KAMU KURUMLARINDA RİSK YÖNETİMİ-BİR UYGULAMA ÖNERİSİ

Evren Güncel ERMİSKET
İç Denetçi
SHÇEK Genel Müdürlüğü

ÖZET: *İç kontrol standartları uyarınca kamu idarelerinin, risklerin tanımlanması, değerlendirilmesi ve izlenmesine yönelik bir sistem kurmaları ve işletmeleri gerekmektedir. Risk, kamu idareleri için oldukça yeni bir kavram olup, risklerin tanımlanması ve değerlendirilmesine yönelik uygulamaları yönlendirecek kapsamlı bir mevzuat düzenlemesi de bulunmamaktadır. Öte yandan; risk tanımlama ve değerlendirme faaliyetlerinin, kamu kurumlarının strateji ve hedeflerinin belirlendiği planlama ve programlama süreçlerine entegre bir şekilde yürütülmesi gerekmektedir. Bu sayede strateji ve hedefler, riskler dikkate alınarak belirlenebilecek ve kaynak tahsileri de bu doğrultuda gerçekleştirilebilecektir. Risk yönetiminin, kurum hedeflerinin gerçekleştirilmesinde, kritik düzeyde önem taşıdığı ve iç denetim birimlerinin de öncelikli danışmanlık alanlarından biri olması gerektiği düşünülmektedir.*

ANAHTAR KELİMELER: *İç kontrol, risk yönetimi, COSO İç Kontrol Çerçevesi, COSO Kurumsal Risk Yönetimi Çerçevesi, Faaliyetlerin Belirlenmesi, Amaç ve Hedeflerin Belirlenmesi, Risk Tanımlaması, Risk Değerlendirmesi, Risk-Kontrol Planı*

1. GİRİŞ

Kamu idarelerinde iç kontrol sisteminin oluşturulması, uygulanması, izlenmesi ve geliştirilmesi amacıyla gerekli standartlar, Maliye Bakanlığı tarafından 26.12.2007 tarihli Kamu İç Kontrol Standartları Tebliği ile belirlenmiştir. Kamu idarelerinden öncelikle, standartlara uyum kapsamında yapılması gereken çalışmaları belirleyerek eylem planına bağlamaları istenilmiştir. İç Kontrol Eylem Planında yer alan çalışmaların ise en geç 30.6.2011 tarihinde tamamlanması gerekmektedir.

Kamu İç Kontrol Standartları uyarınca kamu kurumlarının; amaç ve hedeflerinin gerçekleşmesini engelleyebilecek riskleri tanımlaması, analiz etmesi ve alınacak önlemleri belirleyerek eylem planına bağlaması

"Tüm kurumlar, büyüklüğü, yapısı, faaliyet gösterdiği sektör ne olursa olsun, sayısız risk ile karşılaşmakta ve bu riskler, kurumun faaliyetlerinin sürekliliğini, başarısını, finansal durumunu, kamuoyundaki imajını, hizmetlerinin kalitesini ve personelini etkileyebilmektedir"

gerekmektedir. Bununla birlikte; kamu kurumları için risk kavramı oldukça yeni bir kavram, risk değerlendirmesi ise ilk defa gerçekleştirilecek bir faaliyettir. Kurumlara bu konuda yol gösterebilecek rehber bir doküman da bulunmamaktadır. Bütün bunlar birlikte değerlendirildiğinde; pek çok kamu kurumu açısından "Risk Değerlendirme" bileşeni gereksinimlerinin etkin bir şekilde karşılanması mümkün görünmemektedir.

Kurumun risk yönetimi ve kontrol süreçlerinden üst yönetim sorumludur. Bununla birlikte, gerek uluslar arası standartlar gerekse kamu iç denetim standartları uyarınca; İç denetim faaliyeti; risk yönetimi süreçlerinin etkililiğini değerlendirmek ve iyileştirilmesine katkıda bulunmak zorundadır. İç denetçiler, danışmanlık görevleri kapsamında, risk yönetimi süreçlerini kurma ve geliştirmede yönetime yardımcı olabilirler. İç denetçilerin bu süreçteki rolü, kurumun gereksinimleri ve üst yönetimin onayı ile risk yönetimi sürecinin yönetimi ve koordinasyonunu da içeren geniş bir aralıkta belirlenebilmektedir.[1] Kamu kurumlarının gereksinimleri dikkate alındığında risk yönetimi, iç denetim birimlerinin öncelikli danışmanlık alanlarından biri olmalıdır. Bununla birlikte, danışmanlık rolünü üstlenen iç denetçilerin, "riskleri gerçekten yönetmekten" yani yönetim sorumluluğu almaktan kaçınmak zorunda olduğu da unutulmamalıdır[2].

Bu çalışma kapsamında tanıtılacak uygulama önerisi, yukarıda belirtilen ihtiyaçlar nedeniyle hazırlanmıştır. Uygulama önerisinin hazırlanmasında COSO İç Kontrol Çerçevesi yanında, COSO Kurumsal Risk Yönetimi Çerçevesinden de yararlanılmıştır. Bu nedenle öncelikle COSO İç Kontrol Çerçevesinin Risk Değerlendirme Bileşeni ve COSO Kurumsal Risk Yönetimi Çerçevesi hakkında özet bilgi verilerek, risk yönetimi, stratejik planlama ve performans süreçleri arasındaki ilişki değerlendirilecek, sonraki bölümlerde ise uygulama önerisi tanıtılacaktır.

2. COSO İÇ KONTROL BÜTÜNLEŞİK ÇERÇEVESİ

COSO'nun İç Kontrol Bütünleşik Çerçeve Final Raporu ilk olarak 1992 yılında yayımlanmıştır. Bu raporda iç kontrol; Kurumun yönetim kurulu, yöneticileri ve diğer personelinden etkilenen, faaliyetlerin etkinliği ve verimliliği, finansal raporlamanın güvenilirliği, kanun ve düzenlemelere uygunluk hedeflerinin gerçekleştirilmesine yönelik olarak makul güvence sağlamak üzere tasarlanan bir süreç olarak tanımlanmaktadır.[3]

Bu tanım doğrultusunda iç kontrolün üç hedefi aşağıdaki şekilde kategorize edilebilir:

- Faaliyetlerin Etkinliği ve Verimliliği; Kurumun, performans ve karlılık hedeflerini de içeren en temel iş hedefleridir.
- Finansal Raporlamanın Güvenilirliği; Yayınlanan veya kamuya açıklanan her türlü finansal durum raporunun güvenilir bir şekilde hazırlanmasına yönelik hedeflerdir.
- Yasa ve düzenlemelere uygunluk; Kurumun faaliyet alanına yönelik yasa ve düzenlemelere uygunluğa ilişkin hedeflerdir.

İç kontrol birbiri ile ilişkili beş bileşenden oluşur. Bu bileşenler, Kontrol Ortamı, Risk Değerlendirmesi, Kontrol Faaliyetleri, Bilgi ve İletişim ile İzlemedir. İç kontrol bileşenleri, yönetim faaliyetlerinden türetilmiş olup, yönetim süreçlerine entegredir. İç kontrol uygulamaları, işletmelerin büyüklüğüne göre farklılık gösterse de, bileşenler tüm kurumlarda uygulanabilir niteliktedir.

Risk Değerlendirme

İç Kontrol Bütünleşik Çerçeve Final Raporunun 3. Bölümü Risk Değerlendirme Bileşenini düzenlemek-

1 Uluslar arası İç Denetim Standartları, Uygulama Önerisi 2120-1

2 Uluslar arası İç Denetim Standartları, Performans Standartları, 2120-C3

3 COSO, "Internal Control Integrated Framework- May 1994",s.3.

tedir. İç kontrol çerçevesinde risk değerlendirmesi; amaç ve hedeflerin gerçekleştirilmesi üzerinde etkili olabilecek risklerin tanımlanması, analiz edilmesi ve risklerin nasıl yönetilmesi gerektiğinin belirlenmesi için sıralanması şeklinde tanımlanmaktadır.

Tüm kurumlar, büyüklüğü, yapısı, faaliyet gösterdiği sektör ne olursa olsun, sayısız risk ile karşılaşmakta ve bu riskler, kurumun faaliyetlerinin sürekliliğini, başarısını, finansal durumunu, kamuoyundaki imajını, hizmetlerinin kalitesini ve personelini etkileyebilmektedir. Bununla birlikte riski sıfıra indirmenin kolay bir yolu bulunmadığı gibi, işin yürütülmesi sırasında verilen tüm kararlar da risk yaratmaktadır. Yönetim, kurum için hangi düzeydeki riskin kabul edilebilir olduğuna karar vermeli ve riskin bu seviyelerde kalmasını sağlamak için çaba göstermelidir.

