INTOSAI GOV 9130

INTOSAI

Kamu Sektörü İç Kontrol Standartları Rehberi - Kurum Risk Yönetimi Hakkında Tamamlayıcı Ek Bilgiler

Çeviri:
Sacit YÖRÜKER
Sayıştay Uzman Denetçisi
2007

PSC-SECRETARIAT
RIGSREVISIONEN • LANDGREVEN 4 • P.O. BOX 9009 • 1022 COPENHAGEN K • DENMARK
TEL.:+45 3392 8400 • FAX:+45 3311 0415 • E-MAIL: INFO@RIGSREVISIONEN.DK

INTOSAI

EXPERIENTIA MUTUA
OMNIBUS PRODEST

INTOSAI General Secretariat - RECHNUNGSHOF
(Austrian Court of Audit)
DAMPFSCHIFFSTRASSE 2
A-1033 VIENNA
AUSTRIA
Tel.: ++43 (1) 711 71 • Fax: ++43 (1) 718 09 69

E-MAIL: intosai@rechnungshof.gv.at;
WORLD WIDE WEB: http://www.intosai.org

F. VANSTAPEL
Senior President of the Belgian Court of Audit

Regentschapsstraat 2 – Rue de la Régence 2
B-1000 BRUSSELS
BELGIUM

Tel : + 32 2 551 8111
Fax : + 32 2 551 8629
E-mail : international@ccrek.be

Kamu Sektörü

İç Kontrol Standartları Rehberi Kurum Risk Yönetimi Hakkında Tamamlayıcı Ek Bilgiler

Önsöz

1992 tarihli INTOSAI İç Kontrol Standartları Rehberi iç kontrolün planlanmasının, uygulanmasının ve değerlendirilmesinin teşvik edilmesi gerektiği düşüncesini yansıtan canlı bir doküman olarak tasarlanmıştı. Bu düşünce rehberi sürekli güncel tutma çabasını gerekli kılmaktadır.

17'nci INTOSAI Kongresi (Seul, 2001) 1992 tarihli rehberin artan güncellenme ihtiyacını saptamış ve Treadway Komisyonu Sponsor Organizasyonlar Komitesi (COSO) iç kontrol bütünleşik çerçevesinden bir model olarak yararlanmada mutabakatını belirtmiştir. Sonradan, güncellenmiş rehber etik değerleri ve bilgi işlenmesine ilişkin kontrol aktivitelerinin genel prensiplerini içerecek şekilde genişletilmiştir.

Güncellenmiş İç Kontrol Rehberi 2004 yılında yayımlanmıştır. Bu rehber de zaman içinde yeni gelişmelerin etkisini, örneğin COSO İşletme Risk Yönetim çerçevesini[1] *içerecek şekilde geliştirilecek ve rafine edilecek yaşayan bir doküman olarak görülmelidir. Dolayısıyla, Rehbere yapılan iş bu ekleme, COSO İşletme Risk Yönetim Modelinde belirtildiği gibi, risk yönetimi alanındaki güncel gelişmeleri yansıtmayı amaçlamaktadır. Bu doküman esas itibariyle kamu kesimindeki okurlara seslendiği için daha çok özel sektör bağlantısına sahip "işletme" (enterprise) terimi yerine "kurum" (entity) terimi kullanılmıştır.*

Burada sağlanan ek bilgiler INTOSAI İç Kontrol Standartları Alt Komitesi üyelerinin ortak çabalarının ürünüdür. Bu güncelleme, Fransa, Macaristan, Bangladeş, Litvanya, Hollanda, Umman, Ukrayna, Romanya, Birleşik Krallık, Amerika Birleşik Devletleri ve Belçika (Başkan) Sayıştaylarının temsilcileri arasından oluşturulan bir çalışma grubu tarafından koordine edilmiştir.

Franki VANSTAPEL

Belçika Sayıştayı Birinci Başkanı
INTOSAI İç Kontrol Standartları
Alt Komitesi Başkanı

[1] *İşletme Risk Yönetimi – Bütünleşik Çerçeve COSO- Eylül 2004)*

Giriş

COSO Kurum Risk Yönetimi temel varsayımına göre, her kurum paydaşlarına değer katmak için vardır. Kamu sektöründe, kamu görevlileri dürüstlük içinde kamu yararına hizmet etmeli ve kamu kaynaklarını doğru şekilde yönetmelidirler. Uygulamada paydaşlar, vatandaşlar ve onların seçilmiş temsilcileridir.

Bütün kurumlar belirsizlikle karşı karşıyadır. Yönetim bakımından temel zorluk, paydaşlara en fazla değeri sağlamaya çalışırken ne miktarda belirsizliğin kabul edileceğini belirlemektir. Ayrıca belirtmek gerekir ki, belirsizlik hem risk hem de fırsat kaynağıdır ve değeri aşındırma veya güçlendirme veyahut kamu sektörü terimiyle kamu yararına daha çok veya daha az hizmet etme potansiyeline sahiptir. Risk yönetiminin amacı, yönetime belirsizlikle ve bununla bağlantılı risklerle ve fırsatlarla etkili şekilde ilgilenme imkânı vermek, değer yaratma kapasitesini güçlendirmek, daha etkili hizmetleri eşitlik ve adalet gibi değerleri dikkate alarak daha verimli ve daha ekonomik şekilde sunmaktır.

INTOSAI Kamu Sektörü İç Kontrol Standartları Rehberi iç kontrolü bir kurumun amaçlarını gerçekleştirmesine imkân veren genel kapsamlı kavramsal bir çerçeve olarak görmektedir. COSO Kurum Risk Yönetim modeli ve benzeri diğer modeller daha uzağa gitmekte ve kurumun potansiyel riskleri ve fırsatları belirlemek suretiyle, amaçlarını netleştirerek ve riskleri en aza indirmek ve fırsatları en üste çıkarmak amacıyla iç kontrolları oluşturarak yönetilebileceğini ileri sürmektedir.

Kurum risk yönetimi yalnızca kurumsal yönetişim rejiminin kavradığı fonksiyonların tanımını genişletmemekte, ama aynı zamanda organizasyonların amaçlarını gerçekleştirmeyi düşünme

tarzında bir değişikliği gerekli kılmaktadır. Bu nedenle etkili olmak için kurum risk yönetimi, strateji belirlenmesinde dikkate alınan, organizasyonun her kademesinde ve her biriminde uygulamaya konan ve organizasyonun amaçlarını gerçekleştirme kapasitesini etkileyebilecek bütün olayları belirlemeyi hedefleyen sürekli bir prosestir.

Bu doküman kamu sektöründe kurum risk yönetiminin uygulanması için tavsiye edilen bir çerçevenin ana hatlarını çizmekte ve kendisine kıyasen kurum risk yönetiminin değerlendirilebilmesi amacıyla bir temel sağlamaktadır. Ancak, doküman Kamu Sektörü İç Kontrol Standartları Rehberinin yerine geçmeyi veya onun yerini doldurmayı amaçlamamakta; ama üye devletlerin uygun gördüğü hallerde bu standartların yanı sıra yararlanabilecekleri tamamlayıcı ek bilgiler sağlamayı hedeflemektedir. Ayrıca, iş bu doküman, yetkili makamların organizasyon bünyesinde mevzuat hazırlama, kural koyma veya siyasa belirleme yetkilerini sınırlamayı veya bu yetkilere müdahaleyi öngörmemektedir.

Sonuç olarak, açıkça belirtmek gerekir ki, bu dokümanın amacı kurumsal yönetişim standartları hakkında ilave yönlendirici ilkeler sunmaktır. Bu yönlendirici ilkeler bir en iyi kurumsal yönetişim rejimi pratiğinin uygulamaya geçirilmesi için detaylı siyasalar, prosedürler ve pratikler getirmediği gibi, bütün hukukî ortamlarda bütün organizasyonlar bakımından uygun değildir. Ne var ki, bu ek kurumların paydaşlara sağlanan hizmetleri en üst düzeye çıkarmalarına yardımcı olacak sistemleri geliştirebilecekleri bir genel çerçeve sağlamaktadır.

