RPA kullanımından kaynaklanan teknoloji risklerini nasıl yönetiyorsunuz?

Kasım 2021

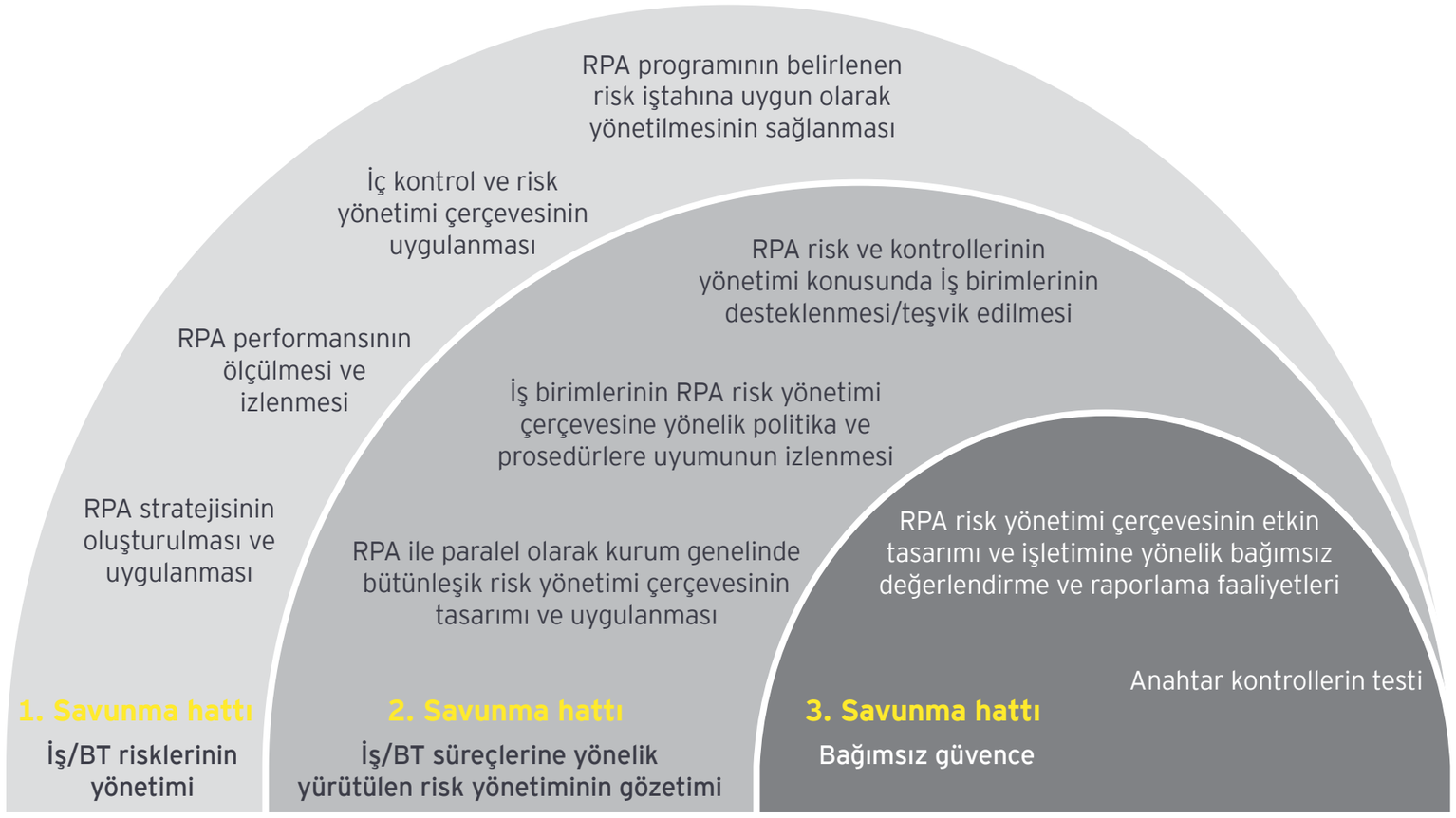
The better the question. The better the answer.
The better the world works.

Building a better working world

RPA yönetişim yapısı ve risk yönetimi çerçevesi

Dijital dönüşüm yolculuğunun önemli adımlarından biri olan Robotik Süreç Otomasyonu (RPA) artık her sektörde yaygın olarak kullanılmaya başlanmıştır. RPA teknolojisinin kullanımı, iş gücünün rutin işlerden katma değerli işlere odaklanmasını, operasyondaki hata riskinin azaltılmasını ve kuruluşların daha fazla değer üretebilmesini sağlayarak, kuruluşlara rekabet avantajı kazandırmaya devam etmektedir. Rekabet ortamında öne çıkabilmek için, şirketlerin bu dijital dönüşüme hızlı adapte olabilmesi ve aynı zamanda da bu dönüşümden kaynaklanan riskleri etkin yönetebilmesi gerekmektedir.

