COSO KURUMSAL RİSK YÖNETİMİ ÇERÇEVESİ GÜNCELLEME PROJESİNİN GETİRDİĞİ YENİLİKLER

Prof. Dr. Ganite KURT*

Doç. Dr. Tuğba UÇMA UYSAL**

Makale Gönderim Tarihi : 20.11.2017 / Kabul Tarihi : 14.01.2018

ÖZ

2004 yılında yayınlanan COSO ERM - Bütünleşik çerçeve, risk yönetimini örgütlerde bir sonraki hayati önem taşıyan bir noktaya çekmiştir. Çerçeve risk hakkında örgüt içerisinde standart düşünme temeli yaratmıştır. Ancak uygulama noktasında birçok örgütte bilinen risklerin uzaklaştırılması, yok edilmesi ve yönetilmesi süreçlerinden çok da öteye geçememiştir. 2014 yılında dünyada en yaygın kabul gören ve uygulama alanı bulan kurumsal risk yönetim çerçevelerinden biri olan COSO ERM - Bütünleşik Çerçeve güncelleme çalışması gündeme getirilmiştir. Bu çalışmada güncellenerek Eylül 2017'de yayınlanan yeni COSO ERM - Riskin Strateji ve Performansla Uyumlaştırılması ile ilgili bilgiler verilmekte ve güncellenen çerçevede getirilen yeniliklere yönelik açıklamalar yapılmaktadır.

Anahtar Kelimeler: Kurumsal Risk Yönetimi, COSO Çerçevesi, Güncelleme Projesi,

THE INNOVATIONS OF COSO ENTERPRISE RISK MANAGEMENT FRAMEWORK UPDATE PROJECT

ABSTRACT

The COSO ERM - Integrated Framework, published in 2004, has put risk management at a crucial point in organizations. The framework has created a standard mindset within the organization about risk. However, at the point of implementation, many organizations have not gone far beyond the processes of removing, mitigating and managing known risks. In 2014, the COSO ERM - Integrated Framework's, which is one of the most widely accepted and applied enterprise risk management frameworks in the world, update project was on the agenda. This study aims to give information about the new COSO ERM - Risk Management–Integrating with Strategy and Performance, updated and published in September 2017, and explain the innovations introduced in the updated framework.

Keywords: Enterprise Risk Management, COSO Framework, Update Project

* Gazi Üniversitesi, Bankacılık ve Sigortacılık Yüksekokulu Öğretim Üyesi, ganitekurt@gmail.com

** Muğla Sıtkı Koçman Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası Ticaret ve Finansman Bölümü Öğretim Üyesi, ucmatugba@gmail.com

1. GİRİŞ

Bilindiği gibi, Treadway Komisyonu[1] olarak bilinen Hileli Finansal Raporlama Üzerine Ulusal Komisyon'u (National Commission on Fraudulent Financial Reporting – NCFFR) 1985 yılında kurulmuştur. Ulusal Komisyon Amerika'da beş önemli meslek kuruluşunun desteğini almaktadır. Bu kuruluşlar Amerikan Muhasebeciler Birliği (American Accounting Association - AAA), Amerika Sertifikalı Kamu Muhasebecileri Enstitüsü (American Institute of Certified Public Accountants - AICPA), Uluslararası Finansal Yöneticiler Birliği (Financial Executives International - FEI), İç Denetçiler Enstitüsü (Institute of Internal Auditors - IIA), ve şu anda Yönetim Muhasebecileri Enstitüsü (Institute of Management Accountants - IMA) olarak faaliyette bulunan Ulusal Muhasebeciler Birliği (National Association of Accountants) şeklinde sıralanabilir. Sayılan her bir destekleyici örgüt yanında Komisyon, sanayi, kamu, yatırımcı firmalar ve New York Sermaye Piyasası'ndan destek almaktadır (http://www.coso.org). COSO, İngilizce Committee of Sponsoring Organizations of Treadway Commision (Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi) kelimelerinin kısaltmasıdır. COSO'nun en önemli misyonu; kurumsal risk yönetimi, iç kontrol ve hilenin tespiti konularında kapsamlı bir çerçeve geliştirerek örgütsel performansı ve kurumsallığı arttırarak örgütlerdeki hileli finansal raporlamanın meydana gelmesini azaltmaktır.(http://www.coso.org/aboutus.htm, http://www.kpmg.com.tr).

