GRC Gündemi

"ADP en iyi uygulamaları kullanarak iş risklerini nasıl yönetiyor?"

Küresel ölçekte ERP

Karar alırken hızlı davranmak ve kendine güvenmek

ERP yatırımlarının etkinliğini artırmak

KPMG Türkiye

kpmg.com.tr

GRC Gündemi:

Yönetişim, Risk ve Uyumluluğu Anlamak

GRC Gündemi, KPMG'nin Risk Yönetimi Danışmanlığı Birimi tarafından hazırlanan ve Yönetişim, Risk ve Uyumluluk (GRC) alanındaki en son gelişmeleri ele alan uluslararası bir yayındır. Yeni yasalar ve düzenlemeler, soyut ve öznel kontrol ortamı ve GRC araçları konularında en iyi uygulamalara ve örnek olaylara yer verir. GRC Gündemi, kendi GRC serüvenlerinde yardımcı olmak ve yeni düşünceleri teşvik etmek için geniş bir okuyucu kitlesine ulaştırılıyor.

İçindekiler

Küresel KRY Çerçevesi, kurumların risklerden kaçınırken aynı zamanda riskler kapsamındaki fırsatları da görmelerini sağlayarak katma değer üreten ve rekabet gücünü artıran açık ve uygulamaya yönelik bir yaklaşımdır.

Kararların incelenip onaylanması sürecinin uygun olmayan ve yetersiz olması, belirsizliklere ve fırsatların kaçırılmasına neden olabilir.

Kurumların ERP yatırımlarından beklentileri yüksektir. Başarılı bir ERP projesi, süreçlerin hızlandırılmasını ve maliyetlerin düşürülmesini sağlayacaktır.

GRC entegrasyonunun amacı, risk, kontrol ve bulguların aynı şekilde sınıflandırılmasını sağlamak da dahil olmak üzere birimler arasındaki geleneksel sınırları ortadan kaldırmak ve bu parçalı yapının yerine tek bir risk yaklaşımı geliştirmektir.

ADP

EN İYİ UYGULAMALARI

kullanarak iş risklerini nasıl yönetiyor?

ADP ile ilgili temel istatistikler

- 100 ülkede 630.000'den fazla müşteriye hizmet veriyor
- Dünya genelinde yaklaşık 55.000 çalışanı var
- ABD'de 24 milyon, diğer ülkelerde 12 milyon çalışanın ücretlerinin ödenmesine aracılık ediyor
- Haziran 2014'te sona eren mali yıl içinde toplam geliri 10,9 milyar dolardır
- Aynı dönemdeki net kârı 1,4 milyar dolardır

Kaynak: www.adp.com

Automated Data Processing, Inc. (ADP), merkezi Roseland, New Jersey'de olan ve dünya genelinde binlerce şirkete bordro hizmetleri de dahil olmak üzere İK çözümleri sunan bir insan sermayesi yönetimi şirketidir. 1949'da kurulan ADP, risklerin yönetilmesinin önemi anlayışını benimsemiş bir kurumdur. ADP'nin ERP (Kurumsal Kaynak Planlama) programı, rekabet ortamının sürekli değişen yapısını ve yeni teknolojilerin etkisini dikkate alan ve basit bir "risk azaltma" programı olmanın ötesine geçerek şirketin risk konusundaki farkındalığını artıran bir programdır.

Süreç

Risk konusunda ortak bir terminolojinin ve çerçevenin kullanıldığı, riske duyarlı bir kültürün oluşturulması, ADP'nin de benimsediği en önemli KRY (Kurumsal Risk Yönetimi) uygulamalarından biridir. Bu hususta ADP, yönetim ve üst yönetimler tarafından oluşturulan temelden yola çıkarak KRY programını dönüştürmüştür.

Bu temelin içinde, risklerin nereden kaynaklanabileceğini temel bir yaklaşımla değerlendiren bir "risk çarkı" da mevcuttur. Risk yönetimi programını geliştirmek ve bunu yeni bir bürokrasi katmanı oluşturmadan yapmak için üst yönetim, Denetim Başkanı'na bağlı olarak ve tam zamanlı çalışacak bir başkan yardımcısı, bir direktör ve bir müdür atamıştır.

KRY ekibi, ticari konularda engel çıkaracak değil fırsat oluşturacak bir vizyon belirledi. Ekip risk konusunda bilgi toplarken, görüştükleri paydaşlarla aynı dili konuşmaya ve ölçülü bir şekilde risk almanın olumlu sonuçlar doğurabileceği fırsatları belirlemeye çalışmıştır.

KRY programının amacı, sürekli destek ve yeni imkanlar sağlayarak paydaşların risk konusunda daha iyi kararlar almalarını sağlamak ve bu sayede iş performansını iyileştirerek ADP'nin itibarının korunmasına katkı sağlamaktır. Bunu başarmak için risk yönetimi şirket süreçlerinin ve kültürünün ayrılmaz bir parçası haline getirilmiş, belli başlı risklerin, tehditlerin ve fırsatların sürekli olarak değerlendirilmesi sağlanmıştır.

Yönetişim

Sorumlulukların ve hesap verebilirliğin açık bir şekilde tanımlanması, en önemli KRY uygulamalarından biridir ve risk yönetimi çerçevesinin benimsenmesini sağlamak açısından kritik öneme sahiptir. ADP üçlü savunma hattı modelini benimsemiştir. Bu modelde ilk savunma hattı, bir başka ifadeyle risk sahibi, işletmedir. İkinci hat ise veri mahremiyeti ve güvenliği, rüşvetle mücadele ve uyumluluk gibi risk yönetimi ve denetiminden sorumlu fonksiyonel birimlerden oluşuyor. Üçüncü hat İç Denetim birimidir.

KRY ekibi, İcra Kurulu Başkanı ve seçilen İcra Kurulu Üyelerinden oluşan KRY Yönlendirme Komitesi tarafından yönetilir. Yönlendirme Komitesi süresince katılımcı yöneticilerin zamanını en etkin ve en etkili biçimde kullanma öncelikli hedeflerden biridir. Bu hedefe hizmet etmek üzere, öne çıkan riskler üzerinde uzun zaman alacak detaylı incelemeler yapmak yerine, temel göstergeleri vurgulamak; bu vurguları sağlamak üzere risk ölçümlerinin geliştirilmesi tekniği uygulanır. Günlük risk yönetimi çalışmaları iş birimleri tarafından gerçekleştirilir. KRY ekibi Denetim Komitesi'ne veya Yönetim Kurulu'na düzenli bir şekilde bilgi verir.

Risk profili yaklaşımı

Risk yönetimi konusundaki iyi uygulamalardan biri de, KRY programını stratejik hedefler ve iş hedefleriyle uyumlu hale getirmek ve programın bunlara yönelik tehditlere odaklanmasını sağlamaktır. Risk ekibi, şirketin karşı karşıya olduğu birincil ve ikincil riskleri içerecek şekilde, risk profilinin belirlenmesi için KRY programının başlangıcından itibaren ADP yöneticileri ve Yönetim Kurulu ile yakın çalışmıştır. KRY/İç Denetim ekibi ayrıca, yönetilmesi, takibi ve denetimi farklı yaklaşımlar gerektiren üç farklı risk kategorisi oluşturmuştur.

Stratejik Riskler: Bu riskler şirketin başlattığı veya başlatmayı planladığı büyük strateji projeleriyle ilgili risklerdir. Bu projeler genellikle yatırım, iş modelinin değiştirilmesi ve ürün ve hizmetlerde değişiklik yapılması gibi konuları kapsar. Bu gibi projeler, daha stratejik bir yaklaşımla ele alınması gereken yeni riskler meydana getirebilir. KRY'nin buradaki rolü, yönetimin iyi yönetişim uygulamaları oluşturmasına ve KRY çerçevesinin, işletmeye bağlı ilgili birimleri söz konusu projeye entegre etmesine yardımcı olmaktır.

Operasyonel Riskler: Bu kategori, risklerin iyi bilindiği ve oturmuş süreçlerin olduğu uyumluluk ve veri güvenliği gibi alanları kapsar. Bu kategorideki risk yönetimi uygulamaları daha olgun bir yapıya sahiptir ve operasyonların takibinde kullanılan mekanizmalar gibi konulara odaklanır. KRY, işletmedeki risk sahiplerinin gelişmiş analiz yöntemleri kullanarak risklerini daha iyi gözetim altında tutmalarına yardımcı olabilir. Ayrıca risk sürecinin daha tutarlı bir hale getirilmesine yardımcı olabilir.

Dış Riskler: Bunlar mevzuat değişiklikleri veya çığır açan bir teknolojik gelişme gibi şirketin dışında gelişen ama şirketi etkileyen faktörlerdir. KRY, yönetimin dış riskleri takip etmek için belli mekanizmalar oluşturmasına yardımcı olabilir veya riskin gerçekleşmesi durumunda kurum bazında alınabilecek önlemlerin belirlenmesi için derinlemesine bir analiz gerçekleştirebilir. Bu şekilde üçlü bir sınıflandırma yapıldıktan sonra, kurumsal strateji ve şirket hedeflerine ulaşmayı engelleyebilecek olası tehditler hakkında üst düzey yöneticiler ve Yönetim Kurulu ile bilgi alışverişi gerçekleştirilir.

Ölçme ve izleme

Lider şirketler, riskleri daha iyi anlamak ve karar alma süreçlerini iyileştirmek için veri toplama ve veri analizine büyük önem veriyor. ADP'nin KRY birimi, veri toplama ve veri analizini iyileştirmek için yeni ve daha etkili yöntemler geliştiriyor. Üst yönetimin ve Yönetim Kurulu'nun dikkatini çekmenin en iyi yolu, kullanışlı ve kaliteli veriler toplamaktır. ADP'nin risk birimi, veri toplama ve analizi konusunda uzmanlaşmayı hedefliyor. Riskleri daha iyi anlamak için sürekli yeni yöntemler geliştirmeye çalışan ekip, gerektiğinde şirketin farklı birimlerinden gelen verileri birleştirerek çok boyutlu risk analizi gerçekleştiriyor.

Kültüre uyum sağlamak

ADP'nin KRY yaklaşımının en önemli özelliği, risk yönetimini şirket kültürü ile uyumlu hale getirmesi ve bunu yaparken toptancı bir yaklaşım benimsememesi olmuştur. Risk yönetiminin yenilikçiliği engelleyen bir faktör olarak algılanması da mümkündür. Ancak KRY ekibi kültürü anlamanın önemini erken kavramış ve KRY programının uygulanma hızında gerekli ayarlamayı yapmıştır. Herkese uygun bir yaklaşım benimsenmesi durumunda KRY programı başarısız da olabilirdi.

