COSO KURUMSAL RİSK YÖNETİMİ - RİSKİN STRATEJİ VE PERFORMANSLA UYUMLAŞTIRILMASINA İLİŞKİN DÜZENLEME ÇERÇEVESİNDE GETİRİLEN GÜNCELLEMELER*

(UPDATES ON THE REGULATORY FRAMEWORK RELATED TO HARMONİZATİON OF COSO ENTERPRİSE RİSK MANAGEMENT INTEGRATİNG WİTH STRATEGY AND PERFORMANCE)

Gencay KARAKAYA**

ÖZ

COSO'nun 2004 yılında yayınladığı KRY çerçevesine ek olarak, 2017 yılının Eylül ayında yayınladığı en güncel düzenleme; COSO Kurumsal Risk Yönetimi-Riskin Strateji ve Performansla Uyumlaştırılması başlığı ile yayınlanmıştır. Söz konusu rapor, KRY'ye ilişkin en güncel bilgileri ve düzenlemeleri içermesi nedeniyle tüm yönleri ve bileşenleri ile birlikte derinlemesine incelenmiştir. Konuya ilişkin Türkçe kaynakların yok denecek kadar az olması bu çalışmanın temel çıkış noktası olmuştur. Çalışmada bir kıyaslama yapmaktan ziyade, yeni çerçeve ile ilgili temel bilgilerin aktarımına odaklanılmıştır. Bu anlamda KRY'ye ilişkin güncel bir uygulamanın irdelenmesi ve çalışmaya eklenmesi, literatüre de olumlu bir katkı sunmuştur.

Anahtar Kelimeler: COSO, Kurumsal Risk Yönetimi, Strateji, Performans

JEL Kodlaması: M4, M41, M42, G32

ABSTRACT

In addition to Enterprise Risk Management (ERM) framework published in 2004, COSO published the most recent regulation in September 2017; COSO Enterprise Risk Management—Aligning Risk with Strategy and Performance. The report is in-depth with all its aspects and components, as it contains the most current information and regulations on ERM. The fact that there are almost any Turkish sources on this subject has been the main starting point of this study. The study focused on explain of basic information about the new framework rather than making a comparison. In this sense, a recent review of the current implementation of ERM and its inclusion in the study has also made a positive contribution to the literature.

Keywords: *COSO, Enterprise Risk Management (ERM), Strategy, Performance*

JEL Classification: *M4, M41, M42, G32*

---

*) Söz konusu çalışma, yazarın doktora tezinden türetilmiştir.

**) Araş. Gör., İstanbul Ticaret Üniversitesi, İstanbul, gkarakaya@ticaret.edu.tr, Orcid:0000-0002-2662-6031, Yazı Gönderim Tarihi: 05.10.2018, Yazı Kabul Tarihi: 11.10.2018

1. GİRİŞ

1980'lerin ilk dönemlerinde ortaya çıkan muhasebe skandalları nedeniyle Hileli Finansal Raporlamalar Komisyonu (yaygın bilinen ismi ile Treadway Komisyonu) bugün halen aktif faaliyet gösteren COSO'yu kurdu (Karakaya, 2016: 9). Söz konusu kurum gerek iç kontrol gerekse de Kurumsal Risk Yönetimi (KRY) konularında çeşitli düzenlemeler yayınlamış ve geniş kabullere ulaşmıştır.

COSO'nun 2004 yılında yayınlanan KRY düzenlemeleri, kurumların/işletmelerin risklerini yönetebilmeleri noktasında çok geniş kabullere ulaşmıştır. Bununla birlikte 2004 yılı düzenlemeleri, KRY konusunda, gelişen rekabet şartları içerişinde kurumların/işletmelerin risklerini yönetebilmeleri için başvurabilecekleri temel adreslerin başında gelmiştir. KRY hakkında yapılan tüm akademik ve pratik uygulamalarda mutlaka COSO düzenlemelerine başvurulmuştur. Bu durum; KRY adına çalışmalar yapan COSO'nun, 2017 yılında geliştirdiği anlayışın da temellerini oluşturmuştur. Bu anlayış; risk yönetim süreçlerini değerlendirirken, ***strateji oluşturma*** ve ***sürdürülebilir performans*** kavramlarının da dikkate alınmasına vurgu yapmaktadır. Bununla birlikte bu 3 kavramın bir arada düşünülmesi ve değerlendirilmesi hususu özellikle belirtilmiştir.

İlgili çalışma yeni getirilen değişiklikler hakkında en temel bilgileri sunma ve bundan sonra konu ile ilgili yapılacak çalışmalara destek olma maksadıyla kaleme alınmıştır. Kapsam noktasında; ilgili çerçeve dışına çıkılmamış, değişiklikler bizzat COSO'da yer alan ifadelerle aktarılmaya çalışılmıştır. Söz konusu düzenleme yeni olduğu için hakkında detaylı araştırmalar yapılabilmesi muhakkak zamanla gerçekleşecektir.