Özellikle birinci savunma hattını oluşturan iş birimleri, finans ve operasyon bölümleri tarafından benimsenen RPA teknolojisinin üçlü savunma hattında kullanımı yaygınlaştıkça, şirketler bünyesinde tutarlılık, hesap verebilirlik ve standardizasyonu sağlamak üzere bir yönetişim yapısının oluşturulması ve risklerinin yönetimine yönelik bir risk yönetim çerçevesinin oluşturulması ihtiyacı daha da öne çıkmaktadır. Bu kapsamda, söz konusu yönetişim yapısının şirketler bünyesindeki üçlü savunma hattına etkin entegrasyonu önem taşımaktadır.



RPA teknolojisinden kaynaklanan risklerin yönetimi için, üçlü savunma hattına entegre bir yönetişim yapısı ve risk yönetimi çerçevesi oluşturulmalıdır.

Teknoloji risklerinin ve kontrollerin belirlenmesi

RPA her geçen gün kullanımı yaygınlaşan bir teknoloji olmasına rağmen, RPA kullanımından kaynaklanan riskleri spesifik olarak adresleyen bir standart veya düzenleme bulunmamaktadır. RPA teknolojisinin tasarımı ve uygulanması aşamasında organizasyonların temel hedefi mümkün olan en kısa sürede maliyetleri azaltmak veya maksimum verimliliği sağlamak olduğu için robotların yaratılması ve sürdürülmesine yönelik yönetişim ve risk yönetimi gereksinimleri genellikle temel odak alanlarının dışında kalmaktadır.

Oysa, RPA teknolojisi, otomatize ettiği süreçlerin risklerine ek olarak kendi yapısal risklerini de beraberinde getirmektedir. Güvenli ve uyumlu bir RPA ortamı, aşağıda belirtilen temel üç risk alanına yönelik risklerin etkin yönetimini ve izlenmesini gerektirmektedir. Her bir risk alanına yönelik alınacak aksiyonlar, şirketler için uygulanabilir olduğu ölçüde, güçlü bir RPA kontrol ortamı sağlayacaktır.

Hem geleneksel riskleri hem de yeni, öngörülemeyen riskleri ortaya çıkaran RPA teknolojisine yönelik risk yönetim çerçevesinin temel olarak yönetişim, organizasyon ve teknoloji unsurlarına yönelik riskleri içerecek şekilde tasarlanması önerilmektedir.

Bu bütünleşik risk yönetimi çerçevesi, RPA teknolojisi kullanılan organizasyonlarda hangi teknoloji kaynaklı risklerin dikkate alınması gerektiği konusunda net bir görüş sunmaktadır. Söz konusu riskleri adresleyen kontrolleri belirlerken her bir RPA risk alanı için risk odaklı yaklaşım benimsenmelidir. Bunun için kuruluşların RPA kullanarak maruz kaldıkları teknoloji kaynaklı risklerin bir risk yönetimi çerçevesinde belirlemesi, analiz etmesi, süreç ve sistemler üzerinde bu riskleri ortadan kaldırmaya yönelik kontrolleri tesis etmesi gerekmektedir.

RPA teknolojisinin sağladığı avantajları dezavantaja çevirmemek için RPA kullanımından kaynaklanan bilgi teknolojileri risklerini iyi yönetmek büyük önem taşımaktadır.