Programın benimsenmesinde önemli rol oynayan bir başka uygulama ise, kurum genelinde kullanılacak ortak bir risk çerçevesinin ve terminolojisinin oluşturulması olmuştur. ADP, KRY konusunda entegre bir yaklaşım geliştirmiş, risk ve kontrol denetimi fonksiyonu için veri mahremiyeti ve güvenliği, rüşvetle mücadele ve uyumluluktan sorumlu birimlerin kullanacağı ortak bir çerçeve oluşturmuştur. Bu sayede ikinci ve üçüncü savunma hatlarının kurum risklerine aynı şekilde yaklaşması ve Denetim Komitesi ile Yönetim Kurulu'na ortak bir dille konuşmaları mümkün olmuştur. Ancak süreç sona ermemiştir çünkü ADP, risk yönetimini gittikçe daha da entegre bir hale getirmeyi amaçlıyor. Tutarlılığı sağlamak adına, KRY ekibi tarafından geliştirilen risk çerçevesi şirketin diğer birimlerine de iletiliyor, bu amaçla işletme ve operasyon birimlerinin kendi süreçlerini ve denetimlerini iyileştirmek için kullanabilecekleri standart bir risk yönetimi paketi paylaşımı mümkün kılınıyor.

ADP'nin risk programındaki kritik başarı faktörleri

1. KRY uygulamalarının, yöneticilerin gündelik faaliyetlerinin bir parçası haline getirilmesi.
2. Katma değer sağlayan ve yenilikçiliği teşvik eden bir faktör olarak görülmeyi amaçlaması.
3. KRY çerçevesinin diğer risk ve kontrol denetimi fonksiyonları ile entegre hale getirilmesi ve risk konusunda ortak bir yaklaşımın oluşturulması.
4. KRY programının, kaçırılan fırsatlar da dahil olmak üzere stratejik hedeflere ve iş hedeflerine yönelik tehditlere odaklanması.
5. Riskleri daha iyi anlamak ve karar alma süreçlerini iyileştirmek için veri toplama ve veri analizine önem verilmesi.
6. Şirket kültürünün anlaşılması ve şirket kültürüyle birlikte gelişecek bir KRY programının oluşturulması.

Daha fazla bilgi için:

Deon Minnaar
Şirket Ortağı, Risk Danışmanlığı
KPMG ABD
E: deonminnaar@kpmg.com

Vishal Mehta
Direktör, Risk Danışmanlığı
KPMG ABD
E: vmehta@kpmg.com


KÜRESEL
ÖLÇEKTE
KRY

Şirket skandalları, başarısızlıklar, bilgi hırsızlığı ve doğal afetler gibi küresel olaylar, risk yönetimini (veya risk yönetiminin yokluğunu!) yatırımcılar, ortaklar, yönetim kurulları, paydaşlar ve müşteriler nezdinde yeniden önemli hale getirdi. Risk sistemlerinin kritik zamanlarda şirket varlıklarını korumayı başaramaması, risk yönetiminin kurumdaki herkesin günlük sorumlulukları ile olan ilgisi konusunu yeniden gündeme taşıdı.

Şirket yöneticileri KRY programlarını yeniden canlandırmaya çalışırken, sağlıklı bir KRY çerçevesine olan ihtiyaç her zamankinden daha fazladır. Üye firmalarının, müşterilerinin ihtiyaçlarını, düzenleyici kurulların beklentilerini ve piyasa şartlarını yakından takip eden KPMG, orijinal KRY çerçevesinin yeni ve güncellenmiş bir sürümünü hazırlayarak kullanıma sundu. Yeni Küresel KRY Çerçevesi, bütün küresel piyasalar ve sektörler için geçerlidir. Yeni KRY Çerçevesi ayrıca kurumsal stratejideki ve günlük operasyon ve süreçlerdeki riskleri tespit etmeye yardımcı olurken, yönetim kurulunun risk yönetimi projeleri, krizleri aşacak bilgi birikimine sahip olma ve önemli risk göstergelerini etkin bir şekilde değerlendirme konularındaki kaygılarını gidermeyi amaçlıyor.

Sade ve Etkin bir Yaklaşım

Yeni Küresel KRY Çerçevesi ve Risk Olgunluğu Ölçeği ile KPMG üye firmaları sade ve etkin bir yaklaşım benimsiyor. Şekil 1'de gösterilen yeni Çerçeve, orijinal çerçeveden farklı olarak Risk Kültürü, Risk İştahı ve Veri & Teknoloji unsurlarına da yer veriyor ve bu sayede mevcut KRY programlarının kültürel ihtiyaçlarını ve olgunluk seviyesini de dikkate alabiliyor. Yeni benimsenen Risk Kültürü unsuru, şirketlerin risk konusundaki kararları ve farkındalıkları sayesinde riskleri yönetebilme kabiliyetini şekillendiren değer ve davranışlara odaklanıyor.

Şekil 1 – Küresel KRY Çerçevesi

Küresel KRY Çerçevesi, kurumların risklerden kaçınırken aynı zamanda risklerin içindeki fırsatları da görmelerini sağlayarak katma değer üreten ve rekabet gücünü artıran açık ve uygulamaya yönelik bir yaklaşımdır.

Kaynak: GRC Gündemi, Ocak 2016, KPMG International

Yeni Çerçeve'de risk kültürünün vurgulanmasının, kurum kültürünün kabul edilemez risklerin önlenmesinde ve yeni ortaya çıkan risklerin tespit edilmesindeki önemi ortaya çıkıyor.

Her seviyede bilgi birikiminin olması ve risklerin anlaşılması, kurum kültürünün tamamında risk farkındalığının artmasını teşvik edecektir. Risk farkındalığının kurum genelinde yaygınlaşması ise, iş stratejisi ile risk stratejisi arasındaki bağların daha iyi kavranması sonucunu doğuracaktır. Çalışanlar risk azaltma ihtiyacı ile risklerle beraber gelen olası fırsatlar konusunda daha fazla düşünme imkanı bulacaktır. Çalışanlar normal faaliyetlerine devam ederken risk yönetimi ile performans yönetimi yer yer birbiriyle örtüşecektir.

Yeni Çerçeve'de risk kültürü, risk iştahı ve risk stratejisinin birleştirilmesi, kurumsal risk yönetimini yeniden tanımlarken, açıklık, şeffaflık ve hesap verebilirliğe dikkat çekiyor. Şirketin bütün birimleri riskleri stratejik, operasyonel ve taktiksel seviyede tespit edip, değerlendirip yönettiğinde, şirketin tamamı KRY'nin katma değerinden faydalanmış olur. Bu değer artışı risk maliyetlerinin düşürülmesi, büyümenin kontrollü bir şekilde gerçekleştirilmesi, risklerin rakiplerden daha önce azaltılması veya kritik karar anlarında daha fazla risk üstlenilmesi yoluyla gerçekleşebilir.

Küresel KRY Çerçevesi, kurumların risklerden kaçınırken aynı zamanda risklerin içindeki fırsatları da görmelerini sağlayarak katma değer üreten ve rekabet gücünü artıran açık ve uygulamaya yönelik bir yaklaşımdır. Yeni Çerçeve'nin birbiriyle bağlantılı unsurları ve birimleri risk stratejisi ile iş stratejisini birbiriyle uyumlu hale getireceği için, yönetim de risk stratejisi, risk iştahı ve risk kültürü hakkında sürecin baştan itibaren bilgi sahibi olabilecektir. Bu anlayışa sahip olmak, oluşabilecek zorluklara karşı aksiyon alma kapasitesinin arttırımı konusunda yardımcı olacaktır.

Güncellenen Unsurlar ve Birimler

Şekil 2, yeni Çerçeve'deki güncellenmiş unsurlar ve birimler arasındaki ilişkileri gösteriyor. Yeni Çerçeve'yi oluşturan unsurların ve birimlerin gruplandırılmasındaki yenilik, KPMG'nin sürdürülebilir kurumsal risk yönetimi programları geliştirme konusuna verdiği önemi gösteriyor ve KRY metodolojisine yeni bir standart getiriyor. Çerçeve'deki risk yönetişimi ile karar desteği, stratejik hedefler ve şirket yapısı bir araya getiriliyor. KRY konusundaki bütünsel yaklaşım sayesinde, her bir fonksiyonel alanın temsil edildiği bir risk yönetimi yapısı oluşturulmuştur.

Şekil 2 – Küresel KRY Çerçevesinin Unsurları

Risk Stratejisi ve Risk İştahı	Risk Yönetişimi	Risk Kültürü	Risk Değerlendirmesi ve Ölçümü	Risk Yönetimi ve Takibi	Risk Raporlaması ve Analizi	Veri ve Teknoloji
Kurumsal Stratejiyle İlişkilendirme	Yönetim Kurulu Denetimi ve Komite	Bilgi ve Kavrayış	Risk Tanımı ve Sınıflandırması	Risk Azaltma Tepkisi ve Eylem Planları	Risk Raporlama	Veri Kalitesi ve Yönetimi
Risk Stratejisi	Şirket Risk Yönetimi Yapısı	İnanç ve Bağlılık	Risk Tespiti	Testler, Geçerlilik Doğrulaması ve Yönetim Güvencesi	İşletme / Operasyon Gereksinimleri	Risk Analizi
Risk İştahı ve Toleransı	Risk Kılavuzu	Yetenekler ve Bağlam	Değerlendirme ve Önceliklendirme	Takip	Dış Gereksinimler	Teknolojik İmkanlar
	Roller ve Sorumluluklar	Eylem ve Kararlılık	Sayısal Yöntemler ve Modelleme	Proje/Girişim Riskleri		
	Karar Desteği		Risk Birleştirme İlişkilendirme ve Yoğunlaştırma			
			Senaryo Analizi ve Stres Testi			
			Sermaye ve Performans Yönetimi			

Kaynak: GRC Gündemi, Ocak 2016, KPMG International

KPMG üye firmaları, deneyim ve uzmanlığının getirdiği avantajla yedi risk unsurunu da dikkate alarak kurum geneli risk değerlendirmesi yapıyor ve bu yolla risk toleransını ve risk iştahını ölçüp değerlendiriyor. Risk unsurlarının uygulanması, KPMG'nin kurumsal strateji ile risk stratejisi arasındaki bağlantıyı inceleyip değerlendirmesine de temel teşkil ediyor. KPMG üye firmaları Küresel KRY Çerçevesi'ni kullanarak kendi ihtiyaçlarına uygun bir risk programı oluşturabilir.