Hedeflerin belirlenmesi risk değerlendirmesinin ön koşuludur. Yönetimin, hedeflerin gerçekleştirilmesi üzerinde etkili olabilecek riskleri tanımlaması ve bu riskleri yönetmek için gereken aksiyonları almasından önce, ilk olarak hedeflerin belirlenmiş olması gerekir. Hedef belirleme, yönetim sürecinin çok önemli bir parçasıdır. İç kontrol bileşenlerinden biri değilse de iç kontrolün birincil şartıdır.

Hedefler

Kurum düzeyinde hedefler, çoğunlukla misyon ve vizyon bildirimleri ile ifade edilir. Kurumun güçlü ve zayıf yönleri ile fırsat ve tehditlerin değerlendirilmesi sonrasında genel stratejisi belirlenir. Genel olarak stratejik plan, en üst düzeyde kaynak dağılımı ve öncelikleri ifade eder. Daha özel hedefler, bu genel strateji doğrultusunda belirlenir. Kurum düzeyindeki hedefler, ilgili alt hedefler(faaliyet hedefleri) ile ilişkilendirilir. Bu alt hedefler kurum düzeyindeki çok çeşitli faaliyetlerden, satış, üretim ve pazarlama gibi, doğar.

Kurum veya faaliyet düzeyindeki hedeflerin belirlenmesi sırasında, kurum kritik başarı faktörlerini tanımlayabilir. Bunlar, eğer hedefe ulaşılmak isteniyorsa, doğru şekilde işlemesi gereken anahtar unsurlardır. Kritik başarı faktörleri, kurum için, bir bölüm, birim, ünite veya görev için belirlenebilir. Hedeflerin belirlenmesi, kritik başarı faktörlerine odaklanmak suretiyle, yönetimin performans kriterlerini belirlemesini sağlar.

Hedef Kategorileri

İç Kontrol Bütünleşik Çerçevesi Hedefleri, operasyonel hedefler, finansal raporlama hedefleri ve uygunluk hedefleri olmak üzere üç başlıkta toplamaktadır. Bir hedefin, birden fazla kategoriye dahil olabilmesi mümkündür.

Operasyonel Hedefler: Bu başlık, kurum faaliyetlerinin etkinliği ve ekonomikliği ile ilgili olup, performans ve karlılık hedefleri ile varlıkların kayıplara karşı korunmasını da içerir. Operasyonel hedefler, yönetimin tercihleri, kararları ve yönetim şekli ile çok yakından ilişkilidir. Örneğin ürün veya hizmet geliştirme konusunda, bir kurum hemen yeniliklere adapte olmayı seçebilirken bir diğeri izlemeyi tercih edebilir. Bütün bu seçimler, organizasyon yapısını, yetkinlik düzeyini, personel politikasını ve araştırma geliştirme fonksiyonu üzerindeki kontrolleri etkileyecektir. Operasyonel hedefler, kurumun temel görevleri ve varoluş sebebine ilişkin hedeflerdir. Faaliyetlerin etkinliği ve verimliliğine yönelik alt hedefleri de içermektedir. Bu hedefler, kurumun faaliyet gösterdiği sektörün gereksinimlerine ve hizmet alanların(müşterilerin) beklentilerine uygun ve anlamlı bir performans değerlendirmesine imkân verecek şekilde belirlenmelidir. **Faaliyet hedefleri ve stratejilerinin açıkça belirlenmesi ve alt hedefler ile ilişkilendirilmesi, başarıyı getiren kritik bir faktördür.** Bu şekilde, kurum kaynaklarını doğru alanlara yönlendirebilecektir. Faaliyet hedefleri açıkça belirlenmemiş veya iyi kavranmamış ise, kaynakların yanlış kullanılabilmesi mümkün olabilecektir.

Finansal Raporlama Hedefleri: Finansal raporlardaki yolsuzlukların önlenmesini de içeren, güvenilir finansal raporların hazırlanmasına yönelik hedeflerdir. Kurumlar, finansal raporlama hedeflerini gerçekleştirme ihtiyacını, dışsal zorunluluklar nedeniyle duymaktadır. Yatırımcılar, kreditörler, hizmet alanlar ve tedarikçiler, yönetimin performansını değerlendirmek ve alternatif yatırımlar ile karşılaştırmak için, finansal raporları kullanmaktadırlar. Dolayısıyla bu raporlarda yer alan bilgilerin, tamlığı, doğruluğu ve güvenilirliği, kurum açısından büyük önem taşımaktadır.

Uygunluk Hedefleri: Kurumun uymakla yükümlü olduğu yasa ve düzenlemelere ilişkin hedeflerdir. Aynı sektörde faaliyet gösteren tüm kurumlar için benzer

olan ve dışsal etkenlere dayalı, iş güvenliği, çevre koruma gibi, hedeflerdir. Kurumlar faaliyetlerini, yasa ve düzenlemelere göre yürütmek ve bu doğrultuda gereken aksiyonları almakla yükümlüdür. Bu yükümlülükler, pazarlama, fiyatlama, vergilendirme, çevre, işçi refahı veya dış ticaret gibi çok sayıda farklı konu ile ilgili olabilir. Bu kanun ve düzenlemeler, kurumun uygunluk amaçlarına entegre etmesi gereken minimum davranış standartlarıdır. Örneğin bir kurum, iş sağlığı ve güvenliği düzenlemeleri doğrultusunda, hedefini "Tüm kimyasal malzemeleri düzenlemelere uygun bir şekilde ambalajlamak ve etiketlendirmek" şeklinde belirleyebilir. Uygunluk hedeflerini gerçekleştirme başarısı, kurumun imajını pozitif veya negatif yönde etkileyebilecektir.

Hedeflerin İlişkilendirilmesi

Hedefler birbiriyle uyumlu ve ilişkili olmalıdır. Kurum düzeyindeki hedeflerin, yalnızca kurumun beklenti ve kapasitesine değil, aynı zamanda iş birimleri ve fonksiyonlarının hedeflerine de uygun olması gerekir. **Kurum düzeyindeki hedefler, genel stratejiye uygun bir şekilde alt hedeflere indirgenmeli ve kurum faaliyetleri ile ilişkisi kurulmalıdır.** Kurum düzeyindeki hedefler, gerçekleşme sonuçları ve performansa uygun olmalı, hedefler kurumun geçmiş uygulama sonuçları ve birimlerin ihtiyaçları dikkate alınarak belirlenmelidir. Örneğin "Yönetici pozisyonlarını daha çok kurum içi terfiler ile doldurmak" hedefi, insan kaynakları sürecine yönelik alt amaçlar/süreçler, planlama, terfi, eğitim ve gelişim ile yakından ilişkilidir. Kurum dışından atanan yöneticilere ilişkin geçmiş tecrübeler doğrultusunda, hedefler değişebilecektir. **Faaliyet hedefleri, kolaylıkla anlaşılabilecek kadar açık belirlenmeli ve ölçülebilir nitelikte olmalıdır. Hem yöneticiler hem de personel neyin başarılmak istendiğini bilmelidir.** Bir faaliyet için, hem kurum düzeyindeki hedeflerden, hem de belirlenmiş standart ve prosedürlerden kaynaklanan uygunluk ve finansal raporlama hedefleri belirlenebilir. Satın alma faaliyetine ilişkin olarak operasyonel hedef örnekleri aşağıda yer almaktadır:

- Teknik şartnamede belirlenmiş gereksinimleri karşılayan malları satın almak
- Kabul edilebilir fiyatlar ve diğer koşullar için pazarlık etmek
- Yıllık olarak tüm tedarikçileri gözden geçirip sertifikalarını yeniden değerlendirmek

Bununla birlikte, bu hedeflerin tamamının gerçekleştirilebilmesi, bir faaliyet için çok fazla kaynak kullanılmasına da yol açabilir. **Bu nedenle faaliyet hedefleri, kullanılabilir kaynaklar ölçüsünde belirlenmeli, kurum düzeyindeki hedefleri veya kurumsal süreçleri desteklemeyen hedefler elenmelidir.** Bu şekilde, geçmiş yıllardan beri sürdürülen bazı fonksiyonların da (örneğin rutinleşmiş ancak faydası olmayan aylık raporlama faaliyeti gibi) hedeflerle ilgisizliği de ortaya çıkabilecektir.

