IIA
ULUSLARARASI İÇ DENETÇİLER ENSTİTÜSÜ

IIA POZİSYON RAPORU:

İÇ DENETİMİN

KURUMSAL RİSK YÖNETİMİNDE

OYNADIĞI ROL

Giriş

Riskleri yönetmenin kuvvetli kurumsal yönetişim açısından önemi giderek daha fazla anlaşılmakta ve kabul görmektedir. Kurumlar, yüz yüze kaldıkları iş risklerinin tamamını (sosyal, etik ve çevresel riskler ve mali ve operasyonel riskler) tanımlama ve bu riskleri kabul edilebilir bir seviyede tutacak şekilde nasıl yönettiklerini açıklama baskısı altındadırlar. Bu arada, kurumlar risk yönetimi konusundaki daha az eşgüdümlü yaklaşımlara kıyasla bu çerçevelerin avantajlarını fark ettikçe ve anladıkça, kurumsal risk yönetimi çerçeveleri daha da genişlemiş ve büyümüşlerdir. İç denetim, riskin yönetilmesine, hem güvence hem de danışmanlık rolleri ve görevleriyle ve çeşitli yollarla katkıda bulunur.

Kurumsal Risk Yönetimi (KRY) Nedir?

İnsanlar, her tür ve her tipte olayları veya durumları tanımlamak, değerlendirmek, yönetmek ve kontrol altına almak gayesiyle risk yönetimi faaliyetlerine girişirler. Bu olay ve durumlar, tek projelerden ya da piyasa riski gibi dar tanımlanmış risk tiplerinden kurumun bir bütün olarak karşı karşıya olduğu tehditlere ve fırsatlara kadar çok değişik konuları kapsayabilirler. Bu makalede sunulan prensipler, iç denetimin her çeşit ve tipte risk yönetimine katılmasında kılavuz olarak kullanılabilirler, fakat bir kurumun yönetişim süreçlerini bu yolla geliştirme olasılığı ve imkanı bulunduğundan dolayı, biz özellikle kurumsal risk yönetimiyle ilgileniyoruz.

Kurumsal risk yönetimi (KRY), kurumun hedeflerine ulaşmasını etkileyen fırsatlar ve tehditlerin tespit edilmesi, tanımlanması, değerlendirilmesi, bunlara verilecek yanıtların kararlaştırılması ve bunların rapor edilmesi için tüm kurum çapında uygulanan, özel yapılandırılmış, istikrarlı, tutarlı ve kesintisiz bir süreçtir.

KRY Sorumluluğu

Risklerin yönetilmesinin genel sorumluluğu yönetim kuruluna aittir. Pratikte, yönetim kurulu, risk yönetim çerçevesinin yönetimi ve işletimini aşağıda sayılan görev ve etkinlikleri ifa etmekten sorumlu olacak bir yönetim ekibine devreder. Bu faaliyetleri koordine eden ve proje bazında yöneten ve gereken uzmanlık becerileri ve bilgi birikimini sağlayan ayrı bir bölüm veya fonksiyon da bulunabilir.

Başarılı bir kurumsal risk yönetiminde normalde kurum içindeki herkesin bir rolü ve görevi vardır, fakat riskleri tanımlama ve yönetme sorumluluğu özel olarak kurum yönetimine aittir.

KRY'nin Faydaları

KRY, bir kurumun hedeflerine ulaşmasının önündeki riskleri yönetmesine yardımcı olmak anlamında çok büyük katkıda bulunabilir. Bu faydalar, şöyle sıralanabilir:

* Kurumun hedeflerine ulaşması olasılığının daha fazla olması;
* Bambaşka risklerin yönetim kurulu seviyesinde konsolide rapor edilmesi;
* Temel risklerin ve onların doğuracağı sonuçların daha iyi anlaşılması ve kavranması;
* Çapraz iş risklerinin tespiti, tanımlanması ve paylaşılması;
* Gerçekten önemli olan konulara yönetimin daha fazla odaklanması;
* Daha az sürpriz veya daha az krizle karşılaşılması;

* Doğru işlerin doğru yol ve yöntemlerle yapılması konusuna kurum içinde daha fazla odaklanılması;
* Değişim inisiyatiflerini gerçekleştirme olasılığı ve imkanının artması;
* Daha büyük ödül ve kazançlar için daha fazla risk alabilme yeteneği ve
* Daha çok bilgiye dayanan risk alma ve karar alma süreçleri.