Risk Stratejisi ve Risk İştahı unsurlarının birleştirilmesiyle, KPMG ekipleri risk iştahını kurumsal stratejiyle uyumlu bir şekilde belirleyebilecek ve kurumsal yönetişimi yönlendirebilecektir. Risk iştahı politikası belli başlı riskleri tespit eder, risk alanlarındaki kabul edilebilir risk seviyesini belirler ve hangi durumlarda risk üstlenileceğini ve hangi durumlarda riskten kaçınılacağını açıklar. Kurumsal stratejinin bir parçası olarak açık ve anlaşılır bir risk iştahı politikasının belirlenmesi risk iştahını kurumun değerleri, stratejik hedefleri ve iş kararları ile uyumlu hale getirirken bir yandan da paydaşların farklı çıkarlarının dikkate alındığını gösterecektir.

Risk stratejisi, risk iştahı ve risk toleransının bir arada sınıflandırılmasıyla, KPMG firmalar ağı kurum ve operasyonel birim seviyelerindeki niteliksel ve niceliksel kayıp ölçümleri dahilinde alınabilecek risk miktarının sınırlarını belirler. Yeni Çerçeve'de risk yönetimi, takibi ve raporlamasına yapılan vurgu, risk ve kontrollerin mali performans ve stratejik hedeflerle ilişkilendirmesini sağlıyor. Yönetimden, şirket süreçlerinin mevcut ve yeni ortaya çıkan riskleri azaltma kabiliyetinin geçerliliğini doğrulaması istenebilir. Yönetim Kurulu veya paydaşlar ise bu bilgiyi risklerle getiriler arasındaki ilişkiyi değerlendirmek için kullanabilir.

Yeni Çerçeve, iç ve dış risklerin sürekli olarak takip edilmesi, takip faaliyetlerine entegre bir şekilde kılavuzluk sağlanması ve olası risklerin aktif bir şekilde takip edilmesini içeren üç adet savunma hattı kurarak risk yönetimi kabiliyetini artırıyor. Risk raporlama, iş birimleri dahilindeki bütün alanları kapsıyor ve karar alma süreçlerini desteklemeye odaklanıyor. Kayda değer bir risk kültürü olduğunda, risk ölçümü ve risk değerlendirmesi birimleri, iyi tanımlanmış bir risk tespit ve risk sınıflandırma sisteminin uygulanmasını sağlayarak strateji geliştirme ve karar alma süreçlerini destekleyecektir.

Kesintisiz Risk Yönetimi

Yeni Çerçeve, Veri ve Teknoloji unsurundaki işletmeye bağlı birimler vasıtasıyla kesintisiz risk yönetimini destekliyor. Veri ve Teknoloji unsurundaki araçlar ve süreçler, kurum kültüründeki risk farkındalığını artırmakta ve üçlü savunma hattı modelini güçlendiriyor. Büyük veri teknolojileri, bütün kademelerdeki çalışanların tahmin modellerinin çıktılarını inceleyebilmesini ve örüntüleri tespit edebilmesini sağlıyor. Farklı kaynaklardan toplanmış güncel ve doğru verilerin veri görselleştirme araçlarıyla birlikte kullanılması, riskler hakkında ileri düzey değerlendirmeler yapılmasını ve yönetim kurulu üyelerinin kararlarını daha hızlı ve daha fazla bilgiye dayalı bir şekilde verebilmesini sağlıyor. Büyük verinin içinde iç ve dış kaynaklardan toplanmış hem geçmiş hem de gerçek zamanlı veriler olacağı için, bu analizler risk envanteri ve risk iştahı konusunda geniş kapsamlı değerlendirmelerin yapılmasını sağlayacaktır.

KPMG'nin benimsediği bireyselleştirilmiş yaklaşım, bazı risklerin sayısal ölçümlerle daha iyi ölçüleceğini, sayısal olarak ölçülmesi zor bazı risklerin ise niteliksel bir yaklaşım gerektirdiğini kabul ediyor. Yaygın olarak bulunan ve yapılandırılmış durumdaki verilerin niceliksel ve sayısal analizlere tabi tutulması, şirketin sağlık durumunun takip edilmesini, sorunların tespit edilip çözülmesini ve fırsatların farkına varılmasını sağlıyor. Gün geçtikçe miktarı artan yapılandırılmamış verilerin niteliksel analizi ise, hem mevcut ve yeni ortaya çıkmakta olan risklerin hem de daha fazla gelir getirecek fırsatların anlaşılmasına yardımcı olacak önemli gözlemler yapma imkanı veriyor.

Risk Olgunluğu Ölçeği

KPMG'nin Küresel KRY Çerçevesi, içerdiği genişletilmiş Risk Olgunluğu Ölçeği ile diğer KRY modellerinden ayrışıyor. Bu ölçek, her seviyeden ve farklı sektörlerden küresel müşterilere aynı olgunluk değerlendirmesinin uygulanabilmesini sağlıyor. Şekil 3'e bakıldığında, Çerçevenin yedi unsurundan her birinin, Risk Olgunluk Ölçeği'nin beş seviyesinden herhangi birinde bulunabileceği görülüyor.

Risk olgunluğu değerlendirmesinde hem benzer şirketler hem de sektördeki en iyi uygulamalar dikkate alınır ve performans farkını kapatacak yapı, yönetişim, politika ve araç değişiklikleri tespit edilir. Bu değerlendirmede ayrıca farklı olgunluk seviyelerine erişmek için gerekli zaman, çaba ve yatırım miktarı ile ilgili tahminler de yer alır. Örneğin, iç ve dış paydaşların beklentilerini karşılamak için gerekli asgari şartları yerine getirdiği ve bazı risk yönetimi stratejilerine sahip olduğu için bir şirketin sürdürülebilir olgunluk seviyesinde olduğu sonucuna varılabilir. Dış ölçütler kullanarak ve Risk Olgunluk Ölçeği ile ölçüm ve takip yaparak yeni ortaya çıkan riskler tespit edilebilir ve kesintisiz bir risk değerlendirmesi gerçekleştirilebilir.

Katma Değer

Hedeflere ulaşmak risk yönetimi ile yakından bağlantılı olduğu için, iyi tasarlanmış ve iyi uygulanan bir KRY, strateji belirlemenin de önemli bir parçasıdır. Küresel KRY Çerçevesi,

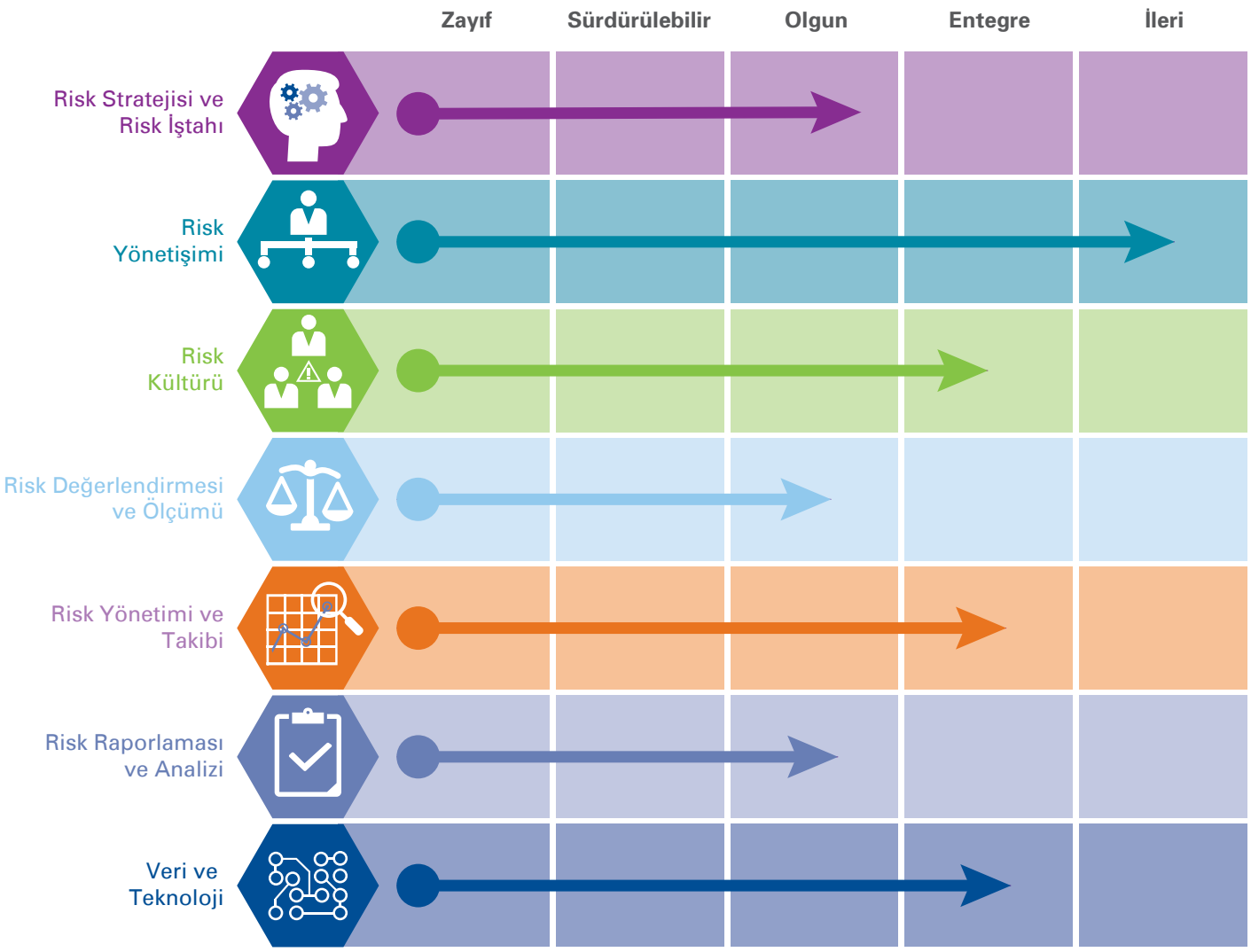
- risk stratejisi ile iş stratejisini uyumlu hale getirir;
- risk kültürüne hak ettiği değeri verir;
- riskleri kurumun risk iştahı dahilinde yönetir;
- kurumun başarısını etkileyebilecek muhtemel olayları tespit eder;
- denetim ve kontrol için ileri analiz yöntemleri kullanır.

Bu gibi faktörler sayesinde risk yönetimi kapasitesinde sürekli bir artış yaşanır.

