www.pwc.com.tr

İç Denetimin Gelişen Teknolojideki Yeni Rolü

Risk, Süreç ve Teknoloji Hizmetleri



pwc

İçindekiler

6 Bulut Bilişim & İç Denetim

8 Siber Güvenlik & İç Denetim

10 Sosyal Medya & İç Denetim

12 Mobil Teknolojiler & İç Denetim

14 İç Denetimin bir sonraki adımı ne olmalı?

Giriş

Firmalar, teknolojilerin getirdiği yeni alanlarda ortaya çıkan riskleri yönetebilmek amacıyla iç denetim birimlerinden yardım istemeye başlıyor.

Teknoloji ile birlikte öne çıkan riskler

Basındaki başlıklarda yer alan veri ihlalleri haberlerinden dolayı, yöneticilerin veri gizliliği ve güvenliği ile ilgili endişeleri her geçen gün artıyor. Sosyal medyanın, mobil cihazların ve bulut bilişimin giderek artan kullanımı firmaları; bilişim teknolojileri güvenlik ihlalleri, müşteri verilerinin kötüye kullanılması ve itibar kaybı riski gibi yeni ve daha tehlikeli riskler ile tanıştırdı. Günümüzde firmalar, teknolojilerin getirdiği yeni ve belirli alanlarda ortaya çıkan riskleri yönetebilmek amacıyla iç denetim birimlerinden yardım istemeye başlıyor.



PwC'nin 2014 yılında yaptığı İç Denetim Anketi ***(http://www.pwc.com.tr/tr/risk-surec-teknoloji-hizmetleri/ic-denetim-anketi.jhtml)*** araştırmasına göre veri gizliliği ve güvenliği firmaların üst yöneticileri ve iç denetim yöneticileri tarafından en büyük risklerden birisi olarak gösteriliyor.

Bu dokümanda, gelişmekte olan teknolojilerin ortaya çıkardığı 4 tehdit ve fırsatı inceliyoruz:

- Bulut Bilişim
- Siber Güvenlik
- Sosyal Medya
- Mobil Teknolojiler

İş dünyasının karşılaştığı sorunlar ile ilgili daha etkili uygulamaların hayata geçirilmesi ile iç denetimin geleneksel yöntemlerden farklı olarak, trendleri yakalayabilmek için odaklanabileceği alanları, bu dokümanda sizinle paylaşmayı hedefliyoruz.



PwC Türkiye İç Denetim ve Kontrol Hizmetleri

www.pwc.com.tr/ic-denetim

PwC Türkiye Bilgi Teknolojileri Risk Hizmetleri

www.pwc.com.tr/bilgi-teknolojileri

PwC Türkiye Bilgi Güvenliği ve Siber Güvenlik Hizmetleri

www.pwc.com.tr/siberguvenlik



İç denetim, bulut bilişim ile ilgili risklerin değerlendirilmesi, yönetilmesi ve kontrol edilmesi ile, firma menfaatlerinin garanti altına alınmasına yardımcı oluyor.

Bulut Bilişim & İç Denetim

Bulut bilişimin sağladığı büyük yararlara rağmen getirdiği riskler neler?

Bulut bilişim, düşük bilgi teknolojileri (BT) maliyeti, karmaşık olmayan altyapısı, daha fazla esneklik sağlaması ve artan işletim verimliliğinden dolayı firmalar tarafından giderek daha çok tercih ediliyor. Firmalar, teknoloji geliştikçe, bulut bilişim kullanmanın finansal engelleri kaldırmayı teşvik edeceğini ve bu nedenle yeni ürünler ve hizmetler ortaya çıkartacağını düşünüyor.

Fakat pazarın durumunu düşünmeden ve dikkatli bir plan yapılmadan bulut bilişime geçilmesiyle beraber oluşan riskler, bulut teknolojilerinin kazanımlarını gölgede bırakıyor.