KRY Kapsamında Yer Alan Faaliyetler

* Kurumun hedeflerinin açıkça ifade edilmesi ve bildirilmesi;
* Kurumun risk alma iştahının tespit edilmesi;
* Bir risk yönetim çerçevesi de dahil olacak şekilde uygun bir kurum içi ortamın kurulması;
* Kurumun hedeflerine ulaşmasının önündeki potansiyel tehdit ve tehlikelerin tespiti ve tanımlanması;
* Riskin değerlendirilmesi (tehdidin gerçekleşme olasılığının ve olası etkilerinin değerlendirilmesi);
* Risklere verilecek yanıtların seçilmesi ve uygulanması;
* Kontrol ve diğer yanıt faaliyetlerinin gerçekleştirilmesi;
* Riskler hakkında edinilen bilgilerin kurum içinde tüm kademe ve seviyelere tutarlı bir tarzda bildirilmesi ve açıklanması;
* Risk yönetim süreçleri ve sonuçlarının merkezi olarak izlenmesi ve koordine edilmesi ve
* Risklerin yönetiminin etkinliği hakkında güvence verilmesi.

KRY Konusunda Güvence Sağlamak

Yönetim kurulunun veya dengi yönetim organlarının temel koşullarından ve isteklerinden biri de, risk yönetimi süreçlerinin etkin ve etkili işlemesi konusunda ve temel risklerin kabul edilebilir bir seviyede yönetilmesi konusunda güvence alabilmektir.

Bu güvencenin farklı kaynaklardan sağlanması olasıdır. Bunlar arasında, yönetimden güvence sağlamak hayati önemi haizdir. Bu, iç denetim faaliyeti ve biriminin bir temel kaynak olduğu objektif güvencenin sağlanmasıyla tamamlanmalıdır. Diğer kaynaklar arasında dış denetçiler ve bağımsız uzman incelemeleri sayılabilir. İç denetçiler, normalde üç alan ve konuda güvence sağlarlar:

* Risk yönetimi süreçleri ve bu süreçlerin hem tasarımı hem de çalışması;
* Kontrollerin ve risklere verilen diğer yanıtların etkinliği de dahil, “kritik” olarak sınıflandırılan risklerin yönetilmesi ve
* Risklerin güvenilir ve uygun bir şekilde değerlendirilmesi ve risk ve kontrol statüsü ve durumunun rapor edilmesi.