Komisyonunun bünyesinde iç kontrol literatürünün yeniden gözden geçirilmesi, hileli finansal raporlamaya yol açan nedenlerin belirlenmesi, hileli finansal raporlamanın önüne geçilmesi (Brief vd. 1996, 183) için bir çalışma grubu oluşturulmuş, destekleyici kurumların iç kontrol sisteminin kurulması ve etkinliğinin değerlendirilmesi için genel kabul görecek standartlar belirleyen bir projeyi üstlenmesi kararlaştırılmıştır. Komisyonunun iç kontrol için kapsamlı ilk çerçevesi 1987 yılında Treadway Komisyonu olarak da bilinen Hileli Finansal Raporlama Üzerine Ulusal Komisyon Raporu (Report of the National Commission on Fraudulent Financial Reporting) olarak yayınlanmıştır. Daha sonra 1992'de Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi "*İç Kontrol Bütünleşik Çerçeve*" raporunu yayımlamıştır. Bu rapor, COSO iç kontrol modeli olarak bilinmektedir (www.bumko.gov.tr, http://www.kpmg.com.tr). 2004 yılında ise COSO örgütler açısından gerek kurumsal yönetim anlayışının sağlanması gerekse de iyi bir risk yönetiminin varlığını sağlayabilmek için Kurumsal Risk Yönetimi – Bütünleşik Çerçeve (COSO Enterprise Risk Management – Integrated Framework) yayınlamıştır. 2008 yılında ortaya çıkan finansal krizler başta olmak üzere değişen iş dünyası gereklilikleri her iki çerçevenin de güncellenme sorununu gündeme getirmiştir. İlk olarak 2013 yılında güncellenen COSO İç Kontrol – Bütünleşik Çerçeve yayınlanmıştır. Ardından da 2014 yılında dünyada en yaygın kabul gören ve uygulama alanı bulan kurumsal risk yönetim çerçevelerinden biri olan COSO ERM - Bütünleşik Çerçeve güncelleme çalışması gündeme getirilmiştir. Bu çalışmada güncellenerek 6 Eylül 2017'de yayınlanan yeni COSO ERM ile ilgili bilgiler verilmekte ve güncellenen çerçevede getirilen yeniliklere yönelik açıklamalar yapılmaktadır.

1 Ulusal Komisyon'un Treadway Komisyonu olarak tanınmasının temel nedeni komisyonun belirtilen dönemdeki başkanının isminin James C. Treadway olmasıdır. Bu nedenle komisyon Treadway Komisyonu olarak ve hazırlanan rapor da Treadway Raporu olarak bilinmektedir (http://www.coso.org/aboutus.htm).

2. GÜNCELLEME PROJESİNİN GELİŞİMİ VE KAPSAMI: "COSO ERM - Riskin Strateji ve Performansla Uyumlaştırılması"

Geleneksel olarak kurumsal risk yönetimi (ERM), örgütlerdeki değeri korumaya odaklanmak için geliştirilmiş ve risk işlevleri, örgütün hedeflerine veya stratejilerine yönelik tehditleri tanımlama ile görevlendirilmiştir. İfade edilen süreç içerinde, örgüt dışında oluşabilecek bir tehdidi ararken bunun yanında örgüt faaliyetlerinin nasıl yerine getirileceği konusunda karşılaşılan zorlukları da bir arada değerlendirmek gerekmektedir. Ancak, bugünkü koşullarda bir örgüt içerisinde yürütülen ERM'den beklenen bir taraftan bilinen tehditlere veya riskin olumsuz yönlerine odaklanması önemli bir karar verme bileşenini oluştururken, diğer taraftan riskin yerinde belirlenip değerlendirilebilmesi, küresel örgütün değer yaratma ve rekabet avantajı elde etme konusunda yardımcı olabilmesidir. 2004 yılında yayınlanan COSO ERM - Bütünleşik çerçeve, risk yönetimi uygulamalarını örgütlerde bir sonraki önem taşıyan bir noktaya çekmiştir. Çerçeve risk hakkında örgüt içerisinde standart düşünme temeli yaratmıştır. Ancak uygulama noktasında birçok örgütte bilinen risklerin uzaklaştırılması, yok edilmesi ve yönetilmesi süreçlerinden çok da öteye geçememiştir. Son dönemde iş dünyasının daha karmaşık, teknoloji temelli ve küresel olması, üst yönetim ve risk yöneticileri kadar tüm yönetim mekanizmasının riski tanımlama, değerlendirme ve hazırlanma süreçlerinde aşağıda ifade edilen nedenlerden dolayı daha fazla yetenek kazanmalarına yol açacak olan güncellenen bir çerçeveye ihtiyaç duymaları sonucunu doğurmuştur (https://www2.deloitte.com/):

- Örgütün stratejisini etkileyen dışsal güçlerin olması (küresel rekabet ortamı, teknoloji temelli işletme süreçleri, paydaşların daha şeffaf raporlamaya ihtiyaç duyması vb.),
- Örgüt stratejisinin dayandığı varsayımları etkileyebilecek koşulların değişmesi,
- Örgüt stratejinin uygulanmasından kaynaklanabilecek risklerin belirlenmesidir.

