp yapılmadığına ve nihai bakiyeye ilişkin bilgilere sahiptir."

Kripto para, muhtemelen bu teknolojiyi kullanan ve merkez bankaları gibi kurumların etkilerinden âri ve bağışık bir adem-i merkezi, açık kaynak para sistemi (veya sistemleri) yaratan en tanınmış ve en iyi bilinen varlıktır, fakat blok zincire dayanan kripto varlıkların diğer örnekleri arasında pek çok başkasının yanı sıra gayri misli sanal jetonlar (NFT), dağıtık hesap defteri teknolojileri (DLT) ve oyun jetonları da sayılabilir.

Bununla birlikte, tüm sektör ve piyasaların da hızla öğrendiği gibi, sadece kripto varlıkların geleneksel yöntemlerle manipüle edilmesi neredeyse olanaksız olan güvenli bir teknolojinin üzerine inşa edilmiş olmaları bu varlıkları benimseyen ve kullananların riskten muaf oldukları anlamına gelmez. FTX'in iflas etmesi bu gerçeği birden fazla şekilde ve yolla göstermiştir. Örneğin, bu iflas, gereken doğru kurumsal yönetişim ve iç kontrollerin bulunmamasının sadece kurumun kendisi için değil, aynı zamanda tüm sektör çapındaki yatırımcılar için de ne kadar zarar verici olabileceğini göstermiştir.

Bu, IIA Başkanı ve CEO'su Anthony Pugliese'nin son zamanlarda A.B.D. Kongresi'ne gönderdiği ve onları Amerika Birleşik Devletleri'nde faaliyet gösteren kripto para borsaları, blok zincir teknolojisi şirketleri, NFT piyasaları ve Web3 platformlarında kurumsal yönetişimi desteklemek ve artırmak için yeni koşullar ve kurallar koymaya davet ettiği mektubunda da işaret ettiği bir konuydu. "FTX'in iflasının bedelini bugün sayısız yatırımcı ödüyor," diyor Pugliese. "Regüle edilmemiş kripto borsalarının kendi başlarına doğruyu bulmalarına ve doğru hareket etmelerine bel bağlayamayacağımız açıktır; daha güçlü kurumsal yönetişim standartları koymamız ve bu borsalar kendi müşterilerini korumadıkları takdirde onların da hesap vermelerini sağlamamız gerekiyor. Kötü kurumsal aktörler iflas ettiğinde, bunun cezasını çeken yatırımcılar olmamalı ve kabak onların başına patlamamalıdır."

Pugliese, FTX'in iflasını vurguladı ve bu iflasın piyasada yarattığı sonuçların sağlam bir iç denetim fonksiyonunun alacağı önlemlerle hafifletilebileceğine işaret etti. "FTX'in iflası etmesi, sağlam bir iç denetim bölümü bulunmayan kuruluşların en hafif deyimiyle ateşle oynadıklarına ve en kötü ihtimalle de kendilerini ve paydaşlarını felaketlere yol açabilecek – ve tamamen önlenebilir olan – bir çöküş ve iflas tehlikesine attıklarına dair en yeni uyarıdır aslında," diyor Pugliese.

Pugliese ve başka kişilerin dile getirdiği bu endişeler duymazdan gelinmedi ve boşa gitmedi. 3 Ocak 2023 günü, Federal Merkez Bankası, Federal Deposit Insurance Corp. (FDIC) (Federal Mevduat Sigortası Şirketi) ve ABD Hazine Bakanlığı Banka Denetim Dairesi (Office of the Comptroller of the Currency) (OCC) kripto para hakkında ilk ortak açıklamalarını yayınladılar. Bu açıklamada, aşağıda sayılanlar da dâhil olmak üzere kripto parayla işlem yapan bankamarın bir şekilde karşılaşabilecekleri çok çeşitli risklere dikkat çektiler:

- **Kripto varlık sektörü katılımcıları arasında suiistimal ve dolandırıcılık eylemleri riski**

- **Saklama uygulamaları, borç ödemeleri ve sahiplik haklarına ilişkin hukuki belirsizlikler**
- **Kripto varlık şirketlerinin yapabilecekleri yanlış ve yanıltıcı beyan ve açıklamalar**
- **Kripto varlık piyasalarında meydana gelen ve etkileri arasında kripto varlık şirketleriyle bağlantılı mevduat akışları üzerinde potansiyel etkilerin de bulunduğu önemli volatilite ve oynaklıklar**
- **Kripto varlık sektöründe, şeffaf olmayan ödünç verme, yatırım, fonlama, borç servisi ve operasyonel düzenlemeler yoluyla kurulan bağlar da dâhil belirli kripto varlık katılımcıları arasındaki iç ve ara bağlardan kaynaklanan bulaşma riski**
- **Kripto varlık sektöründe olgunluktan ve sağlamlıktan uzak gözüken risk yönetimi ve yönetişim uygulamaları ve**
- **Açık, kamusal ve/veya adem-i merkezi ağlarla veya benzeri sistemlerle bağlantılı risk artışları**

Bu risklerin tümü aslında tartışmaya değer olmalarına (ve çoğu durumda kripto ile işlem yapan bankalar dışındaki kurum ve kuruluşlara da uygulanabilecek olmalarına) rağmen, bu brifingin odak noktası, kripto katılımcılarına yönelik yapılan suiistimal fiilleri ve bunların mevcut ortamda aldıkları belirgin formlarla sınırlı tutulacaktır.

Suiistimaller için Olgunlaşmış bir Ortam

Sürekli büyüyen ve genişleyen bir risk ortamı

Kötü adamların takım çantasında yeni bir araç

Kripto varlıklar manipülasyona karşı kayda değer düzeyde artırılmış şifreleme ve şeffaflık gibi **bazı avantajlı özelliklere sahip olsalar da,** bu varlıkları (ve onların arkasındaki blok zincir teknolojisini) suiistimal ve dolandırıcılık yapmayı amaçlayanların kullanabileceği güçlü bir araç haline getiren de yine onların bu aynı özellikleridir.

Gerçekten de, düzenleyici otoritelerin ve kanunları uygulamakla görevli kurumların dikkatini çeken şey de kripto varlıkların kötü adamları cezbeden bu özellikleri olmuştur. "Düzenleyici otoritelerin kripto varlıklara bu kadar ilgi göstermelerinin tek sebebi kötü adamların bu varlıkları operasyonlarını finanse etmek ve kara para aklamak amacıyla kullanmalarıdır," diyor neredeyse 30 yıldır CIA ve FBI adına mali suçları soruşturan Miranda. "Blok zinciri manipüle etmek çok zordur, fakat yine de blok zincir kötü ve alçakça amaçlara yönelik fiilleri kolaylaştıran şekillerde de kullanılabilir."

Örneğin, bu yöntemlerden biri, blok zincir içinde sahte kimliklerin kullanılmasıdır. "Bu, kripto dünyada devasa kullanım alanı olan bir yöntemdir," diyor Miranda. "Kötü adamlar, hesap cüzdanları açtıkları zaman KYC (Müşterini Tanı) uzaktan müşteri edinimi sürecini geçebilmek için karaborsada satın aldıkları geçerli ve meşru kimlikleri kullanmaktadırlar. Bu kimliklerin herhangi bir suç kaydı yoktur ve herhangi bir kara listede değildirler – tamamen temizdirler. Daha sonra, bu temiz ismi kullanarak, soruşturmacılar suiistimal ve dolandırıcılık eylemlerini kendi gözleriyle görene kadar hiç fark edilmeden kara parayı oradan buraya dolaştırabilmektedirler."

Kripto varlık endüstrisi de tüketicilere kolaylık sağlamak amacıyla tasarlanmış olmalarına rağmen rahatlıkla kötüye kullanılabilecek çeşitli farklı yasal boşlukları bulunan çeşitli araçlar geliştirmiş ve kullanıma sunmuştur. Örneğin, bir dolandırıcılık eyleminin başlatıcısı, kolluk güçlerinin uyarı ve alarmlarına yakalanmamak için bir kullan-at telefonla birlikte Bitcoin ATM gibi bir kripto işlem merkezini de kullanabilir.

"Diyelim ki New York'tayım, mali amaçlarla para aktarmak istiyorum ve Miami'de bulunan kötü adamlarıma ödeme yapmam gerekiyor. Kötü adamlar paralarını istiyorlar ve paralarının hızla ellerini geçmesini istiyorlar. Ödeme karşılığında bir makbuz almayacağım ve masaüstü veya dizüstü bilgisayar kullanamam, çünkü IP adresi uyarı ve alarm verir. Bu sebeple, ne yapıyorum? New York'da bir Bitcoim ATM'ye gidiyorum ve nakit para ve bir kullan-at telefon kullanıyorum. Bu yolla, hem kara para aklamanın önlenmesi protokollerini boşa düşürmüş, hem de kötü adamlara para ödemiş oluyorum. Bu bir suiistimal ve dolandırıcılıktır," diyor Miranda.

Pig butchering (Domuz Kesmek)

Kötü adamların kullanabilecekleri **başka bir yaygın suiistimal ve dolandırıcılık taktiği** de "pig butchering" (domuz kesmek) çarpıcı terimi adıyla bilinen bir yöntemdir. "Bu yöntem, temelde, bir dolandırıcının güven tesis etmek amacıyla uzunca bir süre birlikte yatırım yapmak suretiyle kurbanlarını metaforik olarak 'şişmanlatması' konseptine dayanır," diyor iş ve teknoloji danışmanlığı firması Fideseo'nun baş uyum görevlisi Dana Lawrence. Lawrence'a göre, dolandırıcıların yatırım yaptıkları bu süreç herhangi bir yerde geçirilebilir, fakat en yaygın olarak haftalar ve hatta aylar boyunca sosyal medya veya metinler aracılığıyla yürütülmektedir. Lawrence, dolandırıcıların favori platformunun özellikle LinkedIn olduğunu, fakat aynı zamanda Twitter gibi sosyal medya sitelerini de kullandıklarını söylemektedir.

Bu yöntemde, kötü adam normalde kendisini kripto paralara yatırım yapmış ve başarılı olmuş bir fenomen veya içeriden bir kimse olarak tanıtır. Zamanla, kurbanlarını da varlıklarını bu alana yatırmaya teşvik etmek gayesiyle kripto paraların faydalarına dair çığırtkanlık yapar. Bazı durumlarda, dolandırıcılar bu yatırımdan çok büyük getiriler elde ettikleri görünümünü vermek amacıyla kurbanlarına sahte ve düzmece mali tablolar bile gönderirler.

Bu işaretleri okumak ve oldukça açık bir şekilde tespit etmek ve yerlerini bulmak kolay olmasına rağmen, dolandırıcılar bu yöntem konusunda kendilerini son derece geliştirmiş bulunmaktadırlar. Örneğin, Kamboçya ve Çin gibi ülkelerde yerleşik dolandırıcılık şebekeleri, insanların hatalı kararlar vermeye daha açık ve daha savunmasız hale nasıl getirilebileceği konusunda psikologlardan derin ve detaylı eğitimler almaktadırlar.

"Dolandırıcılık şebekeleri, insanları manipüle etmenin en iyi yolunu bulmak konusunda psikologlardan eğitim alıyorlar," diyor Kaliforniya Santa Clara Şehri bölge savcısı Jeff Rosen, CNN'e verdiği bir röportajda. "Sizi savunmasız hale getirmek ve paranızı onlara kendi isteğinizle aktarmaya teşvik etmek için sürekli olarak farklı psikolojik teknikler kullanan insanlarla uğraşıyorsunuz." [1]

Pump and dump (Doldur ve boşalt)

Kripto dünyasında gözlemlenen diğer büyük dolandırıcılık yöntemlerinden biri de menkul kıymetler borsasında gözlemcilerin uzun süredir bildikleri ve gözlemledikleri bir yöntemdir: "pump and dump" (doldur ve boşalt) yöntemi.

"Bu tertip, normalde, bir grup kişinin bir jeton gibi yeni bir kripto projesini başlatmak için bir araya geldikleri ve ardından o projeyi Twitter veya Discord gibi platformlarda coşturmak amacıyla – genellikle fenomen kişilerin de yardımıyla – çeşitli kaynakları kullandıkları bir sisteme dayanmaktadır," diyor Lawrence. "Şu anda kripto pazarında likiditeden dolayı çok dalgalanma var. Bundan ötürü, çok sayıda insan hepsi bir anda bir şeyi satın almaya çalıştıkları takdirde, bunun fiyatı yükseltmek yönünde piyasaya bir tür şok etkisi yapması doğaldır. Bu olduğunda, o varlıktan ellerinde büyük miktarlarda tutan kötü adamlar aniden devreye girerler, ellerindeki varlıkları büyük bir kârla satarlar, fiyatı keskin bir şekilde düşürürler ve geri kalan tüm yatırımcıları ellerinde aslında hiç değeri bulunmayan varlıklarla baş başa bırakırlar."