Bu dokümanın yapılanması nasıldır?

Bu ekin yapısı INTOSAI Kamu Sektörü İç Kontrol Standartları Rehberininkine benzerdir. Birinci bölümde kurum risk yönetimi tanımlanmakta ve kapsamı resmedilmektedir. İkinci bölümde kurum risk yönetiminin öğeleri sunulmakta ve iç kontrol standartlarına ekler vurgulanmaktadır.

Bölüm 1: Kurum Risk Yönetiminin Tasviri

1.1 Tanım

1.1.1 *COSO'nun "Kurum Risk Yönetimi: Bütünleşik Çerçeve" modeline göre, kurum risk yönetimi değer yaratmayı ve değer korumayı etkileyen riskleri ve fırsatları ele alıp işlemekte ve şu şekilde tanımlanmaktadır:*

"Kurum risk yönetimi; yönetim kurulu, yöneticiler ve diğer personel tarafından uygulamaya geçirilen; strateji hazırlanmasında ve organizasyonun bütün aktivitelerinde dikkate alınan; kurumu etkileyebilecek potansiyel olayları belirlemek ve risk iştahı sınırları içinde riskleri yönetmek için tasarlanan ve organizasyonun amaçlarına ulaşma konusunda makul güvence sağlayan bir prosestir" (COSO KRY modeli 2004)

1.1.2. *Kamu sektöründe "değer yaratma" ve "değer koruma" terimleri özel sektördeki gibi doğrudan doğruya ilgili olma özelliğine sahip değildir. Ancak, bu tanım, olabildiği kadar çok sektörü ve organizasyon türünü kapsamak amacıyla bilerek geniş tutulmuştur. Aslında tanımın kamu sektörü kurumlarına bütünüyle uygulanabilmesi için, "değer yaratma" ve "değer koruma"*

terimlerini "hizmet yaratma" "hizmet sürdürme" terimleri ile değiştirmek mümkündür.

1.2 Misyonun Belirlenmesi

***1.2.1** Kurum risk yönetimi için hareket noktası kurum tarafından belirlenen misyon veya vizyondur. Bu misyon çerçevesinde yönetim stratejik amaçları saptamalı, bu amaçları gerçekleştirecek stratejileri seçmeli ve bütün organizasyon kademelerine yayılan ikincil amaçları belirlemelidir.*

1.3 Amaçların Saptanması

***1.3.**1 INTOSAI İç Kontrol Standartları Rehberine göre, amaçlar aşağıdaki dört kategoride (amaçların çoğu birden fazla kategoriye giriyor olsa da) sınıflandırılabilir.*

***Stratejik**- organizasyonun misyonuna hizmet eden amaçlar*

***Operasyonel**- operasyonların düzenli, etik, ekonomik, verimli ve etkili şekilde uygulanması ve kaynakların kayıplara, kötüye kullanımlara ve hasarlara karşı korunması ile ilgili amaçlar.*

***Raporlama-** hesap verme sorumluluğu ile ilgili yükümlülüklerin yerine getirilmesi dahil olmak üzere raporlamanın güvenilirliğine ilişkin amaçlar*

***Uygunluk-** yürürlükteki yasalara ve yönetmeliklere uygunlukla ilgili ve hükümet siyasalarına uygun davranma kapasitesi ile ilişkili amaçlar*

1.3.2 *İlk iki kategorideki amaçlar tamamıyla kurumun kontrolünde değildir. Bu nedenle, risk yönetim sistemi, bu risklerin tatmin edici bir şekilde yönetildiği hakkında ancak makul güvence sağlayabilirse de yönetime bu amaçların ne ölçüde zamanında karşılanacağının farkında olma imkânını vermelidir. Buna karşılık, raporlamanın güvenilirliği ve uygunluk ile ilgili amaçlar kurumun kontrolü içindedir ve dolayısıyla etkili risk yönetimi, genellikle, bu amaçların karşılanmakta olduğu konusunda yönetime güvence verecektir.*

1.4 Hadiselerin- Risklerin ve Fırsatların Belirlenmesi

1.4.1 *Amaçların saptanmasının hemen ardından organizasyonun kurum risk yönetimi çerçevesinde, bu amaçların gerçekleşmesi üzerinde etkide bulunabilecek hadiseleri (events) belirmesi gerekir. Hadiseler olumsuz ya da olumlu bir etki doğurabileceği gibi her iki yönden etki yaratabilir. Olumsuz etki doğuran hadiseler kurumun amaçlarını gerçekleştirme kapasitesini engelleyebilen risklerdir. Bu riskler içsel ve dışsal etkenlerden kaynaklanabilir. Aşağıdaki 1 no'lu şema kamu kurumlarının karşılaştığı risklerden pek çoğunu göstermekte ise de, belirli kurumları ilgilendiren başka riskler de söz konusu olabilir.*

1.4.2 *Olumlu etki doğuran hadiseler olumsuz etkileri telafi edebilir veya fırsatlar oluşturabilir. Fırsatlar; meydana gelecek hadisenin kurumun amaçlarını gerçekleştirme kapasitesini artırma veyahut kuruma amaçlara daha verimli ulaşma imkânı verme olasılığıdır. Yönetim sadece riskleri en aza indirmeyi araştırmakla kalmamalı, fırsatları kavrayan planlar hazırlamalıdır.*

1.5 İletişim ve Öğrenme

1.5.1 *Bir kurumun risk yönetiminin "arzulanan etkiye sahip" olup olmadığının belirlenmesi sürecinin çok önemli bir öğesidir. Yönetimin, kurum risk yönetiminin öğelerinin uygulamaya konulup konulmadığını ve etkili şekilde işleyip işlemediğini, yani önemli yetersizlikler bulunup bulunmadığını ve bütün risklerin, kurum risk iştahı sınırları içinde kabul edilebilir parametrelere indirilip indirilmediğini değerlendirmesi gerekir. Kurum risk yönetiminin arzulanan etkiye sahip yönetim olduğu ahvalde, kurum yönetimi, dört kategorideki amaçların misyona ne ölçüde uygun düştüğünü ve amaçlara ne derecede ulaşıldığını anlayacaktır. Bütün kurumda dikine ve enine etkili bir iletişim bu süreci kolaylaştırmak için elzemdir.*