KPMG'nin Küresel KRY Çerçevesi'nin uygulanması ayrıca yönetimin iş hedeflerine ulaşmak için sağlam bir risk yönetimi stratejisi kullandığını yönetim kurulu üyelerine göstermiş olur. Risk kültürü, risk stratejisi ve risk iştahına yapılan vurgu, kurum genelinde risk farkındalığını artırarak şeffaflığı teşvik eder. Modeldeki unsurların ve birimlerin birbiriyle bağlantılı olması, sürecin kurumun tamamına ulaşmasını ve her kademede katkı yapılabilmesini sağlar.

Risk stratejisinin ve risk iştahının anlaşılması, performans ve değer artışı ile markanın güçlenmesini de beraberinde getirir.

Şekil 3 – Küresel KRY Çerçevesi Risk Olgunluğu Ölçeği



Kaynak: GRC Gündemi, Ocak 2016, KPMG International

Küresel KRY Çerçevesi'nde belirlenen esaslar sayesinde kurumun risk olgunluğunu artıran süreçlerin ve kuruma özel çözümlerin uygulanmasına bütün paydaşlar dahil olur ve bu durum bütün paydaşların iş stratejilerini ve bu stratejilerin içerdiği riskleri daha iyi anlamasını sağlar.

Çerçeve bir yandan KRY esaslarını kurumun işleyişinin bir parçası haline getirecek pratik yaklaşımlar geliştirirken, bir yandan da stratejik hedefler ile kurumsal riskleri birbiri ile uyumlu hale getirir. Küresel KRY Çerçevesi'nin ve Risk Olgunluk Ölçeği'nin uygulanması, süreçlerin ölçülmesini, raporlanmasını ve takip edilmesini gerektirir ve bu sayede risk tespiti ve değerlendirmesi işleminin kesintisiz olarak sürdürülmesini sağlar.

Daha fazla bilgi için:

Deon Minnaar
Şirket Ortağı, Risk Danışmanlığı
KPMG ABD
E: deonminnaar@kpmg.com

Vishal Mehta
Direktör, Risk Danışmanlığı
KPMG ABD
E: vmehta@kpmg.com

Karar alırken hızlı davranmak

KENDİNE GÜVENMEK

sorumluluk ve hesap verebilirlik kültürü

Şirket çalışanları ve ekipleri her gün binlerce hatta milyonlarca konuda karar veriyor. Bu kararların verilmesinde ve tercihlerin yapılmasında deneyim, vasıflar, cinsiyet, yaş, kültür, kişilik ve (stres seviyesi, uyku düzeni gibi) sağlık faktörlerinin her biri bir rol oynuyor.

Birçok konuda karar vermek (daha önce benzer durumlarla karşılaşıldığı için) rutin bir işlem olsa da, rutin olmayan, doğaçlama kararların verilmesini gerektiren (yani ortak deneyimlerden faydalanma imkanının pek olmadığı) durumların sayısı da çoktur. Böyle durumlarda bireyler sorunları çözmek için kendi deneyimlerine başvurur.

Bu durumda yönetim kurulu, yöneticiler ve paydaşlar, şirket genelinde verilen kararların (söz konusu bireyin değil) şirketin hedefleri ve değerleri doğrultusunda ve hissedarların çıkarını en iyi koruyacak şekilde alındığından nasıl emin olabilir?

İlk olarak, şirketler yasalara ve düzenlemelere uygun olmak için şirketin yapması gerekenlerin belirtildiği, bu bağlamda yönetim kuruluna verilen yetkilerin açıklandığı bir esas sözleşme hazırlamakla yükümlüdür. Bununla beraber esas sözleşmelerde çalışanların günlük faaliyetleri esnasında farklı konularda karar verirken uyacakları kurallar ayrıntılı bir şekilde belirtilmez.

Bu yüzden birçok şirket, çalışanlardan beklenen davranışları ve karar verirken veya kararları onaylarken dikkate alınacak sınırları belirleyen yetki paylaşımı kuralları ile ayrıntılı politika ve prosedürler belirler. Bazı şirketler bir adım ileri giderek, verilen kararlarda dikkate alınacak risk iştahı / risk toleransı sınırlarını da belirler.

Bununla beraber bu mekanizmalar, şirketin gereksiz yere ciddi riskler üstlenmesi sonucunu doğuran yetki aşımlarının olmasını her zaman engelleyemiyor.

Örneğin, yatırım bankası çalışanlarının daha büyük kar elde etmek için kendilerine tanınan işlem limitlerini usulsüz bir şekilde aştığı çok sayıda olay gerçekleşmiştir (özellikle de küresel finans krizi öncesinde).

Kararların incelenip onaylanması sürecinin hantal veya iyi tanımlanmamış olması, belirsizliklere ve fırsatların kaçırılmasına neden olabilir.

Bu durumun arkasında yatan temel sebepler konusunda çok farklı açıklamalar olmakla beraber, yapılan işlemlerin risk iştahı ile uyumsuz olduğu ve uygunsuz işler yapanların hesap vermesini sağlayacak bir kültürün olmadığı konusunda herkes hemfikirdir.

Öte yandan, kararların incelenip onaylanması sürecinin hantal olması veya iyi tanımlanmamış olması, belirsizliklere ve fırsatların kaçırılmasına da neden olabilir.

Örneğin, kar amacı gütmeyen bir kuruluşun, elindeki fazla fonları değerlendirilebileceği bir emlak yatırımı fırsatıyla karşılaştığını varsayalım. Böyle bir işlem için yönetim kurulu onayı gerekip gerekmediği konusunda esas sözleşmede herhangi bir hüküm bulunmadığını da varsayalım. Yönetim, söz konusu işleme izin verilip verilmediğini açıklığa kavuşturmak için esas sözleşmede bir değişiklik yapılmasını talep eder. Esas sözleşmenin değiştirilmesine kadar geçecek sürede söz konusu yatırım fırsatının kaçırılması büyük bir ihtimaldir.

Karar verme hiyerarşisinin açık bir şekilde tanımlanması bu kadar önemliyse, şirketler neden bu konuda etkin politikalar geliştiremiyor?

En sık karşılaşılan, uzmanlık ve tecrübe isteyen konular engeller

Yetki devri, en üstte yönetim kurulundan başlayarak sırasıyla icra kurulu başkanına, üst düzey yöneticilere, onların altındaki yöneticilere ve şirketin tamamına yayılacak şekilde karar verme (veya onay isteme) yetkisinin dağıtılması demektir. Yetki devri kurumsal yönetimin ana ilkelerinden biridir ve sorumlulukları tanımlayan, onay mekanizmalarında tutarlılığı sağlayan, beklentileri yöneten ve yetkisiz kararları engelleyen bir iç kontrol mekanizmasıdır.

Ancak yeterli ve etkin bir yetki devri mekanizması oluşturulmasında bazı zorluklarla karşılaşılabiliyor:

- **Kapsam** – Bazı şirketlerde yetki devri dendiğinde sadece mali işlem limitleri ve yasal / bağlayıcı imza yetkisinin kimde olduğu anlaşılıyor. Belli bir tesisin veya birimin kapatılması, yönetici adaylarının

belirlenmesi gibi önemli stratejik ve operasyonel kararlarda kimin yetkili olduğu ise belirsiz bırakılıyor.

- **Detaylandırma** – Yetki devrinin ne kadar detaylandırılması gerektiği konusu uygulamada karşılaşılan zorluklardan biridir. Yetki devrinin çok genel ifadelerle belirtilmesi belirsizliklere ve boşluklara neden olurken, fazla detaylı olması ise verimliliğin düşmesine neden olabiliyor.
- **Uygunluk** – Şirketler zamanla büyüyüp genişlediğinde, yetki devri ile temel politikalar eskiyebilir ve şirketin büyüklüğü, kapsamı ve operasyonların doğası ile aynı seviyede olmayabilir.
- **Uygulanabilirlik** – Şirketin bütün kademelerinde ve bütün iş yerlerinde yetki sınırlarının uygulanabilirliğini belirleyecek bir süreç oluşturmak, özellikle de yerel mevzuatlarla uyuşmazlıklar söz konusu olduğunda zor olabilir.

Uygulamada şirketler mevcut yetki devri politikalarını geliştirme konusuna daha fazla odaklanmaya ve yetki sınırlarının belirlenmesinin yanı sıra risk iştahı / risk toleransı konusunda kılavuz ilkeler de belirlemenin önemini kavramaya başlamıştır.

Risk iştahı, bir şirketin stratejik hedeflerine ulaşmak için üstlenmeye hazır olduğu risk değerini ifade eder. Risk toleransı ise şirketin üstlenmeyi kabul edeceği riskin sınırlarını belirler.

Bazı sektörlerde (örneğin finansal hizmetler sektöründe) ve/veya piyasalarda bu kavramlar oturmuş ve açık bir tanıma kavuşturulmuş iken, başka sektörlerde ise uygulama daha yeni başlamıştır. Özelikle de finansal hizmetler dışındaki sektörlerde risk iştahı/risk toleransı konusunda karşılaşılan temel zorluklar şunlardır:

- **Kavramın anlaşılması** – Bazı sektörlerde veya şirketlerde risk iştahı/ risk toleransı kavramları ilk defa karşılaşılan kavramlardır. Dolayısıyla iyi bir şekilde anlaşılmaları ve karar verme süreçlerinde yaygın bir şekilde kullanılmaları biraz vakit alabilir.

- **Ölçüm** – Stratejiler ve riskler iyi bir şekilde tanımlanmazsa veya paylaşılmazsa, doğru risk alanlarını tespit etmek, ölçmek ve takip etmek zor olabilir.
- **Veri toplama** – Risk toleransı ölçümlerinin yapılabilmesi için gerekli olan sayısal verilerin verimli bir şekilde toplanamaması.
- **Denetim** – Verilerin kolayca erişilebilir olmadığı ve manuel olarak toplanmasının gerektiği durumlarda, takip süreçlerini vaktinde ve hatasız bir şekilde yürütmek zor olacaktır.

Uygulamada genellikle yetki devrinin ve risk iştahı/risk toleransı sınırlarının geliştirilmesi ve takip edilmesi eşgüdüm içinde gerçekleştirilemediği için, karışıklıklar meydana geliyor ve onay limitleri eskiyerek anlamsızlaşıyor veya eksik kalıyor.

Ayrıca yetki devri ve risk iştahı stratejiden bağımsız bir şekilde belirlenirse bu durum şirketin gelişmesini engelleyebilir. Yetki devri ve risk limitleri çok düşük belirlenmişse (veya çok sayıda onaydan geçmesi gerekiyorsa), bu durum verilen kararların hızını ve değişen durumlara tepki verme kabiliyetini olumsuz etkileyecektir. Yetki devrinin ve risk limitlerinin çok yüksek olduğu durumlarda ise, karar verilmeden önce üst kademelerin fikri yeterince alınmadığı veya üst kademeler yeterince bilgilendirilmediği için gereksiz / aşırı harcamaların yapılması veya optimum kararların alınamaması durumuyla karşılaşılabilir.