Beliritlen nedenlerin yanında güncelleme gerekçeleri olarak COSO ERM – Bütünleşik Çerçeveyi uygulamadaki eksiklikler de sayılabilir. 2004 yılında ilk çerçeve yayınlandıktan sonra günümüze kadarki süreçte kurumsal risk yönetimi uygulamaları incelendiğinde, işletmelerin tamamına yayılan bir risk yönetimi uygulamasının yapılamadığı dikkat çekmektedir. Bunun oluşmasındaki nedenlerden biri bütünleşik çerçevede yer alan ve iç kontrol bütünleşik çerçevesine benzer nitelikteki COSO ERM küpünün işletmeler tarafından iyi anlaşılamaması olarak gösterilebilir. Küpün üst kısmında yer alan faaliyetler ve strateji belirleme sürecine işletmenin tüm şube, birim, bölüm ya da işletme genelinde ilişkilendirilerek tanımlanan bileşenlere bağlanması uygulama süreçlerinde zorluklar meydana getirmiştir. Örgütler faaliyetlerini yerine getirmede ve strateji belirlemede işletme içerisindeki birimleri ya da işletmenin bütününü karar alım sürecine dahil edememiştir. Bir diğer neden ise, bazı işletmelerin kurumsal risk yönetimini işletme faaliyetlerini daha iyi hale getiren bir süreçten ziyade güvence aracı olarak algılamalarıdır. Bu yaklaşım da özellikle iç denetim faaliyetleri sırasında ciddi sıkıntılara yol açmıştır. Sayılan nedenlere ek olarak 2008 yılında ortaya çıkan finansal kriz ve 2011 yılında Japonya'da meydana gelen tsunami kurumsal risk yönetimi uygulamalarının işletme içerisindeki artan önemine dikkat çekmektedir (https://www.protiviti.com/US-en/insights/bulletin-vol-6-issue-2).

Günümüzde risk yönetimi, örgütlerin karşılaştıkları belirsizlikleri daha anlaşılır hale getirmek ve asla karşılaşılmayacak olasılıkları da dikkate alacak şekilde kurumsal bir yapı içerisinde ger-

çekleştirilmek durumundadır. Literatürde bu durumu ifade etmek amacıyla Taleb (2007) tarafından ortaya atılan ve belirsizliğin derecesini tanımlamak amacıyla kullanılan metaforik bir ifade yer almaktadır. ***Siyah kuğu (black swan)*** olarak adlandırılan teoriye göre, örgüt içerisinde her ne kadar gelişmiş kurumsal risk yönetimi araçları uygulansa da belirli bir türdeki ve tahminlenmesi çok güç olan bir felaket durumu işletme faaliyetlerini aksatabilecek bir sonuca neden olabilmektedir (Locklear, 2012: 14). Bu da örgütlerin hiç karşılaşamayacakları zorluklara karşı da hazırlıklı olmaları gerekliliğini ortaya çıkarmaktadır.

Açıklamalar doğrultusunda sayılan gerekçeleri de göz önüne alarak 2014 yılında COSO ERM - Bütünleşik Çerçeveyi güncellemek amacıyla bir proje başlattı ve PwC'yi proje ekibine alarak taslak hazırlıklarına başladı. Taslak çerçevede özellikle gelişen koşulların dikkate alınarak tüm örgüt seviyesine yayılabilecek hatta riskin strateji ve performans ile uyumunu da gözetecek bir hazırlık süreci yürütüleceği ifade edildi. 15 Haziran 2016'da, COSO ERM - Riskin Strateji ve Performansla Uyumlaştırılması başlıklı güncellenmiş bir taslak yayınlandı. Taslak riskin oluşturulması, korunması, sürdürülmesi ve değer kazanması için geliştirilmiş bir yol yaklaşımın gereğine işaret ederek yaklaşık 100 günlük kamuoyu açıklaması dönemi içerisinde geri bildirimleri toplamıştır. PwC tarafından yapılan açıklamada, güncellenen taslak çerçeveye 2.000'den fazla bireysel yorum gelmiştir. Taslak çerçeve için yapılan pozitif derecelendirme negatif puanlamanın 4.5 katı olarak ölçülmüştür. Ardından gelen bildirimler PwC proje ekibi tarafından; ilkelerin sayısını azaltmak, grafikleri güncellemek, iç kontrol ile bağlantıları netleştirmek, bileşenlerin başlıklarını değiştirmek, entegrasyon ve karar verme üzerine daha çok vurgular yapmak, kültürün temel örgüt değerleri ile olan ilişkisini vurgulamak, bilgi ve teknoloji ile ilgili bileşeni daha detaylı sunmak olmak üzere yedi temel değişiklik önerisi (https://www.pwc.com) halinde özetlenerek yayınlanmıştır.