Hedefler ve kaynaklar arasındaki dengeyi sağlamanın bir diğer yolu ise, faaliyet hedeflerini, kurumsal hedefler üzerindeki etkisi doğrultusunda, çok önemli veya kritik şeklinde tanımlayarak önceliklendirmektir. Kritik olarak tanımlanan hedeflere yönelik faaliyetler yakından izlenir. Bu şekildeki bir önceliklendirme ile kurumsal hedeflerin gerçekleştirilmesi için gereken kritik başarı faktörleri de belirlenmiş olur.

Hedeflerin Gerçekleştirilmesi

Daha önce de belirtildiği gibi, hedeflerin belirlenmesi etkin iç kontrolün ön koşuludur. Etkin bir iç kontrol sisteminin, kurumun finansal raporlama, uygunluk ve operasyonel hedeflerinin gerçekleştirileceğine ilişkin makul güvence sağlaması gerekir. Bununla birlikte; bu her durumda tüm hedefler için geçerli olmayabilir. Şöyle ki; Finansal raporlama ve uygunluk hedefleri, Kurumdan bağımsız bir şekilde belirlenmiş, dışsal standartlardan kaynaklanan hedeflerdir, ancak bu standartları sağlamak büyük ölçüde kurumun kontrolündedir. Ancak operasyonel hedeflerde farklı bir durum söz konusudur. Bu hedeflere ilişkin standartlar dışsal standartlar olmamakla birlikte, bu hedefleri sağlamak genellikle bütünüyle kurum kontrolünde değildir. Operasyonel hedefler, hükümet değişikliği, elverişsiz hava koşulları gibi, çok sayıda dışsal nedene bağlı olarak gerçekleştirilemeyebilir. Bu konuların bir kısmı, hedeflerin belirlenmesi sırasında dikkate alınarak acil durum planları hazırlanabilir. Bununla birlikte, böyle bir plan sadece dışsal olayların etkilerini azaltabilir, ancak hedeflerin gerçekleştirilebileceğine ilişkin güvence sağlamaz.

İç kontrolün bu alandaki hedefi, öncelikle: Kurum ge-

nelinde amaç ve hedeflerin tutarlı bir şekilde geliştirilmesi, kritik başarı faktörlerinin tanımlanması ve performans gerçekleşmeleri ile beklentilerin yönetime zamanında raporlanmasına odaklanmak olmalıdır. Başarı sağlanamasa da, hedeflerin gerçekleştirilmesinin tehlikeye girdiği anda yönetimin uyarılacağına ilişkin makul güvence sağlamalıdır.

RİSKLER

Risklerin tanımlanması ve analiz edilmesi süreci, tekrarlanan bir süreç olup, etkin bir iç kontrol sisteminin kritik bileşenidir. Yöneticiler, kurumun her düzeyindeki risklere dikkatli bir biçimde odaklanmalı ve bunları yönetmek için gereken aksiyonları almalıdır.

Risk Tanımlaması

Bir kurumun performansı, içsel ve dışsal nedenlerle risk altında olabilir. Bu içsel ve dışsal faktörler hedeflere etki edebilir. Risk tanımlama sürecinde, hedefler üzerinde etkili olabilecek bu faktörlerin tanımlanması gerekir. **Risk tanımlama, genellikle planlama sürecine entegre bir süreçtir.** Riskler, kurum ve faaliyet düzeyinde tanımlanmalıdır.

Kurum Düzeyi

Kurum düzeyindeki riskler, içsel ve dışsal faktörlerden kaynaklanabilir. Dışsal ve içsel faktörlere ilişkin aşağıdaki örnekler sayılabilir:

Dışsal Faktörler

- Teknolojik gelişmeler, araştırma ve geliştirme faaliyetlerinin zamanlamasını ve niteliğini etkileyebilir.
- Müşterinin değişen beklenti ve ihtiyaçları, ürün geliştirme, üretim, müşteri hizmetleri, fiyatlandırma süreçlerini etkileyebilir.
- Rekabet koşulları, pazarlama ve servis hizmetlerini değiştirebilir.
- Yeni kanun ve düzenlemeler, faaliyetlere yönelik politika ve stratejilerin değiştirilmesini zorunlu kılabilir.
- Doğal afetler, faaliyetlerde ve bilgi sistemlerinde değişiklik yapılmasını gerekli kılıp, acil durum planlarına yönelik gereksinimi ön plana çıkarabilir.
- Ekonomik değişiklikler, finansal kararlar ile büyümeye ilişkin kararlar üzerinde etkili olabilir.

İçsel Faktörler

- Yönetimin sorumluluklarında meydana gelecek bir değişim kontrollerin uygulama biçimini değiştirebilir.
- Kurumun faaliyetlerinin niteliği ve personelin varlıklara erişim yetkileri, kaynakların uygunsuz kullanımı sonucuna yol açabilir.
- Etkin olmayan bir yönetim kurulu veya denetim komitesi, suistimallere fırsat verebilir.

Risklerin tanımlanması için geliştirilmiş pek çok teknik bulunmaktadır. Çoğunluğu, özellikle iç ve dış denetçiler tarafından faaliyetlerinin kapsamını belirlemek için geliştirilenler, yüksek risk içeren faaliyetleri tanımlamak ve önceliklendirmek için, niteliksel veya niceliksel metotlar kullanır. Diğer yöntemler arasında; Kurumu ilgilendiren ekonomik ve endüstriyel faktörlerin düzenli olarak gözden geçirilmesi, üst yönetim iş planlama konferansları ve toplantıları sayılabilir. **Kurumun riskleri tanımlamak için hangi yöntemi tercih ettiğinin fazla bir önemi bulunmamaktadır, önemli olan yönetimin, riskleri artıran faktörleri dikkate almasının sağlanmasıdır.**

Risk tanımlama aşamasında; Geçmişte hedeflere ulaşılamaması sonucuna yol açan nedenler, personelin niteliği, rekabet koşulları, yasa-düzenlemelerdeki önemli değişiklikler, faaliyetlerin coğrafi olarak yaygın olması ya da karmaşıklığı dikkate alınmalıdır.

Faaliyet Düzeyi

Kurum düzeyinde risk tanımlamasına ek olarak, faaliyet düzeyinde de tanımlama yapılması gerekir. Bu düzeydeki risk belirlemesi, risk değerlendirmesinin önemli iş birimleri veya fonksiyonlarına(satış, üretim, pazarlama, teknoloji geliştirme gibi) odaklanmasına yardımcı olur. Faaliyet düzeyindeki risklerin başarılı bir şekilde değerlendirilmesi, aynı zamanda kurum düzeyindeki risklerin de kabul edilebilir seviyelerde tutulabilmesine katkı sağlar.

Örneğin Kurum tarafından, satın alma sürecine ilişkin

"Son olarak; Risk değerlendirmesi teorik bir çalışma değildir. Kurumun başarısı üzerinde kritik öneme sahiptir. Potansiyel risk maruziyetinin bulunduğu anahtar iş süreçlerine ilişkin tanımlamaları içermesi halinde, en etkili şekilde uygulanabilir"

olarak "Hammadde stoğunun yeterliliğini sağlamak" şeklinde bir faaliyet hedefi belirlenmiş olsun. Faaliyet hedefinin başarılmasını engelleyebilecek riskler arasında "Malların şartname gereksinimlerini karşılayamaması veya istenilen miktarda, istenilen zamanda veya kabul edilebilir bir fiyattan teslim edilmemesi" sayılabilir. Bu riskler, şartnamelerin hazırlanması, üretim tahminlerinin uygunluğu ve kullanımı, alternatif tedarikçilerin tanımlanması ve pazarlık uygulaması gibi, kurum düzeyindeki pek çok karar üzerinde etkili olabilecektir.