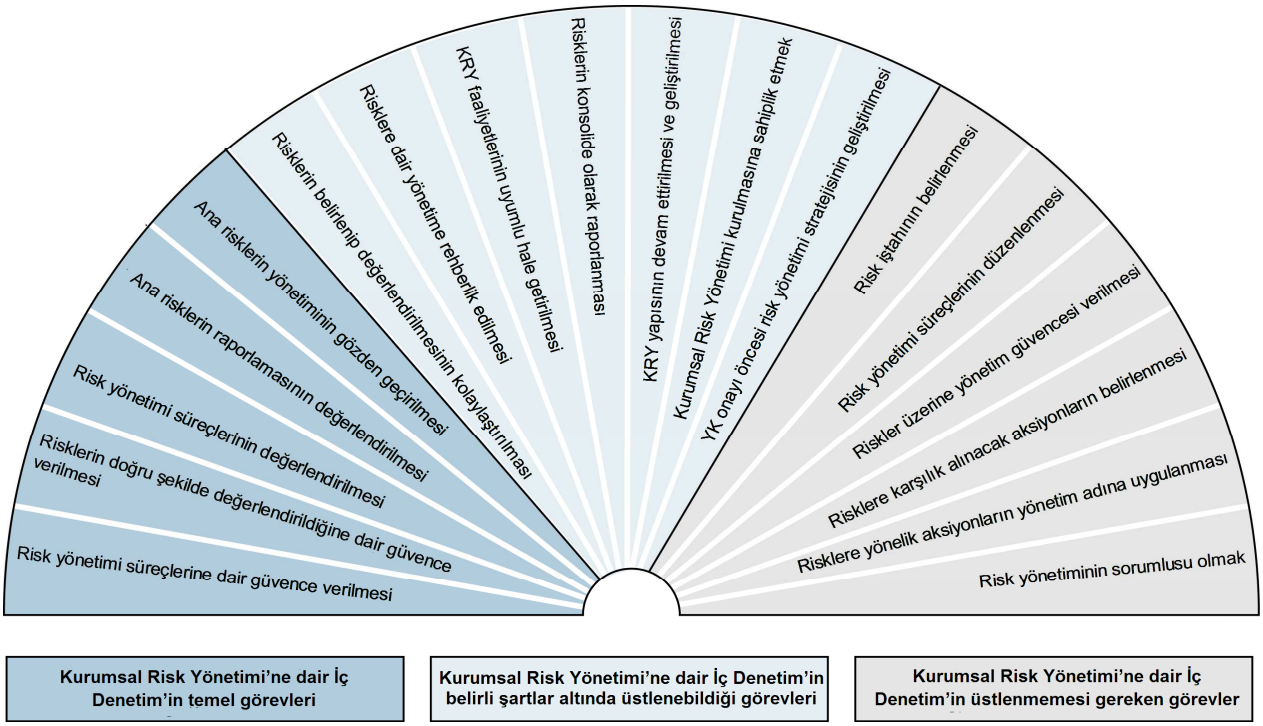
İç Denetimin KRY’deki Rolü

İç denetim; bağımsız ve objektif bir güvence ve danışmanlık etkinliğidir. KRY’ye ilişkin temel rolü ve görevi, risk yönetiminin etkinliği hakkında yönetim kuruluna objektif güvence sağlamaktır. Gerçekten de, araştırmalar, iç denetimin kuruma değer kazandırdığı ve kattığı en önemli iki etkinliğin, büyük iş risklerinin uygun bir şekilde yönetildiği hakkında objektif güvence sağlamak ve risk yönetimi ve iç kontrol çerçevesinin etkin ve verimli çalıştığı

hakkında güvence sağlamak olduğu konusunda iç denetim birimi ve iç denetçilerin mutabık kaldıklarını göstermiştir.[1]

Şekil 1, bir KRY faaliyetleri dizisi sunmakta ve hem bir profesyonel iç denetim biriminin hangi rolleri üstlenmesi gerektiğini hem de en azından onun kadar önemli bir konu olan bir profesyonel iç denetim biriminin hangi rolleri üstlenmemesi gerektiğini göstermektedir. İç denetimin rolünün tespitinde hesaba katılması gereken temel faktörler, bu faaliyetin iç denetim biriminin bağımsızlığına ve objektifliğine yönelik bir tehdit oluşturup oluşturmadığı ve kurumun risk yönetimi, kontrol ve yönetişim süreçlerini geliştirme olasılığının mevcut olup olmadığı faktörleridir.

Şekil 1 – İç Denetimin KRY'deki Rolü



Şekil 1'in sol tarafında gösterilen faaliyetlerin tamamı güvence faaliyetleridir. Bunlar, risk yönetimi hakkında güvence sağlamak olarak ifade edilebilecek daha geniş hedefin bir parçasıdır. *İç Denetimde Uluslararası Mesleki Uygulamalar Çerçevesi'ne (Standartlar)* uyan bir iç denetim birimi, bu faaliyetlerin en azından bir kısmını yapabilir ve yapmalıdır.

[1] The Value Agenda (Değer Gündemi), Uluslararası İç Denetçiler Enstitüsü – İngiltere ve İrlanda ve Deloitte & Touche 2003.