Böylelikle geri bildirimler de göz önüne alınarak 6 Eylül 2017 tarihinde güncelleme projesi tamamlanmış ve COSO ERM - Riskin Strateji ve Performansla Uyumlaştırılması başlıklı yeni çerçeve yayınlanmıştır. Güncellenen çerçeve, örgütlerin risk yönetimine daha kurumsal çapta yaklaşımları tasarlamalarına ve uygulamalarına yardımcı olabilecek şekilde ilke temelli bir sunumu benimseyerek, örgüt içerisinde risk bilincine sahip bir gözetimi ve karar almayı sağlayarak daha iyi değer yaratabilmeleri için büyüklük, yasal yapı ve faaliyet alanı gözetmeksizin tüm yararlanıcılara sunulmuştur.

3. GÜNCELLENEN ÇERÇEVENİN GETİRDİĞİ YENİLİKLER

Güncellenen çerçeve, kurumsal risk yönetiminin stratejik planlamadaki önemini vurgulamakta olup, risk örgüt çapında strateji ve performansı etkilediğinden, kurumsal risk yönetimini de bir örgütün içerisinde tüm karar süreçlerine gömülü olarak kabul etmektedir. 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. Böylelikle örgütlerde kurumsal risk yönetiminin örgüt stratejisinin uygulanmasına ve örgütün performansına nasıl entegre edilebileceğini ortaya koymaktadır bu aynı zamanda örgüt içerisindeki tüm yönetim mekanizmasının strateji belirleme sürecinden başlayarak strateji uygulama sürecinde ve örgütün başarısını gösteren performans değerlendirmesinde de riski yönetmesine imkan tanımaktadır (http://markets.businessinsider.com).

Yeni COSO ERM yönetici özetinde, güncelleme süreci son dönemde kurumsal risk yönetimi pratikleri ve riski anlamak ile ilgili büyük gelişmeler yaşanması ile birlikte açıklanmaktadır. Aynı zamanda Dünya Ekonomik Forumu'nda da üzerinde durulan konuların başında gelen iş dünyasının artan esnekliği, karmaşıklığı ve belirsizliği yürütülen güncelleme projesinin de temel gerekçeleri olarak gösterilmektedir. Yeni çerçeveye göre yaşanan değişimler birer olgudur ve her örgüt bu olguları gözetmek zorundadır. Yayınlanan çerçevede belirtilen gözetim sürecinin örgütlerin stratejik olarak nasıl dikkate almaları gerektiğine yardımcı olmaktadır. Bunu yaparken de çerçeve bir taraftan tüm örgütlerin kurumsal risk yönetimini bir işlev ya da departman olarak görmekten vazgeçmelerine vurgu yapmakta diğer taraftan da örgüt değerinin yaratılması, korunması ve anlaşılmasında riskin yönetimi amacıyla strateji belirleme ve strateji yürütme ile entegreli örgütün kültürü, yetenekleri ve pratikleri olarak tanımlanmaktadır. Ayrıca kurumsal risk yönetimi iç kontrolden daha kapsamlı bir faaliyet olarak ifade edilmektedir (COSO ERM – Executive Summary, 2017). Bu noktada ilk farklılık ortaya çıkmaktadır. Çünkü güncellenen çerçevede kurumsal risk yönetiminin tanımı daha da basitleştirilerek sunulmaktadır. 2004 yılında çıkarılan COSO ERM – Bütünleşik Çerçevede kurumsal risk yönetimi;

"Kurum genelinde olan ve oluşturulan stratejileri uygulayan; kurumun yönetim kurulu, yönetimi ve diğer personelinden etkilenen; kurumun hedeflerini elde etmesi için makul bir güvence sağlamak için kurumu etkileyebilecek potansiyel olayları tanımlamak ve risk kapasitesi içinde yönetmek amacıyla tasarlanmış bir süreçtir."

şeklinde tanımlanmaktadır (Arslan, 2008: 27). Yeni çerçevede verilen tanımda ilk göze çarpan nokta örgütün değerinin ön plana çıkarılmasıdır. Bunu yaparken de değerin kazanılması ve korunması noktasında örgüt kültürünü ifade eden kapsamlı bir kavram olan kültür yelpazesini (culture spectrum) gündeme getirmektedir. Böylelikle yönetimin risk alma davranışları ile doğrudan bağlantılı olan risk kültürünün de belirlenmesine yardımcı olmaktadır. Sonuçta yeni tanım riskin yönetimini örgütün değeri ile uyumlaştırmaktadır.