Bulut teknolojisini kullanmak isteyen tüm firmaların, bulut teknolojisinin tüm potansiyelinden ve sağlamış olduğu değerden tam olarak faydalanabilmesi için teknolojinin özünde bulunan güçlü yanların ve eksikliklerin bilincinde olması gerekiyor.

Buna göre, firmalar bulut teknolojilerini kullanmaya başlamadan önce;

- güvenlik ile ilgili açıkları ortadan kaldırmalı,
- kendi verilerinin ve bulut bilişim uygulamalarının uygunluğunu gözden geçirmeli,
- potansiyel hizmet sağlayıcısını yetkinlik, veri güvenliği, uygunluğu, ulaşılabilirliği ve ölçülebilirliği gibi konularda değerlendirmelidir.

Aynı zamanda, olası bir hizmet verememe durumunda verilerin ve uygulamaların başka bir hizmet sağlayıcısına taşınabilmesi durumu da göz önünde bulundurulmalıdır.

Nelerin yanlış gidebileceği ile ilgili gerçek hayattan örnekler

Bulut bilişim teknolojileri firmalar tarafından genel olarak başarılı bir şekilde kullanılıyor. Ancak operasyonel aksaklıklara neden olabilecek düzeyde hataların yapıldığını görmek de mümkün. Örneğin;

- ***Uluslararası Web Servis Sitesi*** - Kullanıcı başına yıllık 4,4 saat olan destek sözüne rağmen 70'in üzerinde müşteriye 36 saat boyunca teknik destek verilemedi.
- ***Uluslararası Oyun Firması*** - Gerçekleşen hacker saldırısı sebebiyle servislere erişim engellendi ve hizmetlerden faydalanan yaklaşık 77 milyon kişiye ait kişisel bilgiler çalındı.
- ***Domain Registrar ve Website Hosting Sitesi*** - Firmanın güvenlik sisteminin kırılması sonucunda, canlı veriler ve ilgili yedeklemeler tahrip edildi. Bunun sonucunda 4.800 web sitesi kayboldu ya da kurtarılamaz duruma geldi.

Risklerin yönetilmesi ile ilgili iyi uygulamalar

Değişimin temposu ve hızlı bir şekilde evrim geçiren teknolojinin olgunluğu göz önüne alındığında; en iyi uygulama ya da tek bir endüstriyel standardın mevcut olmadığı artık biliniyor. Fakat var olan standartlardan yola çıkılarak birtakım sistemler belirlenmiş durumda. Örnek olarak aşağıdaki standartlar gösterilebilir;

- Cloud Security Alliance'ın Bulut Kontrol Matrisi (Cloud Controls Matrix)
- ***ISACA'nın Bulut Bilişim için Kontrol Hedefleri:*** Bulutta Kontroller ve Güvenceler (Control Objectives for Cloud Computing: Controls and Assurance in the Cloud)

Bulut bilişim artan bir şekilde benimsendiğinden, endüstri standardı olgunluk modelinde olduğu kadar, risk yönetimi ve icrasında da yeni uygulamalar gerektiriyor.

Daha fazla bilgi için..

PwC Türkiye İç Denetim ve Kontrol Hizmetleri
www.pwc.com.tr/ic-denetim

PwC Türkiye Bilgi Teknolojileri Risk Hizmetleri
www.pwc.com.tr/bilgi-teknolojileri

PwC Türkiye Bilgi Güvenliği ve Siber Güvenlik Hizmetleri
www.pwc.com.tr/siberguvenlik

İç Denetim bu alanda nerelere odaklanmalı?

Bulut bilişimin, firmanın risk profili üzerindeki etkilerine odaklanması için iç denetimin BT yönetişim yapısı, BT altyapısı, hizmet sağlayıcısından temin edilen hizmetlerin riskleri ve yasal regülasyonları gözden geçirmede kullandığı geleneksel yaklaşımını tekrar gözden geçirmesi gerekebilir.