İç denetim, bir kurumun yönetişim, risk yönetimi ve kontrol süreçlerini geliştiren danışmanlık hizmetleri sağlayabilir. Bir iç denetçinin KRY'ye başvurma ölçüsü ve kapsamı, hem yönetim kurulunun erişebileceği diğer iç ve dış kaynaklara hem de kurumun risk olgunluğuna[2] bağlıdır ve bu ölçü ve kapsamın zaman içinde değişmesi de olasıdır. İç denetçinin riskleri değerlendirme ve riskler ile yönetişim arasındaki bağları kavrama ve amaca ulaşmayı fasilitasyon konularındaki uzman olması, iç denetim biriminin özellikle erken aşamalarında KRY için lider olarak ve hatta proje müdürü olarak görev yapmaya ehil ve kalifiye olduğu anlamına gelir. Kurumun risk olgunluğu arttıkça ve risk yönetimi işletmenin operasyonlarına daha fazla gömüldükçe, iç denetimin KRY'ye liderlik yapma rolü azalabilir. Benzer şekilde, bir kurum bir risk yönetim uzmanının veya fonksiyonunun hizmetlerinden yararlandığı takdirde, iç denetim biriminin daha fazla danışmanlık faaliyetlerine girmektense güvence rolü üzerinde yoğunlaşarak kuruma değer kazandırması olasılığı ve imkanı daha fazladır. Bununla birlikte, iç denetim birimi, *Şekil 1*'in sol tarafındaki güvence faaliyetlerinin temsil ettiği risk-bazlı yaklaşımı henüz benimsememişse, şeklin ortasında gösterilen danışmanlık faaliyetlerini üstlenmek için yeterince donanımlı olmama olasılığı daha fazladır.

Danışmanlık Rolleri

Şekil 1'in orta bölümü, iç denetim biriminin KRY konusunda üstlenebileceği danışmanlık rollerini göstermektedir. Genelde, iç denetim birimi kadranın sağ tarafına ne kadar fazla girer ve girişirse, iç denetim biriminin bağımsızlığının ve objektifliğinin korunması için gereken koruma önlemlerine o kadar fazla gereksinim duyulur. İç denetim biriminin üstlenebileceği bazı danışmanlık rolleri ve görevleri şunlardır:

* İç denetim biriminin riskleri ve kontrolleri analiz etmek için kullandığı araçları ve teknikleri yönetimin kullanımına sunmak;
* KRY'nin kuruma tanıtılması ve kazandırılmasına, kurumun risk yönetimi ve kontrolü hakkında uzmanlığının yükseltilmesine ve kurumun genel bilgi düzeyinin artırılmasına liderlik etmek;
* Risk ve kontrol konularında tavsiye ve önerilerde bulunmak, atölye çalışmalarında kolaylaştırıcı rol üstlenmek ve kurumu yönlendirmek ve ortak bir dil, çerçeve ve anlayışın geliştirilmesini teşvik etmek;
* Risklerin koordinasyonu, izlenmesi ve raporlanması konusunda merkez nokta olarak işlev göstermek ve
* Bir riski hafifletmenin en iyi yolu ve yöntemini belirleme çabalarında yöneticilere ve müdürlere destek olmak.

Danışmanlık hizmetlerinin güvence rolüne uyumlu ve uygun olup olmadığına karar verirken dikkate alınması gereken kilit faktör, iç denetçinin herhangi bir yönetim sorumluluğu üstlenip üstlenmediğini tespit etmektir. KRY konusunda, iç denetim birimi, risklerin fiili yönetimi – kurum yönetiminin sorumluluğundadır – konusunda herhangi bir rol üstlenmediği sürece ve kurumun üst yönetimi KRY'ye aktif destek ve yardımcı olduğu sürece danışmanlık hizmetleri verebilir. İç denetim birimi risk yönetim süreçlerinin kurulması, oluşturulması veya geliştirilmesinde yönetim ekibine yardımcı olduğu takdirde, iç denetim biriminin çalışma planının bu hizmetlerle ilgili sorumluluğun yönetim ekibinin üyelerine devredilmesi amacına yönelik açık bir strateji ve zaman programı da içermesini öneriyoruz.

[2] IIA-İngiltere ve İrlanda: Risk Bazlı İç Denetim Hakkında Görüş Açıklaması 2003

Koruma Önlemleri

İç denetim birimi, belirli koşulların gerçekleşmesi şartıyla, *Şekil 1*'de gösterildiği gibi KRY konusundaki görevlerini genişletebilir ve artırabilir. Bu koşullar şunlardır:

* Risk yönetimi sorumluluğunun kurum yönetiminde kaldığı açıkça belirtilmelidir.
* İç denetçinin sorumluluk ve görevleri, iç denetim yönetmeliğinde açıkça ifade edilmeli ve denetim komitesi tarafından da onaylanmalıdır.
* İç denetim birimi, herhangi bir riski kurum yönetimi adına yönetmemelidir.
* İç denetim birimi, risk yönetimi kararlarını kendisi almak yerine, kurum yönetiminin karar alma sürecine tavsiye ve önerileriyle ve diğer yollarla destek olmalıdır.
* İç denetim birimi, KRY çerçevesinin kendi sorumluluğunda olan herhangi bir kısmı hakkında objektif güvence de veremez. Bu güvence, uygun uzmanlığa sahip başka taraflarca verilmelidir.
* Güvence faaliyetlerinin ötesindeki iş ve görevler, bir danışmanlık görevi olarak algılanmalı ve bu göreve ilişkin uygulama standartlarına uyulmalıdır.