2. COSO KRY'DE YENİ BİR GÜNCELLEME NEDEN GEREKLİ?

Son dönemlerde değişen risk türleri, risklerin kapsamı ve kaynakları, risklere ilişkin geliştirilecek raporlamaları ve düzenlemeleri değer üretebilen mekanizmalar olmaktan uzaklaştırdı (COSO, 2017:1). Bu konuda temel karar vericiler olan yönetim kurulu üyeleri ve yöneticiler farkındalık oluşturabilmek adına çeşitli arayışlara başvurmak zorunda kaldılar. Çerçeve; kurumsal risk yönetimini günümüz iş dünyasının beklentileri, ekonomideki değişimler ve belirsizlikler, teknolojik gelişmeler ve örgüt içerisinde karar almayı destekleyebilecek tüm demografik değişkenleri de göz önüne alan bir yapıda geliştirilmesine yardımcı olmaktadır (Kurt ve Uysal, 2018: 22).

COSO 2017 KRY çerçevesi temelde, bütünleşik KRY'nin tesisi edilmesi için stratejik planlama süreçlerine ihtiyaç duyulduğunu vurgulamaktadır. Yeni düzenlemenin "performans" ve "bütüncül strateji" vurguları, işletmelerin hedeflerine ulaşma gayeleri ile günlük operasyonlar arasında ki ilişkiyi ortaya koymaktadır. (Pierce & Goldstein, 2018: 52).

Söz konusu ifade ile anlatılmaya çalışılan, Kurumsal Risk Yönetimi'ni günlük operasyonlara da entegre ederek ve kurum hedeflerini riske daha yakın bir şekilde ilişkilendirerek genel performansını artırabileceğidir (COSO, 2017: 5). COSO'nun 2017 KRY düzenlemesi, günlük operasyonel risklerin, nihai olarak stratejik hedefleri nasıl etkilediğini ve karşılıklı ilişkinin düzeyini açıkça belirtmektedir (Pierce & Goldstein, 57).

Yayınlanan yeni KRY çerçevesi tüm seviyelerdeki yönetim ve risk süreçleri için uygulanabilmektedir (COSO, 2017: 1). Bu yeni düzenleme ile bütüncül risk yönetimi uygulamalarının (risk yönetimi -strateji oluşturma -sürdürülebilir performans), kurumların/işletmelerin hızlı büyüme ve performanslarını artırmak üzere nasıl uygulanacağı noktasında katkılar sunmaktadır. Bununla birlikte 2017 düzenlemesinin geçmiş düzenlemelerden temel 10 farkı şu şekilde ifade edilebilir (COSO, 2017);

1. Yeni bir doküman yapısı ve sunumu,
2. Ana ve alt ilkeleri detaylı bir şekilde aktarma,
3. Düzenlemeye yeni grafiklerin dâhil edilmesi,
4. Bütüncül yaklaşıma odaklanma (risk yönetimi-strateji oluşturma- sürdürülebilir performans),
5. Temel çıktı olarak değer/katma değer kavramına vurgu yapma,
6. "Strateji" kavramı ile doğrudan ilişki kurma,
7. "Performans" kavramı ile doğrudan ilişki kurma,
8. İşletme kültürünün önemini vurgu yapma,
9. Karar aşamalarına odaklanma,
10. COSO İç kontrol sistemi ile bağlantı kurma.

COSO KRY 2017 düzenlemesinin, (gerek tanım gerekse bileşenler itibariyle) temel kaygısı, süreç sonunda bir değer oluşturmak ya da mevcut değeri artırmaktır. COSO'nun bundan önceki düzenlemeleri de bu anlamda bir değer üretmekten bahsederken, yeni düzenleme sürecin odak noktasında "***değer***" kavramını işlemiştir. Değer oluşturma süreci; misyon/vizyon ve temel değerler, stratejik gelişim, iş hedeflerinin geliştirilmesi, uygulama ve performans aşamalarının sonucudur. COSO 2017 KRY güncel çerçevesi kapsamında değerlendirildiğinde, 2014 sürümüne ilave olarak belirtilen ana katkının kurumsal yönetim, kültür ve strateji oluşturma noktalarında olduğu görülmektedir (Prewett & Terry, 2018: 16).

2014 ve 2017 sürümleri arasında ki temel farklılıkların en önemlileri, teknolojik gelişim/değişimlere verilen tepkiler ile tüm yönetim süreçlerinde risk yönetiminin artan rolünün daha iyi anlaşılması ve anlatılması yönündedir (Prewett & Terry: 17).