Lawrence'a göre, bu durumlarda dikkate alınması gereken tehlike işareti, her şeylerini kaybetmenin de bariz bir olasılık olduğunu potansiyel yatırımcılara gösteren ve bildiren kamusal açıklamaların bulunmamasıdır. Kötü adamlar normalde sosyal medyada ve tartışma panolarında benzer ekran isimleriyle posterlerle yazılmış kuvvetli kopyala-yapıştır mesajlar kullanırlar. Ve bu tertip sona erdiğinde, bu ekran isimleri genellikle ortadan kaybolurlar ve anonimlikleri hiç dokunulmamış kalır.

Bir kripto varlık bağlamında başka suiistimal ve dolandırıcılık örnekleri

Kripto-bazlı suiistimal ve dolandırıcılığın daima bu kadar sofistike ve karmaşık olması da şart değildir. Kripto-bazlı organizasyonlarda, bir kötü adamın sıklıkla ihtiyaç duyduğu tek şey bir anda ortaya çıkabilecek doğru fırsattır. Örneğin, blok zincirin kendisi dijital varlıkları güvenli ve emin bir ortamda tutmasına rağmen, bu güvenliği aşmak ve bir kripto cüzdanını boşaltmak için ihtiyaç duyulan tek şey bir özel anahtardır – bir lokanta peçetesine sığabilen ve herhangi bir kimsenin bulabilmesi için herhangi bir yerde rahatlıkla bırakılabilen bir uzun rakam dizisi.

"Özel anahtarınız sizin kripto para piyasasına giriş için dijital kimliğinizdir ve bu kimliği eline geçiren herhangi bir kimse sizin kripto paralarınızı çalmak veya sahte işlemler yapabilmek için bu kimliği kullanabilir," diyor Lawrence. "Herhangi bir kimse bu kimliğe bir şekilde erişirse ve Bitcoin'lerimin tümünü alır giderse, bu konuda yapabileceğim hiçbir şey yoktur. Paramı geri alamam, suç duyurusu veya şikâyette bulunamam ve buna itiraz edebilecek herhangi bir tüketici koruma dairesi veya düzenleyici otorite de yoktur – kelimenin tam manasıyla o artık gitmiştir."

Kripto pazarı geliştikçe ve olgunlaştıkça, bireysel ve kurumsal anahtarların yanlış kişilerin eline geçmesine karşı alınabilecek koruma önlemlerinde uzmanlaşan kripto güvenlik hizmetleri de ortaya çıkmış ve gelişmiştir, fakat bazı durumlarda bu hizmetlerin uyguladıkları

1 Josh Campbell, "Beware the 'Pig Butchering' Crypto Scam Sweeping Across America," December 26, 2022, https://www.cnn.com/2022/12/26/investing/crypto-scams-fbi-tips/index.html

metodolojiler şaşırtıcı bir şekilde ilkeldir. Lawrence'a göre, bu hizmetlerin bazılarının kullandığı çözüm yolu, anahtarları ıssız dağlarda bulunan kasalarda saklamaktan ibarettir. Bedelini karşılayabilen şirketler için bir güvenlik ağı olarak kripto sigortası da mevcuttur, fakat bu aşamada endüstrinin tamamı kârlılık sorunlarıyla boğuşmakta ve sigortacıları bir yandan yıldan yıla daralmakta olan bir sigorta teminatı sağlarken bir yandan da son derece seçici davranmaya zorlamaktadır.

İngiltere'nin Insurance Times dergisinde yayınlanan bir makalesinde, RPC sigorta grubu ortağı James Wickes, kripto sigorta pazarının zorluklarını ve sorunlarını tartışmaktadır. "Kripto varlık sigortası piyasasında şu anda faaliyet göstermekte olan nispeten az sayıda sigortacı, son iflasın da gösterdiği gibi kripto pazarlarının istikrarsızlığı ve dalgalanmalarından kaynaklanan potansiyel riskleri sınırlandırmak amacıyla poliçe metinlerindeki küçük puntolu yazıları gözden geçirmeye çok istekli görünüyorlar," diyor Wickes. "Bu varlıkların sigorta pazarı henüz emekleme aşamasında ve yeterli sayıda sigortacının mevcut talebi karşılamak için yeterli kapasiteyi sağlamaya hazır olup olmadıkları ve sigorta pazarının geleneksel hırsızlık riskinin ötesine geçen bir sigorta teminatını nasıl sağlayacağı konuları hâlâ belirsizliklerini korumaktadır."[2]

Bununla birlikte, alınan tüm bu önlemlere rağmen, kötü adamların kripto varlıkları ve blok zinciri herhangi bir yerleşik hesabı doğrudan doğruya aşmadan kullanabilecekleri, mikser olarak adlandırılan – tambur olarak da bilinen – belirli bazı araçlar hâlâ mevcuttur. Bir blok zincirin temel özelliklerinden biri de onun şeffaflığıdır; herhangi bir blok zincir kaşifinin içinde, herhangi bir kimse 2009 yılında kripto paranın piyasaya çıkartıldığı günden bu yana gerçekleştirilen tüm blok zincir işlemlerinin kayıtlarını görebilir. Mikserler, kullanıcının bunları hedeflediği alıcılara teslim etmeden önce söz konusu çok sayıda kripto varlıkları karmakarışık etmesine ve böylece, kimin kaç tane varlığı kime gönderdiğini tam ve kesin olarak tespit etmek son derece güç olduğu için ona bir dereceye kadar anonimlik kazandırmasına olanak sağlarlar. Mikser kullanıldığında, bir kaşifin gösterdiği tek şey, hem bir kişinin hem de düzinelerce başka kişilerin bir miksere varlıklar gönderdikleri ve sonra mikserin de bu varlıkları çeşitli başka kişilere çeşitli farklı miktarlarda tekrar gönderdiği olacaktır. Nihai sonuç, aslında, mükemmel tamamlanmış bir kara para aklama sistemini andırmaktadır.

Bu gerçeklerle yüzleşen ve yine de kripto dünyasında varlık göstermeyi tercih eden kuruluşlar, bu aşamada riski hafifletmek söz konusu olduğunda tamamen kendi başlarına ve yalnız olduklarını kabul etmelidirler. Bu, kriptodan kaçınmak gerektiği anlamına gelmez; uyum, sağlam iç kontrol, suiistimal ve sahtecilik tespit ve caydırma çabalarının ve iç denetimin yönetim kurulu düzeyinden aşağıya kadar tüm kripto konuşmalarında açık ve belirgin bir rol oynaması gerektiği anlamına gelir.

2. Isobel Rafferty, "Cryptocurrency Crisis Leading to Insurance Policy Wording Amendments," Insurance Times, 18 Temmuz 2022, https://www.insurancetimes.co.uk/news/cryptocurrency-crisis-leading-to-insurance-policy-wording-amendments/1441786.article.

İç Denetim Nerede Başlayabilir

Regülasyon var, fakat daha fazlası gerekiyor

Yayınlanan kılavuz kaynakları

Daha önce de söylediğimiz gibi, şirketlerin kripto varlıklarla ve onlarla bağlantılı suiistimal ve dolandırıcılık temeline dayanan risklerle ilgili güvenlik ve yönetişim için başvurabilecekleri düzenleyici çerçeveler dar ve kısıtlıdır. Bununla birlikte, finans hizmetleri gibi belirli bazı sektörler dijital varlık korumasını düzenleyen ve çoğu kripto paraya uygulanan doğru ve uygun yönetişim prensiplerini ele alan kaynaklardan da tamamen yoksun değildirler.

Ekim 2022'de, Avrupa Birliği, global düzeyde kripto para pazarlamasının kapsamlı regülasyonunu sağlamak hedefine yönelik ilk teşebbüslerden biri olan ve üzerinde mutabık kalınan The Markets in Crypto-Assets (MiCA) Regulation (Kripto Varlık Pazarları (MiCA) Yönetmeliği) başlıklı yönetmeliği yayınladı, ancak bu yönetmelik 24 farklı dile tercüme edilmesi için Nisan 2023'e kadar masada tutuldu. Resmen benimsenmesi ve uygulamaya konulması halinde, bu yönetmelik:

- Kripto varlığı resmen "dağıtık hesap defteri teknolojisi veya benzeri bir teknoloji kullanılarak elektronik ortamda aktarılabilen ve depolanabilen ve değer veya hakları temsil eden bir dijital işaret" olarak tanımlamaktadır. Ek olarak, kripto varlıklar için dört farklı kategoriden söz etmektedir: varlık-referanslı jetonlar, e-para jetonları, fayda jetonları ve ilk üç kategorinin hiç birisine girmeyen kripto varlıklar için dördüncü kategori;
- Yatırımcılarının kripto varlıklarını kaybettikleri takdirde kripto sağlayıcılarını bu zarardan resmen sorumlu tutmaktadır;
- Kripto varlık piyasalarındaki aktörleri kendi çevre ve iklim ayakizleri hakkında bilgileri açıklamakla yükümlü tutmaktadır;
- Kara para aklamanın önlenmesine dair güncellenmiş mevzuatla örtüşmektedir ve Avrupa Bankacılık Otoritesi'ni (EBA) yönetmeliğe uymayan kripto varlık hizmet sağlayıcılarını içeren bir kamu sicili tutmakla görevlendirmektedir;
- Kripto varlık sağlayıcılarının AB'de faaliyet gösterebilmek için gerekli yetki ve izni almaları gerektiğini öngörmektedir ve
- "Stablecoin" kripto paralara (bir dış referans varlığa bağlanan ve sabitlenen bir kripto para türü) uygulanan ve her stablecoin sahibine ihraççı tarafından herhangi bir zamanda ücretsiz olarak bir alım hakkı teklif edilmesini gerektiren güçlü ve sağlam bir çerçeve getirmektedir.[3]

A.B.D.'de, Federal Merkez Bankası, Federal Mevduat Sigortası Şirketi (FDIC) ve ABD Hazine Bakanlığı Banka Denetim Dairesi'nin (OCC) yayınladıkları bir ortak açıklama, A.B.D. firmalarına "bankacılık kuruluşlarına önerilen ve mevcut kripto varlık faaliyetleri ve işlemleri konusunda sağlam denetleyici istişarelere girmelerinde" yardımcı olacak şekilde tasarlanmış bir kılavuzluk sağlayan çeşitli farklı kaynaklar sunmaktadır."[4] Bu kaynaklar şunları içermektedir:

- OCC Yorumlama Mektubu 1179 "Baş Hukuk Danışmanı'nın (1) bir Bankanın Belirli Kripto Para Faaliyetlerine Girmi Yetkisini ve (2) OCC'nin bir Ulusal Tröst Bankasına Ruhsat Verme Yetkisini Açıklığa Kavuşturan Yorumları."

3.Konsey Genel Sekreterliği, "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)," Avrupa Birliği Konseyi, 5 Ekim 2022, https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf.
4. Federal Rezerv Sistemi Guvernörler Heyeti, Federal Mevduat Sigortası Şirketi ve ABD Hazine Bakanlığı Banka Denetim Dairesi'nin (Office of the Comptroller of the Currency) Bankacılık Kurumlarının Kripto Varlık Risklerine İlişkin Ortak Açıklaması, 3 Ocak 2023, https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf.

- Federal Rezerv (Federal Merkez Bankası) SR 22-6/ CA 22-6: "Federal Merkez Bankasının Denetimindeki Bankacılık Kuruluşlarının Kripto Varlıklarla İlgili Faaliyetlere Girmeleri"
- FDIC FIL-16-2022 "Kriptoyla Bağlantılı Faaliyetlere Giren FDIC Denetimindeki Kuruluşlar için Bildirim ve Denetleme Geribesleme Prosedürleri"

Şu an itibariyle mevcut olan kaynaklar sadece bunlardan ibarettir. FTX'in iflas etmesinin ardından, SEC, şirketlere dijital emtia firmalarıyla olan ilişki ve işlemlerini açıklamaları tavsiyesinde bulunan bir kılavuz da yayınlamıştır.

Eğitimin değeri

Benimsendiğini ve kanunlaştırıldığını varsayarsak, teklif edilen bu AB yönetmeliği 2024 yılında yürürlüğe girecektir, fakat bu yönetmeliğin bu konuda bir son olmayacağı da neredeyse kesindir. Bu mevzuat ve düzenleyici çerçeve aydan aya tamamlanır ve doldurulurken, bir iç denetçinin yapabileceği en değerli şey, bu değişikliklerden haberdar olabilmek ve onlara uyum sağlayabilmek ve bu değişiklikleri yönetim kuruluna ve ilgili diğer paydaşlara açıkça bildirmek için elinden gelen her türlü çabayı göstermektir.