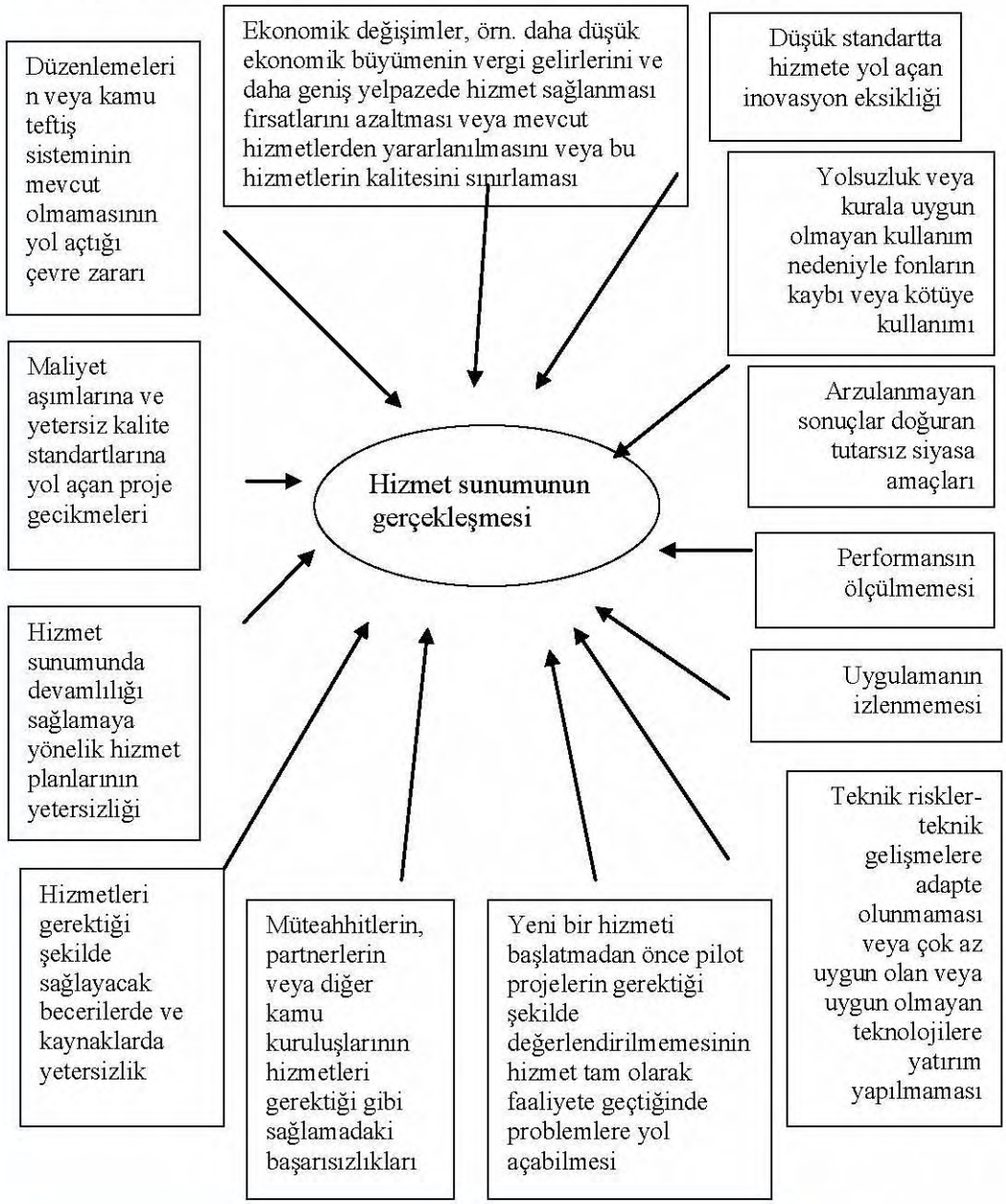
1.6 Sınırlamalar

1.6.1 *Sistem ne kadar iyi tasarlanıp işlerse işlesin kurum risk yönetimi yöneticilere genel amaçlara ulaşıldığı hakkında mutlak güvence sağlayamaz. Bu nedenle iş bu doküman ancak makul bir güvence düzeyine ulaşılabileceğini kabul etmektedir.*

1.6.2 *Makul güvence; amaçlara ulaşılması veyahut amaçlara ulaşılması olası değilse yönetimin zamanında bilgi sahibi olması hakkında tatmin edici bir güven düzeyine tekabül etmektedir. Tatmin edici güven düzeyine erişmek için ne kadar güvence gerektiğinin belirlenmesi bir değer hükmü meselesidir. Bu değer hükmünü verirken yöneticilerin kurumun risk iştahını ve amaçlara ulaşılma üzerinde etkisi olabilecek hadiseleri değerlendirmeleri gerekir.*

1.6.3 *Makul güvence; belirsizliğin ve riskin gelecekle ilgili olduğu, bunu da kimsenin kesinlikle tahmin edemeyeceği düşüncesini yansıtmaktadır. Ayrıca, kurumun kontrolü veya etkisi dışındaki faktörler, örneğin siyasi faktörler, amaçlara ulaşma üzerinde etkide bulunabilir. Kamu sektöründe kurumun kontrolü dışındaki faktörler çok kısa sürede temel amaçları bile değiştirebilir. Diğer sınırlamalar şu gerçeklerin sonucu olabilir: karar alırken verilen değer hükmünün hatalı olması, aksaklıkların beşerî kusurlar örneğin hatalar veya yanılmalar nedeniyle vuku bulması, risklere karşı alınan kararların ve belirlenen kontrolların maliyetleri ve faydaları dikkate alma zorunluluğu, iki veya daha fazla kişinin hileli anlaşması yoluyla kontrollardan sıyrılınması ve üst yöneticilerin iç kontrol sistemini umursamaması. Bu sınırlamalar yönetimin amaçlara ulaşma konusunda mutlak güvence elde etmesini engellemektedir. 1 no'lu şemada karşılaşılabilecek tipik risklerden bazıları gösterilmektedir. Şema açıklayıcı olmayı amaç edinmiş olup sınırlayıcı değildir.*

Şema 1: Kamu Kurumlarının Karşılaştıkları Bazı Tipik Riskler



1.7 İç kontrol ile Kurum Risk Yönetimi Arasındaki İlişki

1.7.1 *Pek çok bakımdan kurum risk yönetimi iç kontrol modelinin doğal bir evrimi olarak görülebilir. Organizasyonların çoğu kurum risk yönetimiyle bütünleşik konseptleri uygulamaya koymadan önce iç kontrol modelini eksiksiz olarak uygulamaya yönelmektedirler. İç kontrol, kurum risk yönetiminin bütünleşik bir parçasıdır. Kurum risk yönetimi modeli iç kontrolü kapsamakla kalmaz, kurum işletim kararlarının nasıl ana misyondan ve bağlantılı amaçlardan akıp geldiği hakkında daha sağlam bir kavramlaştırma oluşturur ve belirli hadise karşısındaki doğru cevabın ne olması gerektiğini belirlemede yönetime yardımcı olacak bir araç sağlar. Kurum Risk Yönetim Modeli, özellikle aşağıda belirtilen alanlarda, INTOSAI İç Kontrol Rehberinden daha ileri gider:*

Amaç kategorileri daha geniştir ve ayrıca daha eksiksiz raporlamayı, finansal olmayan bilgileri, stratejik amaçları içerir;

Risk değerlendirme öğesini kapsar ve risk iştahı, risk toleransı, risk cevabı gibi değişik risk konseptlerini ortaya getirir;

Yönetim kurulunda bağımsız yöneticilerin önemine vurgu yapar ve onların rollerini ve sorumluluklarını ayrıntıları ile açıklar.

Bölüm 2: Kurum Risk Yönetiminin Öğeleri

Kurum risk yönetimi birbiriyle karşılıklı ilişkili sekiz öğeden oluşmaktadır. Bu öğeler organizasyonun yönetilme biçiminden kaynaklanmakta olup yönetim süreciyle bütünleşmişlerdir. Bu öğeler şunlardır:

- *Kontrol ortamı,*
- *Amaç belirlenmesi,*
- *Hadiselerin (event) tanımlaması,*
- *Risklerin değerlendirilmesi,*
- *Risk cevabı,*
- *Kontrol faaliyetleri,*
- *Bilgi ve iletişim,*
- *İzleme.*

Risk yönetiminin öğelerini uygularken kurum, organizasyonun tüm kademelerindeki faaliyetlerinin bütününü dikkate almalıdır. Yönetim, ayrıca, risk yönetim modelini uygularken yeni projeleri ve girişimleri incelemelidir.

Risk Yönetiminin Kurumun Bütününe Uygulanması

Yönetimin bütünsel bir risk yaklaşımına sahip olması gerekir. Pratikte bütün yönetim kademeleri, kendi faaliyet alanlarını etkileyebilecek hadiseleri değerlendirmeli ve bu konuda üst düzey yöneticileri bilgilendirmelidirler. Bu değerlendirme nitel ya da nicel olabilir. Üst yönetim, organizasyon bütününde global bir risk değerlendirmesi oluşturmak amacıyla kurumun bütün faaliyet kademelerini ve alanlarını kapsayan bu değerlendirmelerden yararlanmalıdır.

İnsanın Önemi

Kurum risk yönetimi yönetim ve diğer personel tarafından uygulamaya konulur ve etkili şekilde işletilir. Kurum risk yönetimi organizasyon bünyesindeki bireylerin yaptıklarıyla ve söylediklerıyle gerçekleşir. Benzer şekilde, kurum risk yönetimi bireylerin eylemlerini etkiler. Her çalışan, farklı ustalıklara ve farklı anlama yetilerine sahip bir bireydir. Kurum risk yönetimi, personele kurumun amaçları bağlamında riskleri kavrama imkânı verecek mekanizmaları yaratmaya yönelir.