3. GÜNCELLENEN COSO KRY BİLEŞENLERİ VE BOYUTLARI

2014 COSO KRY düzenlemesi ile güncel düzenleme arasında ki en temel farklılıklar bileşenler ve alt boyutlar itibariyle gerçekleşmiştir. Yeni düzenlemede, bileşenlerin her birinin birbirleri ile olan sıkı ilişkilerini ifade etmek adına bir sarmal gösterimi tercih edilmiştir. Dolayısıyla bu tercih bir tesadüfe değil, sistematik bir ifade maksadıyla gerçekleşmiştir. COSO'nun KRY 2017 düzenlemesinde yer verdiği ve anlatılmaya çalışılan ilişkinin tematik gösterimi ve açıklamaları şu şekildedir (COSO, 2017: 6);

Diyagramın üç şeridi (Strateji & Hedef Oluşturma, Performans, Gözden Geçirme & Düzeltme) kurum boyunca akan genel süreçleri temsil ettiği, diğer iki şeridin ise (Yönetişim & Kültür ve Bilgi, İletişim & Raporlama) kurumsal risk yönetiminin destekleyici unsurlarını temsil ettiği ifade edilmiştir (Burca, 2017).

Bu farklı yaklaşım, klasik KRY bileşenlerinden (COSO 2004/1 ve 2004/2) farklı unsurlar oluşmasına neden olmaktadır. Yenilenen COSO KRY çerçevesi kullanıcılara 5 ana bileşen ve 20 alt bileşen ile daha detaylı ve bütüncül bir KRY yapısı tesis etme imkânı sunmaktadır. Söz konusu ana bileşenler ve alt bileşenler, düzenlemede yer aldığı şekilde aktarılmıştır.

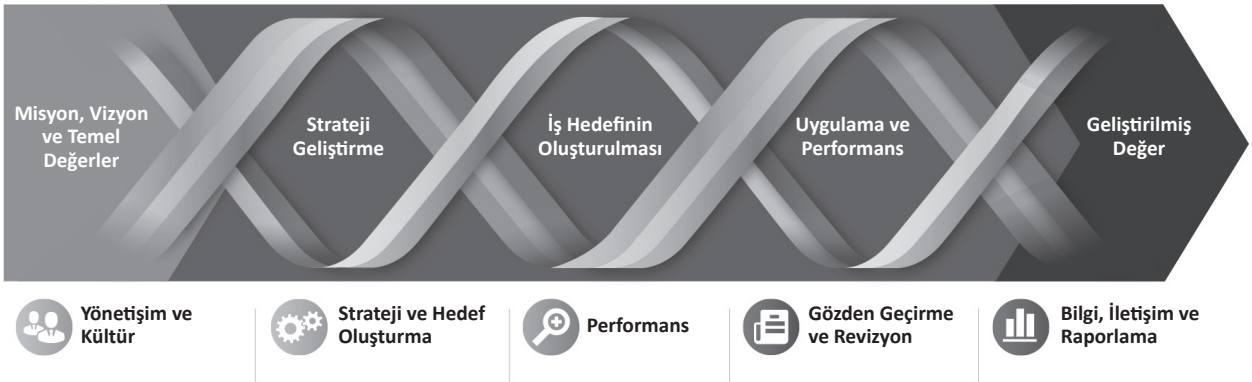
Detaylı olarak ifade edilecek olan **5 ana bileşen şu şekilde tasarlanmıştır (**COSO, 2017: 7);

- Yönetişim ve Kültür
- Strateji ve Hedef Belirleme
- Performans
- Gözden Geçirme ve Düzenleme
- Bilgi, İletişim ve Raporlama

3.1. Yönetişim ve Kültür (Governance and Culture)

Yönetişim ve kültür bileşeni, COSO KRY 2017 düzenlemesinin ilk bileşenidir. COSO'nun işlenecek ve hakkında açıklama yapılacak konulara ilişkin temel

Şekil 1. KRY Sarmalı



Kaynak: COSO Enterprise Risk Management - Aligning Risk with Strategy and Performance, (2017: 6)

prensibi; en temel unsur/bileşen ile başlayıp, nihai sonuca doğru kademe kademe açıklama yapma şeklindedir. Bu nedenle yeni KRY düzenlemesinin başlangıç noktasının yönetişim ve kültür bileşeni olması tesadüfi değildir.

Yönetişim; kurumun/işletmenin kendine özgü yönetim anlayışının (yönetim tarzının) tesis edilmesini ifade etmektedir. Yönetişim yaklaşımında geniş bir aktörler yelpazesinin var olması kararlara katılımı, amaçlara ortak bir şekilde ulaşılmasını sağlamaktadır (Aydın ve Durgun, 2017: 25).