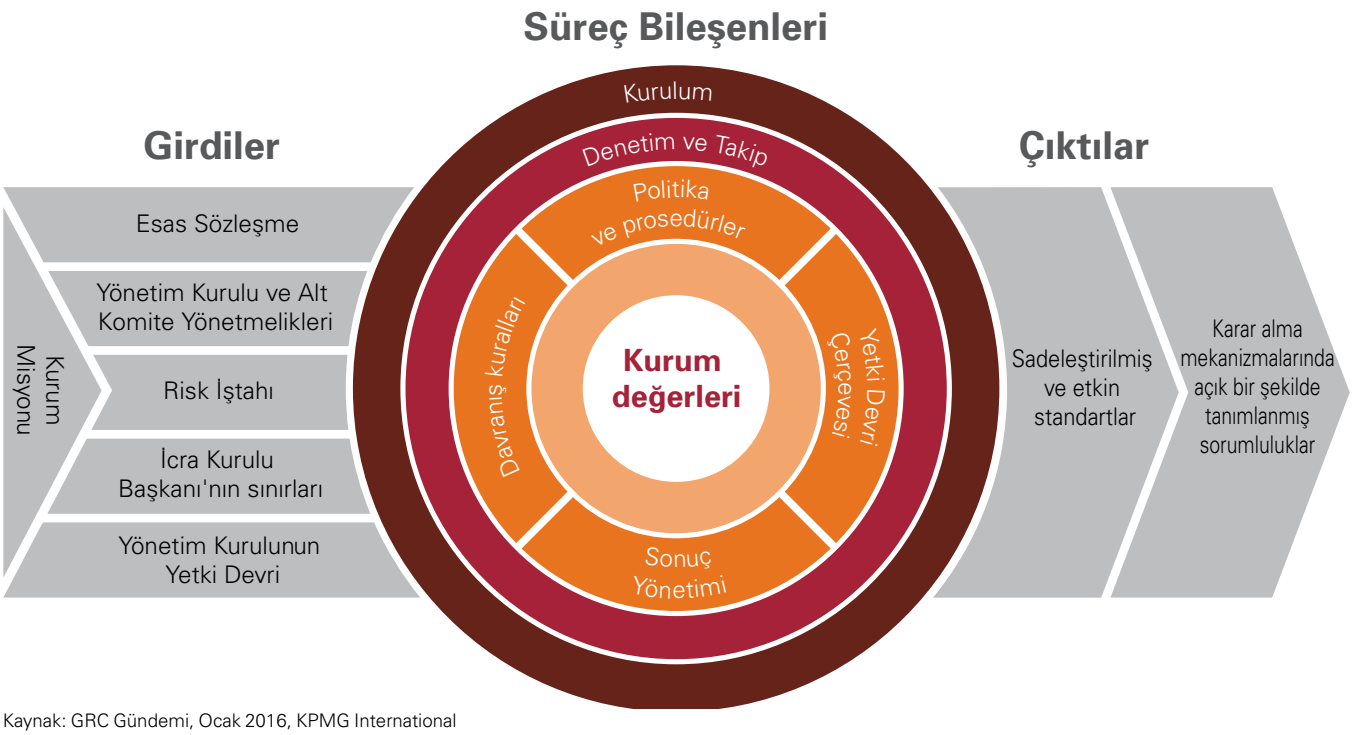
Uygulamada strateji, risk iştahı ve yetki sınırlarını şirket değerleri, değişen risk profilleri, denetim ve takip fonksiyonları ve sonuç yönetimi prosedürleriyle ilişkilendiren bütüncül, entegre ve dinamik bir hesap verebilirlik çerçevesine sahip şirket sayısı son derece sınırlıdır.

Bu da fırsatların kaçırılması, rekabet avantajının kullanılamaması anlamına gelir. Yeterli, etkin ve verimli bir karar verme modeline sahip olan şirketler daha hızlı hareket edebilir, karşılarına çıkan fırsatları daha iyi değerlendirebilir ve bir krizle karşılaştıklarında daha tutarlı ve kararlı davranışlar sergileyebilir. Rolleri ve sorumlulukları açık bir şekilde belirlendiğinde çalışanlar gerekli yetkilere sahip olduklarını ve idarenin desteğinin arkalarında olduğunu hissedecektir. Bu durum, tecrübeli çalışanların elde tutulmasını da sağlayacaktır.

Bu eksiklikleri gidermek için şirketler ne yapabilir?

Atılması gereken ilk adım, kurum genelindeki hesap verebilirlik çerçevesini oluşturan mevcut kontrol mekanizmalarının hepsinin birbiri ile bağlantılı olduğunun farkına varmaktır. Hızlı ve etkin karar alma için şirketteki bütün kademeler gerekli yetkilerle donatılmalı, karar alma süreçleri

Şekil 4 – KPMG Hesap Verebilirlik Çerçevesi



Kaynak: GRC Gündemi, Ocak 2016, KPMG International

hakkında bilgilendirilmeli ve eğitilmelidir. Ayrıca gereken yerlerde denge ve fren mekanizmaları da oluşturulmalıdır.

KPMG Hesap Verebilirlik Çerçevesi aşağıda ana unsurlarıyla gösterilmiştir.

Hesap verebilirlik çerçevesi sayesinde ana **girdiler** birbiriyle uyumlu hale getirilir ve strateji (kurum misyonu), şirket anayasası (esas sözleşme), yönetim kurulu ve alt komitelerinin kullanacağı kriterler, risk iştahı ve yetki devri gibi mekanizma ve belgelerle karar verirken sergilenmesi beklenen davranışlar açıklığa kavuşturulur.

Ancak beklenen davranışları operasyonel hale getirecek ve benimsenmesini sağlayacak **süreç bileşenleri** olmazsa bu girdilerin hiçbir anlamı kalmaz. Şirket değerleri, hesap verebilirlik çerçevesinin temelini oluşturur. Farklı şirketlerin farklı değerleri olabilir ancak bu değerlerin anlaşılması bütün şirketler için aynı derecede önemlidir. Çünkü hesap verebilirlik modelinin ana unsurlarını şekillendiren, nasıl tanımlanacaklarını ve uygulanacaklarını ve ne dereceye kadar benimseneceklerini belirleyen değerlerdir. Diğer kolaylaştırıcıları belirlemek için şirketin işletim modeline bakmak gerekir. İş modelleri, yapılar (ör. grup ve bağlı şirketleri) ve mekanlar (ör. yerel ve çok merkezli) zamanla değiştiği için bu son derece önemlidir.

Denetim ve takip çerçevesi, ihlallerin tespit edilmesi ve raporlanmasında çok önemli bir rol oynar. Bu çerçevenin bir parçası olarak, sorunların uygun bir şekilde çözülebilmesi ve/veya gerekiyorsa disiplin işlemlerinin gerçekleştirilmesi için ihlallerin altında yatan nedenlerin tespit edilmesi ve değerlendirilmesi gerekir.

Yetki ihlalinin yetki sınırlarının iyi tasarlanmamış olmasından mı (yetki sınırının belirlenmemiş olması veya riske uygun olmaması), kontrollerin uygun bir şekilde işletilmemesinden mi (ilgili kişinin limitleri bilmemesi veya limitlere uyma konusunda gerekli eğitimi almamış olması), yoksa kötü niyetten mi kaynakladığını tespit etmek önemlidir.

Bu tür analizler gerçekleştirilerek çerçeve sürekli geliştirilebilir. Hesap verebilirlik çerçevesinin başarılı olabilmesi için, özellikle de sonuç yönetimi protokollerinin şeffaf bir şekilde kullanıma sokulması konusunda üst yönetimde sağlam bir iradenin olduğunun gösterilmesi gerekir.

Örneğin, şirketin satış müdürü bir yetki sınırını ciddi biçimde ihlal ettiyse ve ortaya çıkan sonuçlar müdürün işten çıkarılmasını gerektiriyorsa, yönetim kurulunun ve üst yönetimin, satışlar üzerindeki olumsuz etkilerini dikkate almaksızın ilgili protokolleri uygulaması gerekir. Bunun amacı, ihlallere anlayış gösterilmeyeceği ve üst yönetimin bu konuda kararlı olduğu mesajını güçlü bir şekilde vermektir.

Bütüncül ve entegre bir çerçeve tesis edilmesinin nihai amacı, pratik ve sade standartların belirlenmesi ve kararlarla ilgili sorumlulukların açık bir şekilde tespit edilmesi şeklinde **çıktılar** oluşturmaktır.

Bu kontrol mekanizmalarının önemi dikkate alındığında, hesap verebilirlik çerçevesinin faaliyetlerini yönetmek için ayrı bir fonksiyon oluşturulması (veya sorumlu atanması) şarttır. Aynı şekilde, çerçevenin güncel kaldığından emin olmak ve risk profilindeki ve/veya iç/dış şartlardaki önemli değişikliklere ayak uydurmak için çerçevenin düzenli bir şekilde gözden geçirilmesi de şarttır.

Yaptığımız her şeyi verdiğimiz kararlar sayesinde yaparız. Karar alma faaliyetiyle ilgili özel yapıların ve süreçlerin oluşturulması, farklı sesleri susturmayı değil, daha hızlı ve daha iyi kararların alınmasını amaçlar.

Yetki seviyelerinin açık bir şekilde belirlenmesi, şirketin bütün kademelerinde iyi kararların alınması için gerekli altyapıyı oluşturur. Bu da uzun vadeli sürdürülebilir başarının olmazsa olmazlarındandır.

Daha fazla bilgi için

Emilie Williams
Direktör, Risk Danışmanlığı
KPMG Singapur
E: emiliewilliams@kpmg.com.sg

Irving Low
Risk Danışmanlığ Lideri
KPMG Singapur
E: irvinglow@kpmg.com.sg

ERP YATIRIMLARININ

etkinliğini artırmak

Şirketler ERP (Kurumsal Kaynak Planlaması) projelerine büyük miktarlarda zaman, çaba ve mali kaynak ayırarak yatırım yapıyor veya yapmayı planlıyor. Yapılan yatırımdan beklenen getirinin elde edilmesi genellikle uzun yıllar alıyor. Bu gecikmenin nedenlerinden biri, temel ERP fonksiyonlarının ötesine geçilememesidir. Bu da temel fonksiyonların ötesine geçmeyi sağlayacak etkin bir proje yönetiminin olmadığını gösterir.