Personelin sorumluluklarını ve yetki sınırlarını bilmeleri gerekir. Bu nedenle, kişinin görevleri ile bu görevleri yerine getirme tarzı arasında açık ve doğrudan bir ilişki bulunmalıdır. Üst düzey yönetim esas itibariyle gözetimle yükümlüdür. Böyle olmakla birlikte, üst düzey yöneticiler, ayrıca, gidilecek yönü belirler, stratejileri, belirli işlemleri ve siyasaları onaylar ve dolayısıyla

organizasyon kültürüne uyulmasını sağlamada yaşamsal bir rol oynar.

2.1 Risk Ortamı/Bağlamı

2.1.1 *Risk ortamı/bağlamı, organizasyondaki bütün bireylerin risk bilincini etkilediği için organizasyonunun kültürünü yansıtır ve bir disiplin ve yapı getirmek suretiyle kurum risk yönetiminin diğer bütün öğeleri için bir temel oluşturur. Kurumun risk yönetim felsefesi, risk iştahı, yönetim kurulunca yapılan gözetim, dürüstlük ve etik değerler, personelin uzmanlıkları ve yönetimin yetkileri ve sorumlulukları dağıtma ve personeli organize etme ve geliştirme tarzı iç ortam faktörleri arasındadır.*

2.1.2 *Bir kurumun risk yönetim felsefesi, kurumun strateji saptamasından günlük operasyonel aktivitelere kadarki her şeyde riski nasıl değerlendirdiğini belirleyen ortak inançlar ve tutumlar setidir. Risk yönetim felsefesi; kültür ve faaliyet tarzı ve özellikle risklerin nasıl belirlendiği, kabul edilen risklerin türü ve risklerin nasıl yönetildiği üzerinde etki yapar. Bir kurumun risk yönetim felsefesi siyasa bildirimlerinde, paydaşlara ve personele yönelik sözlü ve yazılı iletimlerde ve alınan kararlarda belli edilmelidir. İletim yöntemi ne olursa olsun, üst yönetimin sadece iletim siyasaları yoluyla değil, ama aynı zamanda gündelik eylemleri aracılığıyla felsefeyi güçlendirmesi son derecede önemlidir.*

2.1.3 *Risk iştahı, bir kurumun amaçlarına ulaşmak için kabul etmeye hazır olduğu risk düzeyine tekabül etmektedir. Risk iştahı, risk yönetim felsefesini yansıtır; kurumun kültürünü ve faaliyet tarzını etkiler. Risk iştahı nicel veya nitel olarak tahmin edilebilir. Risk iştahı strateji belirlemede dikkate alınmalıdır ki, bu durumda*

bir stratejinin tahmin edilen yararı ile risk iştahı yani riski kabul veya tolere etme arasında bir paralellik bulunmalıdır.

***2.1.4** Öte yandan, risk ortamının kimliğini saptarken ve uygun risk iştahını seçerken kamu sektöründeki kurumların "genişletilmiş kurum" kavramını dikkate almaları gerekir. Diğer kamu organları veya yasama organları söz konusu olsun sponsorluk yapan veya sponsorluk edilen kuruluşların görüşleri ve beklentileri ve partner konumundaki kuruluşların düşünceleri uygun risk yönetme felsefesi ve risk iştahı konusunda doğrultuyu net bir şekilde gösterebilir.*

***2.1.5** Bir kurumun üst yönetimi iç ortamın yaşamsal bir parçasıdır ve iç ortamın öğelerini önemli derecede etkiler. Organizasyon kültürünün "üst yönetimin anlayışı" tarafından belirlendiği veya tersine altının oyulduğu malumun ilâmıdır. Üst yönetimin icra yönetiminden bağımsızlığı, üyelerinin deneyimi ve çapı, müdahil olma ve denetleme dereceleri ve faaliyetlerinin isabetliliği gibi hususlar bir rol oynar. Üst icra yönetiminin üyeleri üst yönetimin parçası olabilirse de, iç ortamın etkili olmasını sağlamak için üst yönetim ekibi içinde kurum dışından bağımsız birkaç üyenin bulunması uygun olur. Bunun nedeni, üst yönetimin faaliyetlerini sorgulayarak ve denetleyerek icra yönetimini hesap vermeyle yükümlü tutmaya ve alternatif görüşler sunmaya hazır olması gerektiğidir.*

2.1.6 *Yönetimin dürüstlüğü ve etik değerleri stratejinin ve amaçların uygulamaya konulmasını etkiler. Kurumun iyi bir şöhrete sahip olması o kadar değerlidir ki, davranış standartlarının asgarî yasal gerekliliklere basitçe bir uymanın ötesine geçmesi gerekir. Etik davranış ve yönetimin dürüstlüğü; etik ve davranış standartlarını ve bu standartların iletilmesini ve bunlara uyulmasını içeren kurum kültürünün yan ürünüdür. Üst yönetim kurum kültürünün belirlenmesinde kilit rol oynar. Genel misyonun gerçekleştirilmesi yerine kısa vadeli sonuçlara gereksiz önem verilmesi uygun olmayan bir iç ortamı güçlendirebilir.*

2.1.7 *Formel davranış kuralları önemlidir ve uygun etik anlayışın temelidir. Çalışanların yönetim kuruluna uygun bilgileri iletme imkânı veren aşağıdan yukarı iletim kanalları (veya formel ihbar prosedürleri) da önemlidir. Ne var ki, yazılı bir davranış kurallarının varlığı, bütün çalışanlar kendilerinden beklenen davranışlar hakkında bilgilendirildiklerini beyan etmiş olsalar bile, kendi başına prosedürlere uyulmasını güven altına almaz. Kuralları ihlal eden çalışanlar için yaptırımların mevcudiyeti de aynı derecede önemlidir. Üst yönetim tarafından gönderilen mesajlar çabucak kurum kültürüyle bütünleşir, öyle ki kompleks yönetim kararlarıyla karşılaşıldığında sahip olunacak "doğru tepkiler" kurum bütününe yerleşir.*

2.1.8 *Uzmanlık, verilen görevlerin yerine getirilmesi için ihtiyaç duyulan bilgileri ve becerileri ifade eder. Uzmanlık; uygun kişilerin işe alınmasına ve yükseltilmesine, bu kişilerin görevlere tahsislerine ve eğitilmelerine ve yetersiz performanslara çözüm bulunmasına ilişkin insan kaynakları pratikleri aracılığıyla desteklenmelidir. Yönetim, belirli görevler için spesifik uzmanlık düzeylerini belirlemeli ve bunları spesifik kadrolarla ilgili uygun*

görev tanımlarına dönüştürmelidir. Uzmanlık ile maliyet arasında bir denge bulunabileceğinin kabul edilmesi işin önemli bir yönüdür.