İç denetimin iş süreçlerinin değerlendirilmesi, yönetilmesi ve bulut bilişim kullanılması ile ortaya çıkan risklerin değerlendirilmesi konusunda firmalara yardımcı olması bekleniyor.

İç denetimin odaklanabileceği noktaları aşağıdaki şekilde sıralayabiliriz:

- ***Sözleşme yönetimi:*** Hizmet sağlayıcısının sorumlulukları, güvenlik ihlalleri ya da diğer ihlallerin neden olduğu olaylar, servis düzeyinin tanımlanması, sözleşmelerin takip edilmesi, yerel ve uluslararası düzenlemelere uyum için hangi haklara sahip olunduğu gibi kritik noktaların sözleşmede açık bir şekilde belirtildiğinden emin olunmalıdır.
- ***Yetkilendirme/Erişim kontrolleri:*** Bulut sağlayıcısı sizin bilgilerinize ulaşmada çalışanları/ortakları/ tedarik zincirini sınırlayabilmek için yönetimsel kontrolleri uyguladığını kanıtlamalıdır. Ayrıca, bilgilere ulaşacak personelin geçmişlerini araştırmalıdır.
- ***Sertifikasyon ve hizmet sağlayıcısı denetimleri:*** Hizmet sağlayıcılarının üçüncü taraf değerlendirme kurallarına tabi olduğundan emin olunması gerekir. (SSAE16, ISAE 3402, ASAE 3402 ya da ISO 27001 sertifikası) Mümkünse, tesis ve operasyonların bağımsız olarak gözden geçirilmesi istenmelidir.
- ***Uyum gereklilikleri:*** Tedarikçinin, firmanın kendi uyum gerekliliklerini sağlayıp sağlamadığından emin olunması gerekir. Kritik faktörlerden biri, hizmet sağlayıcının sunucularının coğrafi konumlarıdır. Verilerin tutulduğu veya işlendiği ülkede firmaya ait veriler için geçerli olabilecek yasalardan haberdar olunması gerekir.
- ***Ulaşılabilirlik, tutarlılık, esneklik:*** Tutarlılık, ulaşılabilirlik gibi konularda ölçülebilir hizmet seviyeleri için anlaşmaların ve sorumlulukların belirlenmesi gerekir.
- ***Yedekleme ve kurtarma:*** Acil durum eylem planı gereklilikleri açıkça tanımlanmalı ve sorumlulukların tam olarak anlaşılması sağlanmalıdır. Hizmet sağlayıcısı ile anlaşmadan önce hizmet sağlayıcısının böyle durumların üstesinden başarı ile gelip gelemediğinden emin olunması gerekir.
- ***Verinin imha edilmesi:*** İhtiyaç duyulmayan verilerin güvenli bir şekilde silinmesi gerekir.
- ***Taşınabilirlik:*** Gerek olduğunda, verilerin ve uygulamaların başka bir bulut sağlayıcısına transfer edilebildiğinden emin olunması gerekir. Bulut sağlayıcısı seçmeden önce sizin başka bir hizmet sağlayıcı kullanmanızı engelleyecek teknolojiler kullanmadıklarından emin olun.



Siber Güvenlik & İç Denetim

Siber güvenlik önceden bilinmeyen birçok riski ortaya çıkardı

Birçok kuruluşta kullanılan geleneksel BT güvenlik kontrolleri saldırganları durdurmak için güçlü sınırlar oluşturmayı hedefliyor. Ancak bu kontroller; ortaklar ve tedarikçilerle karmaşık ilişkiler, sosyal medya ve mobil erişimdeki aşırı artış karşısında yetersiz kalabiliyor.

Firmaların sahip oldukları bilginin değerini; bilginin nerede bulunduğunu, kaybı ya da çalınması durumunda yaratacağı finansal etkiyi ve bir saldırganın bu bilgiyle ilgilenme ihtimalini göz önünde bulundurarak net olarak kavraması gerekiyor.