Kamu idareleri için yapılabilecek diğer bir yönetişim tanımı ise; "*Kamu politikalarının belirlenmesinde ve uygulanmasında; sivil topluma, aktif vatandaşlığa, stratejik vizyona, etkileşime, katılımcılığa ve işbirliğine önem vermektedir.*" şeklinde ifade edilebilir (Ayhan ve Önder, 2017: 23).

Bu yönüyle yönetim (government) kavramı ile yönetişim (governance) kavramı; kapsam, hedef ve uygulama yöntemleri bakımından farklılıklar göstermektedir. Yönetim kavramı ayrı ayrı bütünler halinde, *yöneten* ve *yönetilen* taraflardan oluşuyorken; yönetişim kavramı karşılıklı etkileşime bağlı olarak birlikte yönetme iradesinin kabul edilmesi ile gerçekleşmektedir.

COSO'nun yeni düzenlemesinde bu ifadeyi (yönetişim) tercih etmesi tesadüf değildir. Yönetim kavramına nazaran; daha güncel, daha katılımcı, daha şeffaf bir içeriğinin olması, güncelleme amaçlı yapılan yeni düzenlemede önemli bir etki oluşturmuştur.

Yine aynı bileşenin ikinci unsuru kültürdür. Kültür; etik değerler, istenen/beklenen davranışlar ve risk anlayışı ile doğrudan ilişkilidir (COSO, 2017:6). Bu kapsam gereğince, kurumda tüm bireyleri ve tüm birimleri ilgilendirmektedir. COSO KRY 2017 düzenlemesinin ifade ettiği; risk yönetimi- strateji oluşturma- sürdürülebilir performans sürecinin neticesinde elde edilmesi beklenen değer kavramının en temel girdilerinden birisi de kültürdür. Kurum içerisinde yerleşik davranışlar ve tutumların tümünü kapsayan kültür kavramı, karar alma, uygulama ve takip etme aşamalarının tamamında doğrudan belirleyici bir rol almaktadır. **Yönetişim ve kültür bileşeni, birbiri ile doğrudan ilişkili 5 alt bileşenden oluşmaktadır.** Bunlar;

- Yönetim kurulunun risk gözetimini uygulaması,
- Operasyonel yapının oluşturulması,
- İstenen/Arzu edilen kültür yapısının tanımlanması,
- Temel değerlere olan bağlılığı gösterme,
- Kabiliyetli Personeli kazanma, geliştirme ve elde tutma.

3.1.1. Yönetim Kurulunun Risk Gözetimini Uygulaması

Bir kurumun çalışma disiplinin oluşumunda esas belirleyici olan yönetim kurulu ile üst yöneticilerdir (Türedi ve Karakaya: 70). Kurumlarda/işletmelerde, risk yönetimine ilişkin temel sorumluluk ya yönetim kurulunun bütününde ya da yönetim kurulunca belirlenen bir üyededir. Bu nedenle KRY'ye ilişkin bütünleşik anlayışın (risk yönetimi- strateji oluşturma- sürdürülebilir performans) temel sorumlusu bu kurul veya belirlenen üyesidir.

İşletme hedeflerine varabilmek adına etkin bir gözetim sistemi tesis etmek kaçınılmazdır. Söz konusu hedeflere ilişkin süreçlerin ne durumda olduğunun ve ne şekilde ilerlediğinin gözetim sorumluluğu yönetim kurullarına aittir. Bu sorumluluğu bizzat kendileri yerine getirebilecekleri gibi, işletme üst yöneticilerine de devredebilirler (Türedi, Karakaya: 72). Bu durumun temel sonucu olarak denebilir ki; kurumun/işletmenin hedeflerine ulaşılabilmesi için gerekli olan stratejilerin belirlenmesi ve gözetimi/izlenmesi, kurumsal yönetişim anlayışının oluşturulması ve yürütülmesi, yönetim kurulu ya da belirlenen üyenin sağlayacağı katkı ve destek ile mümkün olabilecektir (COSO, 2017: 10).

3.1.2. Operasyonel Yapının Oluşturulması

Kurumlar/işletmeler; stratejilerini uygulayarak hedeflerine ulaşabilmeleri için operasyonel yapılarını oluşturmak zorundadırlar (COSO, 2017: 10). KRY'ye ilişkin etkin bir yönetişim ve kültür bileşenini tesis edebilmek için, süreçlerin nasıl işleyeceği, kimler tarafından yürütüleceği, sorumluluk ve yetki alanlarının ne olacağı gibi temel operasyonel konuların belirlenip, standart uygulamalar haline getirilmesi gerekmektedir. Gerek yönetişim gerek kurum kültürünün

temel girdilerinden birisi de söz konusu operasyonel alışkanlıkların belirlenip uygulanmasıdır.