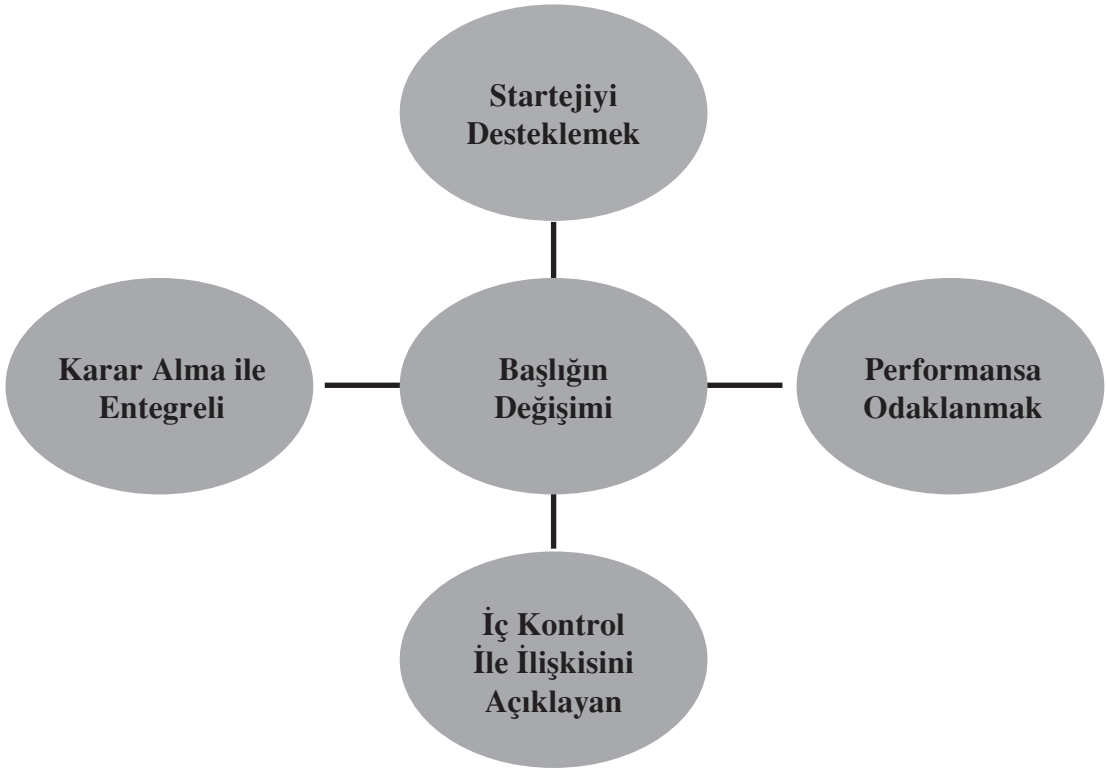
Çerçevedeki bir diğer yenilik olarak çerçevenin güncelleme nedenleri gösterilebilir. Yayınlanan yönetici özetinde değişim nedenleri aşağıdaki başlıklar halinde ifade edilmektedir (COSO ERM Executive Summary, 2017):

- Strateji oluşturma ve yürütmede kurumsal risk yönetimi rolünü ve stratejiyi kararların içerisine dahil etmek,
- Kurumsal risk yönetimi ve performans arasındaki ilişkisini arttırmak,
- Yönetişim ve gözetim için gerekli algıyı sağlamak,
- Küreselleşmeyi gözeterek, daha karmaşık yapıdaki işletme çevresine yönelik örgütün amaçlarına ulaşmasına ve amaçların belirlenmesinde riskin gözetimini sağlamak,
- Daha şeffaf olarak raporlama yapılmasına yardımcı olmak,
- Teknoloji içeren işletme süreçlerini yaygınlaştırmak,
- Her seviyedeki yönetim kademesinin dahil olabileceği kurumsal risk yönetimi pratiklerini tasarlamak, uygulamak ve yürütmek için temel tanımlar, kavramlar, unsurlar ve ilkeler belirlemektir.