Günümüzde ERP proje ekipleri hala temel ERP fonksiyonlarına odaklanıyor, uygulama faaliyetlerinin takvim kısıtları ve bütçe sınırları dahilinde gerçekleştirilmesine öncelik veriyor. Bu taktiksel yaklaşım, önemi proje hayata geçirildikten sonra anlaşılan risk ve kontrol sorunlarına yol açıyor. Finansal raporlama kurallarına uyma konusundaki eksikliklerin giderilmesi ve Kimlik Yönetimi sayesinde BT maliyetlerinin düşürülmesi gibi faydalar gereksiz yere gecikiyor. Şirketler ERP çözümü hayata geçirildikten sonra denetimin önemini ve verdikleri ödünlerin büyüklüğünü anlıyor ve gerekli düzeltmeleri yapmak için geriye yönelik iyileştirme projeleri başlatmak zorunda kalıyor. Bu projeler ise işlerin yürüyüşünü aksatıp, kat kat fazla maliyete neden oluyor ve zaman alıyor.

Kurumların ERP yatırımları ile ilgili beklentileri yüksektir. Başarılı bir ERP projesi, süreçlerin hızlandırılmasını ve maliyetlerin düşürülmesini sağlayacaktır. ERP'lerin potansiyel getirisi çok yüksek olmakla beraber, yönetimin beklentilerini tam olarak karşılayabilmeleri için güçlendirilmeleri gerekir. Bu beklentiler arasında şu hedefler sayılabilir:

- Operasyonel Risklerin Azaltılması
- Süreç Etkinliğinin ve Verimliliğinin Artırılması
- Gelirlerin Artırılması ve/veya Maliyetlerin Düşürülmesi

ERP'yi Güvenceye Almak

KPMG üye firmaları, şirketlerin bu hedeflere ulaşmalarına yardımcı olmak için ERP güvenliği ve kontrolleri konusunda ERP'yi Güvenceye Almak adı altında kendi yaklaşımını geliştirmiştir. KPMG'nin ERP'yi Güvenceye Almak yaklaşımı, ERP güvenliği ve kontrollerini her açıdan ele alan bir yaklaşımdır ve sektör lideri şirketlerin, ERP kullanıcılarına gerekli yetkileri vermek ve bunu yaparken hassas veri ve işlemleri korumak şeklindeki birbirinden çok farklı iki hedef arasında dengeyi tutturmalarına yardımcı oluyor.

ERP'yi Güvenceye Almak yaklaşımı, güvenlik ve kontrolle ilgili dört ana alanı kapsıyor:

1 Gelişmiş Kontroller

2 Uygulama Güvenliği

3 Veri ve Altyapı

4 Kullanıcı Erişimi Yönetimi

Alan: Gelişmiş Kontroller

Gelişmiş Kontroller, programdaki kontrolleri iş süreçleri ile uyumlu hale getirmeye odaklanır. Program kontrollerinin bir kısmı fabrika ayarı şeklinde önceden tanımlanmış kontrollerdir. Bunun yanı sıra mevcut kontrolleri destekleyen veya programda yer almayan yenilerini eklemeyi sağlayan ilave özellikler de mevcuttur.

Gelişmiş Kontroller: Kilit Ticari Amaçlar

Temel iş süreçlerinin ötesine geçen ilave özellikler eklenmezse, ERP yatırımlarının getirisi yönetimin beklentilerinin gerisinde kalır. Bu ilave özellikler genellikle şu alanlara yöneliktir:

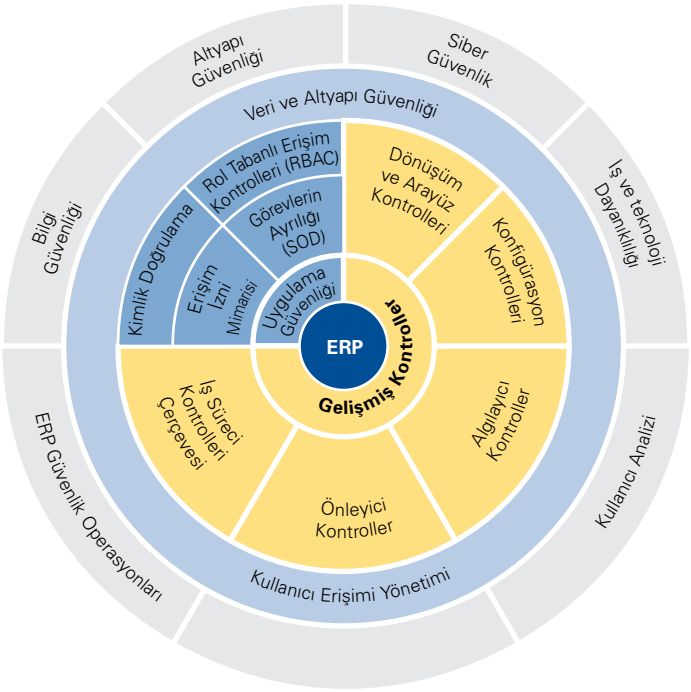
- karmaşık veya verimsiz ERP merkezli süreçlerin iyileştirilmesi
- gelir kaybı
- nakit açığı
- yüksek yapılandırma ve bakım maliyetleri
- hassas işlemlerde daha fazla şeffaflık
- yolsuzluk ve hata riskini azaltmak

ERP uygulanırken, bu konulara yönelik program özellikleri ve kontrolleri genellikle proje uygulamaya geçtikten sonra tamamlanacak ertelenmiş özellikler listesine dahil edilir.

İleri Kontroller: Odak ve Kapsam

İleri Kontroller, yönetimin iş süreçlerini ve belgelendirilmiş kontrollerini etkin ve verimli bir şekilde destekleyecek bir programın oluşturulmasına odaklanır. Bu hedef dahilinde aşağıdaki faaliyetler gerçekleştirilir:

- manuel kontrollerin, ERP programındaki kontrollerin ve otomatik kontrollerin düzenlenmesi amacıyla şirketin iş süreci kontrolleri çerçevesini güncellemek
- manuel süreçleri mümkün olduğunca otomatize bir hale getirmek



Kaynak: GRC Gündemi, Ocak 2016, KPMG International

- süreç risklerini azaltmak için otomatik ve önleyici kontrolleri kullanmak
- hassas işlemleri ve veri değişikliklerini takip etmek için otomatik algılayıcı kontrolleri kullanmak
- yapılandırma ayarlarındaki ve ana verilerdeki değişiklikleri takip etmek ve bunları referans ERP belgeleri ile karşılaştırmak için yapılandırma yönetimini iyileştirmek
- etkin ve verimli dönüştürme ve arayüz kontrolleri oluşturmak ve uygulamak
- kullanıcıların görevlerin ayrılığı ile ilgili sorunlarını incelemek, raporlamak ve çözüme kavuşturmak

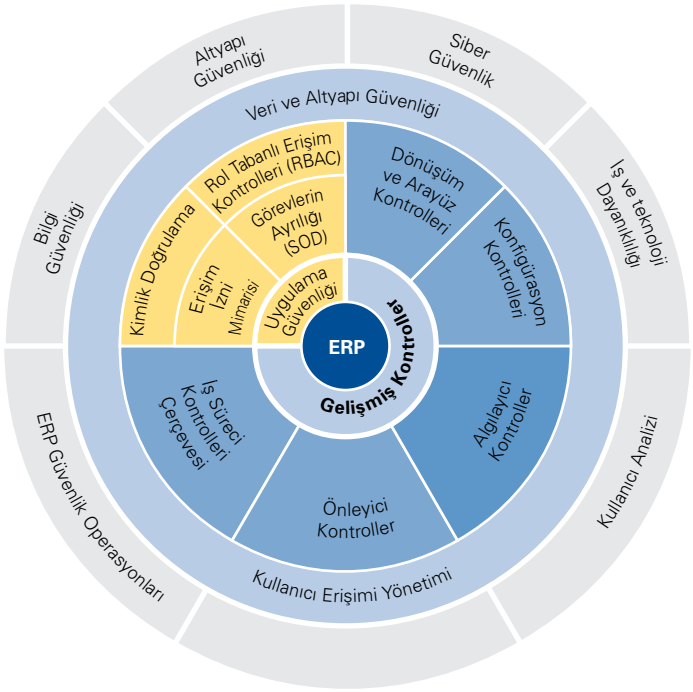
Gelişmiş Kontroller: Elde Edilen Katma Değer

Programın gelişmiş kontrollerinin yönetilmesinin yaratacağı en önemli katma değer, şirketin ERP yatırımını daha fazla kullanmasıdır. Gelişmiş kontroller kullanıldığında bunun dışında aşağıdaki faydalar da elde edilecektir:

- otomatik kontrollerin daha fazla kullanılması
- yapılandırma yönetimi programının daha etkin hale gelmesi
- mevzuata uygunluk programının daha etkin hale gelmesi

Alan: Uygulama Güvenliği

Uygulama güvenliği kontrolleri konusunda birçok şirket sıkıntı yaşıyor. En sık karşılaşılan sorunlardan biri, tanımlanan rol ve sorumlulukların kullanıcılara gereğinden fazla erişim hakkı vermesidir. Bir başka sorun ise, şirket yeniden yapılandırmaya gittiğinde veya başka bir şirketle birleştiğinde, yeni pozisyonlar



Kaynak: GRC Gündemi, Ocak 2016, KPMG International

için yeni roller ve sorumluklar tanımlama ihtiyacının ortaya çıkmasıdır.

Kullanıcı tepkisini ölçmek amacıyla programdaki rol ve sorumluluklara son halinin verilmesinin geciktirilmesi bir başka sorundur. Sonrasında da rol ve sorumluluklar sadece ticari işlemlerin tamamlanmasını desteklemek için geliştirilir. Şirketin görevler ayrılığı politikasına uyulup uyulmadığını incelemek amacıyla güvenlik tasarımının detaylı bir şekilde incelenmesi, proje uygulamaya geçtikten çok sonra gerçekleştiriliyor.

Uygulama Güvenliği: Ticari Amaçlar

Uygulama güvenliğinin en önemli amacı, şirket sistemine erişimin şirket politikalarına uygun bir şekilde gerçekleşmesini ve sürdürülebilir bir şekilde kontrol edilmesini sağlamaktır. Uygulama güvenliği şu konuları kapsar:

- çalışanların programdaki uygulamalara erişimi
- hassas ERP işlemlerine ve verilerine erişimin sadece yetkili kişilerle sınırlandırılması
- yolsuzluk ve hata riskinin azaltılması
- karmaşık mevzuata uygunluk konularının etkin bir şekilde yönetilmesi

Uygulama Güvenliği: Odak ve Kapsam

Uygulama güvenliğinin temelinde yetkilendirme ve kimlik doğrulama kavramları vardır. Kimlik doğrulama, hangi kullanıcı hesabının hangi gerçek kişi ile ilişkilendirildiğini programdaki bütün uygulamaların anlaması demektir. Kimlik doğrulamada, tek girişle birden fazla uygulamaya erişme ve programa giriş için birden fazla güvenlik işaretinin kullanılması hedeflenir.