3.1.3. İstenen/Arzu Edilen Kültür Yapısının Tanımlanması

Kurumlarda/işletmelerde istenen/arzu edilen kültür yapısını oluşturan temel unsur, kurumun tüm birimlerinde var olan davranışlardır. Yani kurumun genelinde oluşturulacak davranışlar, neticede kurumun istenen/arzu edilen k**ültür yapısını oluşturacaktır** (COSO, 2017: 10).

3.1.4. Temel Değerlere Olan Bağlılığı Gösterme

Yönetişim ve kültür bileşenin diğer alt bileşenlerinden birisi de temel değerlere olan bağlılığın gösterilmesi hususudur. Bu noktada ifade edilmek istenen, kurumlarda/işletmelerde KRY'nin bir girdisi, temel değerlerin varlığının tespit edilmesi ve bunun tüm ilgili birimlere ya da kişilere aktarılmasıdır (COSO, 2017: 10).

3.1.5. Kabiliyetli Personeli Kazanma, Geliştirme ve Elde Tutma

Kurumların/işletmelerin KRY odaklı değer üretme süreçlerinin en büyük girdilerinden birisi de insan kaynakları ya da beşeri sermayedir. İşletmelerde insan kaynaklarının artık maddi kaynaklar kadar önemli unsurlar olduğu gerçeği unutulmamalıdır (Türedi, Karakaya: 69). Her süreç ne kadar mükemmel tasarlanmış olursa olsun, uygulayıcıları ve kullanıcıları bireyler olacaktır. Bunun için etkin insan kaynakları politikaları belirlemek ve bunları uygulamak birinci derecede önem arz etmektedir (Türedi, Karakaya: 69).

Bu nedenle kurumlar/işletmeler; insan kaynakları politikalarını, kurumsal hedefleri ve stratejileri ile mutlaka bütünleşik ve uyumlu hale getirmelidir (COSO, 2017: 10). Gerek mevcut çalışanların eğitilmesi ve geliştirilmesi, gerekse de yeni istihdamların sağlanması konusunda ne kadar dikkatli ve güçlü olunursa, işletme hedeflerine ulaşma yolunda o kadar muktedir olunacaktır (Türedi, Karakaya: 70).

3.2. Strateji ve Hedef Belirleme

KRY, strateji ve hedeflerin belirlenmesi; strateji planlama süreçlerinin temel noktalarıdır ve birlikte hareket ederler (COSO, 2017: 6). Kurumların/işletmelerin risk iştahları, stratejiler ile birlikte belirlenir. Çünkü risk iştahı seviyesinin belirlenmesi ve bu yönde politikaların belirlenmesi, stratejilerin belirlenmesi ile birlikte yapılır. Bu düzenlemeye özgü olan diğer bir nokta ise, iş ortamı/içeriği ile stratejilerin belirlenmesi arasında ki temel ilişki irdelenmiştir. **COSO 2014 güncellemesine ek olarak belirlenen alt bileşenler** ise şu şekildedir;

- İş ortamını/içeriğini analiz etme,
- Risk iştahının tanımlanması/belirlenmesi,
- Alternatif stratejileri değerlendirme,
- İş hedeflerini oluşturma.

3.2.1. İş Ortamını/İçeriğini Analiz Etme

COSO'nun 2017 düzenlemesinde "Business Context" olarak ifade ettiği şey esasında iş ortamıdır. Kurumlar/işletmeler; faaliyetlerin gerçekleştirildiği iş ortamının, stratejileri ve risk seviyeleri/iştahları ile ilgili olası etkilerini analiz eder (COSO, 2017: 10). İş ortamı kavramı bu yönüyle; kurumların/işletmelerin strateji ve hedefleri ile ilgili kararlarında güncellemelere, düzenlemelere ya da açıklamalara gidebileceği olası tüm faktörleri/etkileri kapsayan temel bir bağlamdan oluşmaktadır.

İş ortamı; tüm kurumların/işletmelerin içinde bulunduğu ve karşılıklı olarak etkilediği ve etkilendiği dinamik bir alanı ifade etmektedir. Rekabet şartlarının değişmesi, rakiplerin değişmesi, malların değişmesi, teknolojilerin değişmesi vb. birçok dinamik etken, iş ortamının temel bileşenleridir ve kurumların hedef ve stratejilerinde değişikliklere, güncellemelere ve açıklamalara neden olabilmektedir.

3.2.2. Risk İştahının Tanımlanması/Belirlenmesi

COSO KRY 2017 düzenlemesi risk iştahını tanımlarken/belirlerken; değer oluşturma, mevcut değeri koruma bağlamında değerlendirmektedir (COSO, 2017: 10). COSO 2014 düzenlemesinden farklı olarak, risk iştahına ilişkin temel ifadeler ve açıklamalar "değer" kavramı ile birlikte değerlendirilmiştir.