Çevrimiçi (Online) işlemlerdeki artış ile bilgiler; firma sistemleri içerisinde veya çalışanların mobil cihazlarında yer alabilir, BT hizmet sağlayıcıları aracılığıyla yönetilebilir, iş ortaklarına iletilebilir ve hatta çevrimiçi servisleri kullanan müşteriler tarafından kendi cihazlarına indirilebilir durumda.



Nelerin yanlış gidebileceği ile ilgili gerçek hayattan örnekler

Medya; fikri mülkiyet hakkı, finansal ve özel müşteri bilgilerine ulaşılması ve kaldırılması ile ilgili hem küçük hem büyük organizasyonlara yapılan birtakım sansasyonel saldırıları haber yapmaya devam ediyor.

- ***Dünyanın önde gelen BT güvenlik firması:*** Firma, güvenlik yazılımının merkezindeki bilgisayar kodunu kaybettiğini kamuya itiraf etti. Bu durum firmanın yazılımının, firmaların en önemli ve hassas bilgilerine erişimi için kullanıldığı yönünde birtakım endişeleri de beraberinde getirdi. Yani, firmanın en değerli bilgisi uzaktaki bir saldırganın bir dizi hedefli saldırısıyla çalınabilirdi.
- ***Ulusal Güvenlik Ajansı:*** İlgili ajansın uluslararası firmaların ana hatlarına gizlice girerek verileri kopyaladığı ortaya çıktı. Bu da ilgili teknoloji firmalarının uluslararası güvenilirliğini zedeledi.
- ***Diplomatik Belge Sızıntısı:*** Dışişleri Bakanlığı ve büyükelçilikler arasında yapılan yazışmalar, gizli belgeler aşamalı olarak 5 büyük gazete desteği altında servis edildi.

Daha fazla bilgi için..

PwC Türkiye İç Denetim ve Kontrol Hizmetleri
www.pwc.com.tr/ic-denetim

PwC Türkiye Bilgi Teknolojileri Risk Hizmetleri
www.pwc.com.tr/bilgi-teknolojileri

PwC Türkiye Bilgi Güvenliği ve Siber Güvenlik Hizmetleri
www.pwc.com.tr/siberguvenlik

Risklerin yönetilmesi ile ilgili iyi uygulamalar

Tehditlere karşı ilk yapılması gereken değerli bilgilerin nerede bulunduğunu belirlemek, daha sonra da merkezi bir kayıt oluşturmaktır.

Firma; öncelikle hangi bilgiler değerli, bu bilgiler nerede saklanıyor, taşıyabileceği risklerin analizi ve etkin güvenlik önlemleri nelerdir gibi konuları belirlemelidir.

Amaç hassas ticari bilgileri, hem tehditlerden hem de etkisi yüksek ancak gerçekleşme olasılığı düşük olaylardan korumaktır. Daha sonrasında ise, risk yönetimi çerçevesinde, tehdit ortamının sürekli denetiminin sağlanması ile ani gelişen risklerin nelerden oluştuğunu belirlemektir.

Firmalar, başka firmalarda gerçekleşen ciddi olaylara ve ortaya çıkan sonuçlara göre kendi firmalarında önleyici ve ortaya çıkarıcı önlemler almalıdır. Bu durum gerçekleşen olayın sıradaki firma olarak sizin başınıza gelme olasılığını azaltacaktır.

İç denetim bu alanda nerelere odaklanmalı?