Mevcut ortamda, iç denetçiler, paydaşlara, kripto çalışmalarına uygulanabilecek başka hangi mevzuatın ve yönetmeliklerin de mevcut olduğunu bildirmelidirler. Lawrence'a göre, örneğin, kendi kripto parasını sunan bir şirket, A.B.D. Mali Suçlar İstihbarat ve Engelleme Ağı'na kaydolma şartını getirebilir ve uygulayabilir – mevzuatta kriptodan özel olarak ve açıkça söz edilmediği için kolaylıkla ihmal edilebilecek ve gözardı edilebilecek kritik bir detay. "Şu anda çok büyük belirsizlikler var," diyor Lawrence. "Neyin uygulanabileceği ve neyin uygulanamayacağı hakkında liderlerini bilgilendirmek iç denetçilerin kendi insiyatifindedir."

Yeni teknolojilere odaklanmak da, şirketleri bir sanal özel ağın (VPN) ve doğru güvenlik tedbirlerinin kullanılması ve başta tüketiciler olmak üzere kullanıcılara ait profil bilgilerinin toplanması ve gerektiğinde elden çıkartılması da dâhil olmak üzere dijital varlık koruma konusunda temel en iyi uygulamaları uygulamaktan uzaklaştırmamalı ve dikkatlerini dağıtmamalıdır. "Kullanıcı profilleri kritik önemi haiz bir örgütsel kontroldür," diyor Miranda. "Ben bir şirketi denetliyor olsaydım, kullanıcı profillerinin işlem faaliyetleriyle eşleşip eşleşmediklerinden emin olmak isterdim. Örneğin, uyum ve soruşturmalarda coğrafi bilgiler inanılmaz ölçüde önemlidirler. Kurumların hem bu bilgileri güvende ve emniyette tutmaları, hem de nerede bulunduklarını çok iyi bilmeleri gerekir." Bu noktada, Miranda, kurumların sıklıkla bir suiistimal ve dolandırıcılık soruşturmasında kritik önemde olabilecek fiziksel adresler gibi kritik profil bilgilerini içeren gizlilik ve ifşa yasağı sözleşmelerini (NDA) gözden kaçırdıklarını söylemektedir.

Bu konuda daha fazla bilgi almak isterseniz, IIA'nın "İç Denetim ve Suiistimal: Suiistimal Riski Yönetişiminin Değerlendirilmesi" başlıklı Ek Kılavuzu, hem sağlam suiistimal riski yönetişim ve yönetimi için örgütsel roller ve sorumluluklar hakkında açık önermelerde bulunmakta hem de COSO'nun Suiistimal Riski Yönetim Kılavuzu gibi ek kılavuzlarla ilgili tavsiyeler vermektedir.

Sonuç

İç denetim hazırdır

Kripto para ve onun dayandığı teknoloji, yönetim kurulunun dikkat ve ilgisini göründüğünden daha fazla hak eden özellikleriyle, iç denetimin gözardı edemeyeceği kadar çok devrimci ve önemlidirler. Bunu ihmal eden risk değerlendirmelerinde kritik önemi haiz bir kör nokta vardır. Kripto para, pek çoğu için nispeten yeni bir kavram olabilir, fakat bu, iç denetimin ölçebileceği ve test edebileceği sağlam bir suiistimal riski yönetim çerçevesinin değerini ve önemini azaltmaz.

İç denetimin her gün büyüyen radarına eklenen başka bir risk alanından da şikâyet etmek ve sızlanmak kolay olmasına rağmen, başka herhangi bir örgütsel departmanın tüm bu sorunların çözümlenmesi için daha iyi bir konumda olmadığını bilmek aslında bir iyi haberdir. Aynen 2002 yılında Sarbanes-Oxley Kanunu'nun (SOX) yaptığı gibi, kripto para yönetmeliğinin çıkartılması iç denetimin önümüzdeki yıllar boyunca masada çok değerli bir pozisyonda olacağını güvence altına almaktadır. Bu departman henüz kriptoyu tam anlamıyla bilmemesine rağmen, suiistimal ve dolandırıcılığı ve aynı zamanda riski de bilmektedir ve bu bile, iç denetimin önümüzdeki sorunların çözümünde liderlik pozisyonunu üstlenmesi için tek başına yeterlidir.

Bölüm 2

İç Denetçiler ve Suiistimal İnceleme Uzmanları: Değerli Bir Ortaklık

Uzmanlar Hakkında

Mason Wilder, CFE

Mason Wilder, bir Suiistimal İnceleme Uzmanıdır ve ACFE'de araştırma müdürü olarak görev yapmaktadır. Bu görevinde, sürekli mesleki eğitim için ACFE materyallerinin hazırlanması ve güncellenmesini denetlemekte, tüm ACFE eğitim etkinliklerinin planlanması ve uygulanmasına yardımcı olmakta, Uluslara Rapor ve karşılaştırmalı değerlendirme raporları gibi araştırma insiyatifleri üzerinde çalışmakta, eğitimler vermekte, ACFE yayınları için makale ve yazılar kaleme almakta ve üyelerin ve medyanın soru ve taleplerine cevap vermektedir. ACFE'ye katılmadan önce, Wilder, on yıldan uzun bir süreyle kurumsal güvenlik istihbarat ve soruşturmaları konusunda çalışmış ve uluslararası fiziksel güvenlik ve kriz cevabı için özgeçmiş ve ayrıntılı teknik inceleme ve soruşturmalarda ve istihbarat analizi konusunda uzmanlaşmıştır. Mason, kritik karar alma sürecine destek olmak amacıyla analiz etmek ve çözümlemek için tüm kaynaklardan önemli bilgilerin toplanması üzerine bir kariyer inşa etmiştir ve suiistimal ve dolandırıcılıkla etkin mücadele etme imkân ve kabiliyetlerini geliştirmeleri konusunda suiistimal ve dolandırıcılıkla mücadele uzmanları ve profesyonellerine yardımcı olmayı arzu etmektedir.

Shawna Flanders, CRISC, CISA, CISM, SSGB, SSBB

Uluslararası İç Denetçiler Enstitüsü'nde (IIA) ürün geliştirme direktörü olan Shawna Flanders, teknik konuşmaları ve görüşmeleri ortak iş diline uyarlama konusuna odaklanan tutkulu bir teknolojist ve teknik eğitim sektörü uzmanı ve profesyonelidir. Shawna, SME İçerek Geliştirme / Katkı, Konuşma / Eğitim, BT İlişkili Riskler, BT Denetim, Bilgi ve Siber Güvenlik, BT Uyum, BT Yönetişim, Tedarikçi Yönetimi, Telekomünikasyonda BT Yönetmeni, Programlama, Ses ve Veriyle İlişkili Mimari Tasarımı / İncelemesi, Mühendislik, Analitik ve Entegrasyon Yönetimi, İş Süreci Yönetimi, İş Analizi, Proje Yönetimi, Program Yönetimi ve Süreç İyileştirme / Six Sigma da dâhil her görev için gereken becerilerin kendine özgü bir tamamlayıcı kombinasyonunu sunmaktadır.

Giriş

İç denetçiler, suiistimallerin tespit edilmesi ve etkilerinin hafifletilmesi de dâhil olmak üzere risklerin yönetimi konusunda kurumlara yardımcı olan yönetişim, riskler ve iç kontroller hakkında **yapıcı anlayışlar sağlarlar.** Bununla birlikte, iç denetim departmanı suiistimallerin tespit edilmesi ve caydırılması sürecinin etkin bir parçası olmasına rağmen, suiistimalleri tespit etmek ve bulmak bir iç denetçinin görevi değildir. Öte yandan, Suiistimal İnceleme Uzmanı (CFE), özellikle suiistimallerin tespit edilmesi ve soruşturulmasıyla görevlidir. CFE, suiistimallere karşı verilen savaşa belirli uzmanlık becerilerini getirir. Sonuçta, bu iki tip uzmanın kurumun en iyi menfaatlerine hizmet eden bir ortaklık içinde işbirliği yapmaları mantıklı ve anlamlı olur.

Suiistimallerle ilgili üç bölümden oluşan bir dizinin ikincisi olan bu Global Bilgi Brifingi, iç denetçiler ile CFE'ler arasında simbiyotik bir ilişki kurmanın ne gibi faydalar sağlayacağını incelemektedir.

Suiistimallerin Kapsamı

Ortalama kayıp ve zarar tutarı yaklaşık 1,8 milyon $

Suiistimal, yaygın ve bulaşıcı bir risk olma özelliğini korumaktadır

Suiistimal, mali veya başka bir kişisel kazanç ve menfaat için yapılan ve aldatma, bilgi gizleme ve emniyeti suiistimal **fiillerini kapsayan bir yasadışı suç fiilidir.** Suiistimalde bulunan insan veya kuruluşlar, başkalarına ait para, mal veya hizmetleri çalmayı; bir şeyin bedelini ödemekten veya onu kaybetmekten kaçınmayı ya da kişisel veya ticari bir menfaat elde etmeyi amaçlıyor olabilirler. Dış dolandırıcı ve sahtekârlara ek olarak, suiistimal fiilleri, çalıştıkları kurumun kendilerine adil davranmadığına inandıkları için ya da başka herhangi bir kinleri sebebiyle aldıkları paranın veya hizmetlerin aslında hakları olduğunu ya da kurumun bu parayı onlara borçlu olduğunu hisseden ya da mali açıdan baskı altında olan şirket çalışanları tarafından da yapılabilir. Her tipte kurum veya şirket, boyutuna bakılmaksızın ya da ister kamu kurumu ister özel kurum, kâr amacı gütmeyen bir kuruluş, devlet kurumu, kamu veya özel hizmet kuruluşları veya başka tüzel kişiler olsunlar, bir suiistimal fiilinin kurbanı olabilirler.

Suiistimal, kuruluşlar için çok ciddi, yaygın ve bulaşıcı bir risktir. Suiistimalin neticeleri yıkıcı etkilerden vahim etkilere kadar farklılık gösterebilir. Bu etkiler, sadece mali zorlukları ve kayıpları değil, aynı zamanda, faaliyetlere, gelirlere veya kârlara zarar veren verimsizlikleri, projelerin iptal edilmesini ve kapsama alanlarına bağlı olarak, ilgili kuruluşun iflas etmesini bile kapsayabilirler.[5]

Suiistimal İnceleme Uzmanları Birliği (ACFE) tarafından dünya çapında yapılan bir CFE (Suiistimal İnceleme Uzmanı) araştırması, 133 ülkeden toplam 2.110 suiistimal vakasını kapsıyordu. Bu grup içinde, suiistimalden kaynaklanan global zarar ve kayıpların toplamı 3,6 milyar $'ın üzerindeydi ve vaka başına zarar ve kayıp ortalaması yaklaşık olarak 1.8 milyon $'dı. Aslında, CFE'ler, kuruluşların her yıl toplam gelirlerinin %5'ini suiistimaller sebebiyle kaybettikleri tahmin etmektedirler. Daha küçük şirketlerin suiistimalle ilgili en büyük risk altındaki grup oldukları da açıktır: En az sayıda çalışana sahip olan şirketler 150.000 $ tutarındaki en yüksek ortanca kaybı yaşamışlardır.

Bu büyüklükteki kayıp ve zararları tespit etmek kolay olabilir, ancak suiistimaller sıklıkla zaman içerisinde küçük miktarlarda artışlarla devam eden bir seyir izlemektedirler. Araştırma sonuçlarına göre, tipik bir suiistimal tertibi, ayda 8.300 $ zarara sebep olabilir ve tespit edilmesi 12 ay alabilir. Bazı suiistimallerde kripto paranın yer aldığının farkında olmak da önemlidir. ACFE, kripto paraların toplam vakaların %8'inde yer aldıklarını tespit etmiştir. Olağan senaryolar, rüşvet ve avanta ödemelerinin yapılmasını ve zimmete geçirilmiş mal ve varlıkların nakde dönüştürülmesini içermektedir.[6]

[5] [5] IIA Görüş Açıklaması, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019.
[6] *Occupational Fraud 2022: A Report to the Nations*, Suiistimal İnceleme Uzmanları Birliği.

Kaynak: *Occupational Fraud 2022: A Report to the Nations*, Suiistimal İnceleme Uzmanları Birliği.

Mesleki Suiistimal Kategorileri

ACFE 2022 Uluslara Raporuna göre, mesleki suiistimallerin üç temel kategorisi bulunmaktadır.

Mali tablolarda yapılan ya da kurumun mali tablolarında önemli bir gerçek dışı beyana veya önemli bir bilginin gizlenmesine sebep olan **suiistimal tertipleri**, en az görülen (%9), fakat vaka başına 593.000 $ ile en pahalı olan kategoriyi oluşturmaktadır.