3.2.3. Alternatif Stratejileri Değerlendirme

Kurumlar/işletmeler, riskler üzerinde ki olası etkilerini de dikkate alarak alternatif stratejileri değerlendirmelidir (COSO,2017: 10). Bu noktada ki temel dayanak; iş ortamında ki güncel değişmelere bağlı olarak risklerin değişmesi ya da artması durumunda stratejilerin uygunluğunun değerlendirilmesidir. Alternatiflerin belirlenip uygulanması, değer oluşturma ya da mevcut değeri koruma anlamında önemli avantajlar sağlayacaktır.

3.2.4. İş Hedeflerini Oluşturma

Kurumlar/işletmeler; iş hedeflerine de katkı sunacak, destekleyici stratejileri oluştururken, çeşitli düzeyde ve türde riskleri değerlendirmelidir (COSO,2017: 10). İş ortamı ve iş hedefi birbiri ile ilgili fakat farklı kavramlardır. En büyük fark kapsam noktasındadır. İş ortamı, gerek kurum içi gerek kurum dışı kaynaklardan oluşabiliyorken, iş hedefleri kurumlara/işletmelere özgü daha mikro unsurlardır. Bu nedenle iş hedeflerinin oluşturulması sırasında risklerin stratejiler ile uyumlu şekilde değerlendirilmesi gerekmektedir.

3.3. Performans

Kurumların/işletmelerin hedefleri ve stratejileri ile doğrudan ilgili olan riskler, tanımlanmak ve değerlendirilmek zorundadır. Bu nedenle riskler, -risk iştahı haritası kapsamında- şiddetleri ve dereceleri bakımından sınıflandırılmalıdır (COSO,2017: 6). **Performans ana bileşeni 5 farklı alt bileşenden oluşmaktadır**. Bunlar;

- Risklerin tanımlanması/belirlenmesi,
- Risk şiddetlerinin değerlendirilmesi,
- Risklerin önceliklendirilmesi/derecelendirilmesi,
- Risk tutumlarının/yanıtlarının uygulanması,
- Bütüncül ve geniş bir akış açısının geliştirilmesi

3.3.1. Risklerin Tanımlanması/Belirlenmesi

Risk tanımlama, risklerin belirlendiği aşamadır (Karakaya ve Karakaya: 300). Kurumlar/işletmeler; stratejik performansı ve işletme hedeflerini doğrudan etkileyebilecek riskleri tanımlamak zorundadır (COSO, 2017: 10). Bu tanımlama sayesinde elde edilecek risk haritaları, hem risk iştahı belirleme süreçlerinde, hem iş ortamına ilişkin risk güncellemelerinde hem de iş hedeflerinde kullanılacak çok önemli bir risk veri tabanı elde edilmesini sağlayacaktır.

3.3.2. Risk Şiddetlerinin Değerlendirilmesi

Risklerin değerlendirilmesi; risklerin tanımlanması ve derecelendirilmesi arasında gerçekleşen bir süreçtir. Bu noktada temel dayanak yine kurumların risk iştahları ile doğrudan ilişkilidir. Riskleri derecelendirmeden önce değerlendirmek, kurumların/işletmelerin hedeflerine ve stratejik performanslarına ilişkin olası etkilerinin göz önüne koyulması maksatlıdır. Bu nedenle değişik değerlendirme teknikleri kullanmak mümkün olacaktır.

3.3.3. Risklerin Önceliklendirilmesi/ Derecelendirilmesi

Risklerin önceliklendirilmesi/derecelendirilmesi risklerin değerlendirilmesinden sonra gelen bir aşama olarak, risklerin etkilerinin önceliklendirilmesi amacıyla yapılmaktadır (Karakaya ve Karakaya: 301). Çeşitli derecelendirme teknikleri arasında en yaygın uygulanan yöntem, risklerin olasılıklarının ve olası etkilerinin değerlendirildiği yöntemdir. Bu anlamda sürecin temel iki girdisi; olasılık ve etkidir. Yapılacak değerlendirmeler sonucunda hem risk önceliklendirilmesi yapılacak hem de risk tutumları/yanıtlarına ilişkin ipuçları elde edilecektir (COSO, 2017: 10).

3.3.4. Risk Tutumlarının/Yanıtlarının Uygulanması

Bu aşamada, kurumlar/işletmeler risklere ilişkin verecekleri yanıtları tanımlar ve seçerler (COSO, 2017: 10). Risklere ilişkin verilecek cevaplar belirlenirken; risk iştahı, iş ortamı, iş hedefleri vb. temel unsurlar dikkate alınmalıdır.