***2.1.9** Bir kurumun organizasyonel yapısı kuruma faaliyetlerini planlama, uygulama, kontrol etme ve izleme imkânını sağlayan çerçeveyi verir. Organizasyonel yapı işletim ihtiyaçlarına uygun olacaktır. Bazı kurumların merkezîleştirilmiş olmasına karşılık diğerleri adem-î merkeziyetçi yapıdadır. Bazı kurumlar coğrafî mahalle göre organize edilmiş oldukları halde diğerlerinin organizasyonu fonksiyona göredir. Yapı ne olursa olsun, bir kurum, riskleri etkili olarak yönetmesine ve amaçlarına ulaşmak üzere faaliyetlerini yürütmesine imkân verecek şekilde organize edilmelidir.*

***2.1.10** Yetkilerin ve sorumlulukların sınırlarının çizilmesi kişilerin ve ekiplerin sorunları ele almak ve problemleri çözmek için inisiyatif kullanmada yetkili olma ve desteklenme derecesini ve yetkilerinin sınırlarını ilgilendirmektedir. Temel zorluklar bütün personelin kurumun amaçlarını anlaması, kendi eylemlerinin bu amaçların gerçekleşmesine nasıl katkıda bulunacağı ve sadece bu amaçlara ulaşma gerektirdiği ölçüde bu sorumlulukların devredilmesidir. Sorumluluk yetki kadar önemlidir. İç ortam, bireylerin hesap vermekle yükümlü olacaklarının bilincinde olma derecesinden büyük ölçüde etkilenir. Bu, icra başkanı dahil olmak üzere bütün kademeler için geçerlidir.*

2.2 Amaçların Belirlenmesi

2.2.1 *Amaçlar stratejik düzeyde belirlenir ve daha alt düzeydeki operasyonlar, raporlar ve uygunluk ile ilgili amaçlar için bir temel oluşturur. Her kurum iç ve dış kaynaklı çeşitli risklerle karşılaşır ve amaçların belirlenmesi, hadiselerin etkili şekilde tanımlanmasının, risklerin değerlendirilmesinin ve risk cevabının hazırlanmasının bir ön koşuludur. Amaçlar yönetimin bu amaçların gerçekleşmesine yönelik riskleri belirleyebilmesi ve değerlendirebilmesi ve bu risklerin azaltılması için gerekli girişimlerde bulunulabilmesi amacıyla belirlenmelidir. Amaçlar, kurum risk tolerans düzeylerini saptayan kurum risk iştahına paraleldir.*

2.2.2 *Kurumun misyon bildirimi, kalın hatlarıyla, kurumun nelere ulaşmayı arzu ettiğini belirler. Yönetim; stratejik amaçları saptar, stratejiyi formüle eder ve tekabül eden faaliyetleri tespit eder. Stratejik amaçlar, kurumun misyonuna paralel olan ve bu misyonu destekleyen üst düzey hedeflerdir. Misyonu ve ilişkili amaçları gerçekleştirmek için uygulanan strateji misyondan daha dinamiktir ve koşullardaki değişikliği yansıtmak üzere ayarlanır.*

2.2.3 *Kurumların amaçları çeşitlilik göstermekte ise de bazı genel kategoriler uygulanabilir. Bütün amaçlar aşağıdaki kategorilerden birisiyle veya daha fazlasıyla ilişkili olmaktadır:*

Operasyonel amaçlar- *Bu amaçlar, performans hedefleri ve kaynakların kayıplara karşı korunması dahil olmak üzere, kurumun faaliyetlerinin etkililiği ve verimliliği ile ilişkilidir. Hesapların kamuoyuna raporlanması bağlamında "kaynakların/varlıkların korunması" tanımı şu şekilde genişletilebilir: kamu fonlarının zimmete geçirilmesinin önlenmesi veyahut ortaya çıkarılması ve*

düzeltilmesi. Operasyonel amaçların içinde kurumun faaliyet gösterdiği belirli bir ortamı yansıtması gerekir. Operasyonel amaçlar tahsis edilen kaynakların yönetilmesinde odak noktaları olduğu için, operasyonel amaçlar net değilse veya iyi kavranmamışsa, bu kaynaklar iyi yönetilmeyebilir.

Raporlamayla ilgili amaçlar- *Bu amaçlar raporlamanın güvenilirliği ile ilişkili olup hem malî hem de malî olmayan verileri içerebilir. Raporlamayla ilgili amaçlar üçüncü kişiler için hazırlanan bilgilerle ilişkili olsa da güvenilir raporlamanın temel amacı, yönetime tespit edilen hedefe uygun, doğru ve eksiksiz bilgiler sağlamaktır. Doğru ve eksiksiz bilgiler olmaksızın iyi kararlar vermek yönetim açısından son derecede zordur.*

Uygunlukla ilgili amaçlar- *Bu amaçlar yasalara ve yönetmeliklere uygunlukla ilgili amaçlardır. Piyasalarla, çevreyle, çalışanların refahıyla ve benzeri konularla ilgili kurallar söz konusu olabilir. Bazı kurumların uluslararası uygunluk amaçlarına uyum göstermeleri de gerekebilir.*

2.2.4 *Etkili risk yönetimi, bir kurumun operasyonel, raporlama ve uygunluk ile ilgili amaçlarının gerçekleşmekte olduğu konusunda makul güvence sağlar.*

2.2.5 *Yönetim ve yönetim kurulu tarafından belirlenen risk iştahı, strateji saptamada ve amaçların göreli önemini değerlendirmede bir yönlendirici işarettir. Gerçekte, risk iştahı, bir kurumun paydaşlar için değer (kamu hizmetleri biçiminde) yaratmada kabul etmeye hazır olduğu risk seviyesidir. Genellikle, hedeflenen misyonu gerçekleştirmek üzere her biri farklı risklere sahip bir çok strateji tasarlanabilir. Yönetim, risk iştahı ile en çok uyuşan stratejiyi ve bağlantılı amaçları seçmelidir.*

2.2.6 *Risk toleransı, amaçların gerçekleşmesiyle ilgili olarak kabul edilebilir fark düzeyidir. Risk toleransı performans hedefleri yardımıyla ölçülebilir. Performans hedefleri; çoğu kez, amaçların ilişkili olduğu aynı birimlerde ölçülür. Risk toleransları çerçevesinde faaliyet göstermek yönetime kurumun risk iştahı içinde kaldığı ve amaçlarını gerçekleştirdiği konusunda çok daha fazla güvence sağlar.*

2.3 Hadiselerin Tanımlanması (Event Identification)

2.3.1 *Yönetim, vuku bulunca, kurumu etkileyecek potansiyel hadiseleri (events) tanımlar. Fırsatları temsil eden hadiseleri, kurumun stratejiyi başarılı şekilde uygulama ve amaçları gerçekleştirme kabiliyetini olumsuz şekilde etkileyen hadiselerden (risklerden) ayırmak gerekir. Hadiseleri tanımlamak için yönetim, kurumun bütünü bağlamında risklere ve fırsatlara yol açabilen iç ve dış faktörler dizisini dikkate alır.*

2.3.2 *Hadiseler; stratejinin uygulanmasını veya amaçların gerçekleşmesini etkileyen iç veya dış orijinli olaylar (incidents) veya vakalardır (occurences). Hadiseler olumlu veya olumsuz*

veyahut da hem olumlu hem de olumsuz etkiye sahip olabilir. Bazı hadiseler apaçık görülür iken bazıları belirsizdir ve hadiseler önemsiz veya hatırı sayılır etkilere sahip olabilir. Hadiselerin gözden kaçmasını önlemek için hadiselerin tanımlanması ile hadiselerin vuku ihtimalinin ve etkilerinin değerlendirilmesinin birbirinden ayrı olarak yapılması uygun olur.

***2.3.3** Yönetimin hadiseleri belirleyen iç ve dış faktörlerin temel kategorilerini anlaması gerekir. Dış faktörler; özellikle, politik, sosyal ve teknolojik ortamdaki değişikliklerden ve kurumu veya tedarikçileri etkileyen ekonomik sorunlardan kaynaklanan faktörlerdir. İç faktörler, yönetimin işleyiş tarzı ile ilgili olarak yaptığı tercihlerden kaynaklanır. İç faktörler, kurumun alt yapısı, kurumun kaç mahalde faaliyet gösterdiği, personelin becerileri ve uzmanlıkları, kurum bilgi sistemlerinin nasıl işlediği gibi hususları içerir.*

***2.3.4** Hadiselerin tanımlanması teknikleri hem geçmişe hem de geleceğe dönüktür. Geçmiş hadiselere odaklanan teknikler, yıllık raporlar ve hesaplar, hatalı ödemelerle ilgili açıklamalar, iç raporlar gibi öğeleri değerlendirebilir. Gelecekteki hadiselere odaklanan teknikler, nüfus değişikliği, yeni piyasa koşulları ve siyasal ortamda beklenen değişiklikler gibi faktörlerle ilgilenebilir. Bu teknikler karmaşıklık ve otomasyon düzeyleri bakımından çok değişkenlik gösterir ve hadiselere yukarıdan aşağıya veyahut da aşağıdan yukarıya bakış açısıyla odaklanabilir.*