Bir personelin şirket kaynaklarını çaldığı veya kötüye kullandığı **mal ve varlıkları zimmete geçirme** fiili vakaların %86'sında görülen bir fiildir. Buna rağmen, bu fiil, vaka başına 100.000 $ ile en düşük ortanca zarar ve kayıptan sorumludur.

Rüşveti, menfaat çatışmalarını ve irtikap fiillerini içeren **yolsuzluklar,** vakaların %50'sinde görülmektedir ve vaka başına 150.000 $ tutarında zarar ve kayba yol açmışlardır.

İç Denetçinin Rolü

Suiistimallerin önlenmesine dair güvence/tavsiye hizmetleri

Suiistimallerin tespit edilmesi/caydırılması: iç denetimin temel görevi

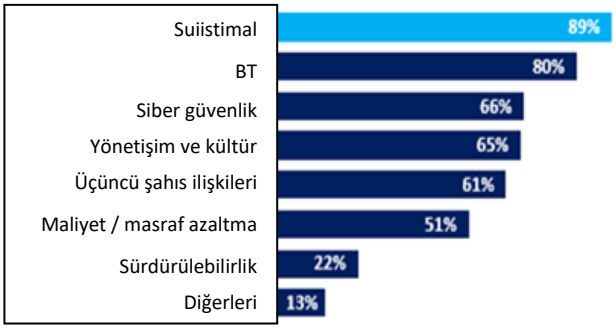
Uluslararası İç Denetçiler Enstitüsü'ne (IIA) göre, "iç denetim, bir kurumun faaliyetlerine değer katmak ve onları geliştirmek amacıyla tasarlanmış bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. İç denetimin rolü; suiistimal risklerinin tespit edilmesi, önlenmesi ve izlenmesini ve bu risklerin denetim ve soruşturmalarda ele alınmasını ve irdelenmesini de içerir."[7]

Kurumlar, iç denetimin beceri setinin suiistimal soruşturmalarını da içermesini beklememelidirler. Koşullar iç denetim biriminin bir soruşturma görevini üstlenmesini gerektirdiği takdirde, iç denetçiler gereken mesleki özeni göstermeli ve soruşturma için gereksinim duyulan uzmanlığa ve deneyime sahip değillerse soruşturma yapmamalıdırlar.

Suiistimallerin önlenmesi yönetimin görevi olmasına rağmen, iç denetim de suiistimalleri tespit edecek ve caydıracak şekilde tasarlanmış iç kontroller yoluyla gereken güvence hizmetlerini vermek suretiyle yönetimin suiistimallere karşı gösterdiği çabalara destek olur. Suiistimaller sıklıkla kurumun yönetim süreçlerini baltalayan zayıf yönetişimden ve kötü tasarlanmış kontrollerden dolayı meydana gelmektedir. ACFE araştırmasındaki vakaların yaklaşık olarak yarısı iç kontrollerin bulunmamasına (%29) ya da mevcut kontrollerin etkisiz hale getirilmesine (%20) bağlanmıştır. Denetçiler, inceledikleri alanlarda suiistimal riski potansiyelini ve iç kontrollerin yeterli olup olmadığını inceler ve değerlendirirler. Araştırmaya göre, suiistimallere karşı kontrollerin mevcut olduğu yerlerde, daha az suiistimal zararı ve kaybı olmakta ve suiistimaller daha çabuk tespit edilebilmektedir.

İç denetimin suiistimalleri önleme çabalarına yapabileceği katkılar küçümsenmemelidir. IIA, iç denetim yöneticilerine iç denetim birimleri ve fonksiyonlarının hangi konularda önemli katkılarda bulunduğunu sorduğunda, aldığı yanıtların %57'sinde suiistimallere, %56'sında ise genel risk değerlendirmesine atıf yapılmıştır.[8] Bu arada, ACFE araştırmasında herhangi bir iç denetim departmanı bulunmayan kurumlarda ortanca suiistimal zararının %50 oranında daha yüksek (100.000 $'a karşı 150.000 $) olduğu tespit edilmiştir.

Gerçekten de, gelecek 2023 Kuzey Amerika İç Denetimin Nabzı raporundaki veriler, suiistimalin iç denetimlerde dikkate alınan mülahazalar arasında en çok atıf yapılan alan olduğuna işaret etmektedir. Kuzey Amerikalı iç denetim yöneticileri yıllık anketi, 500'den fazla katılımcıdan, genel olarak hangi alanları denetim çalışmalarına aldıklarını sormaktadır. Mart ayında 2023 GAM Konferansında açıklanacak olan rapora göre: "Yanıtlar, denetçilerin sıklıkla bütüncül bir yaklaşım benimsediklerini ve siber güvenlik, üçüncü şahıslar ve yönetişim de dâhil pek çok konuyu dikkate aldıklarını göstermektedir. Bir bütün olarak, CAE'lerin %89'u, genelde her denetime en sık atıf yapılan risk kategorisi olan suiistimalle ilgili mülahazaları dâhil ettiklerini ve BT mülahazalarının da %80 ile ikinci sırada geldiğini ifade etmektedirler.



Kaynak: 2023 Kuzey Amerika İç Denetimin Nabzı raporu

IIA'nın Kuzey Amerika İç Denetimin Nabzı Araştırması, 20 Ekim – 2 Aralık 2022. Q25: Genel olarak denetim görevleri yürüttüğünüz zaman, aşağıda sayılan alanların hangilerini genellikle mülahazalarına dâhil ediyorsunuz? (Dikkate aldığınız alanların tümünü seçin.) n = 555.

[7] IIA Görüş Açıklaması, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019.
[8] 2022 Premier Global Araştırma, *Internal Audit: A Global View*, İç Denetim Vakfı, 2022.

IIA'nın *Fraud and Internal Audit: Assurance Over Fraud Controls Fundamental to Success*[9] (Suiistimal ve İç Denetim: Suiistimal Kontrollerine İlişkin Güvence Başarının Temelidir) başlıklı Görüş Açıklamasına göre, iç denetimin:

- Bir suiistimal yapıldığını gösterebilecek tehlike işaretlerini tespit edebilmek;
- Suistimalin ve suiistimalde bulunmak için kullanılan tekniklerin özelliklerini ve suiistimal tertipleri ve senaryolarının tiplerini anlayabilmek;
- Herhangi bir ek tedbire ve eyleme ihtiyaç olup olmadığına ya da bir soruşturma yapılmasının tavsiye edilmesine gerek olup olmadığına karar verebilmek ve
- Suiistimalleri önlemek veya tespit etmek ve gelişme ve ilerleme fırsatlarını yakalayabilmek için kullanılan kontrollerin etkinliğini kontrol edebilmek

için gereken suiistimal bilgisine sahip olması gerekir.

[9] IIA Görüş Açıklaması, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019

Suiistimal İnceleme Uzmanının Rolü

Aldatma eylemlerini soruşturmak

Gerekli yeteneklere dayanan suiistimal soruşturması kritik önemdedir

Suiistimal inceleme uzmanı, kurumun genel suiistimal inceleme ve soruşturma programlarına **katılır ve destek olur.** Uzmanlar, bu görevi, kısmen, "ne olduğunun ve kimin sorumlu olduğunun tespit edilmesine yardımcı olan maddi olguları ve kanıtları bulmaya çalışan ve gerektiğinde tavsiyelerde bulunan" suiistimal soruşturmaları yaparak ifa ederler."[10] Bir suiistimal inceleme uzmanının bir soruşturmaya başlarken değerlendirdiği konulardan biri de *dayandırmaktır*; yani, bir bütün olarak mevcut koşullar ve kanıtlar, bir suiistimal fiilinin yapıldığı iddiasının iyi eğitilmiş bir uzmana makul gözükmesini temin etmelidir.

Bir suiistimal inceleme uzmanının bir soruşturmada attığı adımlar, gerekli kanıtların toplanmasını, bulguların rapor edilmesini, gerekiyorsa bu bulguların ispatlanmasını ve doğrulanmasını ve suiistimallerin tespiti ve önlenmesi konusunda gerekli yardımların yapılmasını içerebilir. Bir suiistimal incelemesinin iki yaygın amacı, bir potansiyel suiistimalin veya suiistimal iddiasının araştırılması ve bir kurumun suiistimallere karşı uyguladığı politikaların ve kontrollerin incelenmesidir. Bir suiistimal incelemesinin arkasındaki daha spesifik ve özel amaçlar ise şunları içerebilir:

- Suiistimalle ilişkilendirilen veya ilişkilendirilebilecek uygunsuz davranışları tespit etmek ve aynı zamanda bu uygunsuz davranıştan kimin sorumlu olduğunu da ortaya çıkartmak;
- Suiistimalden kaynaklanan veya kaynaklanabilecek kayıp ve zararları veya sorumlulukları tespit etmek;
- Kurumun suiistimalleri tespit etme ve hafifletme taahhüdünü ve sözünü göstermek;
- Zararın telafisinin kolaylaştırılmasına yardımcı olmak;
- Gelecekteki olası suiistimalleri ve bunlara bağlı zararları veya sorumlulukları önlemek;
- Mali zararların dışındaki olumsuz neticeleri de tanımlamak;
- İç kontrollerdeki zayıf noktaları bulmak ve gerekli güçlendirme işlerini yapmak ve
- Bazı durumlarda gerekli olduğu zaman, kanunlara, yönetmeliklere, sözleşmelere veya örf ve adet hukukundan doğan görevleri yerine getirmek ve yükümlülüklere uymak.[11]

[10] "Planning and Conducting a Fraud Examination," *Suiistimal İnceleme Uzmanları Elkitabı: 2022 Baskısı*, ACFE.
[11] A.g.e.

Yaklaşımları karşılaştırmak

Bu tablo, iç denetçiler ve CFE'lerin rolleri, yaklaşımları ve amazları arasındaki bazı önemli farklara bir genel bakış sunmaktadır.

Özellikler	**İç Denetim**	**Suiistimal İncelemesi**
Amaç	İç denetim prosedürleri suiistimalleri ortaya çıkartabilir, fakat suiistimallerin ortaya çıkartılacağını garanti etmez. Örneğin denetçiler bir incelemede şüpheli bir işlem veya durum görebilirler ve bu işlem veya durumun bir suiistimal olduğu daha sonra tespit edilebilir. Buna rağmen, suiistimalleri bulmak, ancak ve sadece, denetim altındaki alanda yapılan daha büyük bir kontroller ve prosedürler incelemesinin neticelerinden biri olabilir.	Bir suiistimal incelemesi, doğrudan doğruya suiistimallerin ortaya çıkartılması ve suiistimallere karşı yapılacak eylemler veya faaliyetlerin tespit edilmesi üzerine odaklanır.
Sıklık	Denetimler normalde düzenli olarak tekrarlanırlar; ancak buna rağmen, herhangi bir belirli alanda özgün bir durumu veya sorunu ele almak için bir seferlik denetimler de yapılabilir.	Suiistimal incelemeleri normalde sadece yeterli dayanak olduğunda yapılırlar; ancak buna rağmen risk yönetimi veya suiistimal risk değerlendirme programının bir parçası olarak ve herhangi bir özel tetikleyiciye ihtiyaç olmadan da yapılabilirler. Bununla birlikte, suiistimal incelemelerini çoğu belli bir ipucu veya iddia üzerine yapılır. ACFE araştırmasında, suiistimallerin %43'ünün ipuçlarına dayanılarak tespit edildiği gösterilmiştir; bu oran, suiistimallerin tespit edilmesindeki ikinci en yaygın yöntemin oranının neredeyse üç katıdır. Tüm suiistimal ipuçlarının yarısından fazlası çalışanlardan gelmiştir.
Hasımlı mı, değil mi?	İç denetimler niteliği gereği hasımsız işlemlerdir. Denetçilerin amacı, örneğin takım liderleri ve üyelerinin kontrolleri veya diğer süreçleri geliştirmek için kullanabilecekleri bilgileri ve anlayışları sağlamaktır.	Suiistimal incelemeleri doğası gereği hasımlı incelemelerdir. Amaç, kısmen, suiistimallerden kimin sorumlu olduğunu ve kimin suçlanabileceğini tespit etmektir.
Standartlar	İç denetçiler, Uluslararası İç Denetçiler Enstitüsü'nün (IIA) yayınladığı *International Standards for the Professional Practice of Internal Auditing*'i (İç Denetim Mesleki Uygulamaları İçin Uluslararası Standartlar) izler ve uygularlar.	CFE'ler ise *Code of Professional Standards*'ı (Mesleki Standartlar Kodu) izler ve uygularlar. CFE'ler incelemelerinde bir ACFE fraud risk assessment tool'u (suiistimal risk değerlendirme aracı) kullanabilirler.