3.3.5. Bütüncül ve Geniş Bir Akış Açısının Geliştirilmesi

Risklerin tanımlanması, değerlendirilmesi, derecelendirilmesi ve yanıtların oluşturulması süreçleri

sonucunda, risklere ilişkin olarak bütüncül bir bakış açısı geliştirilmiş olacaktır. KRY' ne ilişkin geliştirilecek bu bütüncül bakış açısının icracısı yönetim kuruludur.

3.4. Gözden Geçirme ve Düzenleme

Kurumlar ilgili birimlerin performanslarını gözden geçirme suretiyle; kurumsal risk yönetiminin temel bileşenlerinin işleyişlerini ve değer oluşturma sürecine yapacakları katkıları değerlendirebilmektedir. Ve bu yolla meydana gelebilecek yapısal/büyük değişimlere intibak konusunda ne gibi güncellemelere ihtiyaç duyulacağı belirlenebilir (COSO, 2017: 6)**. Gözden geçirme ve düzenleme ana bileşeni 3 farklı alt bileşenden oluşmaktadır;**

- Önemli/Yapısal değişiklikleri değerlendirme
- Risk ve Performansı gözden geçirme
- KRY ile ilgili gelişim/değişimleri takip etme

3.4.1. Önemli/Yapısal Değişiklikleri Değerlendirme

Söz konusu alt bileşenin vurgu yaptığı temel nokta; kurumların/işletmelerin stratejilerine ya da kurumsal amaçlarına etki edebilecek yapısal değişiklikleri tespit edip değerlendirmesi hususudur (COSO, 2017: 10).

3.4.2. Risk ve Performansı Gözden Geçirme

Söz konusu alt bileşenin vurgu yaptığı temel nokta; kurumların/işletmelerin performanslarının gözden geçirilerek mevcut ya da potansiyel risklerin tanımlanıp değerlendirilmesi hususudur (COSO, 2017: 10).

3.4.3. KRY İle İlgili Gelişim/Değişimleri Takip Etme

Klasik risk yönetiminin ihtiyaçları karşılayamaması ile birlikte ortaya çıkan KRY kavramı dinamik bir yapıya sahiptir. Bunun temel nedeni, giderek artan risk çeşitlerinin ve türlerinin varlığıdır. Bu nedenle gözden geçirme ve değerlendirme bileşenin en son alt bileşeni olan KRY ile ilgili değişimleri takip etme hususu büyük önem arz etmektedir. Risklerin yönetilmesi hususunda en temel ihtiyaç, güncel değişimlerin ve gelişmelerin takip edilmesidir (COSO, 2017: 10).

3. 5. Bilgi, İletişim ve Raporlama

Kurumlarda/işletmelerde katma değer oluşturma süreçlerinde kullanılacak bilgilerin elde edilmesi, iletilmesi, paylaşılması ve raporlanması için, etkin ve daimi bir KRY yapısı oluşturulmalıdır. Söz konusu bilginin kaynağı hem iç hem de dış kaynaklı olabilmektedir. Bununla birlikte elde edilen bilgi, kurum genelinde ilgili tüm birimlere iletilmelidir (COSO, 2017: 6). **Bilgi, İletişim ve Raporlama ana bileşeni 3 farklı alt bileşenden oluşmaktadır**;

- Bilgi Yönetim Sisteminin güçlendirilmesi
- Riske ilişkin bilginin iletilmesi/paylaşılması
- Risk, risk kültürü ve performans ile ilgili raporlama yapmak

3.5.1. Bilgi Yönetim Sisteminin Güçlendirilmesi

Kurumlar, KRY'nin desteklenmesi ve geliştirilmesi için; her bir birimin bilgi, teknoloji ve yönetim sistemlerini güçlendirmelidir (COSO, 2017: 10). Bu sayede güvenli bilginin elde edilmesi süreçlerinin tamamında, yeknesak uygulamaların icrası sağlanacak ve bu noktada ki teknolojik imkânlar da kullanılacaktır.

3.5.2. Riske İlişkin Bilginin İletilmesi/Paylaşılması

Bu alt bileşenin ifade etmeye çalıştığı temel husus; KRY yapısının desteklenmesi ve geliştirilmesi için, kurumların iletişim kanallarını tesis etmesi ve geliştirmesi gerektiği yönündedir (COSO, 2017: 10).

3.5.3. Risk, Risk Kültürü ve Performans İle İlgili Raporlama Yapmak

Yalnız bilgini elde edilmesi değil, gerekli tüm birimlere ve farklı seviyelerde raporlanması gerektiği hususu bu alt bileşenin ifade ettiği temel hususdur (COSO, 2017: 10).