Risk Analizi

Kurum düzeyinde ve faaliyet düzeyinde risklerin tanımlaması sonrasında, bir risk analizi gerçekleştirilmesi gerekir. Risk analizi metotları çok çeşitlidir, bunun öncelikli nedeni, risklerin büyük kısmının sayısal hale dönüştürülmesindeki güçlüktür. Her durumda, seçilen yöntem ne olursa olsun genellikle risk analizi aşağıdaki faaliyetleri kapsar:

- Riskin öneminin tahmin edilmesi,
- Riskin ortaya çıkma ihtimalinin(olasılığının) değerlendirilmesi,
- Riskin nasıl yönetilmesi gerektiğinin belirlenmesi, başka bir deyişle, hangi aksiyonların alınması gerektiğinin değerlendirilmesi.

Kurum üzerinde önemli bir etkisi bulunmayan ve ortaya çıkma ihtimali de düşük olan risklere ilişkin, genellikle aksiyon gerektiren bir durum bulunmamaktadır. Diğer taraftan, yüksek etki ve yüksek olasılığa sahip riskler, özel önem gerektiren risklerdir. Bu iki uç durum arasında yer alan risklere ilişkin karar verilmesi ise oldukça güç olup, analizin rasyonel ve dikkatli bir şekilde yapılması gerekir. Bir riskin neden olacağı kaybın tutarını tahmin etmeye imkân veren çeşitli metotlar bulunmaktadır, yönetim bunların farkında olmalı ve uygun olması halinde bu yöntemlerden birini tercih etmelidir. Büyüklüğü bu şekilde ifade edilemeyen riskler ise, büyük, orta, küçük şeklinde tanımlanabilir.

Riskin önem ve olasılığının değerlendirilmesinden sonra, yönetim riskin nasıl yönetileceğine karar vermelidir. Riskin önemini veya ortaya çıkma olasılığını azaltmaya yönelik aksiyonlar alınması gerekebilir. Bazen alınan aksiyonlar, riski tamamen ortadan kaldırabilirken bazen de ortaya çıkması halindeki etkisini azaltabilir. Dikkat edilmesi gereken nokta, iç kontrolün bir parçası olan risk değerlendirmesi ile nihai planlar, programlar ve yönetim tarafından risklere ilişkin yürütülen diğer faaliyetler arasında bir ayrım olduğudur. Alınan önlemler, daha geniş bir yönetim sürecinin önemli bir parçasıdır, ancak iç kontrol sisteminin bir unsuru değildir.

Yönetimin, risklere ilişkin alınan önlemlerin uygulaması ve etkinliğinin izlenmesine yönelik prosedürler oluşturması gerekir. Örneğin Kurum "Kritik bilgisayar hizmetlerinin kaybı" riskine karşı bir "Felaket kurtarma planı" hazırladığında, bu planın uygun bir şekilde tasarlandığı ve uygulandığını izlemeye imkan veren bir prosedür de oluşturmalıdır. Bu prosedürler "Kontrol Faaliyetleri" olarak adlandırılmaktadır.[4] Bununla birlikte yönetim, risklere yönelik ilave prosedürler oluşturmadan önce, mevcutların yeterliliğini değerlendirmeli ve etkinliklerini artırma imkânını dikkate almalıdır.

Son olarak; Risk değerlendirmesi teorik bir çalışma değildir. Kurumun başarısı üzerinde kritik öneme sahiptir. Potansiyel risk maruziyetinin bulunduğu anahtar iş süreçlerine ilişkin tanımlamaları içermesi halinde, en etkili şekilde uygulanabilir.

Kamu İç Kontrol Standartları-Risk Değerlendirme Bileşeni

Risk değerlendirme, Kamu İç Kontrol Standartlarının ikinci standardıdır. Bu standart altında iki genel şart bulunmaktadır. Bunlardan ilki "Planlama ve Program-

4 İç Kontrol Bütünleşik Çerçeve Final Raporunun 4. Bölümünde bu konuya ilişkin detaylı bilgiler yer almaktadır.

lama" diğeri ise "Risklerin belirlenmesi ve değerlendirilmesidir" Bu iki standardın sağlanabilmesi için gereken genel şartlar aşağıda sıralanmıştır:

Planlama ve Programlama

1. İdareler, misyon ve vizyonlarını oluşturmak, stratejik amaçlar ve ölçülebilir hedefler saptamak, performanslarını ölçmek, izlemek ve değerlendirmek amacıyla katılımcı yöntemlerle **stratejik plan** hazırlamalıdır.
2. İdareler, yürütecekleri program, faaliyet ve projeleri ile bunların kaynak ihtiyacını, performans hedef ve göstergelerini içeren **performans programı** hazırlamalıdır.
3. İdareler, **bütçelerini** stratejik planlarına ve performans programlarına uygun olarak hazırlamalıdır.
4. Yöneticiler, faaliyetlerin ilgili mevzuat, stratejik plan ve performans programıyla belirlenen amaç ve hedeflere uygunluğunu sağlamalıdır.
5. Yöneticiler, görev alanları çerçevesinde idarenin hedeflerine uygun özel hedefler belirlemeli ve personeline duyurmalıdır.
6. İdarenin ve birimlerinin hedefleri, spesifik, ölçülebilir, ulaşılabilir, ilgili ve süreli olmalıdır.

Risklerin Belirlenmesi ve Değerlendirilmesi

1. İdareler, her yıl sistemli bir **şekilde amaç ve hedeflerine yönelik riskleri** belirlemelidir.
2. Risklerin gerçekleşme olasılığı ve muhtemel etkileri **yılda en az bir kez analiz** edilmelidir.
3. Risklere karşı alınacak önlemler belirlenerek **eylem planları** oluşturulmalıdır.

Yukarıdaki şartlar incelendiğinde; Kamu kurumları 5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu doğrultusunda, stratejik plan ve performans programı hazırlamaktadır. Stratejik Plan ve bütçe ilişkisi ise, performans programları aracılığı ile kurulmaktadır. Yine performans programları ile kurum performans hedeflerinden sorumlu birimler belirlenmektedir.

Bununla birlikte; kamu kurumlarında stratejik plan ve performans programı kurum düzeyinde hazırlanmaktadır. Misyon, vizyon, amaç ve hedefler **kurum düzeyinde** belirlenmektedir. Kurum stratejik planını destekleyecek şekilde birim hedeflerinin de belirlenmesine ilişkin genel bir düzenleme bulunmamaktadır.

Diğer taraftan; kamu kurumlarında, yine 5018 sayılı Kanun uyarınca faaliyet raporları hazırlanmaktadır. Stratejik plan ve performans programından farklı olarak faaliyet raporları, **kurum ve harcama birimi** düzeyinde hazırlanmaktadır. Faaliyet raporlarında yer alması gereken bilgiler ve rapor formatları "Kamu İdarelerince Hazırlanacak Faaliyet Raporları Hakkında Yönetmelik" ile belirlenmiştir. Bu Yönetmelik uyarınca; Birim faaliyet raporlarında, faaliyetlere ilişkin bilgi ve değerlendirmeler yanında, birime özgü misyon, vizyon, amaç ve hedef bilgilerinin de yer alması gerekmektedir. Ancak birim düzeyindeki bu bilgilerin, ne zaman ve nasıl belirleneceğine ilişkin genel bir düzenleme bulunmamaktadır.

Görüldüğü üzere, kurum stratejik planı doğrultusunda, birimler tarafından misyon, vizyon ile birim amaç ve hedeflerinin belirlenmesi halinde, hem iç kontrol standartlarının ilgili şartına hem de Faaliyet Raporlarına ilişkin Yönetmelik hükümlerine uygunluk sağlanması mümkün olabilecektir. Diğer taraftan, birim düzeyinde amaç ve hedef belirlenmesi, kurum stratejik plan ve performans programı hazırlık süreçleri ile birim performansının ölçülmesi ve izlenmesini de kolaylaştıracak, aynı zamanda kurum stratejik hedeflerinin birimlerce içselleştirilmesini sağlayarak hedeflere ulaşılma ihtimalini de artıracaktır.

COSO İç Kontrol Çerçevesi ile Kamu İç Kontrol Standartlarının Risk Değerlendirme Bileşenlerinin Karşılaştırılması

Kamu iç kontrol standartlarının risk değerlendirme standardı, COSO İç Kontrol Çerçevesinin risk değerlendirme bileşeni altında yer alan önemli hususları büyük ölçüde içermektedir. Bununla birlikte; COSO iç kontrol çerçevesinde, "Hedef" kavramına özel bir vurgu yapılmaktadır. Hedeflerin belirlenmesi, hem risk değerlendirmesinin ön koşulu hem de iç kontrolün birincil şartı olarak ifade edilmektedir. Hedefler, operasyonel, finansal raporlama ve uygunluk olarak üç başlıkta toplanmakta, kurum ve birim düzeyinde hedeflerin belirlenmesi, ilişkilendirilmesi başarıyı getiren kritik faktör olarak tanımlanmaktadır.