İşte İşbirliğini Kullanmak

Karşılıklı Saygı ve Sorumluluklar

Suiistimale karşı savaş

Denetçiler ile suiistimal inceleme uzmanları arasında kurulabilecek **faydalı işbirliğine yönelik çok fırsatlar vardır.** Bu kişiler aşağıda sayılan konularda birbirlerine danışabilirler:

- Bir suiistimal incelemesi başlatmak;
- Denetimler ve suiistimal incelemeleri yıllık planlaması;
- Risk değerlendirmeleri;
- Kontrollerin ve suiistimal karşıtı programların incelenmesi ve değerlendirilmesi;
- Suiistimal çıkarımları yapılan denetim bulgularının iletilmesi ve
- Kontrol eksiklikleri ve zayıflıklarının onarılması

Pek çok kurumun iç denetim birimi bir suiistimal bulgusunu dış veya iç suiistimal inceleme ekibine bildirdiğinde uygulanacak protokolleri düzenleyen kuralları vardır. İç denetim ekibi bir suiistimal bulgusunu not eder ve ardından, incelemenin sonunda ilgili suiistimal inceleme uzmanıyla birlikte bir ortak rapor yayınlar.

Ek olarak, iç denetim, kontrollerinin yeterli olduğundan emin olmak için bir kurumun suiistimalle mücadele departmanını da denetleyebilir. Bir suiistimalle mücadele ekibi, hiyerarşik olarak, diğer alanların yanı sıra iç denetim de dâhil kanuni risk veya kurumsal risk yönetim ekiplerine bağlı olabilir. Bir suiistimal ekibinin iç denetime bağlı olması halinde, objektifliği garanti etmek için o departmanın her türlü denetiminde dış kaynakların kullanılması gerekir.

İşte işbirliğini gösteren vaka etüdü

Aşağıdaki vaka etüdü, iki ekibin nasıl birlikte çalışabileceklerini göstermektedir. Bu vaka etüdü, *İşbirliğini Teşvik Etmek: Denetçi ve Suiistimal İnceleme Uzmanı* başlıklı yeni yapılan bir IIA ve ACFE webinarında IIA ürün geliştirme direktörü Shawna Flanders, CRISC, CISA, CISM, SSGB, SSBB, tarafından gündeme getirilen bir tartışmaya dayanmaktadır.

Normalde, iç denetim, suiistimali akla getiren ve suiistimal inceleme uzmanlarını alarma geçiren bir işlem dizisi tespit eder. Flanders tarafından sunulan vakada, iç denetim görevi otomobil kredilerine yönelik bir incelemeyi de içeriyordu. Denetim ekibinin yaptığı işlerden biri de gecikmiş borç ödemelerini değerlendirmekti. Bu tip 40 hesaptan oluşan bir grupta beş tanesi öne çıkıyordu. Sistem, takip edilmesi gereken gecikmiş borç ödemelerini gösterecek şekilde kurgulanmıştı, fakat bir sebeple bu beş hesap için hiç alarm verilmemişti. Ek olarak, bu hesapların tümü çok olağandışı özelliklere sahipti: %0 faiz oranı, 72 ay vade ve sıfır asgari ödeme.

Flanders konuyu araştırdığında, kredilerle bağlantılı kullanıcı kimliğinin bir müşteri hizmetleri temsilcisine ait olduğunu tespit etti, fakat bu çok anlamsızdı, çünkü bu görevdeki bir kimse genellikle kredileri onaylamıyordu. Bunun üzerine, kredilerle ilgili dosyaları gözden geçirdi ve bunların her birinin sunulması ve onaylanmasından yaklaşık bir saat önce, kullanıcı kimliği sahibine sisteme ek erişim hakkı verildiğini gördü. Bu erişim hakkı, krediler onaylandıktan ve aktive edildikten yaklaşık bir saat sonra kaldırılmıştı. Olağandışı kredi koşullarını, müşteri hizmetleri temsilcisinin devreye girmesini ve sisteme erişim değişikliklerini göz önüne alarak, denetim ekibi, dosyanın şirketin suiistimal departmanına gönderilmesi gerektiğine karar verdi.

Kurumun politikaları ve prosedürlerine bağlı olarak, suiistimal departmanının bir şüpheli işlem alarmı aldıktan sonra bu vakada atabileceği adımlar şunları içermektedir:

- Denetçilerden aldığı bilgilerin doğru olup olmadığını tespit etmek;
- Bu hesaplarla bağlantılı işlem ve faaliyetlerin tamamını incelemek;
- Bu beş hesabın açılmasının bağımsız bir işlem mi yoksa devam eden bir potansiyel tertibin bir parçası mı olduğunu tespit etmek;
- Varsa, suç ortaklarını ortaya çıkartmak ve
- Başka şubeler veya ofislerin de suça katılıp katılmadığını ve suiistimalin genel kapsamını tespit etmek.

Bu noktada, suiistimal inceleme uzmanları, suiistimalin durdurulması gerekip gerekmediğini ve nasıl durdurulması gerektiğini de değerlendirebilirler. Daha fazla bilgiye veya kanıta ihtiyaç varsa, suiistimalin en azından geçici olarak bir süre daha devam etmesine izin verilmesine karar verilebilir. ACFE'de araştırma müdürü olan ve webinara katılan Mason Wilder, CFE'ye göre, bu karar, şirketin o ana kadar ne kadar kaybının olduğuna, suiistimalin devam etmesi halinde şirketin ne kadar daha kaybetme potansiyelinin bulunduğuna ve kurumun risk iştahına bağlı olarak yapılabilecek karmaşık bir tespite dayanır. Bu vakada, suiistimali sona erdirmeden önce atılabilecek adımlar, daha fazla bilgi almak için müşteri hizmetleri temsilcisiyle görüşmeyi ve suiistimalin genel kapsamını tespit etmeyi ve varsa, başka ek suiistimalleri veya yeni planları da ortaya çıkartmayı içerebilir.

Gerekli kanıtları topladıktan ve analiz ettikten sonra, suiistimal inceleme uzmanları bulgularını kurum içindeki uygun kişilere yazılı veya sözlü olarak rapor ederler. Bu uygun kişiler arasında yönetim, yönetim kurulu veya denetim komitesi de bulunabilir. *ACFE Suiistimal İnceleme Uzmanları Elkitabına* göre "Bir suiistimal inceleme raporu, suiistimal inceleme uzmanının spesifik faaliyetleri, bulguları ve uygunsa tavsiyelerini içerir." Bunun üzerine, kurum yönetimi bu raporu gereken uygun gelecek adımları tespit etmek için kullanabilir.

Suiistimal inceleme uzmanları durumu inceler ve herhangi bir suiistimal bulunmadığına karar verirlerse, ilk tehlike işaretinin suiistimal riski yönetim kontrollerindeki bir eksiklikten dolayı verildiğini tespit etmeleri halinde dosyayı geri gönderebilirler. Bunun üzerine, iç denetim bu eksikliği de raporuna dâhil edebilir.

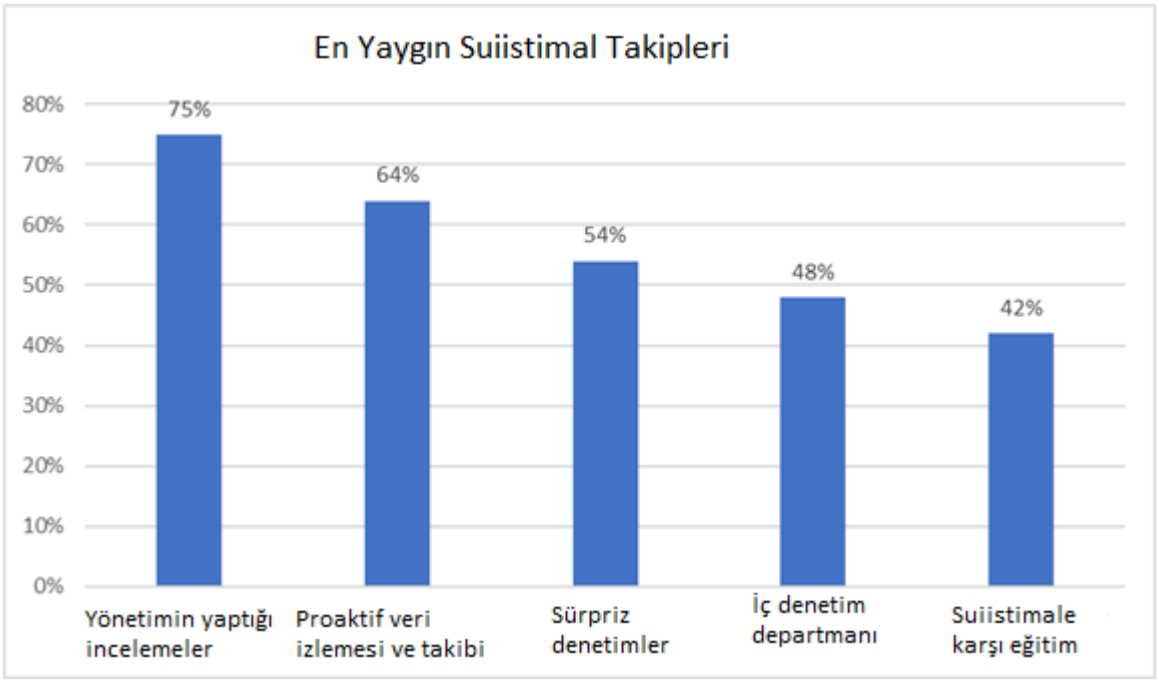
Güçleri birleştirmek

Suiistimalle ilgili kişiler, riski azaltmanın önemli olduğunu unutmamalıdırlar. ACFE araştırma raporunda, suiistimalleri bulmak amacına yönelik proaktif adımların daha erken tespite olanak sağlayabileceği ve zararları azaltabileceği, reaktif çabaların ise tertiplerin daha uzun bir süre devam etmesine yol açabileceği ve kurbanın maruz kaldığı mali etkileri artırabileceği not edilmektedir.

Bununla birlikte, kurumlar mevcut tüm suiistimal risklerini tespit edemez veya ortadan kaldıramazlar. Kurumlar, çeşitli farklı suiistimal tipleriyle, bunların arkasında çeşitli farklı motivasyonlarla ve çok çeşitli ve farklı faillerle karşılaşabilirler. Buna rağmen, tüm kademelerde – yönetim, yönetim kurulu ve personel – kişiler ne kadar bilgiliyse, bu kişiler makul risk azaltma çabalarını yürütmekte ve suiistimalleri veya bunların varlığını gösterebilen tehlike işaretlerini tespit etmekte o kadar daha iyi olurlar. Kendi özgün beceri ve tecrübelerini birleştirerek, iç denetçiler ve suiistimal inceleme uzmanları kurumun bu yöndeki genel çabalarına güçlü bir katkıda bulunabilirler. Kurumlar, onların çalışmalarını, suiistimal riski yönetim yaklaşımları hakkında daha çok bilgiye dayanan kararlar almak için kullanabilirler.

Suiistimallerin tekrarını önlemek için adımlar

ACFE araştırmasına katılan kurumların toplam olarak %81'i, bir suiistimalden sonra suiistimalle ilgili kontrollerinde bazı değişiklikler yaptılar. Aşağıdaki şema, kurumların kontrollerde yaptıkları veya uyguladıkları en tipik değişiklikleri göstermektedir. ACFE'nin tavsiye ettiği diğer suiistimalle mücadele kontrolleri arasında otomatik işlem/veri izleme, gözetim ve hesap mutabakatları bulunmaktadır.



Kaynak: ***Occupational Fraud 2022: A Report to the Nations*****, Suiistimal İnceleme Uzmanları Birliği.**

Sonuç

Yönetişim, risk ve iç kontrol konularında **üçüncü sıradaki güvence sağlayıcı olarak iç denetimin rolü,** objektif ve bağımsız güvenceyi sağlayan yapılar, süreçler ve uygulamaların kullanılmasını gerektirir. Fakat IIA'nın Üç Hat Modelinde belirtildiği gibi bu bağımsızlık izolasyon ve tecrit demek değildir.

Modele göre, "İç denetimin çalışmasının anlamlı olmasını ve kurumun stratejik ve operasyonel gereksinimlerine uyumlu olmasını sağlamak için iç denetim ile yönetim arasında düzenli etkileşim bulunmalıdır. Tüm faaliyet ve işleri yoluyla, iç denetim, kurum hakkında bir bilgi birikimi inşa eder ve bu da, iç denetimin güvenilir bir danışman ve stratejik ortak olarak verdiği güvence ve tavsiyelere katkıda bulunur."

Bu, açıkça, iç denetimin ve suiistimal inceleme uzmanlarının suiistimale karşı savaşta müttefikler olarak ortak bir zeminde buluştukları yerdir.