Yönetici özetindeki gerekçeleri destekler nitelikte güncelleme projesinin ortağı olan PwC de yeni risklerin geçmişe oranla daha hızlı ortaya çıkması ve karmaşık olmasını gerekçe olarak ifade etmekte olup, değişen tüketici davranışlarının örgütler üzerinde önemli baskılar yaratması ve küresel

ekonominin daha az öngörülebilir hale gelmesi yani değişen iş dünyası gerekliliklerine cevap verebilmek için hem teknolojiyi kullanan hem de daha şeffaf raporlama yapılmasına imkan tanıyan bir çerçeve oluşturulduğunu açıklamaktadır. Bu da bir taraftan örgütlerin belirtilen zorlukların üstesinden gelmesini sağlayan, diğer taraftan da riski yönetmek için yeni bir yaklaşım benimsemesini gerektiren ilke temelli bir yapıya yöneldiklerini göstermektedir (http://pwc.com). Sonuçta yeni çerçevenin ortaya çıkma gerekçesinin temelinde geçmişte uygulanandan daha fazla riski yönetebilmek yatmakta olup, bütünleşik çerçevenin gözden geçirilerek daha kapsamlı bir risk yönetimi için yeni bakış açısı sunmak yer almaktadır. Bu çerçevedeki farklılıkların temel felsefesini oluşturmaktadır.

Çerçevede yer alan bir diğer önemli değişiklik ise başlıkta olmuştur. Başlığın değiştirilmesini etkileyen nedenler aşağıdaki şekil üzerinde gösterilmektedir.

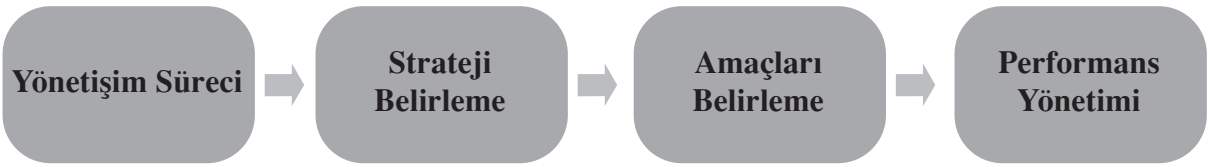


Şekil 1. Çerçevede Benimsenen Yeni Başlığın Gerekçeleri

Kaynak: http://www.dallasiia.org/wp-content

Şekilde de görülebileceği gibi, çerçevenin adının değiştirilme nedeni olarak strateji ve performans ile kurumsal risk yönetiminin bağlantısını gözetmek gösterilebilir. Bununla birlikte iç kontrol ve kurumsal risk yönetimi arasındaki bağın kurulması/belirginleştirilmesi ve kurumsal risk yönetimi ile karar almayı entegreli hale getirmek de çerçevenin başlığını değiştirme nedenleri olarak sunulmaktadır (https://www.corporate-compliance.org).

Çerçevede yer alan bir diğer yenilik olarak tanımlanan ilkeler gösterilebilir. Yeni çerçeve, sadece beş bileşen ve iş döngüsüne uyumlu 20 ilke ile yeni bir yapı getirmektedir. İlkelerin hazırlanmasında kurumsal risk yönetiminin tüm örgüt süreçlerine yayılma şekli aşağıdaki gibi ifade edilmektedir:



Şekil 2. Kurumsal Risk Yönetimi ve Örgüt Süreçleri İlişkisi

Kaynak: https://www.corporatecompliance.org

İlke temelli geliştirilen yeni yapıda bileşenlerin güncellenmesi ve ilkelerin uyumu, tanımların basitleştirilmesi, değerin gözetilmesi, entegrasyon üzerine odaklanan bir yapının kurulması, kültürün rolünün analiz edilmesi, stratejiyi tartışmanın kolaylaştırılması, performans ile bağlantının güçlendirilmesi, karar alma ile ilişkili bir risk yönetim sürecinin gündeme getirilmesi, iç kontrol ile kurumsal risk yönetimi bağlantılarının sağlanması, risk iştahının tanımlanması ve performansın kabul edilebilir seviyedeki değişkenliğinin belirlenmesi üzerinde durulmuştur (https://www.corporatecompliance.org). Sonuçta yeni yapı içerisinde kurumsal risk yönetimi ilkeler temelinde örgütün diğer tüm süreçleri ile entegreli bir hale dönüştürülmüştür. Çerçevede belirlenen ilkeler yasal yapıları, büyüklükleri ve amaçları farklı olabilecek her örgütte uygulanabilir seviyede bir yönetim süreci tanımlamakla beraber, ilkeler spesifik kurallar değildir, yönetimin kararının yerine de geçmemektedir. Bu noktada güncellenen çerçevedeki bileşenler 2004 yılında yayınlanan bütünleşik çerçeveden farklılık göstermektedir. Aşağıda buna ilişkin sunum yer almaktadır.