4. SONUÇ

COSO, gerek iç kontrol gerekse KRY süreçlerine ilişkin yayınladığı raporlar ile belirtilen konulara ilişkin başvurulan kaynakların başında gelmektedir. KRY ile ilgili sistematik ve en güncel bilgilerin yayınladığı son güncelleme ise (2017) COSO Kurumsal Risk Yö-

netimi-Riskin Strateji ve Performansla Uyumlaştırılması olmuştur. Söz konusu çalışma ile 2014 yılı KRY düzenlemelerine ek olarak "strateji ve performans" odaklı bir değer oluşturma sürecinin ön izlemesini ilgililere duyurmuştur.

KRY'nin bütüncül ve çok taraflı risk yönetimi anlayışı ile son derece uyumlu olan düzenleme, Türk muhasebe literatüründe henüz detaylı şekilde incelemeye başlanmamıştır. Bu sayede ilgili çalışmanın bu noktada ufak da olsa bir açığı kapatması arzu edilmektedir.

KRY'nin mevcut boyutlarını ve bileşenlerini de dikkate alarak, farklı ve ihtiyaca uygun bir kompozisyonun oluşturulması gayesinin açıkça görüldüğü bu çalışmada; yöneticilere, karar vericilere ve uygulayıcılara yön gösteren çok önemli noktalar yer almaktadır. İlgili çerçeve; kurumlarda ya da işletmelerde KRY'ye ilişkin güncel, analitik, sistematik ve ihtiyaca uygun süreçlerin tesisini daha da mümkün hale getirmektedir.

"Değer" oluşturma kaygısının daha net olarak ifade edildiği bu düzenleme ile birlikte, risk yönetimi, stratejik yönetim ve performans yönetimi kavramlarının birbirleri olan ilişkileri açıkça ortaya koyulmuştur. Risk yönetiminin tesisi sırasında, kurumun stratejileri ve sürdürülebilir performansı odak noktasına alan bir yaklaşımın katma değer oluşturulacağı ifade edilmiştir.

Bir araştırma türü olarak, COSO 2017 düzenlemesine ilişkin yapılan ilk çalışmalardan olan bu makalede, düzenlemenin özüne sadık kalınmaya çalışılmış, bilgilere kişisel yorumlar ve görüşler dâhil edilmemeye çalışılmıştır. Bu vesile ile güncel düzenlemeye ilişkin yapılacak çalışmalara destek olması ve temel bir bakış açısı sunması beklenmektedir.

Kaynakça

1) AYDIN, A. H., & DURGUN, S. (2017, May). Yeni Bir Yönetim Anlayışı Olarak Yönetişimin Gelişmesinde Bilgi Edinme Hakkının Önemi. In 1st Eurasian Conference on Language and Social Sciences (p. 25).
2) AYHAN, E., & ÖNDER, M. (2017). Yeni Kamu Hizmeti Yaklaşımı: Yönetişime Açılan Bir Kapı, Gazi İktisat ve İşletme Dergisi, 3(2).
3) BURCA, N. (2017), Yenilenen COSO Kurumsal Risk Yönetimi Çerçevesi, https://nazifburca.com/2017.09.20/yenilenen-coso-kurumsal-risk-yonetimi-cercevesi/
4) COSO, (2017), Enterprise Risk Management Integrating with Strategy and Performance, Executive Summary, Eylül
5) COSO, (2004/1). Enterprise Risk Management-Integrated Frmaework Executive Summary Framework. Eylül.
6) COSO, (2004/2), Enterprise Risk Management – Integrated Framework , Application Techniques, Eylül
7) KARAKAYA, G. (2016). Çalışan Hileleri ve İç Kontrol İlişkisi. Vergi Sorunları Dergisi, 330, 159-172
8) KARAKAYA, E., & KARAKAYA, G. (2017), Developing a Risk Management Framework and Risk Assessment for Non-profit Organizations: A Case Study, In Risk Management, Strategic Thinking and Leadership in the Financial Services Industry (pp. 297-308). Springer International Publishing.
9) KURT, G. ve UYSAL, T. U. (2018), COSO Kurumsal Risk Yönetimi Çerçevesi Güncelleme Projesinin Getirdiği Yenilikler. *Muhasebe ve Denetime Bakış- Accounting & Auditing Review*, *18*(54), 19-34
10) PİERCE, E. M., & GOLDSTEİN, J. (2018). ERM And Strategic Planning: A Change İn Paradigm. International Journal Of Disclosure And Governance, 15(1), 51-59
11) PREWETT, K., & Terry, A. (2018). COSO's Updated Enterprise Risk Management Framework—A Quest For Depth And Clarity, Journal of Corporate Accounting & Finance, 29(3), 16-23
12) TÜREDİ, H., & KARAKAYA, G. (2015), COSO İç Kontrol Modeli ve Kontrol Ortamı. Finans Politik & Ekonomik Yorumlar Dergisi, 52(602).