"Kurumsal risk yönetimi; Kurumun yönetim kurulu, yöneticileri ve diğer personelinden etkilenen, kurum genelinde ve strateji belirlenmesi sırasında uygulanan, kurumu etkileyebilecek potansiyel olayların tanımlanması, kurum risk iştahı içinde yönetilmesi ve kurumun hedeflerine ulaşması konusunda makul güvence sağlaması için tasarlanan bir süreçtir"

3. COSO KURUMSAL RİSK YÖNETİMİ BÜTÜNLEŞİK ÇERÇEVESİ

İç Kontrol-Bütünleşik Çerçevesi COSO tarafından ilk olarak Eylül 1992 tarihinde yayımlanmıştır. O tarihten itibaren, bu çerçeve esas alınarak dünyanın pek çok ülkesinde çok sayıda yasal düzenleme yapılmış, binlerce kurum, iç kontrol sistemlerinin kurulması veya geliştirilmesinde bu çerçeveden yararlanmıştır. Ancak zaman içerisinde yaşanan iş skandalları risk yönetimine ilişkin kaygıları artırmış ve risklerin etkin bir şekilde tanımlanması, değerlendirilmesi ve yönetilmesine yönelik bir çerçeve ihtiyacını ortaya koymuştur. Bunun üzerine COSO, 2001 yılında Pricewaterhouse Coopers şirketi ile birlikte çalışmalara başlamıştır. Bu tarihten sonra yaşanan ve Amerika'da 2002 yılında Sarbanes-Oxley yasalarının çıkarılmasına neden olan skandallar, risk yönetimine ilişkin ortak bir dil oluşturabilecek ve kurumlara rehberlik edebilecek nitelikte bir çerçeve ihtiyacını zorunlu hale getirmiştir. 2004 yılında COSO Kurumsal Risk Yönetimi Bütünleşik Çerçevesini yayımlamıştır. Bu çerçevenin geliştirilmesindeki amaç, yöneticilerin kurumlarını değerlendirmek ve geliştirmek için kolaylıkla kullanabilecekleri bir çerçeve sağlamaktır.

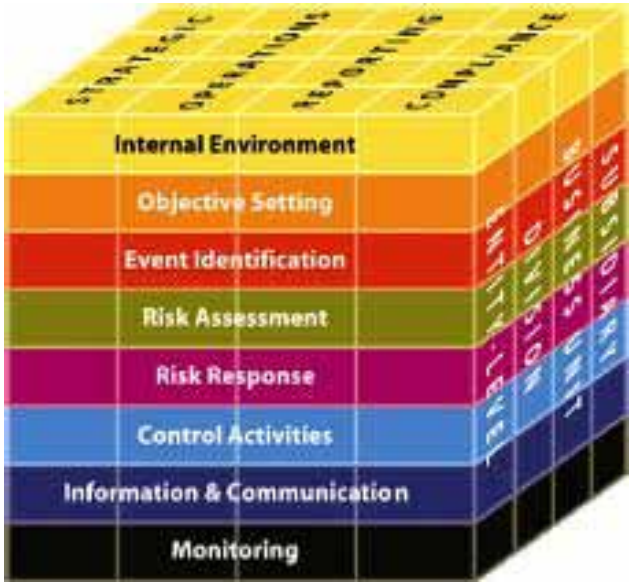
Kurumsal risk yönetimi; Kurumun yönetim kurulu, yöneticileri ve diğer personelinden etkilenen, kurum genelinde ve strateji belirlenmesi sırasında uygulanan, kurumu etkileyebilecek potansiyel olayların tanımlanması, kurum risk iştahı içinde yönetilmesi ve kurumun hedeflerine ulaşması konusunda makul güvence sağlaması için tasarlanan bir süreçtir[5].

Bu tanımdan da anlaşılacağı üzere, Kurumsal Risk Yönetimi:

- Kurumun amaç ve hedeflerinin gerçekleştirilmesini sağlamaya yöneliktir.
- Kurumun bütününe yaygın ve sürekli gelişen bir süreçtir.
- Her seviyedeki kurum çalışanından etkilenmektedir.
- Stratejilerin belirlenmesi sırasında uygulanmaktadır.
- Kurumun tüm birim ve bölümlerinde uygulanmakta ve kurum düzeyinde risk portföyü elde edilmesini sağlamaktadır.
- Gerçekleşmesi halinde kurumu etkileyebilecek potansiyel olayların tanımlanması ve risk iştahı dâhilinde yönetilmesi için tasarlanmaktadır.
- Üst yönetime ve yöneticilere amaç ve hedeflerin gerçekleştirilebileceğine ilişkin makul güvence sağlayabilmektedir.

İç Kontrol Çerçevesinde olduğu gibi Kurumsal Risk Yönetimi çerçevesi de 3 boyutlu bir matris ile ifade edilmektedir. Matrisin tepesinde, stratejik, operasyonel, uygunluk ve raporlama olmak üzere 4 kategoride toplanan hedefler; ön yüzünde Kurumsal Risk Yönetiminin, İç Ortam, Amaç ve Hedeflerin Belirlenmesi, Olay/Durum Tanımlamaları, Risk Değerlendirmesi, Risk Yanıtlanması, Kontrol Faaliyetleri, Bilgi ve İletişim ile İzleme olmak üzere sekiz bileşeni, yan yüzünde ise, kurumsal risk yönetiminin uygulanacağı seviyeler, kurum, birim, bölüm ve ünite/alt birim, yer almaktadır.

5 COSO, "Enterprise Risk Management-Integrated Framework Executive Summary,September 2004",s.2.



COSO, Kurumsal Risk Yönetimi Çerçevesi ile İç Kontrol Çerçevesini ortadan kaldırılmamıştır. Her iki Çerçevede yürürlüktedir. COSO tarafından 2004 yılında yayımlanan Raporda; İç Kontrol Çerçevesinin, gerek Amerika gerekse diğer ülkelerde geniş kabul gördüğü, Amerika'daki pek çok şirketin, bu çerçeveyi Sarbanes-Oxley Yasasının raporlama gereksinimlerini karşılamak amacıyla kullandığı, bu nedenle İç Kontrol Bütünleşik Çerçevesinin, bir süre daha yürürlükte kalmaya devam edeceği belirtilmiştir. Bununla birlikte, Kurumsal Risk Yönetimi Çerçevesi, risk yönetimini odağına alarak ve güçlendirerek iç kontrolü genişletmektedir. COSO, bu çerçevenin iç kontrolü kapsadığını ve iç kontrolün bu çerçevenin ayrılmaz bir parçası olduğunu ifade etmektedir. Şirketler veya kurumlar, bu çerçeveyi hem iç kontrol gereksinimlerini karşılamak hem de daha kapsamlı bir risk yönetimi süreci geliştirmek amacıyla kullanabilmektedirler[6].

Hedeflerin Gerçekleştirilmesi

Kurumsal risk yönetimi çerçevesi, kurumsal hedeflerin gerçekleştirilmesini sağlamayı hedeflemektedir. Kurumsal hedefler, dört başlıkta toplanmaktadır:

- **Stratejik Hedefler;** Kurumun misyonunu ve vizyonunu destekleyen üst düzey hedeflerdir.
- **Operasyonel Hedefler;** Kurumun temel görevlerinin gerçekleştirilmesine yönelik, faaliyetlerin etkinliği ve verimliliği, performans standartları ve varlıkların kayıplara karşı korunmasını da içeren hedeflerdir.
- **Raporlama Hedefleri;** Hesap verme sorumluluğu da dâhil olmak üzere raporlamanın güvenilirliğine ilişkin hedeflerdir. Güvenilir raporlamanın temel amacı, sağlıklı karar verebilmesi için yönetime, uygun, doğru ve tam bilgi sağlamaktır.
- **Uygunluk Hedefleri;** Yürürlükteki yasa ve düzenlemelere uygunlukla ilgili hedeflerdir.

Kurumsal hedeflerin bu şekilde kategorize edilmesi, kurumsal risk yönetiminin farklı yönlerine odaklanılabilmesine imkân sağlar. Bu farklı ama birbirleri ile örtüşen hedefler (bir hedef, birden fazla kategoriye dâhil olabilir) farklı kurumsal ihtiyaçlara hitap etmektedir, aynı zamanda farklı birimlerin sorumluluk alanında da olabilir.