2004 COSO ERM - Bütünleşik Çerçeve Bileşenler	**İç Ortam**
	İç Ortam
	Hedef Belirleme
	Olay Tanımlama
	Risk Değerlendirmesi
	Riske Karşılık Verme
	Kontrol Faaliyetleri
	Bilgi ve İletişim
	İzleme
2017 COSO ERM - Riskin Strateji ve Performansla Uyumlaştırılması Bileşenler	**Risk Yönetişimi ve Kültürü**
	Strateji ve Amaçları Belirleme
	Performans
	İnceleme ve Gözden Geçirme
	Bilgi, İletişim ve Raporlama

Şekil 3. Bileşenlerin Karşılaştırmalı Sunumu

Şekilden de görülebileceği gibi güncellenen çerçeve içerisinde bileşenlerin sayısı azaltılarak, çerçevenin ilk bileşeni olan risk yönetişimi ve kültürü, kurumsal risk yönetiminin diğer dört bileşeni için bir temel olarak ele alınmıştır. Bu yaklaşım ve basitleştirilmiş yeni yapı bileşenlere ilişkin ilkelerin belirlenmesi noktasında da yansımıştır. Belirlenen ilkeler ise aşağıdaki tabloda özetlenmektedir.

Tablo 1. Güncellenen Çerçevedeki Bileşenler ve İlkeler

Risk Yönetişimi ve Kültürü	Strateji ve Amaçları Belirleme	Performans	İnceleme ve Gözden Geçirme	Bilgi, İletişim ve Raporlama
1. Yönetim Kurulunun Risk Gözetimini Uygulaması **2.** Çalışma Yapısının Oluşturulması **3.** İstenilen Örgüt Kültürünün Tanımlanması **4.** Örgütün Temel Değerlerine Bağlılığın Gösterilmesi **5.** Yetenekli Bireyleri Cezbetme, Geliştirme ve Elde Tutma	**6.** Örgütün Genel Durumunu Analiz Etme **7.** Risk İştahını Belirleme **8.** Alternatif Stratejileri Değerlendirme **9.** Örgütün Amaçlarını Belirleme	**10.** Riskleri Tanımlama **11.** Riskin Önem Derecesini Değerlendirme **12.** Riskleri Önceliklendirme **13.** Risk Cevapları Belirleme ve Seçme **14.** Portföy Bakış Açısı Geliştirme	**15.** Önemli Değişiklikleri İzleme **16.** Risk ve Performansın İzlenmesi **17.** Kurumsal Risk Yönetiminde Gelişimin Sürdürülmesi	**18.** Bilgi Sistemini Güçlendirme **19.** Risk Bilgisini İletme **20.** Risk, Kültür ve Performans Raporlama

Kaynak: COSO ERM – Executive Summary, 2017

Güncellenmiş çerçevedeki ilk bileşen risk yönetişimi ve kültürüdür. Risk yönetişimi, örgütün atmosferini (organization's tone) belirlemekte ve kurumsal seviyede yürütülen risk yönetiminin önemini güçlendirmektedir. Böylelikle gözetim noktasındaki sorumluluklarını da yerine getirmektedir. Risk kültürü ise, etik değerlere, sorumlu iş davranışına ve iş durumunun anlaşılmasına ilişkindir ve karar verme süreçlerinin tamamına yansımaktadır (https://www.protiviti.com). Bu bileşen örgütlerde risk zekası (risk intelligence)[2] adı verilen bir kavramın gelişmesine ve yaygınlaşmasına imkan tanımaktadır (https://www2.deloitte.com/). Çerçevede belirlenen ilk bileşen ikinci ve üçüncü sıradaki bileşen ile birlikte daha anlamlı bir şekilde sunulmaktadır. Yeni çerçevede özellikle riskin strateji ve performans kavramları ile ilişkilendirilerek sunumu benimsenmektedir. Yani gerek örgütteki strateji belirleme ve yürütme ile performansın değerlendirilmesinde riskin nasıl süreç ile ilişkilendirileceği açıklanmaktadır. Bunu yaparken de risk yönetişimi ve kültürü olarak ifade edilen yönetimin risk alma davranışları ile ilgili bir kavramın geliştirilmesini gerekli olmaktadır. Kültür yelpazesi (culture spectrum) adı verilen ve risk iştahı ile uyumlaştırılmış strateji belirleme sürecini esas almaktadır.

Bilindiği gibi bir örgütteki paydaşların paylaşılan davranışları, duyguları ve düşüncelerini her örgütün kültürünü oluşturmakta ve stratejisi kadar kendine özgü bir felsefeyi ifade etmektedir. Çerçeve kültür ve davranışın önemini ayrıntılı bir şekilde incelemektedir. Örgüt içerisindeki kurullar ve yönetim, örgütün ve paydaşlarının, temel işletme değerlerine ve riske yönelik tutumlarını yansıtan davranışları ifade etmektedir. Bunun yanında örgüt içerisindeki günlük karar verme süreçlerini de yönlendiren en temel kavram kültürdür (https://www.pwc.com). Çerçeve, bir örgütün bir kültür yelpazesine neresinde yer aldığı ardındaki farklı faktörleri ve zaman içinde riske duyarlı bir kültür elde etmek için gereken özellikleri değerlendirmekte olup, stratejinin belirlenmesinde ve yürütülmesinde ne gibi etkiler yaptığını açıklamaktadır.