Yetkilendirme, her bir kullanıcı hesabına hangi yetkilerin verildiğini anlatan bir kavramdır. Yetkilendirme aşağıdaki parçalardan oluşur:

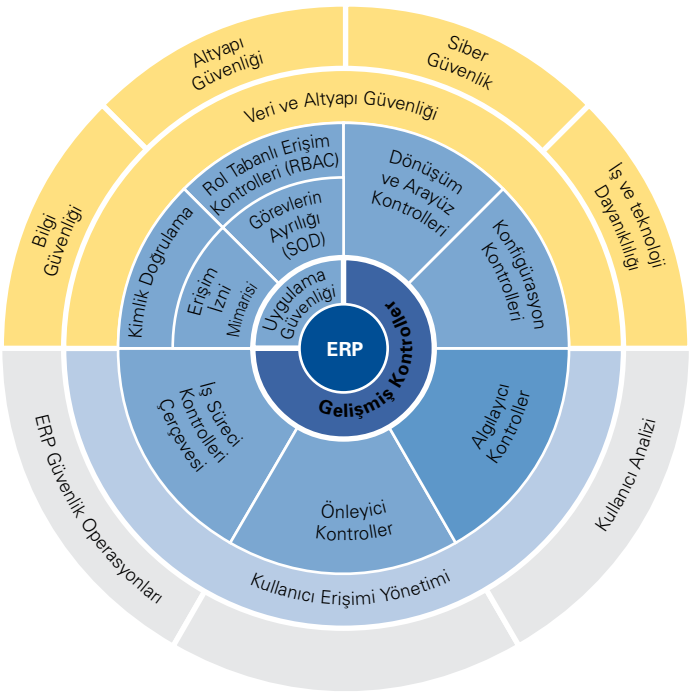
- Rol tabanlı erişim kontrolü
- Kullanıcı özelliklerine göre dinamik erişim
- Fonksiyon güvenliği - ERP'ye işlem seviyesinde erişim
- Veri güvenliği - kilit verilere erişim
- Operasyonel görevler ayrılığı çerçevesi

Uygulama Güvenliği: Elde Edilen Katma Değer

Uygulama Güvenliği'nin yaratacağı katma değer, programa erişimle kullanıcıların iş tanımlarının birbiriyle daha uyumlu hale getirilmesidir. Bu uyum, güvenlik tasarımının bakımı düzenli olarak yapıldığında, kullanıcı yönetimi maliyetlerini de düşürecektir. Ayrıca Uygulama Güvenliği, uyum çerçevesinin sürdürülebilirliği açısından da son derece önemlidir.

Alan: Veri ve Altyapı Güvenliği

Son zamanlarda resmi kurumlarda ve büyük şirketlerde yaşanan büyük veri hırsızlığı olayları, şirketleri dış güvenlik konusuna daha fazla eğilmeye zorlamıştır. Bu veri ihlalleri sonrasında şirketler, verilerinin nerede depolandığı, hangi kanallarla iletildiği ve veri bütünlüğünün, doğruluğunun ve güvenliğinin nasıl sağlandığı konularında daha hassas davranmaya başlamıştır. Dış çevre ve veri kontrolleri, şirketin ve müşterilerinin gizli bilgilerinin ve ticari sırlarının korunması açısından son derece önemlidir.



Kaynak: GRC Gündemi, Ocak 2016, KPMG International

Veri ve Altyapı: Ticari Amaçlar

Günümüzde şirketlerin işleyişinde her şey birbirine bağlı olduğu için, altyapı ve veri güvenliğine yönelik en büyük tehdit, verilere dışarıdan yetkisi olmayan kişilerin erişmesi ve bilgi hırsızlığıdır. Veri ihlali ve hırsızlığı, şirketin içinden de kaynaklanabilir. Söz konusu ihlaller saldırı ve sızma faaliyetleri sonucu ortaya çıkabileceği gibi, basit sosyal mühendislik yöntemleriyle de gerçekleştirilebilir.

Veri ve altyapı güvenliğine yönelik tek tehdit veri hırsızlığı değildir. Şirketler küreselleştikçe, internet erişiminin ve çevrimiçi sistemlerin kalitesi ve sürekliliği de gittikçe daha önemli hale geliyor. Teknoloji arızalarından kaynaklanan kopmalar, kısa süreli de olsalar gelirler üzerinde olumsuz etki yapabilir.

Veri ve Altyapı: Odak ve Kapsam

Veri ve altyapı güvenliğinde en önemli unsurlar şunlardır:

- Veri koruma programı: Şirketler hassas verilerinin nerede depolandığını ve ne şekilde iletildiğini anlamak ve veri maskeleme, veri tabanının ve ağların güçlendirilmesi ve güvenlik açığı yönetimi gibi kontrolleri gerekli yerlerde ve gerektiği seviyede kullanmak zorundadır.
- Siber güvenlik programı: Şirketlerin savunma hatları oluşturması, siber faaliyetleri takip etmesi, ihlalleri kısa sürede tespit etmesi ve acil durum protokollerini etkin bir şekilde devreye alabilmesi gerekir.
- İş ve Teknoloji Dayanıklılığı programı: Şirket işleyişindeki aksamalar şirketlere büyük zarar verebilir. Bu aksamalar sadece kullanılan teknolojiyi değil, şirketin tamamını etkileme potansiyeline sahiptir. Bu alanda kullanılan yöntemlerden bazıları sistem performans takibi, saldırı sonrası yeniden toparlanma prosedürleri, iş sürekliliği yönetimi, sürekli erişim altyapısı ve kriz yönetimidir.
- Yönetici hesaplarının yönetimi: Sistem yöneticisi hesaplarının doğru bir şekilde yönetilmesi şirket verilerinin güvenliğini sağlamak açısından son derece önemlidir.

Veri ve Altyapı: Elde Edilen Katma Değer

Veri ve altyapı güvenliğinin ürettiği en önemli katma değer, ERP varlıklarının korunmasını sağlayan risk-temelli bir bilgi güvenliği programının oluşturulmasıdır. Bu program ayrıca mevzuata uygunluk inisiyatifinin daha etkin olmasına da katkı sağlar.

Alan: Kullanıcı Erişimi Yönetimi

Kullanıcı yönetiminin etkin bir şekilde yapılması, şirketlerin uzun yıllardan beri üzerine eğildiği bir konudur. On beş yıl önce, dot-com balonunun tepe noktasında, şirketler kimlik yönetimi ve kullanıcı erişimi alanlarında büyük yatırımlar yapmaktaydı. Bu yatırımlar ilk zamanlarda erişim sağlama maliyetlerinin nasıl düşürülebileceği üzerine odaklanıyordu. Sonrasında ise şirketler kurum genelinde kullanıcı erişimi istatistiklerini anlamak ve raporlamak konusunda zorluklar yaşadı.

Kullanıcı Erişimi Yönetimi: Ticari Amaçlar

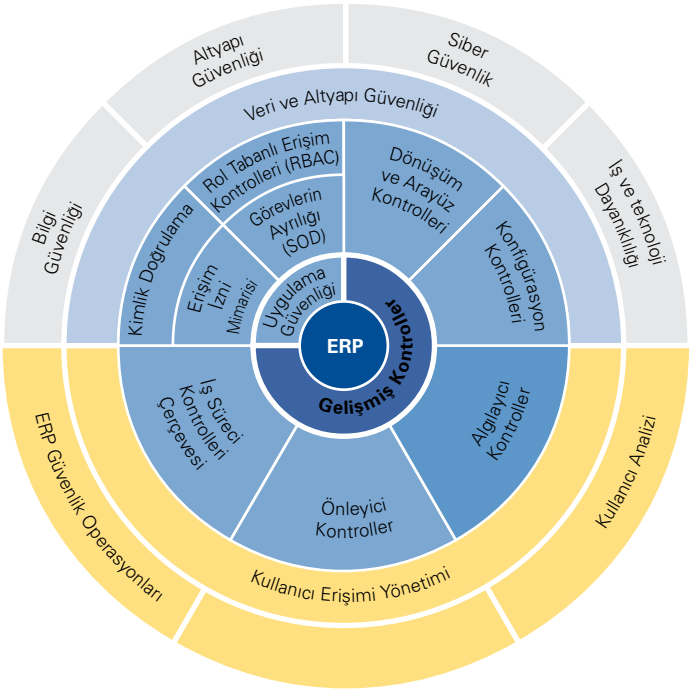
Kullanıcı erişimi yönetiminin arkasındaki en önemli ticari amaçlar şunlardır:

- Maliyetlerin düşürülmesi:
  - Şirketler hesap yönetimi işlemlerinin maliyetini düşürmeye çalışıyor. Baştan iyi tasarlanır ve düzenli olarak bakım gerçekleştirilirse, kullanıcı hesaplarının yönetimini büyük oranda kendi kendine işleyen dinamik bir faaliyet haline getirmek mümkündür.
  - Kullanıcı erişiminin raporlanması da çok zaman alan ve yüksek maliyetli bir iştir. Kurum genelinde kullanıcı erişimi verilerinin toplanması ve analizi otomatik hale getirildiğinde, maliyetler düşecek ve üretilen raporların güvenilirliği artacaktır.
- Kullanıcı faaliyetleri: ERP'deki ticari işlemleri takip edebilmek için şirketlerin kullanıcı erişimi konusunda kaliteli verilere sahip olmaları gerekir. Bunun yanı sıra, kurum genelinde yönetici yetkileriyle donatılmış kullanıcıların faaliyetleriyle ilgili yeterli kontrollerin de olması gerekir.

Kullanıcı Erişimi Yönetimi: Odak ve Kapsam

Kullanıcı erişimi yönetimindeki en önemli husus, iyi tasarlanmış politika ve prosedürlere ve sağlam bir teknolojik altyapıya sahip olmaktır.

- Politika ve prosedürler: Kullanıcı erişimi yönetiminde başarılı şirketler, organizasyon yapısı, kurumsal yönetim, raporlama, kurum genelinde ve kullanıcı özelinde görevler ayrılığı, ERP kontrolleri stratejisi ve düzeltme süreçleri konularında iyi tasarlanmış politika ve prosedürlere sahiptir.