Bölüm 3

Hangover: COVID Sonrası Dönemde Suiistimal

Uzman Hakkında

David Dominguez, CIA, CRMA, CPA, CFE

David, Houston'da Itafos'da denetim ve uyum direktörüdür. David, çeşitli farklı sektörlerdeki çokuluslu şirketlerde kurumsal ve bölgesel iç denetim birimlerini kurma, yönetme ve dönüştürme görevlerini üstlenmiştir. David; Kuzey Amerika, Güney Amerika, Avrupa ve Asya'da finansal, operasyonel ve BT güvence ve danışmanlık projelerini yönetmiş ve hayata geçirmiştir. Birden fazla ülkeyi kapsayan çok sayıda çeşitli soruşturmalara, veri analiz inisiyatiflerine ve çok çeşitli uluslararası hissedar, ortak girişim ve tedarikçi denetimlerine de katılmış ve bunları yönetmiştir. Uzmanlık alanları arasında kurumsal ve örgütsel yönetişim, kurumsal risk yönetimi, suiistimal riski yönetimi, Sarbanes-Oxley Kanunu 2002 ve etik ve uyum programları da bulunmaktadır.

Giriş

Devam ettiği iki yıllık sürenin büyük çoğunda, COVID-19 pandemisi, insanların çalışma yöntemleri ve tarzları, nerede çalıştıkları, kurumlarının tedarikçilerle ve arz zinciri sorunlarıyla nasıl baş ettiği ve iç kontrollerin sürdürülmesi ve suiistimallerin tespit edilmesi ve önlenmesi gibi önemli kaygı ve endişelerle nasıl başa çıktıkları gibi herkesi ilgilendiren pek çok konuda karışıklıklara ve bozulmalara sebep olmuştur.

Bugün, dünya daha rahat nefes almaktadır, çünkü pandeminin en kötüsü artık yavaş yavaş tarihe karışmaktadır, fakat yine de, COVID-19 ile bağlantılı risklerin artık bir sorun olmadığının kesinlikle düşünülmemesi gerekir. Aslında, böyle düşünen ve bu varsayımı yapan kurumlar çok büyük bir hata yapıyor olabilirler. Uluslararası İç Denetçiler Enstitüsü'nün (IIA) suiistimallerle ilgili üç bölümden oluşan bir dizisinin üçüncüsü olan bu Global Bilgi Brifingi, *2022 ACFE Uluslara Raporda* tespit edilen pandemiyle ilişkili çeşitli farklı suiistimal faktörlerini ve bunların kurumlara nasıl etki ettiklerini ve bu suiistimal riski faktörlerinin etkisini azaltmaya yönelik kurumsal çabalarda iç denetimin oynadığı rolü incelemektedir.

Suiistimaller ve Suiistimal Riskleri Devam Ediyor

Pandemiyle bağlantılı değişiklikler de bir endişe sebebi olmaya devam ediyor

COVID'in ilham verdiği yeni suiistimal fiilleri ortaya çıkacaktır

Mesleki suiistimallerle ilgili en yeni *Uluslara Raporunda,* Suiistimal İnceleme Uzmanları Birliği (ACFE), suiistimallerin ortanca süresinin – yani, bir suiistimalin başladığı ve tespit edildiği anlar arasındaki tipik süre – 12 ay olduğunu tespit etti.[12] Bu, kurumların pandemiyle bağlantılı ve ilişkili olan ve daha henüz keşfedilmemiş bulunan çeşitli suiistimallerle karşılaşmaya devam edecekleri anlamına gelmektedir.

Pandemiyle bağlantılı değişikliklerin suiistimal riskini etkilemeye devam etmesinin pek çok sebebi vardır. Örneğin, uzaktan çalışmanın geçici olması amaçlanmıştı, fakat uzaktan çalışma bugün pek çok şirkette standart çalışma usulü ve yöntemi haline geldi. Uzaktan çalışma, sıklıkla, kendisiyle birlikte, suiistimalleri tespit etmek veya etkilerini azaltmak için tasarlanmış uygulamalar ve prosedürlerde önemli değişiklikler – ve hattı bazı durumlarda gevşemeler – de getirdi. Sonuç olarak, pandemiyle bağlantılı olumsuz etkiler azalmasına rağmen pandemiyle ilişkili riskler şirketler için tehdit oluşturmaya devam etmektedir.

İç denetimin pandemiyle bağlantılı devam eden suiistimal riskleriyle mücadelede kilit önemi haiz bir rolü vardır ve iç denetim bu rolünü oynamaya devam edecektir. İç Denetim Vakfı (IAF) ve Kroll tarafından dünya çapındaki IIA üyeleri arasında yapılan bir araştırmada, ilgili yuvarlak masa toplantılarına katılanların çoğu, pandeminin "iç denetimi suiistimal riski yönetimi konusunda şoför koltuğuna daha fazla koyduğunu" hissettiklerini ifade ettiler."[13] Bu, operasyonel zorluklarla ilgili stratejik değerlendirmelere daha fazla katılmayı, kesintisiz ve sürekli güvence sağlamayı ve şirket departmanları arasında işbirliğinin artırılmasını – ve tüm bu süreçler boyunca denetçi bağımsızlığının korunmasını – içermektedir.

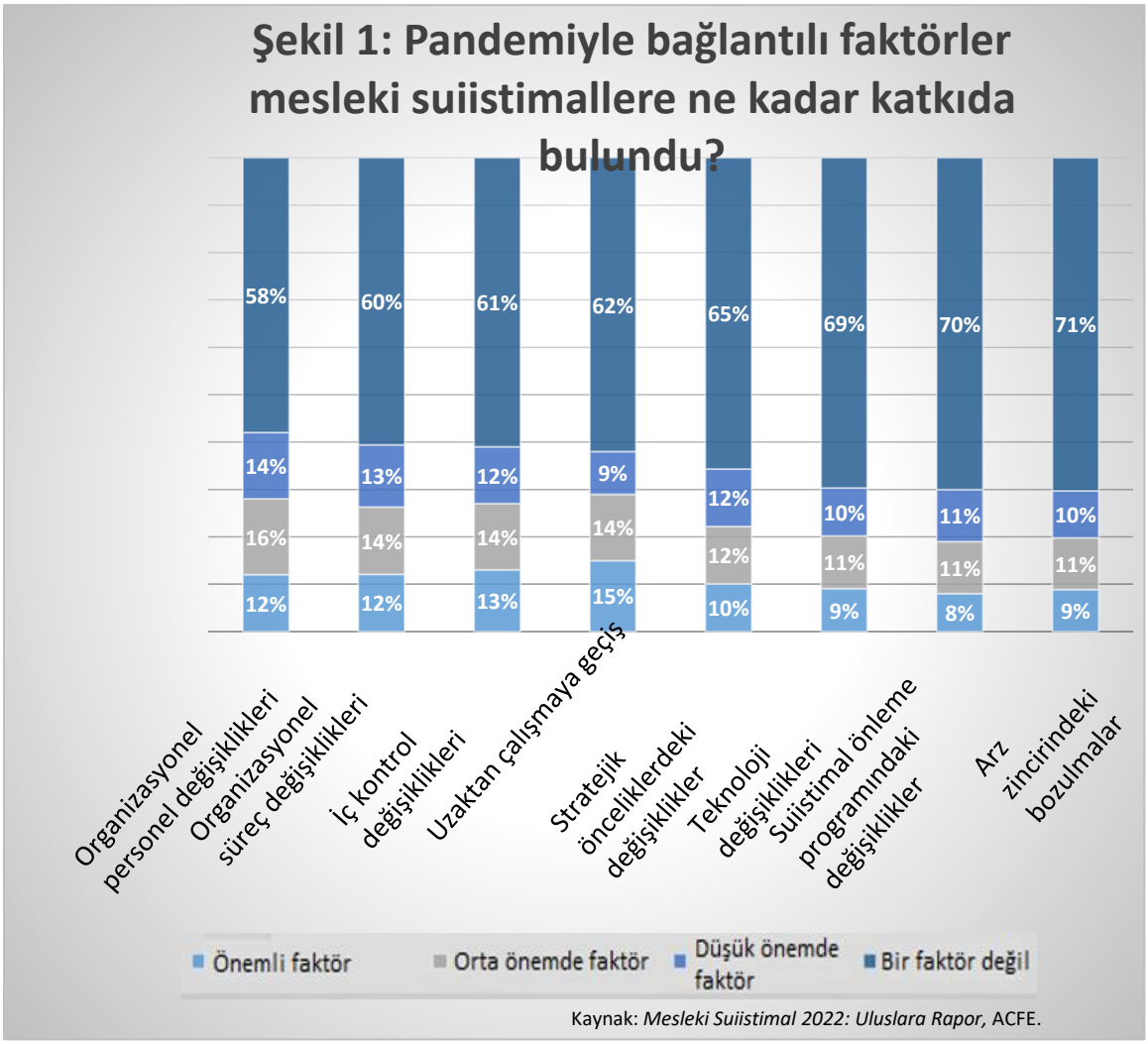
[12] *Occupational Fraud 2022: A Report to the Nations*, ACFE.
[13] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, İç Denetim Vakfı ve Kroll, Mart 2022.

Pandemiyle Bağlantılı En Önemli Suiistimal Riskleri

Personel değişiklikleri ve uzaktan çalışma en büyük endişe sebepleridir.

Katılımcıların yarıdan fazlası, pandemi faktörlerinin suiistimallere katkıda bulunduğunu düşünüyor.

Mesleki suiistimallerle ilgili raporunu hazırlarken, ACFE, katılımcıların %52'sinin soruşturdukları suiistimal olaylarında suiistimale pandemiyle ilişkili birkaç sorundan en az bir tanesinin katkıda bulunduğunu rapor ettiklerini tespit etti. Bu sorunlar arasında, pandemiyle bağlantılı organizasyon ve personel değişiklikleri en yaygın olandı. Katılımcıların toplam olarak %42'si personel değişikliklerinin mesleki suiistimallere katkıda bulunan önemli, orta veya düşük önemde faktörler olduklarını söylediler. Uzaktan çalışmaya geçmek en yaygın olarak önemli olduğu rapor edilen faktördü (%15) ve onu iç kontroller takip ediyordu (%12) (Şekil 1'e bakınız).



Kaynak: *Mesleki Suiistimal 2022: Uluslara Rapor,* ACFE.

ACFE raporunda tespit edilen en önemli pandemiyle bağlantılı sorunlardan bazıları hakkında yapılan daha derin bir inceleme, bunların etkilerinin sıklıkla kompleks ve zor fark edilen etkiler olabileceğini göstermektedir.

Personel değişiklikleri çeşitli suiistimal riskleri oluşturmaktadır

Pandemi, pek çok kurumu ve şirketi yüz yüze geldikleri pek çok olumsuz etkinin altında işlerini sürdürebilmek için çalışanların görev ve sorumluluklarını değiştirmek veya genişletmek ya da işlerine alışabilmek için sınırlı zamanları bulunan yeni insanları getirmek de dâhil çeşitli farklı çözümler veya kısayollar bulmaya zorladı. Ek olarak, bir fosfat ve spesiyal gübre şirketi olan Itafos'un denetim ve uyum direktörü David Dominquez'e göre, pandemiyle bağlantılı ekonomik belirsizliklerin sebep olduğu geçici işten çıkarmalar veya izinler de sıklıkla kalıcı hale geldi. "Pandemi, riski çeşitli bakımlardan ve açılardan kesinlikle artırdı," diyor Dominquez.

Pandeminin çalışma uygulamalarında ve protokollerinde yol açtığı pek çok ayarlama, uyarlama ve değişiklikleri – ve yeni görevler üstlenen kişiler için potansiyel öğrenme eğrisini – dikkate alarak, kurumlar, bu değişikliklerin hangi tip istenmeyen etkiler yapabileceklerini düşünmeli ve değerlendirmelidirler. Bu konuda değerlendirilmesi gereken bazı alanlar şunlardır:

Kültür

Pandeminin ardından kurumsal kültürü ve değerleri yeniden değerlendirmek ve belki de yeniden teyit etmek için pek çok sebep vardır. "Çalıştırmak" pandemi sırasında bir avantajdı, fakat bu, aynı zamanda, bazı önemli etik uygulamaların ve özniteliklerin unutulmuş olabileceği anlamına da gelmektedir. Yeni işe alınanlar şirketin etik değerleriyle düzgün bir şekilde tanıştırılmamış ve onları hiç deneyimlememiş olabilirler. Eğer durum buysa, kurumların çalışanlarına etik davranışlarla ilgili beklentilerini hatırlatmaları tavsiye edilmelidir.