İç denetim için önemli noktaları aşağıdaki şekilde sıralayabiliriz:

- Bilgilerin depolanması, kritiklik seviyelerine ve işe etkisine göre farklılaştırıldı mı?
- Önemli bilgi varlıklarına ait merkezi kayıtlar tutuluyor mu?
- Önemli bilgi varlıklarına ait riskler uygun bir şekilde hesaplanıp, yönetim ile risk iştahı konusunda anlaşıldı mı?
- Bilgi varlıkları, BT ağları ve sistemler ile eşleştirildi mi?
- Önemli bilgilerin ayrıştırılması ve sadece yetkili kişilerin erişebilmesi için hangi güvenlik kontrolleri uygulanıyor?
- Uygulanan güvenlik önlemleri müşterilerin veri güvenliği konusunda beklentilerini karşılayacak düzeyde mi?
- Firma, düzenli olarak tehdit ortamını ve kontrolleri gözden geçirerek gerekli düzenlemeleri yapıyor mu?
- Firmanın hassas bilgilerin kaybolmasına ya da zarar görmesine ilişkin bir aksiyon planı var mı? Bu süreç kriz ve medya yönetimi planı ile ilişkilendirilmiş mi?

Sosyal ağların yaygınlaşması beraberinde kötü amaçlı yazılımların da hızla yayılabilmelerine imkan sağlıyor.

Sosyal Medya & İç Denetim

Firmaların sosyal medyaya olan ilgisi her geçen gün artıyor

Firmaların hem çalışanlarıyla hem de müşterileriyle olan iletişimlerinde sosyal medyanın potansiyeli göz ardı edilemez. Sosyal medya üzerinden gerçekleşen bu iletişim firmaların paydaşları ile daha kolay bilgi paylaşımını ve marka sadakati oluşturmalarını sağlamakla birlikte, beraberinde belli başlı riskleri de getiriyor;

- ***Olumsuz marka imajı:*** Sosyal medya, firmanın ürünleri ve firma hakkında yorum yapılmasına olanak sağlıyor. Bu yorumlar eğer yapıcı yorumlar ise firmaya değer katıyor ancak art niyetle yazılan yorumlar firmanın marka değerini olumsuz yönde etkiliyor.
- ***Veri kaybı:*** Çalışanların pek çok insana doğrudan ulaşabilmesi, özel veya gizli bilgilerin yanlışlıkla paylaşılması riskini arttırıyor. Bu bağlantıların fazla olması nedeni ile hacklenme gibi olayların olma olasılıkları artabilir ve müşteri verileri bu nedenle silinebilir veya kullanılamayacak duruma gelebilir.
- ***Kötü amaçlı yazılımların etkisi:*** Sosyal ağların yaygınlaşması beraberinde kötü amaçlı yazılımların da hızla yayılabilmelerine imkan sağlıyor. Tiny URL, Bit.ly ve Cligs gibi URL programlarının kullanımı gün geçtikçe artıyor. Bununla birlikte, bu tür programlar kötü amaçlı yazılımları da içinde barındırabiliyorlar.

Nelerin yanlış gidebileceği ile ilgili gerçek hayattan örnekler

Sosyal medya genelde firmalar tarafından başarılı bir şekilde kullanılıyor. Ancak marka değerine zarar veren veya veri kayıplarına neden olan olayları da görmek mümkün.

Örneğin;

- ***Uluslararası Araba Firması*** - 5 seneden fazla süredir Twitter'ı aktif olarak kullanan firmanın resmi Twitter hesabından uygun olmayan yazılar yazıldı. Firma daha sonrasında aynı hesaptan özür dilemesine rağmen marka imajı olumsuz etkilendi.

Daha fazla bilgi için..

PwC Türkiye İç Denetim ve Kontrol Hizmetleri
www.pwc.com.tr/ic-denetim

PwC Türkiye Bilgi Teknolojileri Risk Hizmetleri
www.pwc.com.tr/bilgi-teknolojileri

PwC Türkiye Bilgi Güvenliği ve Siber Güvenlik Hizmetleri
www.pwc.com.tr/siberguvenlik