2.3.5 *Hadiselerin soyutlanmış şekilde vuku bulması az rastlanan bir durumdur. Bir hadise diğerini tetikleyebilir ve hadiseler eş zamanlı olarak vuku bulabilir. Yönetim, hadiselerin karşılıklı olarak birbirleriyle nasıl bağlantılı olduklarını anlamalıdır. İlişkileri değerlendirmek suretiyle risk yönetim çabalarının nerelere yönlendirileceğini belirlemek mümkün olabilir.*

2.3.6 *Potansiyel hadiseleri kategoriler içinde gruplandırmak da yararlı olabilir. Hadiselerin yatay olarak bütün kurum bünyesinde, dikine olarak da faaliyet birimleri bünyesinde toplanması yönetime hadiseler arasındaki ilişkileri kavrama imkânı verir. Hadiselerin gruplandırılması, ayrıca, en maliyet etkin cevapların neler olduğu konusunda işaretler verebilir. Her kurum hadise gruplandırmasında kendi metodunu oluşturabilirse de, standart araçlara örneğin "PEST" Piyasa Analizi2 metoduna dayanabilir.*

2.4 Risklerin Değerlendirilmesi

2.4.1 *Risklerin değerlendirilmesi, kuruma, potansiyel hadiselerin amaçların gerçekleşmesi üzerinde ne derecede bir etkiye sahip olduğunu değerlendirme imkânı verir. Yönetim, hadiseleri, nicel ve nitel tekniklerin bir kombinasyonundan yararlanmak suretiyle iki perspektiften –etki ve olasılık- değerlendirmelidir. Hadiselerin olumlu ve olumsuz etkileri ya bireysel olarak ya da kurum bütününü kavrayan kategori itibariyle değerlendirebilir. Risk değerlendirmesi hem bireysel riskler hem de artık riskler temelinde yapılmalıdır.*

"PEST" analizi kurum amaçları üzerindeki dış faktörlerin etkisini kavramaya ve değerlendirmeye imkân veren yararlı bir araçtır. PEST Politik (Political), Ekonomik (Economic), Sosyal (Social) ve Teknolojik (Technological) faktörlerin kısaltılmış adıdır.

2.4.2 *"Risklerin değerlendirmesi" terimi zaman zaman tek bir aktiviteyi belirtmek için kullanılmakta ise de, kurum risk yönetimi bağlamında risk değerlendirme öğesi daha çok kurumun bütününde gerçekşeşen devamlı ve tekrarlanan etkileşimli eylemler olarak kabul edilir. Risk değerlendirmesinin amacı hangi hadiselerin yönetimin dikkatinin odaklanacağı kadar önemli ve anlamlı olduğunu belirlemektir.*

2.4.3 *Potansiyel olaylara ilişkin belirsizliklerin olasılık ve etki perspektiflerinden değerlendirilmesi gerekir. Olasılık (likelihood), bir hadisenin belirli bir zaman periyodu içinde vuku bulma ihtimalini (possibility) ifade etmesine karşılık, etki (impact) hadisenin kurumun kendi amaçlarını gerçekleştirme kabiliyeti üzerindeki tesir (effect) derecesi anlamına gelmektedir. Yönetimin süresince olasılığı değerlendirdiği zaman süresi, ilgili strateji ve amaçların zaman ufkuna tekabül etmelidir. En önemli riskler vuku olasılığı ve etkisi yüksek olan risklerdir. Bunun tersine en az önem taşıyan riskler vuku olasılığı ve etkisi düşük olan risklerdir. Yönetim çabalarını yüksek olasılıklı ve yüksek etkili risklere odaklamalıdır. (Aşağıdaki 2 numaralı şemaya bakın.) Sürecin nihaî neticesi her bir riski olasılık ve etki açısından derecelendirmek olacaktır. Bazı kurumlar "yüksek-düşük" şeklindeki derecelendirmeyi kullandıkları halde, diğer bazı kurumlar "trafik ışığı" sisteminde olduğu gibi kırmızı, sarımsı kahverengi ve yeşil renkleri ve başkaları nicel bir ölçüyü, örneğin yüzde oranını kullanmaktadırlar.*

Şema 2: Basit Risk Değerlendirmesi ve Cevap Matrisi

2.4.4 *Risk değerlendirme metodolojisi nicel veya nitel olabilir; objektif ya da sübjektif metotlara dayanabilir. Ayrıca, bir kurumun bütün faaliyet alanlarında klasik değerlendirme tekniklerini kullanması gerekmez. Ancak, yönetimin riskleri değerlendirirken insanî faktörlerin farkında olması ve ilgili bütün personelin bu değerlendirme için kullanılan derecelendirme sisteminin anlamını kavramalarını sağlaması gerekir. Bu gerçekleşmezse, üst yönetimin çeşitli risklerin her birinin önemini belirlemesi zor olacaktır.*

2.4.5 *Risk değerlendirmesi tamamlanır tamamlanmaz, kurumun risk öncelikleri belli olmalıdır. Eğer riske maruz olma kurumun risk iştahı çerçevesinde kabul edilemez ise, risk "yüksek öncelikli"*

veya "kilit risk" olarak sınıflandırılmalıdır. Kilit risklere kurumun en üst kademesinde düzenli olarak dikkat gösterilmelidir. Kurum başka amaçlar belirledikçe, risk ortamı değiştikçe ve temel risklere cevap verildikçe spesifik risk öncelikleri zaman içinde değişiklik gösterecektir.

2.4.6 *Yukarıda ana hatlarıyla açıklanan risk değerlendirmesi "bünyesel risk" ile ilişkilidir. Bünyesel risk, yönetimin hadisenin vuku ihtimalini veya etkisini değiştirmek üzere yapacağı eylemlerinin yokluğunda kurumun karşılaşacağı risktir. Artık risk, aşağıdaki paragrafta ana hatlarıyla açıklanan yönetim risk cevabının (karşılığının) dikkate alınmasından sonra geriye kalan risktir. Bu metodun avantajı, kurumlara diğer sorunları çözmek için daha iyi harcanabilecek iken yönetim tarafından bu zaman kendilerine ayrılan riskleri belirleme imkânı vermesidir. (Örneğin, bünyesel riskin vuku ihtimalinin düşük olması nedeniyle böyledir.)*

2.5 Riske Cevap (Risk Response)

2.5.1 *İlgili riski değerlendirdikten sonra yönetim bu riske nasıl cevap verileceğini kararlaştırır. Tanımlanmış riske cevap verme biçimleri arasında riskin transferi, riskin iyileştirilmesi, faaliyetlerin sona erdirilmesi ve riske katlanılması yöntemleri yer almaktadır. Kendi cevap türünü belirlerken, arzulanan risk toleransı çerçevesinde artık riski taşıyacak cevabı seçmek amacıyla, yönetim olasılık ve etki üzerindeki tesiri değerlendirir ve her bir cevabın maliyetini ve faydasını dikkate alır. Yönetim, ayrıca, yararlanılabilir bütün fırsatları belirlemeli ve global risk visyonu elde edilmesine imkân sağlamalıdır.*

2.5.2 *Risk cevapları aşağıdaki kategorilerde dizilmektedir:*

Paylaşma/Riskin Transferi- *Riskin bir bölümünün transfer edilmesi veya paylaşılması suretiyle bu risk olasılığının veya etkisinin azaltılması. Bu, klasik sigorta yoluyla veyahut üçüncü kişiye riski bir başka şekilde üstlenmesi için ödeme yapılması suretiyle gerçekleştirebilir. Bu seçenek, özellikle, finansal riskleri, varlıklarla ve dışarıya yaptırılan faaliyetlerle ilgili riskleri azaltmada yararlıdır. Ne var ki, risklerin çoğu bütünüyle transfer edilemez. Özellikle, hizmet dışarıdan sağlanmış olsa bile, tanınmışlıkla ilgili riskin transferi genellikle mümkün değildir.*