ACFE raporunda, "Kültüre proaktif bir yaklaşım, çeşitli farklı kötü davranışları caydırabilir ve ahlâkı ve üretkenliği artırabilecek davranışları teşvik edebilir," denilmektedir. "Kültürün insanların işlerini nasıl yaptıklarını, kalite, uyum ve diğer kritik endişe sebepleriyle ilgili kararların nasıl alındığını ve kurumun hem içeriden hem de dışarıdan nasıl algılandığını etkileme kabiliyeti güçlüdür."[14]

İnsan kaynaklarıyla ilgili mülahazalar

Hibrid ve uzaktan çalışmada işçi eksikliği ve vardiya politikaları, anonim ihbar telefon hatları gibi uzun süredir uygulanmakta olan bazı insan kaynakları uygulamalarını sona erdirmiştir.

Suiistimallerin önlenmesinde kullanılan önemli bir insan kaynakları aracı da anonim ihbar telefon hattıdır. ACFE raporuna göre, suiistimallerin %42'si ihbarlar ve ipuçları sayesinde tespit edilmiştir ve bu oran, en yaygın ikinci yöntemin etkisine göre üç katından daha fazladır.

İç denetim, bu süreci hedeflendiği gibi çalışıp çalışmadığını inceleyerek destekleyebilir. Dominquez'e göre, ilk adım, bu telefon hatlarının ne kadar iyi izlendiklerini ve şikâyetlerin takip edilip edilmediğini tespit etmek olabilir. Dominquez, telefon hattıyla ilgili şu soruların sorulmasını tavsiye etmektedir:

- **İnsanlar telefon hattına nasıl erişiyorlar?** Bunun seçenekleri arasında ofisteki bir kutuya ipuçları bırakmak, bir telefon numarasını aramak ve şikâyetleri çevrimiçi rapor etmek bulunmaktadır. Ofisteki kutunun – ve telefon hattını tanıtan posterlerin – uzaktan çalışanlara faydasının olmayacağını unutmayın.
- **Telefon hattı gerekiyorsa farklı dillerde çalıştırılabilir mi?**
- **İpuçları ne kadar iyi takip ediliyor?** Dominquez, bazı şirketlerin düşük şikâyet adetleriyle övündüklerini söylüyor. Bu, iyi yönetilen bir kurumu yansıtıyor olabileceği gibi, bazı telefon çağrılarının cevaplanmadığını ya da şikâyetlerin sadece nadiren takip edildiğini de gösteriyor olabilir.

[14] *Assessing Corporate Culture: A Proactive Approach to Deter Misconduct*, Suiistimale Karşı İşbirliği, Mart 2020.

İç denetim, ihbarın alınmasından çözüm bulunmasına kadar uygun bir sürenin uygulanmasını ve ihbarı takip edip etmeme kararlarının sağlam temellere oturmasını sağlamak için şikâyetlere cevap verme sürecini gözden geçirebilir. Kurumlar bazen bir şikâyetin ardından gelebilecek misillemeden korkarak geçerli suiistimal ipuçlarını bile kaçırabilirler. İç denetim, kurum elkitabının veya davranış kurallarının misillemeyi açıkça yasaklayıp yasaklamadığını inceleyebilir. Dominquez'e göre, daha da ileri giderek, iç denetim, muhbirlerin terfi alma ihtimallerinin daha az ya da düşük performans değerlendirmesi alma ihtimallerinin daha fazla olup olmadığını takip etme konusunda da şirkete yardımcı olabilir. Bir şikâyet sağlam temellere dayanmasa bile, şirketler bu cevap süreci yoluyla güncellenmesi veya açıklığa kavuşturulması gereken politikalar olduğunu da tespit edebilirler.

Kurumların uygulamaya sokmaları veya devam etmeleri gereken diğer değerli tedbirler/kontroller ise şunlardır:

- Kredi geçmişi veya olası diğer mali problemleri ya da zimmet suçuyla bağlantılı olabilecek maaş hacizleri, rehinler veya mahkeme kararları geçmişini tespit etmek amacına yönelik özgeçmiş kontrolleri ve
- Referansların doğrulanması.

ACFE, suiistimalde bulunanların %50'sinin suiistimal olayından önce ya da suiistimal esnasında insan kaynaklarıyla ilişkili en az bir adet tehlike işareti gösterdiklerini bildirmiştir. Davranış ipuçları bakımından, bir kimsenin gelir seviyesinin üzerinde bir yaşam sürdürmesi, 2008 yılından beri yapılan her ACFE araştırmasında görülen en yaygın işaret olmuştur. Bu durum vakaların %39'unda tespit edilmiştir ve bu oran, %25 oranında görülen mali güçlüklerin oluşturduğu en yaygın ikinci faktörün oldukça önündedir.

İş belirsizlikleri

ACFE, bir suiistimal fiiline katkıda bulunabilir çeşitli iş belirsizliği örnekleri tespit etmiş ve zorlu ekonomik koşulların bu belirsizliği ve güvensizliği artırabildiğini tespit etmiştir. Spesifik tehlike işaretleri şunlardır:

- İşini kaybetme korkusu;
- Yükselme veya terfinin reddedilmesi;
- Yan sosyal haklarda kesintiler;
- Ücrette kesintiler;
- Çalışma saatlerinde istemeden yapılan azaltmalar ve
- Tenzil-i rütbe.

Ekonomik iklim ve koşullar pandeminin en kötü günlerinden bu yana stabilize olmasına rağmen, global iş dünyasında zorluklar hâlâ devam etmektedir. İş belirsizliğiyle ilgili sorunların etkisinin ACFE'ye göre 2022 yılından beri yüksek düzeyde kalması hiç şaşırtıcı değildir. Bu belirsizliklerin bazılarının çalışanları kötü davranış ve suçlara itme konusunda hâlâ bir faktör olabilmesi mantıklı ve akla yakın görünmektedir.

Bu tehlike işaretleri genel olarak tüm çalışanlar için geçerlidir, fakat özellikle üst düzey yöneticilere uygulanan birkaç ilave işaret ve sinyal de bulunmaktadır:

- **Fiziksel şiddet veya gözdağı ve tehditler**. Sahipler/yöneticiler için %23; sahip ve yönetici olmayanlar için %8.
- **Kontrol sorunları.** Sahipler/yöneticiler için %18; sahip ve yönetici olmayanlar için %12.
- **"Alavere-dalavere" davranışları.** Sahipler/yöneticiler için %17; sahip ve yönetici olmayanlar için %9.
- **Kurum içerisinden gelen aşırı baskı.** Sahipler/yöneticiler için %13; sahip ve yönetici olmayanlar için %6.
- **Geçmiş hukuki problemler.** Sahipler/yöneticiler için %11; sahip ve yönetici olmayanlar için %3.

COVID ile ilişkili iç kontrol değişiklikleri yeniden değerlendirilmelidir.

İç kontroller, bir kurum içerisinde yapılan eylemler ve alınan kararların kurumun politikalarına, raporlama koşullarına ve uyum görevlerine uyumlu ve uygun olmasını sağlamak amacıyla uygulanan prosedürlerdir. Suiistimale karşı kontroller, suiistimal zarar ve kayıplarını azaltabilir ve suiistimallerin daha hızlı tespit edilmesini kolaylaştırabilir. ACFE araştırmasında, suiistimal zarar ve kayıplarının neredeyse yarısı iki faktöre bağlanmıştır: iç kontrollerin bulunmaması (%29) ve mevcut kontrollerin etkisiz hale getirilmesi (%20). İç kontrolleri uygulamak ve güçlendirmek, açıkça, kurumlara önemli ve olumlu faydalar sağlayabilir. İç denetim, iç kontrollerin rapor edilmesi ve iç kontrollerde iyileştirmelerin tavsiye edilmesi konusunda önemli bir rol oynamaktadır. Gerçekten de, ACFE araştırmasında, bir kurumda iç denetim departmanı bulunmadığı zaman ortanca suiistimal zararının %50 oranında daha yüksek olduğu (100.000 $'a karşı 150.000 $) tespit edilmiştir.

IAF/Kroll anketine cevap veren iç denetçiler, "uzaktan çalışmanın getirdiği güçlüklerden ve çoğu durumda, hastalık, izinler ve personel sayısı yoluyla kadronun azaltılmasından dolayı iç kontrol çerçevesinin zayıfladığına" inandıklarını ifade etmişlerdir."[15]

Dominquez'e göre, kuruma kriz dönemlerinde katılan yeni insanlar yeterli eğitim almamış olabilirler veya onlara yeterli bilgi aktarımı yapılmamış olabilir ya da sadece acil durum protokollerini öğrenmiş olabilirler ve bu protokoller de uzun süreli süreçleri ve kontrolleri içermiyor olabilir. "Kontroller sulandırıldı ya da belki de sadece ihmal edildi," diyor Dominquez. Sadece belirli bir süre boyunca veya belirli bir durumda kullanılmaları amaçlanmış olmasına rağmen bu kısayollar süreç içerisinde ve zamanla standart çalışma prosedürü haline gelmiş olabilirler – ve böyle de kalabilirler.

Bu endişe, çoğu kurumda olumlu yönde değişikliklere yol açmıştır. Örneğin, Deloitte Yönetim Kurulu Etkinliği Merkezi ve Denetim Kalitesi Merkezi'nin bir ortak anketine cevap veren denetim komitesi üyelerinin kabaca dörtte üçü, uzaktan çalışma ortamı sebebiyle geçen yıl iç kontrollerini güncelleddiklerini ifade ettiler.[16]

İç kontrollerdeki zayıflıklar, suiistimallere karşı alınan sağlam tedbirleri ihmal etmenin veya gözardı etmenin daha kolay olduğu bir ortam yaratarak veya böyle bir ortamı teşvik ederek suiistimallere katkıda bulunabilirler. Örneğin, pandemi sırasında, farklı yerlere dağılmış işçilerle işleri yürütmek daha güç olduğu ya da birtakım personel eksiklikleri veya kesintileri söz konusu olduğu için, görev ayrımı ve dağılımı – yaygın ve etkin bir suiistimal karşıtı tedbir – bir kenara bırakılmış olabilir. Bu, bir şirketin eski ayarlarına döndüğünden ve etkin çalıştığından emin olmak için şimdi gözden geçirmesi gereken bir iç kontrol tipidir.

İç denetim, yaşamsal önemi haiz protokol ve süreçlerin uygulanmasını sağlayarak kurumların bu risklerle baş etmelerine yardımcı olabilir. Süreç haritalama teknolojisini kullanarak, kurumlar bu süreçleri yakın bir süre boyunca – altı ay veya bir yıl – takip edebilir ve normal uygulamalardan veya en iyi uygulamalardan sapmaları tespit edebilirler. "Standart prosedürler veya politikalardan sapmaları görebilir ve hangi süreçlerin güncellenmesi veya uygulamaya sokulması gerektiğine karar verebilirsiniz," diyor Dominquez.

Yeniden değerlendirilecek diğer alanlar ise, tedarik, çek keşidesi, banka hesap mutabakatları ve masraf geri ödemeleriyle ilgili iç kontrolleri ve ayrıca, mali mülahazalarda dikkate alınan diğer alanları kapsamaktadır.