Raporlamaların güvenilirliği ile yasa ve düzenlemelere uygunluk hedefleri, kurumun kontrolünde olduğu için, kurumsal risk yönetiminin bu hedeflere ilişkin olarak makul güvence sağlaması beklenir. Bununla birlikte, stratejik ve operasyonel hedefler, kurumun her zaman kontrol edemeyeceği dışsal olaylarla da ilgilidir. Kurumsal risk yönetimi, bu hedeflere ilişkin olarak, yönetimin hedeflere ulaşma yönündeki ilerleme hakkında zamanında haberdar olmasını sağlayarak makul güvence sağlar.

COSO Kurumsal Risk Yönetimi(KRY) Çerçevesi ile COSO İç Kontrol Çerçevesinin Karşılaştırılması

İki çerçeve arasındaki temel farklılıklar aşağıdaki gibi sıralanabilir[7];

- KRY Çerçevesi, risk yönetimini odağına alarak iç kontrol tanımını genişletmekte ve iç kontrol çerçevesini kapsamaktadır.
- KRY Çerçevesinde, operasyonel, raporlama ve uygunluk hedefleri arasına "Stratejik Hedefler" isimli yeni bir hedef kategorisi eklenmiş ve Raporlama Hedefleri, içsel raporları da içerecek şekilde genişletilmiştir.

6 A.g.e, s.v.

7 Protiviti, "Guide to Enterprise Risk Management: Frequently Asked Questions", January 2006, s.20.

- KRY Çerçevesi "Risk İştahı[8]" ve "Risk Toleransı[9]" şeklinde iki yeni kavramı içermektedir.
- KRY Çerçevesi, iç kontroldeki risk değerlendirme bileşenini dört farklı bileşene ayırmaktadır. Bunlar;

  ✓Hedeflerin Belirlenmesi

  ✓Olay/Durumların (Risk ve Fırsatlar) Tanımlanması

  ✓Risk Değerlendirmesi

  ✓Risk Yanıtlaması

- KRY'de risklerin değerlendirilmesi sonrasında, risk yanıtları oluşturulmakta ve bu yanıtlar arasında kontrol dışında, üstlenme, kaçınma ve transfer şeklinde alternatif risk yanıtları da bulunmaktadır.
- KRY'deki "İç Ortam" bileşeni, İç Kontrol Çerçevesindeki "İç Kontrol Ortamı" bileşenini kapsamakta, ilave olarak üç yeni kavram tanımlamaktadır. Bunlar; risk yönetimi felsefesi, risk kültürü ve risk iştahıdır.
- KRY'de amaç ve hedefler üzerinde etkili olabilecek risklerin yanında fırsatlar da tanımlanmaktadır.
- İç Kontrol Çerçevesinin birim ve faaliyet düzeyinde uygulanması öngörülürken, Kurumsal Risk Yönetimi Çerçevesinin, kurum, bölüm, birim ve alt birim düzeyinde uygulanması öngörülmektedir.

Yukarıda belirtilen hususlar yanında, KRY Çerçevesinin, İç Kontrol Çerçevesinin uygulanması sonrası tecrübeleri de içeren daha yeni bir çerçeve olması nedeni ile uygulama önerisinin geliştirilmesinde bu çerçeveden de yararlanılması tercih edilmiştir.

Risk Yönetimi ve Stratejik Planlama İlişkisi

Stratejik plan, kurumun amaç, hedef ve stratejilerinin belirlenmesi, önceliklendirilmesi ve kaynakların bu öncelikler doğrultusunda kullanılması için yapılan **geleceğe yönelik** bir faaliyettir. Risk yönetimi ise, amaç ve hedefler üzerinde etkili olabilecek olayların tanımlanması, değerlendirilmesi ve yönetilmesi için yapılan yine **geleceğe yönelik** bir faaliyettir. "Stratejik plan ile riskler arasında yüksek düzeyde bir ilişki vardır. Eğer stratejilerin belirlenmesi aşamasında riskler dikkate alınmazsa, kurum stratejileri etkinliklerini kaybedebilir, tam tersi durumda, riskler belirlenirken stratejiler ihmal edilirse, kurum açısından çok önemli ve belki de yüksek riskli alanlar göz ardı edilmiş olur"[10].

Oysa stratejik planlama süreçlerine entegre bir şekilde yürütülecek bir risk yönetimi ile kurumsal stratejilerin, amaç, hedef ve faaliyetlerin gerçekleştirilmesini engelleyebilecek riskler önceden tanımlanarak, alınması gereken önlemlerin belirlenmesi, bu sayede yüksek riskli strateji, amaç veya hedeflerden vazgeçilebilmesi veya fırsatlardan azami ölçüde yararlanılabilmesi mümkün olabilecektir.

4. RİSK YÖNETİMİ-BİR UYGULAMA ÖNERİSİ

Uygulama önerisi, risklerin kurum ve birim düzeyinde belirlenmesi, değerlendirilmesi ve yönetilmesi esasına dayanmaktadır. Risklerin belirlenmesi ve değerlendirilmesi faaliyetleri stratejik plan ve performans programı hazırlık dönemlerinde gerçekleştirilecektir. Planlama ve programlama dönemlerinde gerçekleştirilen risk değerlendirme çalışması ile hedeflere ilişkin riskler tanımlanarak değerlendirilecek, yüksek risklere ilişkin mevcut kontrollerin etkinliğinin nasıl izleneceği planlanacaktır. Yıl boyunca planlanan kontroller yürütülecek, yılsonunda risk ve kontrollere ilişkin değerlendirmelere, birim faaliyet raporlarında yer verilecektir.

Risk yönetimi uygulama önerisine ilişkin iş adımları aşağıda sıralanmaktadır. Kurum bünyesinde yer alan her birim;

- Kurumun stratejik planı ve mevzuatı doğrultusunda, birim düzeyinde amaç ve hedeflerini belirler,
- Bu amaç ve hedefler üzerinde etkili olabilecek risk ve fırsatları tanımlar,
- Belirlenen risk değerlendirme modelini kullanarak risklerini puanlar ve en yüksek risk puanından başlayarak sıralar,

8 Yönetimin risk alma istekliliği

9 Kabul edilebilir risk düzeyi

10 Davut Pehlivanlı, Modern İç Denetim Güncel İç Denetim Uygulamaları, Beta Yayınları, İstanbul, 2010,s.75

- Kritik risklere ilişkin mevcut kontrollerin etkinliği ve yeterliliğini hangi yöntem ve sıklıkta izleyeceğini planlar,
- Kontrol eksikliği bulunan risklere ilişkin kontrol veya tedbir önerilerini hazırlar,
- Bütün bu bilgileri, Risk-Kontrol Planı olarak tanımlanan bir plana dokümante eder ve Strateji Geliştirme Dairesi Başkanlığına gönderir,
- Strateji Geliştirme Dairesi, birimlerden gelen Risk Kontrol Planlarını konsolide ederek Kurum Risk Kontrol Planını hazırlar ve üst yönetimin değerlendirmelerine sunar,
- Üst yönetim bu riskleri, kurumsal amaç ve hedefler doğrultusunda gözden geçirip değerlendirir ve nihai risk stratejilerini belirler. Kurum Risk Kontrol Planının Üst Yönetici tarafından onaylanması sonrası, Birim Risk Kontrol Planlarına son hali verilir.
- Yıl içerisinde, Birimler tarafından kontroller, planlanan şekilde yürütülür. Yılsonunda, bu faaliyetlerin sonuçları birim yöneticisi tarafından değerlendirilir. Değerlendirmede, kontrol faaliyetlerinin ne düzeyde yerine getirildiği, yeterliliği, yerine getirilemediyse nedenleri belirlenir. Değerlendirme sonuçlarına Birim Faaliyet Raporlarında yer verilir.

RİSK-KONTROL PLANLARININ HAZIRLANMA SÜRECİ

BİRİM AMAÇ VE HEDEFLERİNİN BELİRLENMESİ

Birim düzeyinde risk ve kontrollerin belirlenmesinin ilk adımı, birim amaç ve hedeflerinin belirlenmesidir. Birim amaç ve hedeflerinin belirlenebilmesi için ise, öncelikle birim faaliyetlerinin belirlenmesi gerekir.