1- Yönetişim Robotlara yönelik mevcut yönetişim çerçevesinin kurumunuzun riskten kaçınma stratejisi ve risk iştahı ile uyumlu olması gerekmektedir.	**1 Kontrol çerçevesi** RPA ile ilgili kontrolleri içeren resmi bir kontrol çerçevesi tanımlanmalıdır.	**2 BT risk yönetimi** Mevcut kontrol çerçevesindeki eksiklikleri belirlemek üzere bir risk değerlendirmesi çalışması yapılmalıdır.	**3 İç denetim / İç kontrol** RPA kontrol çerçevesine yönelik kontrollerin testleri iç denetim/iç kontrol planlarına dahil edilmelidir.
	4 Standardizasyon RPA kullanımı standartlaştırılmış süreçleri gerektirmektedir. Bu süreçleri belirleyebilmek için gerekli kriterlerin tanımlanması gerekmektedir.	**5 Yasal uyum** RPA kullanımından kaynaklanan yasal uyum yükümlülüklerinin etkisinin değerlendirilmesi gerekmektedir.	**6 Süreç belirleme** RPA uygulanabilecek süreçlerin belirlenmesi için gerekli kriterlerin tanımlanması gerekmektedir.
2- Organizasyon Robot operasyonlarının, doğru ve yeterli yetkinliklere sahip iç/dış kaynaklar tarafından yönetilmesi gerekmektedir.	**1 Dış hizmet alımı** Dış hizmet alınan firmaların BT kontrollerinin izlenmesi gerekmektedir.	**2 Eğitim** Uygun yetkinliklere sahip ekipler oluşturulmalı, süreçlerde tutarlılığı sağlamak adına eğitim programları düzenlenmelidir.	**3 Kaynak sağlama** Robot performansının geliştirilmesi/eğitimini sağlamak ve kurum içinde konu uzmanı olarak hareket edecek nitelikte kaynak tahsis edilmesi gerekmektedir.
3- Teknoloji Teknoloji kaynaklı risklerin yönetimi açısından, robotların şirketin BT risk ortamına entegre bir BT sistemi olarak kurulması gerekmektedir.	**1 Erişim güvenliği** Robotların rol ve sorumluluklarını içeren ve minimum yetki prensibi uyarınca yetkilerini kısıtlayan yetki profilleri oluşturulmalıdır.	**2 Bilgi güvenliği** Robotların hassas verilere erişimleri ve bu erişimlerden kaynaklanan risklere yönelik alınacak aksiyonlar belirlenmelidir.	**3 Siber güvenlik** Robotun yalnızca güvenli kanalları kullanarak üçüncü partilerle iletişime geçmesi sağlanmalıdır. Robotların yapısını içerecek şekilde sızma testi çalışması yapılmalıdır.
	4 BT operasyonları Robotların 7/24 çalışmasını ve sürekliliği garanti altına almaya yönelik izleme ve eskalasyon prosedürleri oluşturulmalıdır.	**5 Değişiklik yönetimi** RPA kullanılan süreçler ve ilgili robot mantık tasarımı üzerinde yapılacak değişikliklerin yetkilendirilmesi, testi ve onayını içeren değişiklik yönetimi prosedürleri oluşturulmalıdır.	**6 Son kullanıcı kontrolleri *(End user computing)*** Verilerin veya bilgilerin yanlış ve eksik işlenmesini ve kaybını engellemek üzere kontrol prosedürleri oluşturulmalıdır.
	7 Lisans yönetimi Robotlar da dahil olmak üzere varlıklar açıkça tanımlanmalı ve lisanslamaların durumu izlenmelidir.		

EY size nasıl destek olabilir?

1

Yönetişim ve risk yönetimi çerçevesinin oluşturulması

- RPA yönetişim çerçevesinin oluşturulması
- RPA risk yönetimi çerçevesinin oluşturulması
- Şirketler için RPA ortamına yönelik risklerin ve kontrollerin oluşturulması ve dokümante edilmesi

2

Mevcut RPA kontrol ortamına yönelik BT risk analizi

- Mevcut RPA ortamına yönelik BT risk analizi gerçekleştirilerek RPA risk kontrol matrisinin oluşturulması
- Kontrol eksikliklerini ve düzeltici aksiyon planlarını içeren yol haritasının oluşturulması

3

Siber güvenlik değerlendirmesi

- Uygulama güvenliği testi
- Sızma testi
- Zaafiyet taraması

EY | Daha iyi bir çalışma dünyası oluşturmak

EY olarak amacımız; müşterilerimiz, çalışanlarımız ve toplum için değer yaratırken aynı zamanda sermaye piyasalarında güvenin ve daha iyi bir çalışma dünyasının oluşmasına katkıda bulunmaktır.

Dünya çapında 150'den fazla ülkede, sahip olduğumuz veri ve teknoloji ile hizmet veren ekiplerimizle, denetimde güveni sağlarken müşterilerimizin gelişmesine ve dönüşmesine destek oluyoruz.

Bağımsız denetim, danışmanlık, hukuk, kurumsal finansman, strateji ve vergi hizmetlerimizle iş dünyasının karşılaştığı zorluklara yeni çözümler sunacak doğru soruları soruyoruz.

ey.com/tr
vergidegundem.com
facebook.com/ErnstYoungTurkiye
instagram.com/eyturkiye
twitter.com/EY_Turkiye

İletişim

Ümit Şen
Siber Güvenlik Hizmetleri Lideri
umit.sen@tr.ey.com

Burak Baysal
Teknoloji Risk Hizmetleri Lideri
burak.baysal@tr.ey.com

Esra Uzalp
Teknoloji Risk Danışmanlık Hizmetleri Lideri
esra.uzalp@tr.ey.com