Risklerin yönetilmesi ile ilgili iyi uygulamalar

- ***Farkındalık programları*** - Çalışanların sosyal medya kullanımı konusunda eğitilmesi (ör: etik kod aracılığıyla) ve belirli mecralardaki iletişimde kimlerin yetkili olduklarının belirlenmesi
- ***Politika & prosedürler*** - Güvenlik, sosyal medya ve etik konularında politikaların belirlenmesi ve bunların çalışanların işe giriş aşamalarına dahil edilmesi
- ***İletişim*** - Yeniliklerin öncelikle pilot bir grup içinde denendikten sonra uygunsa herkesle paylaşılması. Firmanın sosyal medya birimi ve çalışanlar arasında düzenli iletişiminin sağlanması ve söz konusu mecralarda olan bitenden çalışanların her zaman haberdar edilmesi
- ***Güvenlik teknolojileri*** - Politikalarınızı destekleyen, kontrolü ve takibine imkan tanıyan teknolojilerin kullanılması
- ***Risk değerlendirme*** - Sosyal medya kullanımının kontrol altında tutulması ve beklenmedik durumlara karşı risklerin, risk yönetiminin ve kriz planının gözden geçirilmesi
- ***Süre kotası*** - Sosyal medya kullanımına, firmanın risk iştahı ve risk profili doğrultusunda süre sınırı getirilmesi
- ***Kriz yönetimi*** - Olası senaryoları da içeren resmi planların oluşturulması

Sosyal medya genelde firmalar tarafından başarılı bir şekilde kullanılıyor. Ancak marka değerine zarar veren veya veri kayıplarına neden olan olayları da görmek mümkün.

İç denetim bu alanda nerelere odaklanmalı?

İç denetim için önemli noktaları aşağıdaki şekilde sıralayabiliriz:

- Sosyal medya stratejisi açık bir şekilde tanımlandı mı? Çalışanlar arasında firma ile ilgili sosyal medya kullanımları konusunda bir farkındalık oluşturuldu mu?
- Firma olarak sosyal ağ teknolojileri nasıl kullanılıyor? İş stratejisi ve marka değerinin yönetilmesine yardımcı olarak veriler elde ediliyor mu?
- Sosyal ağ analizlerine bağlı olarak aşağıdaki parametreler tanımlandı mı?
  - Sosyal medya kullanımı firmanın marka değerini nasıl etkiliyor?
  - Müşteri, çalışan ve firmaya ilişkin olarak veri kaybı riskini arttırıyor mu?
  - E-ticaret işlemlerinde riski arttırıyor mu?
- Firma, yeni mecralara adapte olma konusunda ne kadar esnek bir yapıya sahip? Yeni mecraların benimsenmesinde herhangi bir düzenleme ve kontrole ihtiyaç var mı?

Mobil Teknolojiler & İç Denetim

Mobil cihazlar gittikçe daha akıllı olmaya başladı ve bu yüzden daha fazla risk arz ediyorlar

Çoğu firma esnek olmak ve iş gereksinimlerini karşılamak için çalışanlarına mobil cihazlar temin ediyor. Ancak, akıllı cihazların sağladığı faydalarla, beraberinde getirdiği risklerin dengelenmesi gerekiyor. Firmaların göz önüne alması gereken ana riskler şöyle:

- ***Artan bilgi kaybı riski -*** Akıllı cihazların kaybolması veya çalınması gibi durumlar güvenlik riskini artırıyor.
- ***İzlenme -*** Casusluk yazılımlarının ve zararlı yazılımların mobil cihazlar için de yapılması ve sayılarının her geçen gün artması riski artırıyor.
- ***Farkındalık ve İletişim -*** Çalışanları zayıf güvenlik uygulamalarının kullanımı konusunda eğitmek gittikçe önem kazanıyor. (ör. Zayıf PIN ve şifre, yetersiz cihaz konfigürasyon ayarları)
- ***Mobil cihazları diğer tüm cihazlar gibi değerlendirme -*** Kurumsal ağlara giriş rotası mobil cihazlar mimarisi ile sağlanıyor ise bu durum hassas bilgilerin sızmasına yol açabilir.
- ***BT çalışanlarının eğitilmesi -*** BT çalışanları mobil cihaz yönetimi konusunda uzman olmayabilirler. Bu yüzden, konfigürasyon tanımlamasını güvenli bir şekilde yapmayabilir veya güncellemeleri sık bir biçimde yapamayabilirler.