Beceriler ve Bilgi Tabanı

İç denetçiler ve risk yöneticileri belirli bazı bilgileri, becerileri ve değerleri paylaşırlar. Örneğin, her ikisi de, kurumsal yönetişim koşulları ve gereklerini anlarlar; proje yönetimi, analitik ve fasilitasyon becerileri vardır ve aşırı risk alma veya riskten kaçınma davranışları yerine sağlıklı bir risk dengesi kurmaya değer ve önem verirler. Bununla birlikte, risk yöneticileri sadece kurumun yönetimine hizmet ederler ve denetim komitesine bağımsız ve objektif güvence sağlamaları gerekmez. KRY'deki rollerini genişletmek isteyen iç denetçiler de, iç denetçilerin çoğunun genel bilgi tabanının dışında bulunan (risk transferi ve risk miktar tayini ve modelleme teknikleri gibi) özel bilgi alanlarında risk yöneticilerinin uzmanlığını küçümsememelidirler. Uygun bilgi ve becerilere sahip olmayan bir iç denetçi, risk yönetimi alanında herhangi bir görev veya işlev üstlenmemelidir. Ayrıca, iç denetim birimi başkanı, iç denetim birimi içinde yeterli beceri ve bilgi birikimi yoksa ve bunları başka kaynaklardan da temin edemiyorsa, bu alanda danışmanlık hizmetleri vermeye girişmemelidir.

Sonuç

Risk yönetimi, kurumsal yönetişimin temel ve esaslı unsurlarından biridir. Yönetim kurulu adına risk yönetimi çerçevesini kurmaktan ve işletmekten kurum yönetimi sorumludur. Kurumsal risk yönetimi, özel yapılandırılmış, tutarlı ve eşgüdümlü yaklaşımı sayesinde pek çok faydalar sağlar. İç denetçinin KRY konusundaki temel ve asli rolü, risk yönetiminin etkinliği hakkında hem yönetim kuruluna hem de kurum yönetimine güvence sağlamak olmalıdır. İç denetim birimi, faaliyetlerini bu temel ve asli rolünün ötesine geçirdiği ve genişlettiği takdirde, angajman ve görevlere danışmanlık hizmetleri muamelesini yapmak ve bu konuyla ilgili Standartların tümünü uygulamak da dahil belirli koruma önlemleri almalıdır. Böylece, iç denetim birimi, güvence hizmetlerinin objektifliğini ve kendisinin bağımsızlığını korumuş olacaktır. Bu kısıtlama ve sınırlamalar dahilinde, KRY, iç denetim biriminin profilinin yükseltilmesine ve etkinliğinin artırılmasına yardımcı olabilir.

Terimlerin Tanımları:

Güvence Hizmetleri: Kurum için yönetişim, risk yönetimi ve kontrol süreçleri hakkında bağımsız bir değerlendirme sunmak amacıyla mevcut kanıtların objektif bir gözle incelenmesi işi. Güvence hizmetlerinin örnekleri arasında finansal, performans, uyum, sistem güvenliği ve detaylı teknik inceleme (due diligence) görevleri sayılabilir.

Yönetim Kurulu: Yönetim kurulu terimi, iç denetim yöneticisinin fonksiyonel olarak bağlı olabileceği bir denetim komitesi de dahil, bir kurumun yönetim kurulu veya icra kurulu ya da bir resmi idarenin veya otoritenin başkanı ya da kâr amacı gütmeyen bir kurumun mütevelli heyeti veya guvernörler kurulu ya da kurumun başka görevli organları gibi yönetim organları anlamında kullanılmaktadır.