Birim Faaliyetlerinin Belirlenmesi

Bu aşamada, birimin mevzuattan kaynaklanan yükümlülüklerinin tespiti ve analizi yapılır. Birimin yasal yükümlülükleri çerçevesinde yürüttüğü faaliyetler ortaya konulur. Yetki, görev ve sorumlulukları ifade edilir. Birime görev ve sorumluluk yükleyen, faaliyet alanını düzenleyen mevzuat gözden geçirilerek yasal yükümlülükleri listelenir. Yasal yükümlülükler ve mevzuat analizi gerçekleştirildikten sonra, bu analizin çıktılarından da yararlanılarak, birimin yürüttüğü temel faaliyetler belirlenir. Birbiri ile ilgili olan faaliyetler başlıklar altında toplanmak suretiyle gruplandırılır. Bu çalışmalar; Birim misyon ve vizyonunun belirlenmesine, görev tanımının hazırlanmasına ve güncellenmesine, birim organizasyon şemasının uygunluğunun değerlendirilmesine, tanımlanmış süreçlerin gözden geçirilip güncellenmesine katkı sağlayacaktır. Ayrıca birim tarafından fiilen yürütülmekle birlikte, mevzuatta karşılığı bulunmayan konularda mevzuat hazırlanması veya mevzuatla verilmekle birlikte, faaliyet sunulamayan alanların belirlenmesine de yardımcı olacaktır. (Ek:1)

Amaç ve Hedeflerin Belirlenmesi

Kurumun stratejik planında yer alan amaç ve hedefleri destekleyecek şekilde birim düzeyinde;

- Misyon,
- Vizyon,
- Misyonu gerçekleştirmeye yönelik amaç ve hedefler,
- Hedefleri gerçekleştirmeye yönelik faaliyetler,

Belirlenir ve dokumante edilir. Bu çalışmalar sırasında, kurum stratejik planı, performans programı, bütçe ve faaliyet raporu hazırlığı sırasında yapılan çalışmalardan faydalanılmalı, mükerrerliğe yer verilmeden, mevcut çalışmalar gözden geçirilerek güncellenmelidir.

Birim düzeyinde belirlenen hedefler, stratejik, operasyonel, uygunluk veya raporlamaya yönelik olup olmadığına göre gruplanmalıdır. (Ek:2)

BİRİM RİSK DEĞERLENDİRMESİ

Risk değerlendirmesi, risk-kontrol planının önemli bir parçasıdır. Birim bünyesinde risk değerlendirmesi, birimin belirlenen hedeflerine ulaşmasını engelleyebilecek risklerin tanımlanması ve değerlendirilmesidir. Bu tanımlama ve analiz risklerin nasıl yönetileceğine ilişkin risk yönetimi stratejisinin esaslarını da şekillendirir.

1. Risklerin Tanımlanması

Risk, hedeflerin gerçekleştirilmesini tehlikeye atabilecek her türlü olay veya durumdur. Birimin her bir hedefine ilişkin riskler tanımlanmalıdır. Risklerin ta-

nımlanması aşamasında, geleceğe yönelik strateji üretmede yararlanmak üzere, fırsatlar da tanımlanmalı ve üst yönetimin dikkatine sunulmalıdır.

Aşağıdaki soruların sorulması risklerin tanımlanmasını kolaylaştırır:

- Neler yanlış gidebilir?
- Neden başarısız olabiliriz?
- Başarmak için ne yapmalıyız?
- En savunmasız olduğumuz alanlar neler?
- Korumamız gereken varlıklarımız neler?
- Hangi hile ve kötüye kullanımlar ile karşılaşabiliriz?
- Faaliyetlerimizi neler durdurabilir?
- Hedeflerimize ulaşıp ulaşamayacağımızı nereden biliyoruz?
- Hangi bilgi en güvenilir?
- En çok parayı neye harcıyoruz?
- Karar vermek için en çok hangi bilgiye ihtiyacımız var?
- Hangi faaliyetlerimiz en karmaşık?
- Hangi faaliyetlerimiz düzenli?
- Yasal yükümlülüklerin en fazla olduğu faaliyetlerimiz hangileri?

Risklerin tanımlanması sırasında, iç ve dış ortamdan kaynaklabilecek tüm durumlar dikkate alınmalıdır. Bir hedefe ilişkin çok sayıda risk tanımlaması yapılabilir. Tanımlanan riskler, belirlenen formatta kaydedilmelidir.

2. Risklerin Analizi

Riskler tanımlandıktan sonra; Ortaya çıkma olasılığı ile ortaya çıkması halindeki potansiyel etkisinin belirlenebilmesi için risk analizi gerçekleştirilir. Bu analiz ile risklerin önceliklendirilmesi sağlanır. Riskler önceliklendirilmelidir, çünkü kurumun hedefleri üzerinde her risk eşit düzeyde önemli değildir ve iç kontrollerin tamamının değerlendirilmesi uzun bir süreç alabilir, bu nedenle yöneticiler hangi alana daha çok yoğunlaşmaları gerektiğini, risklerini analiz ederek belirler.

2.1. Risk Faktörlerinin(Kriterlerinin) Belirlenmesi

Risk analizi için öncelikle risk faktörlerinin belirlenmesi gerekir. Kamu kurumları için kullanılabilecek etki faktörleri arasında; finansal etki, itibar etkisi, operasyonel etki ve stratejik etki faktörleri; olasılık faktörleri olarak ise, otomasyon düzeyi, insan kaynağı yeterliliği, mevzuat ve düzenlemelerin yeterliliği sayılabilir. Kullanılacak kriterler mutlaka ayrıntılı şekilde tanımlanmalıdır.

2.2. Risklerin Puanlanması

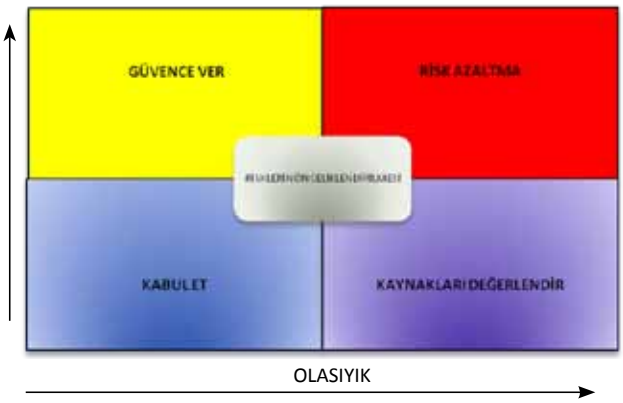
Risk kriterleri belirlendikten sonra, risklerin puanlanmasına geçilir. Bu aşamada, her bir risk, belirlenen kriterler kullanılmak suretiyle puanlanır. Bu puanlar, seçilen risk analizi yöntemi doğrultusunda değerlendirilerek her bir riske ilişkin etki ve olasılık puanları belirlenir. Risklerin puanlanması çalışmaları sırasında aşağıda belirtilen hususlar dikkate alınmalıdır:

- Değerlendirmelerin mümkün olduğunca objektif olmasını sağlayabilmek için, kilit personelin bir araya gelmesine ve puanlamaların tartışma ortamı içerisinde yapılmasına özen gösterilmelidir.
- Puanlamalar sırasında, kriter tanımları sürekli gözden geçirilerek, risk faktörünün neyi ölçmekte olduğu hatırlanmalıdır.
- Puanlar verilirken, en düşük (1) ve en yüksek (5) puanlar için birer örnek düşünülmeye çalışılmalıdır.
- Her bir risk ayrı ayrı ele alınmalı ve ölçüm yatay bir şekilde uygulanmalıdır.
- Her bir risk, etki ve olasılık kriterleri açısından 1-5 arası puanlar verilerek değerlendirilmelidir. Bu değerlendirmede (1) en düşük ya da ilgili olmayan etkiyi/olasılığı, 5 ise en yüksek etkiyi/olasılığı ifade etmektedir.

2.3. Risklerin Önceliklendirilmesi

Risk yönetiminin öncelikli amacı, kurumun amaç ve hedefleri üzerinde etkili olabilecek kritik risklerin belirlenmesi ve sınırlı kaynakların bu alanlarda yoğunlaştırılmasıdır. Bu nedenle, her bir riske ilişkin nihai etki ve olasılık puanları belirlendikten sonra, bu puanlar doğrultusunda risklerin önceliklendirilmesi gerekir. (Ek:3)

Aşağıda; Risklerin önceliklendirilmesinde kullanılabilecek bir matris önerisi yer almaktadır.