Azaltma/Riskin İyileştirilmesi- *Risklerin büyük çoğunluğu bu şekilde çözümlenir. Risk olasılığını veya etkisini veyahut her ikisini azaltmak için önlemler alınır. Bu tür bir cevap; detaylı şekilde 2.6 numaralı bölümde ve İç Kontrol- Bütünleşik Çerçevede ele alınan kontrol prosedürleri dahil olmak üzere, genellikle, çok sayıda günlük yönetsel kararları kapsar.*

Kaçınma/Faaliyetin Sona Erdirilmesi- *Bu tür cevapta riske yol açan aktivitelere son verilir. Kamu sektörü kurumlarının bir ana program unsurunun sağlanmasından vazgeçmeleri çok seyrek bir durum olmakla birlikte, yeni bir hizmet sunum metodunun uygun olup olmadığının değerlendirilmesi veyahut spesifik bir projeye devam etmenin yerinde olup olmadığının belirlenmesi söz konusu olduğunda kaçınma (vazgeçme) yararlı bir cevap olabilir.*

Kabul/Katlanma- *Risk olasılığını veya risk etkisini azaltmak için hiçbir önlem alınmaz. Bu cevap; etkiyi veya olasılığı kabul edilebilir bir düzeye indirmek için verimli bir metot belirlenmemiş olduğunu veyahut bünyesel riskin zaten kabul edilebilir düzeyde bulunduğunu varsaymaktadır. Kuşkusuz, riske katlanılması, eğer risk gerçekleşirse doğacak etkileri ele alan müdahale önlemleri ile desteklenebilir.*

2.5.3 *"Kurum Risk Yönetim" modeli sadece riskleri önceden tahmin edip yönetmeye değil, ama aynı zamanda, aynı yaklaşım çerçevesinde fırsatları belirlemeye vurgu yapmaktadır. Hangi durumla karşılaşırsa karşılaşsın, yönetim sadece olumsuz etkileri olan riskleri veya hadiseleri değil, olumlu etkiler barındıran fırsatları veya hadiseleri dikkate almalıdır. Bu konuda iki husus söz konusudur. İlkin, tehditlerin azalmasına paralel olarak, olumlu etkiden yararlanmaya yönelik bir fırsatın ortaya çıkıp çıkmadığını; ikinci olarak da tehditler doğurmaksızın olumlu fırsatlar yaratan koşulların ortaya çıkıp çıkmadığını incelemek gerekir.*

2.5.4 *Yönetim; riski ele alan çeşitli metotların etkilerini değerlendirmenin ardından risk tolerans sınırları çerçevesinde hem risk olasılığına hem de risk etkisine yönelik olarak tasarlanmış bir cevabı veya cevap kombinasyonunu seçmek suretiyle riskin en iyi nasıl yönetileceğine karar vermelidir. Seçilen cevabın zorunlu*

olarak, en az miktarda artık risk sonucunu doğurması gerekmez. Ancak, eğer cevap yine de risk tolerans derecesini aşıyorsa, yönetimin ya cevabı ya da risk tolerans düzeyini yeniden incelemesi gerekecektir.

2.5.5 *Bünyesel riske yönelik alternatif cevapların değerlendirilmesi, bir cevaptan kaynaklanabilen ilave risklerin dikkate alınmasını gerektirir. Bu durumda üst yönetimin cevapları global perspektiften değerlendirmesi yararlı olur. Bu değerlendirme, üst yönetime genel risk cevap profiline ilişkin genel bir bakış vereceği gibi varlığını sürdüren artık risklerin türlerinin ve niteliğinin genel misyona ve risk iştahına uygun düşüp düşmediğini inceleme imkânı sağlar.*

2.5.6 *Riskleri karşılamak için tercih edilen metotların seçiminin hemen ardından yönetimin bir uygulama planı hazırlaması gerekir. Her uygulama planının kritik kısmı kontrol faaliyetlerinin risk cevabının etkili şekilde icra edilmesini sağlamasıdır.*

2.6 Kontrol Faaliyetleri

2.6.1 *Kontrol faaliyetleri; yönetimin risklere yönelik cevaplarının uygulanmakta olduğunu güven altına alan siyasalar ve prosedürler bütünüdür. Kontrol faaliyetleri bütün organizasyonda, bütün kademelerde ve bütün fonksiyonlarda cereyan eder. Kamu Sektörü İç Kontrol Standartları Rehberi etkili kontrolları oluşturulmasıyla ilgili ayrıntılı bilgiler içermekte olduğundan, bu Ek iç kontrolları kurum risk yönetimi bağlamı içine yerleştirmekten başka bir amaç taşımamaktadır.*

2.6.2 *Kurum risk yönetimi, kontrol faaliyetlerini, bir kurum tarafından yönetim amaçlarına ulaşmak için uygulanan prosesin*

önemli bir parçası olarak görmektedir. Kontrol faaliyetleri sadece kendi başına bir amaç olmadığı gibi "yapılacak doğru şey" olarak ortaya çıkmaz. Bu faaliyet, daha çok, yönetim amaçlarının gerçekleşmesini sağlamaya imkân veren mekanizmalar olarak hizmet görür.

2.6.3 *Kontrol faaliyetleri, genellikle, risk cevaplarının gerektiği şekilde uygulanmalarını sağlamak üzere oluşturulmakta ise de bazı amaçlar bakımından bizatihî kontrol faaliyetleri risk cevabıdır. Kontrol faaliyetlerinin seçimi veya revizyonu işi bu faaliyetlerin risk cevabı ve ilişkili amaçlar yönünden uygunluklarının ve isabetliliklerinin incelenmesini içermelidir.*

2.6.4 *Her bir kurum kendine özgü amaçlara ve uygulama yaklaşımına sahip olduğu için risk cevaplarında ve bağlantılı kontrol faaliyetlerinde farklılıklar bulunmaktadır. İki kurum aynı amaçlara sahip olmuş ve bu amaçları gerçekleştirmek için benzer kararları almış olsa bile, sonuç olarak ortaya çıkan kontrol faaliyetleri farklı olabilecektir. Bunun nedeni iki farklı yönetim ekibinin farklı risk iştahına ve farklı risk toleransına sahip olmasıdır.*

2.6.5 *Ancak, risk yönetimi bağlamında bütün kontrol prosedürleri aşağıdaki dört kategoriden birine girmektedir:*

Önleyici kontrollar *riskin gelişmesi ve istenmeyen sonucun gerçekleşmesi olasılığını sınırlamak üzere tasarlanır. Kurumun amaçlarını gerçekleştirme kabiliyeti üzerindeki riskin etkisi ne kadar büyükse, uygun nitelikte önleyici kontrolların uygulanması o kadar önemli hale gelir.*

Yönlendirci kontrollar *belirli bir sonuca ulaşılmasını sağlamak üzere tasarlanır. Bu kontrollar arzu edilmeyen bir hadiseden*

(örneğin güvenlik ihlalinden) kaçınılması zorunlu olduğunda özellikle önemlidir ve dolayısıyla, çoğu kez, uygunluk amaçlarının gerçekleşmesini desteklemek amacıyla kullanılır.