Lider: Bir kişiyi veya olayı destekleyen ve savunan bir kimse anlamına gelir. Dolayısıyla, bir risk yönetimi lideri, risk yönetiminin faydalarını destekler ve kurumun yönetimi ve personelini risk yönetimi uygulamalarında yapmaları gerekenler hakkında eğitir ve onları bu eylemleri yapmaya teşvik eder ve onlara bu eylemlerinde destek olur.

Danışmanlık Hizmetleri: Niteliği ve kapsamı denetlenen kurumla birlikte kararlaştırılan ve iç denetçi yönetimle ilgili bir sorumluluk üstlenmeksizin kurumun yönetişim, risk yönetimi ve kontrolü süreçlerini geliştirmeyi ve onlara değer katmayı hedefleyen danışmanlık faaliyetleri ve bunlarla bağlantılı hizmet ve faaliyetler anlamına gelir. Bu hizmetlerin örnekleri arasında danışmanlık, tavsiye, fasilitasyon ve eğitim faaliyetleri sayılabilir.

Kontrol: Yönetimin, yönetim kurulunun ve diğer tarafların riski yönetmek için ve belirlenmiş hedef ve amaçlara ulaşma olasılığını artırmak için alabilecekleri önlemler ve yapabilecekleri eylemler anlamına gelir. Hedeflere ve amaçlara ulaşılacağı konusunda makul güvence sağlayabilmek için gereken yeterli eylemleri kurum yönetimi planlar, organize eder ve uygulamayı yönetir.

Kurum: Belirli bir dizi hedefi gerçekleştirmek amacıyla kurulmuş bir kuruluş anlamına gelir.

Kurumsal Risk Yönetimi (KRY): Kurumun hedeflerine ulaşmasını etkileyen fırsatlar ve tehditlerin tespit edilmesi, tanımlanması, değerlendirilmesi, bunlara verilecek yanıtların kararlaştırılması ve bunların rapor edilmesi için tüm kurum çapında uygulanan, özel yapılandırılmış, istikrarlı, tutarlı ve kesintisiz bir süreç anlamına gelir.

Fasilitasyon: Bir grubun (veya bireyin) ilgili toplantı veya etkinlik için kararlaştırılmış bulunan hedeflere ulaşmasını kolaylaştırmak gayesiyle o grupla (veya bireyle) birlikte çaba göstermek ve çalışmak anlamına gelir. Bu çalışma; grubu ve üyelerini dinlemeyi, sınamayı, gözlemlemeyi, sorgulamayı ve desteklemeyi kapsar. Bu çalışma, işi onlar adına yapmak veya onlar adına kararlar almak gibi hususları kapsamaz.

Risk: Hedeflere ulaşmak üzerinde bir etkisi olacak nitelikte bir olayın gerçekleşmesi olasılığı anlamına gelir. Risk, etki ve olasılık açılarından ölçülür.

Risk İştahı: Bir kurumun kabul etmeye ve üstlenmeye istekli olduğu risk seviyesi anlamına gelir.

Risk Yönetim Çerçevesi: Bir kurumun risk yönetim süreçlerini uygulamak için kullanmayı seçtiği yapılar, metodolojiler, prosedürler ve tanımların toplamı anlamına gelir.

Risk Yönetim Süreçleri: Kurumun hedeflerine ulaşması konusunda makul güvence sağlayabilmek amacıyla, potansiyel olayları veya durumları tespit etmek, tanımlamak, değerlendirmek, yönetmek ve kontrol etmek için uygulanan süreçler anlamına gelir.

Risk Olgunluğu: Kurumun hedeflerine ulaşmasını etkileyen fırsatlar ve tehditlerin tespit edilmesi, tanımlanması, değerlendirilmesi, bunlara verilecek yanıtların kararlaştırılması ve bunların rapor edilmesi için yönetimin planlandığı gibi ve tüm kurum çapında sağlam bir risk yönetim yaklaşımı benimseme ve uygulama ölçüsü ve derecesi anlamına gelir.

Risk Yanıtları: Bir kurumun münferit riskleri yönetmek için seçtiği araç ve yollar anlamına gelir. Bunların ana kategorileri, riski tolere etmek; riskin etkisini veya olasılığını azaltacak şekilde davranmak; riski başka bir kuruma veya kuruluşa devretmek ya da riski yaratan faaliyete son vermektir. İç kontroller de, riske cevap verme yollarından biridir.