Kaynak: GRC Gündemi, Ocak 2016, KPMG International

- Yeni imkanlar sunan teknolojiler: Kullanıcı erişimi yönetimi konusunda başarılı olan şirketler, aşağıdaki özelliklerin birçoğuna sahiptir: Kayıt, self servis, kullanıcı hesaplarının onay süreci sonrasında otomatik olarak oluşturulması, şifre yönetimi, hesap doğrulama.

Kullanıcı Erişimi Yönetimi: Elde Edilen Katma Değer
Kullanıcı erişimi yönetiminin ürettiği en önemli katma değer, ERP kullanıcı yönetiminin daha düşük maliyetle ve daha etkin bir şekilde gerçekleştirilmesidir. Kullanıcı erişimi yönetiminin başarılı olması ayrıca uyum programının da daha başarılı olmasına katkı sağlar.

ERP Yolculuğunu Güvenceye Almak

KPMG'nin ERP'yi Güvenceye Almak yöntemi, şirketlerin ERP'nin tam olarak sağlayamadığı ilave hedeflere ulaşmasına yardımcı olur. Şirketlerin ERP'yi Güvenceye Alma yolculuğu, yapılan bir atölye çalışmasıyla başlar. Bu atölye çalışmasında müşteriye ERP'yi Güvenceye Almak modelinin farklı yönleri hakkında bilgi verilir. Daha sonra müşterinin kendi programını hemen başlatması için gereken destek verilir ve ön hazırlık niteliğindeki faaliyetlerden optimize edilmiş ve kendi kendine yürüyen kontrollere kadar olan süreçte rehberlik sağlanır.

Kaynak: GRC Gündemi, Ocak 2016, KPMG International

Örnek Olay - Sanayi Üretimi

Yüksek teknolojili üretim yapan şirketlerde şirket dışına çıkarılması sakıncalı bilgilerin olması sıkça rastlanan bir durumdur. Bu şirketler söz konusu bilgilerin nerede saklanacağı ve bu bilgilere kimlerinin erişiminin olacağı konularında bazı zorluklarla karşılaşıyor. Bu zorluk program kontrolleri, altyapı güvenliği, siber güvenlik, kullanıcı güvenliği ve kullanıcı yönetimi gibi çok sayıda alanı ilgilen çok boyutlu bir sorundur. KPMG yakın zamanda ERP'yi Güvenceye Almak yaklaşımını kullanarak, yüksek teknolojili üretim yapan bir şirketin dışarı çıkarılması yasak bilgilerini yönetmesine yardımcı olmuştur.

Daha fazla bilgi için

Laeeq Ahmed
Danışmanlık Hizmetleri Başkanı
GRC Teknolojileri, KPMG ABD
E: laeeqahmed@kpmg.com

Brian Jensen
Çözüm İlişkileri Direktörü
Piyasa Uygulamaları Merkezi,
KPMG ABD
E: brianjensen@kpmg.com

GRC ve

FİLM SANATI

Filmler bizi bir yolculuğa çıkarır, dünyaya farklı bir açıdan bakmamızı ve farklı şeyler görmemizi sağlar, bize farklı duygular yaşatır. Ancak bu "sanat" bir yönüyle diğer bütün sanatlardan ayrılır. Film yapımı için ileri teknolojilerin kullanılması, birçok paydaşın işbirliği içinde ve belirli rutinlere uyarak çalışması ve dikkatli bir mali planlama yapılması gerekir. Bütün bunlar bir sanat dalı olarak filmi film yapan ve sürekliliğini sağlayan unsurlardır. Aynı şekilde GRC de bir yolculuktur; dikkatli bir planlama yapılmasını, birçok iş biriminin işbirliği içinde çalışmasını, farklı süreçlerin bir araya gelmesini ve programın işleyişi ve sürekliliği için bir teknolojik altyapının olmasını gerektirir.

Film konusunda kısa bir süre eğitim almış biri olarak, söz konusu sanatın temel prensiplerine uymadığım için dıştan basit gözüken birçok "çekim"de başarısızlık yaşadım. Ancak, tecrübeli bir GRC yöneticisi olarak, bütün denemelerde yaptığım hataları ve eksiklikleri, ileride tekrarlamamak için, düzenli bir şekilde kaydettim. Aşağıda belirtilen temel prensiplere uyduğunuz takdirde GRC yolculuğunuz daha başarılı geçecektir.

GRC Vizyonuna Sahip Olmak

Öncelikle ulaşmak istediğiniz hedefi belirleyin. GRC vizyonunuzun (sıkça yapıldığı üzere) aracın kendisine değil uygulamaya odaklanması için, bir GRC stratejisi geliştirin ve üst seviyeli, uygulamaya yönelik bir yol haritası belirleyin. Vizyon, projenin şirket açısından değerini açık bir şekilde dile getirmeye yardımcı olur. "Etkin" [risk yönetimi], "verimli" [risk takibi] veya "standart" [güvence süreçleri] gibi eyleme yönelik ifadeler kullanın. Bunun yanı sıra, GRC'nun geniş bir şekilde benimsenip kullanılmasını sağlamak için, vizyona eşlik edecek yol gösterici prensipler belirleyin. Planlama çalışması ayrıca şirketin önündeki zorlukları

anlamasına ve aracı kendisine uydurmaktansa gerekli değişimi gerçekleştirme iradesini göstermesine yardımcı olacaktır. Buna ilave olarak, risk/güvence süreçlerinin hangi seviyede olduğunu ölçün ve birleştirilmiş bir GRC platformuna taşınmaya hazır olup olmadığını değerlendirin. Bütün bunlar GRC'nin başarılı ve etkin bir şekilde uygulanmasına katkı sağlayacaktır.

Sadece Otomasyon Değil, Entegrasyon

GRC, entegrasyon ve birleştirme yoluyla risk ve kontrol denetiminin maliyetini düşürüp etkinliğini artırıyor. GRC entegrasyonunun amacı, risk, kontrol ve sorunların aynı şekilde sınıflandırılmasını sağlamak da dahil olmak üzere birimler arasındaki geleneksel sınırları ortadan kaldırarak, bu parçalı yapının yerine tek bir risk yaklaşımı geliştiriyor. Bu sayede farklı denetim birimleri risk bilgilerini daha iyi kullanabilecek, ortak bir çerçeve kullanarak öncelikli riskleri belirleyebilecek ve en önemlisi, üst yönetime, yönetim kuruluna ve diğer paydaşlara ortak bir risk haritası sunabilecektir.

Bugün GRC süreçlerine sahip olan şirketler de bu süreçleri inceleyerek örtüşen yönleri tespit etmeli, fazlalıkları ortadan kaldırmalı ve mevcut uygulamaların işlevlerinden en iyi şekilde yararlandıklarından emin olmalıdır.

GRC entegrasyonunun amacı, risk, kontrol ve sorunların aynı şekilde sınıflandırılmasını sağlamak da dahil olmak üzere birimler arasındaki geleneksel sınırları ortadan kaldırmak ve bu parçalı yapının yerini alacak tek bir risk yaklaşımı geliştirmektir.

Değişimi Planlamak

GRC uygulaması bir değişim projesidir ve diğer değişim projelerinde olduğu gibi, başta işleyişi değiştirdiği için şüpheyle karşılanacak, zamanla daha iyi anlaşılacak ve en sonunda resmi olarak benimsenecektir. Ancak bu ilerleme kendiliğinden olmaz. Bunun için değişime direnenlerin olacağını baştan kabul etmek ve bu durumla baş etmek için kapsamlı bir bilgilendirme ve iletişim planı hazırlamak gerekir. GRC programının hedeflerine ulaşması için düzenli bir iletişim ve eğitim faaliyetinin gerçekleştirilmesi şarttır, dolayısıyla GRC yol haritasında değişim yönetimine ayrı bir başlık açılarak yer verilmesi son derece önemlidir. Paydaşlar uygulama aşamalarının nasıl ilerleyeceği ve kendi günlük işlerinin nasıl etkileneceği konusunda belirsizlik yaşayabilir. Bazıları GRC'yi kendilerine yönelik bir tehdit olarak da algılayabilir. Bu sorunu çözebilmek için paydaşların düşüncelerinin anlaşılması, projeye olan destek seviyelerine göre sınıflandırılması ve her grup için ayrı bir değişim yönetimi stratejisinin uygulanması gerekir. Nihai kullanıcılarla sürekli irtibat halinde kalmak için sık sık iletişim kurulmalı ve toplantı, intranet, e-posta, dar katılımlı görüşme ve eğitim programı gibi farklı kanallar kullanılmalıdır.

Erken Sonuç Almak ve Başarıyı Duyurmak

Başarıyı duyurmak başarının sürekliliği açısından son derece önemlidir ve bu durum GRC uygulamaları için de geçerlidir. Başka hiçbir etkisi olmasa bile olumlu bir mesaj verilmiş olur ve programa olan direnci azaltır. Erken sonuç alabilmek için, ilk uygulamayı SOX veya İç Denetim gibi nispeten gelişmiş bir süreç üzerinde yapın. Bu süreçlerde, (kurumsal hiyerarşi ve ortak terminoloji gibi) yapısal unsurlar ile entegrasyon ve birleşme noktaları gibi konularda geniş bir tartışmayı başlatacak raporlama standartları, üzerinde düşünülmüş risk ve kontroller ve istikrarlı ve resmi iş akışları zaten mevcuttur.

Geleceği İnşa Etmek

Konuya geniş bir açıdan yaklaşın ve kontrol ve uyum fonksiyonlarını birleştirmenin dışında ne gibi ilave faydaların getirilebileceğini, başka hangi fırsatların olduğunu anlamaya çalışın. Örneğin, satıcı riski gibi geleneksel olmayan süreçleri de programa dahil etmeyi düşünebilirsiniz. Paydaş havuzu ne kadar geniş olursa GRC programının temeli de o kadar sağlam olacak ve program daha sürdürülebilir olacaktır.

Son olarak, sinema sanatından alabileceğimiz önemli bir derse dikkat çekmek istiyorum: Son 125 yılda hem teknolojide hem de sektörde yaşanan büyük değişimlere rağmen sinema başarılı bir şekilde gelişimini sürdürmüştür ve halen de gelişmeye devam ediyor. GRC programı da sürekli kendini yenileyerek şirketin iş ortamındaki veya iş modelindeki değişimlere ayak uydurmayı bilmelidir.

Saygılarımla,
Deon Minnaar, KPMG ABD

İletişim

İdil Gürdil
Risk Yönetimi
Danışmanlığı, Şirket Ortağı
E : igurdil@kpmg.com

Naciye Kurtuluş
İç Denetim, Risk ve Uyum
Hizmetleri, Direktör
E : nkurtulus@kpmg.com

kpmg.com.tr

Download on the App Store

ANDROID APP ON Google play