Ortaya çıkarıcı kontrollar *"hadiseden sonra" arzu edilmeyen sonuçların vuku bulmuş olup olmadığını belirlemeyi hedefler. Ne var ki, uygun nitelikte ortaya çıkarıcı kontrolların mevcudiyeti, caydırıcı bir etki yaratmak suretiyle arzu edilmeyen sonuçların oluşması riskini de azaltabilir.*

Düzeltici kontrollar *ortaya çıkmış arzulanmayan sonuçları düzeltmeyi amaçlar. Bu kontrollar, fonları ve servisleri kayıplara veya hasarlara karşı korumayı amaçlayan müdahale önlemi olarak da hizmet görebilir.*

2.7 Bilgi ve İletişim

2.7.1 *İç kontrol amaçlarını desteklemek üzere kullanılan verilerin kalite kriterleri ile kurum risk yönetimini desteklemek üzere kullanılan verilerin kalite kriterleri arasında çok küçük bir farklılık vardır. Kamu Sektörü İç Kontrol Standartları Rehberi bilgi ve iletişim hakkında ayrıntılı bilgiler içerdiğinden bu Ek kurum risk yönetim bağlamı içinde bu kriterlerden daha fazlasını vermeyi amaçlamamaktadır.*

Bilgi

2.7.2 *Kurum risk yönetimi, özellikle, iç kontrol amaçlarının gerçekleşmesi için gerekli olandan daha geniş kapsamda bilgi toplanmasını öngörmektedir: Örneğin, stratejik amaçlara odaklanmak daha çok çıktı ve sonuç bilgisine ihtiyaç göstermektedir. Ayrıca, içine bu verilerin yerleştirildiği kullanım biraz farklıdır. Geçmişle ilgili veriler; kuruma, fiilî performansı*

hedeflere, planlara ve beklentilere kıyasen izleme imkânı verir ve yönetimin dikkatini gerektiren potansiyel hadiselerle ilgili olarak önceden uyarılar getirebilir. Güncel veriler, yönetime, işletme biriminde/prosesinde mevcut riskler hakkında eş zamanlı bir fikir elde etme ve beklentilerden sapmaları belirleme imkânı verir. Kurum böylelikle faaliyetinin risk tolerans sınırları içinde olup olmadığını belirleyebilir.

2.7.3 *Tutarlı bilgiler belirlenip toplanmalı ve personele, sorumluluklarını yerine getirmelerine imkân verecek bir formatta ve zamanda iletilmelidir. Etkili bir iletişim, ayrıca, bütün kurum içinde yukarıdan aşağıya, enine ve aşağıdan yukarıya gerçekleşmelidir. Bütün personel üst düzey yönetimden kurum risk yönetim sorumluluklarının ciddiyetle yerine getirilmesi gerektiği hususunda net bir mesaj almalıdır. Çalışanların kurum risk yönetim prosesi içinde kendilerine düşen rolleri ve bu rollerin diğer kişilerin çalışmalarıyla olan ilişkisini anlamaları gerekir. Personel önemli bilgileri yönetimin uygun kademesine iletme araçlarına sahip olmalıdır. Dış paydaşlarla da etkili bir iletişime ihtiyaç vardır.*

2.7.4 *Doğru bilgilerle donanmış kişilere, istenen zamanda ve uygun mahalde sahip olunması etkili kurum risk yönetimi bakımından gereklidir.*

İletişim

2.7.5 *İletişim, bilgi sistemlerinden ayrı düşünülemez. İlgili personele görevlerini yerine getirme imkânı veren bilgileri sağlamanın yanı sıra iletişim, kurum kültürünü yansıtan, beklentilere cevap veren, bireylerin ve grupların sorumluluklarını*

ve diğer önemli meseleleri kapsayan daha geniş bir anlamda düşünülmelidir.

***2.7.6** Yönetim, personelden beklenen davranışlarla ve onların sorumluluklarıyla ilgili olarak spesifik ve hedefli bir iç iletişim sağlar. Bu iletişim kurumun risk yönetim felsefesinin ve yaklaşımının açık ve seçik bir beyanını içermelidir. Süreçlere ve prosedürlere ilişkin iletişim arzulanan kültüre paralel olmalı ve bu kültürün tesisine hizmet etmelidir. İletişim aşağıdaki hususlara duyarlı olmalıdır:*

Kurum risk yönetiminin önemi ve yerindeliği

Kurumun amaçları

Kurum risk iştahı ve risk tolerans derecesi

Riskleri tanımlamada ve değerlendirmede kullanılan ortak dil

Risk yönetim öğelerini uygulamaya geçirmede ve desteklemede personelin rolleri ve sorumlulukları

***2.7.7** Bunun yanı sıra çalışanlar, risk temelli bilgileri operasyonel yönetime ve bütün organizasyona iletmek için araçlara sahip olmalıdırlar. İşleyiş problemleriyle her gün ilgilenmek durumunda olan ilk hat çalışanları, çoğu kez, problemler oluşur oluşmaz bu problemleri fark etmek bakımından çok iyi konumdadırlar. Raporlanacak bu tür bilgiler bakımından açık iletişim kanallarının ve belirgin dinleme iradesinin bulunması gerekir. Eğer kurum kültürü "mesajı iletenin öldürülmesi"ne imkân veriyorsa, çalışanlar problemleri üstlerine iletmeyecekler ve riskler zamanında belirlenmeyebilecektir.*

***2.7.8** Pek çok durumda normal raporlama kanalları raporların hiyerarşi içinde iletilmesi için uygundur. Ne var ki, bazı koşullarda*

alternatif iletişim kanalları gerekir (ihbar hatları örneğinde olduğu gibi). Önemi nedeniyle, etkili kurum risk yönetimi doğrudan üst yönetime bağlı bir alternatif iletişim kanalının bulunmasını ve bu kanalın geri tepme korkusu olmaksızın bütün personelin kullanımına hazır olmasını gerektirir.

***2.7.9** Uygun iletişim yalnız kurumun içinde değil, kurumun dışında da bulunmalıdır. Kurumun beklentileri karşılayacağı ve bu beklentileri yöneteceği konusunda güvence vermek amacıyla kurumun riskleri yönetme tarzı hakkında dış paydaşlara bilgi verilmesi gerekir. Bu, özellikle, halkı etkileyen riskler söz konusu olduğunda ve halk hükümetin riskleri kendisi için yönetme kapasitesine bağımlı olduğunda önem taşımaktadır. Kurum dışı taraflarla iletişim ciddiyetle ve dürüstlükle gerçekleştirildiğinde, bu tür iletişim bütün kuruma önemli mesajlar gönderir ve örgüt kültürü üzerinde önemli bir etkiye sahip olabilir.*

2.8 İzleme

***2.8.1** Kurum risk yönetimi, kendi öğelerinin zaman zarfındaki işleyişini değerlendirmek amacıyla izlemeye konu olmalıdır. İzleme, rutin izleme faaliyetleri, ayrı değerlendirmeler (evaluations) ya da ikisinin kombinasyonu aracılığıyla gerçekleştirilebilir. Kurum risk yönetim sistemindeki yetersizlikler, kurumun süreçlerini iyileştirmesi amacıyla, yönetimin uygun kademesine iletilmeli, ciddi meseleler de üst yönetime veya kurula raporlanmalıdır.*

***2.8.2** Bir kurumun amaçları zaman içinde değişebilir. Risk portföyü ve bu portföydeki risklerin göreli önemi de zaman zarfında değişebilir. Eskiden etkili olan risk cevapları yetersiz veya uygulanamaz hale gelebilir ve kontrol faaliyetleri etkililiğini*

kaybedebilir veyahut tamamıyla terk edilebilir. Hâlâ uygun ve etkili olup olmadığını belirlemek amacıyla yönetimlerin kendi risk yönetim sistemlerinin etkililiğini sürekli olarak izlemeleri gerekir.

***2.8.3** Risk yönetiminin etkililiğine ilişkin değerlendirmeler; risk gruplarının anlamlılığına, bu riskleri yönetmedeki risk cevaplarının ve bu cevaplarla ilişkili kontrolların önemine bağlı olarak kapsam ve sıklık bakımından değişiklik gösterir. Yönetim, risk yönetim çerçevesinin bir kapsamlı değerlendirmesini yapma kararı aldığında, dikkat strateji belirlenmesi dahil olmak üzere, sürecin bütün yönlerinin ele alınmasına yöneltilmelidir. Ancak, olağan yönetim aktiviteleri, örneğin risk kayıtlarının güncellenmesi ve organizasyonel veya fonksiyonel "periyodik kontrollar" da risk yönetim sürecini izlemenin bir parçasını oluşturur.*

Kaynakça

Australian Standard® for risk management (Standards Australia, 2004)

Entity Risk Management – Integrated Framework (COSO, 2004)

Integrated Risk Management Framework (Treasury Board of Canada Secretariat, 2001)

Internal Control - Integrated Framework (COSO, 1992)

Risk Management Standard (ARMIC, IRM&ALARM, 2002)

The Orange Book: Management of Risk – Principles and Concepts (HM Treasury, 2004)