Nelerin yanlış gidebileceği ile ilgili gerçek hayattan örnekler

Mobil teknolojiler genelde firmalar tarafından başarılı bir şekilde kullanılıyor. Ancak bu da belli başlı riskleri beraberinde getiriyor. Bu nedenle firmayı ve veri güvenliğini olumsuz etkileyen olayları da görmek mümkün.

Örneğin;

- ***Mobil Teknoloji Firmaları:*** Yapılan bir hacker saldırısı, teknoloji devleri ve bir hükümetin de içinde bulunduğu karmaşık bir ilişkiyi ortaya çıkardı.

Hackerlar, ülkenin askeri birimine yönelik saldırı düzenledi ve ele geçirdiği verilerin bir kısmını internet üzerinden paylaştı. Hackerlara göre pek çok cep telefonu üreten teknoloji firması, hükümete kullanıcıların verilerini görebilmesi için özel bir program altında arka kapı açmış oldu. Bu nedenle pek çok firmanın gizli bilgileri de risk altına girdi.

Daha fazla bilgi için..

PwC Türkiye İç Denetim ve Kontrol Hizmetleri
www.pwc.com.tr/ic-denetim

PwC Türkiye Bilgi Teknolojileri Risk Hizmetleri
www.pwc.com.tr/bilgi-teknolojileri

PwC Türkiye Bilgi Güvenliği ve Siber Güvenlik Hizmetleri
www.pwc.com.tr/siberguvenlik

Risklerin yönetilmesi ile ilgili iyi uygulamalar

Firmaların risk iştahları firmadan firmaya, sektörden sektöre pek çok farklılık gösteriyor, ancak akıllı cihazlarla ilgili riskleri yönetmek için etkili yöntemlerden biri organizasyonunuz için bir Mobil Cihaz Yönetim Çözümü seçmek. Bu yöntemi seçen firmalar güvenilir yayınlara ve araştırmalara dayanan sağlayıcıları seçmeyi tercih ediyorlar. Firmalar, seçtikleri sağlayıcılarla, güvenlik kuralları, cihaz güvenliği, cihaz yönetimi ve güvenli bir çevre oluşturabilmek için birlikte çalışmalı.

İç Denetim bu alanda nerelere odaklanmalı?

İç denetim için önemli noktaları aşağıdaki şekilde sıralayabiliriz:

- ***Akıllı cihaz stratejileri*** - Akıllı cihaz çözümlerinin firma stratejilerine uygun ve işin ihtiyaçlarına azami yarar sağlayacak nitelikte olduğundan emin olunması gerekiyor.
- ***Politika, prosedürler ve farkındalık*** - Politika, prosedür ve farkındalık uygulamalarının uygunluğunun, verimliliğinin ve çalışanların firma bilgilerini korumadaki sorumluluklarına aşinalığının araştırılması gerekiyor.
- ***Teknoloji değerlendirmesi*** - Mobil cihazlarla birlikte mobil cihaz yönetimi için kullandığınız teknoloji de, sektörün en iyisi olup olmadığı ile ilgili gözden geçirilmeli. İç denetimin, güncel kötü içerikli yazılımlardan haberdar olmak için mobil güvenlik gelişmelerini yakından takip etmesi gerekiyor.



Firmanın yeni riskleri yönetme yolunda olduğundan emin olmak için iç denetimin hemen atabileceği adımlar olduğunu düşünüyoruz.

İç Denetimin bir sonraki adımı ne olmalı?