Uzaktan çalışma da kritik bir suiistimal faktörü olmaya devam etmektedir

Pandemi esnasında çoğu kurum için en önemli değişiklik, muhtemelen, uzaktan çalışma yöntemine – ofisleri kapatmak ve çalışanların işlerini evden yapmalarına izin vermek – dramatik geçişti. Sonuç olarak, bu yeni yaklaşım, ACFE raporunda suiistimale büyük katkılarda bulunduğundan en çok bahsedilen faktördü. Normal koşullarda, bir şirket, böyle bir geçişin ve değişimin stratejik etkilerini değerlendirmek için aylar harcayabilir, fakat pandeminin ilk haftalarının belirsizliği ve aciliyetinden dolayı bunu yapmak tabii ki

[15] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge,* İç Denetim Vakfı ve Kroll, Mart 2022.
[16] *Audit Committee Practices Report: Common Threads Across Audit Committees*, Deloitte Yönetim Kurulu Etkinliği Merkezi ve Denetim Kalitesi Merkezi, 25 Ocak 2022.

olanaksızdı. Başka hiçbir şey olmasa bile, insanın tek başına ve tüm iş arkadaşları ve âmirlerinin gözetimi dışında çalışması bile çeşitli farklı suiistimalleri yapmasını kolaylaştırabilir. ACFE'ye göre, uzaktan veya hibrid çalışmaya kalıcı bir şekilde geçen veya geçmekte olan personel, "çözümlenmediği takdirde yıkıcı ve feci neticeleri olabilecek fay hatlarını keşfetmek için" değişim yönetimi planlamasına dâhil edilmelidir.[17]

Bu süreç boyunca, iç denetimin üzerinde odaklanabileceği çeşitli potansiyel fay hatları bulunmaktadır. Örneğin, bölümlere ayrılmış bir uzaktan çalışma ortamında insanları etkin yönetmenin güçlükleri ve bunun kültür üzerindeki etkisi, IAF/Kroll raporuna göre, çözümlenmesi gereken temel sorunlardır. [18] Etik davranış, sıklıkla, işyerinde bunu açıkça gösteren diğer çalışanlarla kurulan etkileşimler yoluyla öğrenilen ve güçlendirilen bir özelliktir. Daha deneyimli iş arkadaşlarına ulaşma olanağına sahip olmak, çalışanların başka bir çalışanın uygun olmayan veya yasalara aykırı olan bir davranış içinde göründüğü durumlar gibi muğlak veya şüpheli durumlarda ne yapmak gerektiğini anlamalarına yardımcı olabilir,

Uzaktan çalışmayla özellikle bağlantılı olan suiistimal tipleri arasında şunları sayabiliriz:

- **Zaman hırsızlığı veya çalışma saatleri konusunda temelsiz ve haksız taleplerde bulunmak:** Doğrudan gözetim ve denetim altında olmayan bir kişi için bunu yapmak daha kolay olabilir.
- **Veri hırsızlığı ya da gizli veya hassas bilgileri kötüye kullanmak veya paylaşmak:** Bu, bir çalışanın cihazlarına erişebilen kişiler ya da ofisten uzaktayken verileri kötüye kullanmak konusunda kendisini daha rahat hisseden çalışanlar tarafından yapılabilir.[19]

Bu konuyla ilgili endişelerden biri de uzaktan çalışanların ikinci bir iş yapmalarıdır. Örneğin, Dominquez'e göre, bir çalışan, asıl birinci işvereni için çalıştığı zannedilen saatlerde başka bir şirket için danışmanlık yapabilir veya geçici görevler ifa edebilir. Bu, kesinlikle bir zaman hırsızlığıdır, fakat dizüstü bilgisayar veya telefon gibi şirket kaynaklarının kötüye kullanılması şirketi siber güvenlik sorunlarıyla da karşı karşıya bırakabilir. Personel bir rakip için çalışıyorsa ve özellikle rekabet açısından önemli ve yararlı olabilecek bilgileri paylaşıyorsa bu yan iş aynı zamanda bir menfaat çatışması da yaratabilir. Yine Dominquez'e göre, iç denetim, personele verilen eğitim tipini ve personel elkitabı ve politikalarının bu yeni çalışma ortamlarına göre güncellenip güncellenmediğini sorgulayarak bu problemin çözülmesine yardımcı olabilir.

Teknoloji değişiklikleri suiistimal tertipleri ve kumpasları yaratıyor

Teknoloji, kurumların iç kontroller ve uzaktan çalışma gibi alanlarda etkin ve verimli prosedürler uygulamalarına olanak sağlayabilir. Kurumlar, siber güvenlik kaygılarını gidermek için zaten teknoloji yatırımları ve teknoloji geliştirme çalışmaları yapıyorlardı; pandemi şirketlerin mevcut sistemlerini hızlandırmalarını ve güçlendirmelerini teşvik etti. Teknoloji yükseltme çalışmalarına pek çok iç denetim birimi ve fonksiyonu da katıldı. Gerçekten de, iç denetçilerin %29'u pandeminin başlamasından bu yana suiistimalleri ve yolsuzlukları tespit etmek için veri analizini de araçları arasına aldılar.[20]

Aynı zamanda, teknolojik araçların kötüye kullanılması veya ihmal edilmesi de suiistimal tertipleri ve kumpaslarının başarılı olmasını kolaylaştırabilir. Yukarıda belirtildiği gibi, veri hırsızlığı, uzaktan çalışmayla bağlantılı endişelerden biridir. ACFE'ye göre, veri hırsızlığı risklerinin olası çözümleri arasında çalışanların evdeki ağlarını emniyete almalarını ve bunları başka aile üyeleriyle paylaşmamalarını istemek de vardır. Ev bilgisayarlarını emniyete almak için VPN'lerin ve daha güçlü ve daha karmaşık şifreler ve ayarların kullanılması da çözüm olabilir. Diğer seçenekler arasında, birden çok faktörlü kimlik denetimi ve veri güvenliği ve mahremiyeti konusunda yıllık personel eğitiminden de bahsedilebilir. Kurumlar, ayrıca, elektronik cihazlar, sosyal medya ve şirket verilerinin kabul edilebilir kullanımına ilişkin politikalar geliştirmeli ve çalışanlarından bu politikaları okumalarını ve anladıklarını teyit etmelerini istemelidirler.

[17] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, 12 Ocak 2023.
[18] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, İç Denetim Vakfı ve Kroll, Mart 2022.
[19] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, 12 Ocak 2023.
[20] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, İç Denetim Vakfı ve Kroll, Mart 2022.

Uzaktan veya hibrid ortamda çalışan kurumlar, aynı zamanda, çalışanlarının kendi ev cihazlarındaki yazılımı ve güvenlik yamalarını güncellemelerini sağlamalı ve şifre avcılığından ve diğer korsan tehditlerinden kaçınmanın en iyi yolları hakkında çalışanlarını eğitmelidirler.[21] Tabii ki, pandeminin etkilerine ayak uydurmak için çabalayan şirketler, güncel olduklarından emin olmak için kendi siber güvenlik tedlbirlerini de gözden geçirmelidirler.

Dominquez, bu endişelerin giderilmesine yardımcı olmak için, iç denetimin hangi güvenlik protokollerinin uygulandığını, kurumun hangi veri kaybı önleme araçlarını kullandığını, birden çok faktörlü kimlik denetimi ve VPN'lere ihtiyaç olup olmadığını ve çalışanlar işten ayrıldığında hesaplarının zamanında kapatılıp kapatılmadığını araştırabileceğini söylemekte ve bunu tavsiye etmektedir.

"Quiet Quitting" (Sessiz İş Bırakma) uyumu ve etik çabaları etkiliyor

"Quiet quitting" (Sessiz iş bırakma), çalışanların işle ilgili görevlerinin sadece asgarisini yapmakla yetindikleri bir uygulamaya atıf yapmaktadır. Gallup'un bir tahminine göre, bu çalışanlar, ABD işgücünün en azından %50'sini oluşturmaktadır. İşine ve görevlerine bağlı çalışanların oranı %32 idi, fakat işle bağlantısını aktif olarak kesmiş olanların oranı %18'di. Gallup, özellikle pek çok işin işbirliği yapılmasını gerektirdiği ya da müşteri isteklerini karşılamak için ekstra bir adımın atılabileceği durumlarda bunun problem yaratabileceğini not etmektedir. Ve sessiz iş bırakmaya yönelik trendin bu kadar ilgi ve dikkat çektiği bir durumda, işverenler, yüksek sesle iş bırakanların – ya da memnuniyetsizliklerini aktif bir şekilde ifade eden ve belki etrafa da yayan kişilerin – hâlâ var olduğunu bilmelidirler.[22]

Bu trend, kurumun üretkenliği, verimliliği ve çalışanlarını elinde tutması açısından kötü haber olabilir. Aynı zamanda, risk yönetimi üzerinde de olumsuz etki yapabilir. "İnsanlar artık yapmaları gerektiği kadar çok ilgi ve dikkat göstermiyorlar," diyor Dominquez. Ve *Corporate Compliance Insights* yayınında belirtildiği gibi, başarılı bir uyum ve etik programı kurumdaki herkesin katılımını ve desteğini gerektiren bir programdır. Yayında şu söylenmektedir: "Bir asgari-geçerli-iş-ürünü yaklaşımıyla işe nispeten olumsuz bir bakış açısını bir araya getirir ve birleştirirseniz, uyum ve etik uzmanlarının insanların sorunları bildirdiklerinden emin olmak için güvendikleri tüm ekstralar artık yok demektir."[23]

Bu, aynı zamanda bir suiistimal risk yönetimi programı açısından da kesinlikle doğrudur. Çalışanlar onayları ve işlemleri bakmadan imzalıyor veya anormallikleri gözardı ediyor olabilirler ya da bir anormalliği bildirmelerine rağmen sadece ilk âmirleri olan müdürlerinin bu ihbarı gözardı ettiğini, çünkü onların sessiz iş bırakma eylemi yaptığını görüyor olabilirler.

Dominquez'e göre, iç denetim, personel sadakati ve bağlılığına ilişkin problemleri anlayabilmek için personel memnuniyet anketleri, personel devir oranları ve işten ayrılma mülakatlarını inceleyebilir. Bunun ne gibi etkiler yapabileceğini anlamak için son trendler pandemi öncesindeki faaliyetlerle kıyaslanabilir.

[21] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, 12 Ocak 2023.
[22] "Is Quiet Quitting Real?" Jim Harter, Gallup Workplace, 6 Eylül 2022.
[23] "Why 'Quiet Quitting' Could Harm Ethics and Compliance Functions," Lisa Beth Lentini Walker, *Corporate Compliance Insights*, 14 Eylül 2022.

Sonuç

Tüm bunlar bize ne anlatıyor? ACFE'ye göre, kurumlar 117.000 $ ortanca zarar ve 1.783.000 $ ortalama zararla her yıl gelirlerinin tahminen %5'ini suiistimaller sebebiyle kaybetmektedirler. Normalde, suiistimal tertibi zararlarının aylık ortalaması 8.300 $ olabilir. Bunlar, tüm kurumlar için çok ciddi sorunlardır.

Pandeminin en kötü olduğu zamanlarda ve o günden bu yana, kurumlar, operasyonel süreçlerin yeniden değerlendirilmesi ve geliştirilmesinde stratejik karar alıcılara yardımcı olmaları için iç denetçilere başvurdular. Bu uygulama, özellikle suiistimallere karşı iç kontrollerin değerlendirilmesi konusunda sürdürülebilir. Dünya pandemiden çıkmış gözükmektedir, fakat pandemiyle bağlantılı ve ilişkili suiistimal tehditlerinden kendisini henüz tamamen kurtaramamıştır.

Pandeminin başladığı günden bu yana, iç denetimin suiistimalların durdurulması veya etkilerinin azaltılması konularında yapabileceği katkılar her zamankinden daha fazla takdir edilmektedir. Geçmişte, iç denetim sıklıkla bir suiistimal olayı vuku bulduktan sonra devreye sokulmaktaydı. Bu durum artık değişmektedir; kurumlar suiistimal eylemlerini çok fazla zarar vermeden önce tespit etmek ve bu zararlarla baş etmek için artık beklemek istemiyorlar ve bekleme ihtimalleri de daha az. Buna yardımcı olabilmek için, kurumlar iç denetçileri de suiistimali önleme temelli konuşmalara dâhil ediyorlar ve bir başka deyişle, iç denetçilerden suiistimal yapılmadan önce suiistimallere karşı kontrolleri gözden geçirmelerini istiyorlar, Dominquez'e göre. İç denetim, aynı zamanda, suiistimal riski değerlendirmesi tartışmalarını ve suiistimal riski değerlendirme çerçevelerini de kolaylaştırıyor; bu değerlendirmelerin ve kontrol testlerinin sıklığını ve etkinliğini değerlendiriyor ve şirketin devamlı risk profilindeki değişiklikleri not ediyor. "Suiistimali tespit etmeyi beklemek yerine, iç denetçiler suiistimali önleme tarafına geçiyorlar", diyor Dominquez.

IIA Hakkında

Uluslararası İç Denetçiler Enstitüsü (IIA), dünya çapında 230.000'den fazla üyeye hizmet eden ve 185.000'den fazla Sertifikalı İç Denetçi (CIA) sertifikası vermiş bulunan kâr amacı gütmeyen bir uluslararası meslek birliğidir. 1941 yılında kurulan IIA, dünya çapında, standartlar, sertifikasyon, eğitim, araştırma ve teknik kılavuzluk ve rehberlik konularında iç denetim mesleğinin lideri olarak kabul edilmektedir. IIA hakkında daha fazla bilgi almak için, theiia.org adresini ziyaret ediniz.

Sorumluluk Reddi Beyanı

IIA, bu dokümanı bilgi ve eğitim amaçlarıyla yayınlamaktadır. Bu doküman, spesifik bireysel durum ve koşullara kesin cevaplar vermek gibi bir amacı gütmemektedir ve sadece kılavuz olarak kullanılmak üzere hazırlanmıştır. IIA, herhangi bir spesifik durumla ilgili olarak doğrudan doğruya bağımsız uzman tavsiyesi ve görüşü alınmasını tavsiye eder. IIA, herhangi bir kimsenin sadece bu dokümana güvenerek yapabilecekleri konusunda hiçbir sorumluluk kabul etmemektedir.

Telif Hakkı

Nisan 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