Güvence Alanı; Bu alanda etkisi yüksek ve olasılığı düşük olan riskler yer almaktadır. Olasılığın düşük olması, kontrollerin(insan kaynakları, mevzuat ve düzenlemeler, otomasyon düzeyi) görece yeterli olduğunu göstermektedir. Dolayısıyla bu alanda yer alan risklere ilişkin kontroller, birim yöneticisi tarafından değerlendirilmeli ve etkinliğine ilişkin olarak güvence verilmelidir. Birim yöneticisi, Birim Faaliyet Raporu ekinde yer alan iç kontrol güvence beyanını, bu değerlendirmeler doğrultusunda imzalamalıdır.

Risk Azaltma Alanı; Bu alanda etkisi yüksek ve olasılığı da yüksek olan riskler yer almaktadır. Olasılığın yüksek olması, kontrollerin bulunmadığı veya yetersiz olduğuna işaret etmektedir. Üst yönetim tarafından, bu risklere ilişkin, risk stratejilerinin(kaçınmak, kontrol etmek, transfer etmek) belirlenmesi gerekir. Birim, Risk-Kontrol Planında bu riskler ile risklere ilişkin önerilerini, üst yönetimin onayına sunmalıdır.

Kaynakları Değerlendir; Bu alan etkisi düşük, olasılığı yüksek olan risklerin yer aldığı alandır. Kurum kaynaklarının yeterli olması halinde, bu risklere ilişkin kontrol faaliyeti geliştirilebilecektir.

Kabul Et; Etkisi düşük, olasılığı da düşük olan riskler bu alanda yer alır. Bu riskler, kurumun risk iştahı sınırları içinde kalması nedeniyle kabul edilebilir olan risklerdir. Bu riskler, üst yönetimin tercihi doğrultusunda, herhangi bir önlem alınmadan olduğu gibi bırakılabilir.

Puanlanan riskler, etki ve olasılık puanları doğrultusunda, yukarıdaki matrise yerleştirilir.

A. KONTROLLERİN BELİRLENMESİ

Bu aşamada, matrisin güvence alanında yer alan risklere yönelik kontroller veya alınan önlemler dokümante edilir. (Ek:4)

B. RİSK-KONTROL PLANININ HAZIRLANMASI

Birim Yöneticisi tarafından, Birim Risk ve Kontrollerine ilişkin hazırlanan Plan, Strateji Geliştirme Dairesine gönderilir. Strateji Geliştirme Dairesi, Birim planlarını gözden geçirir, konsolide eder ve üst yönetimin onayına sunar. Üst yönetim tarafından onaylanmasını müteakip, birim planlarına son hali verilir. (Ek: 5)

C. YILLIK RAPORLAMA

Yıl boyunca, Risk-Kontrol Planında tanımlanan kontroller yürütülür ve birim yöneticisi tarafından yine planda tanımlanan şekilde, kontrollerin etkinliği değerlendirilir.

İç kontrollerin etkinliğine ilişkin değerlendirmelere, yılsonunda birim tarafından düzenlenen faaliyet raporunda yer verilir.

5. SONUÇ

İç kontrol standartları uyarınca kamu kurumlarının, risklerin tanımlanması, değerlendirilmesi ve alınacak önlemlerin belirlenmesine yönelik bir sistem kurmaları ve işletmeleri gerekmektedir. Risklerin belirlenmesinin ilk adımı, hedeflerin belirlenmesidir. Kurum düzeyindeki hedefler, en üst düzeyde kurum stratejik planları ile belirlenmektedir. Bununla birlikte, stratejik hedefleri destekleyecek şekilde birimler düzeyinde, alt hedefler belirlenmeli ve bu hedeflerin faaliyetler ile ilişkisi kurulmalıdır. Hedeflerin sağlıklı bir şekilde tespiti için, kurum tarafından yürütülen hiçbir faaliyetin kapsam dışında bırakılmamasına önem verilmelidir. Hedeflerin belirlenmesi sonrasında yapılması gereken, bir model doğrultusunda risklerin tanımlanması, değerlendirilmesi ve önceliklendirilmesidir. Risk değerlendirmesi, teorik bir süreç değildir, önemli olan tüm risklerin eşit düzeyde olmadığının bilinmesi ve kurum hedeflerine olan etkileri dikkate alınarak önceliklendirilmesi gerektiğinin bilinmesidir. Risk yönetiminin, stratejik planlama ve performans programı hazırlık süreçlerine entegre bir şekilde yürütülmesi, hedeflerin riskler dikkate alınarak belirlenmesi ve kaynakların da bu doğrultuda tahsisini sağlayacaktır.

(Ek: 1) .....BİRİMİ BAŞKANLIĞI YASAL YÜKÜMLÜLÜKLER LİSTESİ

S.No	Tarih	Sayı	Mevzuat Türü	Kaynağı	Adı	Konusu	İlgili Olduğu Faaliyet (ler)

(Ek:2) BİRİMİ BAŞKANLIĞI FAALİYETLER LİSTESİ

S.No	Faaliyetin Adı	Faaliyet Amacı	Faaliyete İlişkin Mevzuat	İlgili Olduğu Süreç

(Ek: 3) .....BİRİMİ BAŞKANLIĞI AMAÇ VE HEDEFLER TABLOSU

MİSYONUMUZ :					
VİZYONUMUZ :					
No.	Amaç	Hedef	Amaç/Hedef Türü	İlgili Olduğu Faaliyet	Faaliyetin İlgili Olduğu Süreç
			Stratejik		
			Operasyonel		
			Raporlama		
			Uygunluk		

(Ek:4) .....BİRİMİ RİSK TABLOSU

RİSK TANIMLAMASI			RİSK DEĞERLENDİRMESİ			RİSK YÖNETİMİ			
Risk No	Tanımı	İlgili Olduğu Hedef	Etki Puanı	Olasılık Puanı	Önceliği	Risk Yanıtı	Risk Kategorisi	Kontrol veya Önlem	Risk Sorumlusu
						Kontrol			
						Üstlenme			
						Kaçınma			
						Transfer			

(EK:5).....BİRİMİ KONTROL TABLOSU

Kontrol No.	Kontrol veya Önlemin Tanımı	İlgili Olduğu Risk	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Yöntemi	Kontrolün İzlenmesi	İzleme Sıklığı

(EK:6)

…….YILI

…….BİRİMİ RİSK KONTROL PLANI

1.MİSYON

2.VİZYON

3.BİRİM AMAÇ HEDEF VE FAALİYETLERİ

4.BİRİM RİSKLERİ VE KONTROLLERİ

5.EKLER

1-Yasal Yükümlülükler Listesi

2-Faaliyetler Listesi

3-Amaç ve Hedefler Tablosu

4-Birim Risk Tablosu

5-Birim Kontrol Tablosu

KAYNAKLAR

1. COSO, “Internal Control Integrated Framework”, May 1994,
2. COSO,”Enterprise Risk Management-Integrated Framework Executive Summary”,September 2004,
3. Protiviti, “Guide to Enterprise Risk Management: Frequently Asked Questions”, January 2006,
4. Onur DERİCİ, Zekeriya TÜYSÜZ, Aydın SARI, “Kurumsal Risk Yönetimi ve Sayıştay Uygulaması”, Sayıştay Dergisi, Sayı: 65(Özel), Nisan-Haziran 2007,
5. Davut Pehlivanlı, Modern İç Denetim(Güncel İç Denetim Uygulamaları), Beta Yayınları, İstanbul,2010
6. Office of the Comptroller, Quality Assurance Bureau, “Internal Control Guide”, 9/13/2007, www.mass.gov/osc
7. The University of California, “Understanding İnternal Controls, A Reference Guide for Managing University Business Practices”, http://www.ucop.edu/ctlacct/under-ic.pdf
8. IRM, “A Risk Management Standard”,2002,
9. Devlet Planlama Teşkilatı, Kamu İdareleri İçin Stratejik Planlama Kılavuzu,Haziran2006,
10. 5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu,
11. Maliye Bakanlığı, Kamu İç Kontrol Standartları Tebliği, 26.12.2007,
12. Maliye Bakanlığı, Kamu İdarelerince Hazırlanacak Faaliyet Raporları Hakkında Yönetmelik,17.03.2006.