Değerlendirme ve farkındalık

- Hizmet seviyesi anlaşmalarının değerlendirilmesi, uygulamasının gözlemlenmesi, dokümante edilmesi ve hedefler doğrultusunda ölçütlerin değerlemesi yoluyla sürecin ölçülmesi için organizasyona "mevcut" ve "olması gereken" süreçlerini tanımlayan stratejilerin geliştirilmesi konusunda yardımcı olunması gerekiyor. Değişen ve gelişen risklerle baş edebilmek için stratejinin gözden geçirilme sıklığını göz önünde bulundurun.
- Gelişen teknoloji karşısında, iç denetim biriminde çalışanların yeniliklere uyum sağlaması amacıyla bir eğitim planı geliştirin.
- Teknolojideki hızlı değişen trendleri ve uygulamaları, kurumsal risk, yönetişim, güvenlik ve teknolojilerle ilgili gizlilik konularındaki gelişmeleri takip etmek için bir uzmanla işbirliği yapın.
- Mevcut uygulamalar için (örneğin bulut bilişim), hizmet sağlayıcınızın kontrollerini değerlendirmek için bağımsız bir firma ile anlaşın veya bu garantiyi sağlamak için sağlayıcınızın bağımsız bir firma ile anlaştığından emin olun.

Daha fazla bilgi için..

PwC Türkiye İç Denetim ve Kontrol Hizmetleri
www.pwc.com.tr/ic-denetim

PwC Türkiye Bilgi Teknolojileri Risk Hizmetleri
www.pwc.com.tr/bilgi-teknolojileri

PwC Türkiye Bilgi Güvenliği ve Siber Güvenlik Hizmetleri
www.pwc.com.tr/siberguvenlik

Bilgi varlıkları yönetimi

- Önemli bilgi varlıklarının merkezi kaydını oluşturun ve sürekli güncel olmasını sağlayın.
- Bu bilgi varlıklarının riskini hesaplayın ve yönetim ile uygun risk iştahı konusunda mutabık kalın.
- Bilgi varlıklarınızı firmanızın BT ağlarına ve sistemlerine eşleştirerek varlık sahiplerini belirleyin.

Güvenlik ve erişim

- Önemli bilgilerin ayrıştırılmış ve sadece yetkili kişiler tarafından erişilebilir olduğundan emin olmak için iç güvenlik kontrollerinizi gözden geçirin.



İletişim



Tumin Gültekin
Risk Süreç ve Teknoloji Hizmetleri Şirket Ortağı

+90 212 326 60 67
tumin.gultekin@tr.pwc.com



Işıl Uysun
İç Denetim ve Kontrol Hizmetleri Lideri

+90 212 326 65 20
isil.uysun@tr.pwc.com

İç denetim ile ilgili gelişmeleri ve gündemi takip etmek, uluslararası ve ulusal düzenlemeler hakkında bilgi sahibi olmak; makale ve yayınlar, eğitim ve etkinlikleri izlemek için sitemizi ziyaret edin.

http://www.pwc.com.tr/tr/risk-surec-teknoloji-hizmetleri/ic-denetim-ve-kontrol-hizmetleri.jhtml

© 2014 PwC Türkiye. Tüm hakları saklıdır. Bu belgede "PwC" ibaresi, her bir üye şirketinin ayrı birer tüzel kişilik olduğu PricewaterhouseCoopers International Limited'in bir üye şirketi olan PwC Türkiye'yi ifade etmektedir. "PwC Türkiye", Başaran Nas Bağımsız Denetim ve Serbest Muhasebeci Mali Müşavirlik A.Ş., Başaran Nas Yeminli Mali Müşavirlik A.Ş. ve PricewaterhouseCoopers Danışmanlık Hizmetleri Ltd. Şti. ticari unvanları ile Türkiye'de kurulmuş tüzel kişiliklerden oluşan PwC Türkiye organizasyonunu ifade ve temsil etmektedir.

2015-0004