Çerçevede ikinci bileşen ve altında yer alan ilkelerde, risk ve stratejinin uyumlaştırılmasında üç ayrı boyut esas alınmaktadır. Bunlar aşağıdaki gibidir (https://www.pwc.com):

- ***Strateji İçin Risk:*** Stratejinin uygulanması sırasında risklerin potansiyel etkisini dikkate almak ve tekrar ne zaman stratejinin gözden geçirilmesi gerektiğini vurgulamak.
- ***Stratejiden Kaynaklanan Sonuçlar:*** Seçilen stratejiden kaynaklanan riskleri göz önüne almak, uygulama sürecinde bu risklere karşı örgütün hazırlık yapmasına yardımcı olmak.
- ***Stratejinin Riski:*** Stratejinin bir örgütün misyonu, vizyonu ve temel değerleri ile uyumunu göz önünde bulundurmak.

Çerçevede yer alan boyutlar örgütün risk profili tanımlama sırasında göz önüne alınması gereken risk boyutlarını göstermektedir. "Strateji için risk" geleneksel olarak, potansiyel risk erozyonunu önlemek amacıyla strateji uygulamalarına getirilmiştir. Uygulama sırasında karşılaşılan yani seçilen örgüt stratejisinin meydana getirdiği riskleri önlemek veya minimize etmek amacıyla ikinci sıradaki "stratejiden kaynaklanan sonuçlar" boyutu geliştirilmiştir. Örgütün temel amaçları

2 Risk zekası (risk intelligence), örgütün genel risk tanımı içerisinde yer bulan hem örgüt değerinin yaratılması hem de örgütün sahip olduğu değerini korumasına imkan tanıyan ve tüm örgütte uygulanması gereken bir programı ifade etmektedir. Yürütülen risk yönetimi uygulamalarında yönetimin tüm kademelerinin risk zekasının oluşturulması ve sürdürülmesi sürecine katılmaları, yeni kurumsal risk yönetimi çerçevesine de referans gösterilebilecek bir şekilde strateji belirleme ve performansın ölçülmesine de yardımcı olabilecektir. (Detaylı bilgi için bknz. Deloitte - Risk Committee Resource Guide, 2014).

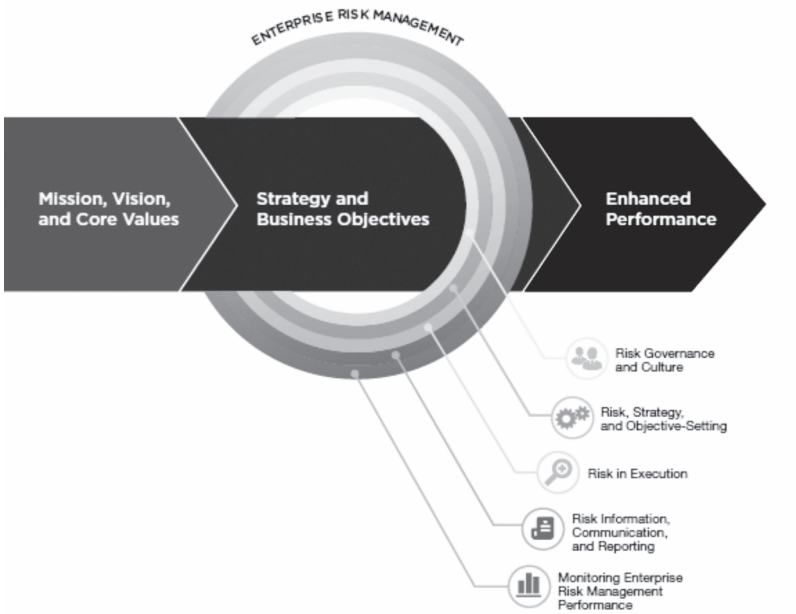
ile uyum sağlamayan bir stratejinin riskini tanımlamak amacıyla da üçüncü sıradaki "stratejinin riski" tanımlanmıştır. Çünkü seçilen strateji örgütün temel değerlerine uyumlaştırılmazsa, performans üzerinde potansiyel olarak daha büyük etkiler yaratabilecektir. Tanımlanan her bir boyutun dikkate alınması ile örgüt içerisinde risk profili çıkartılabilecek, bu profilin belirlenmesinde kullanılan varsayımlar ve gerçekleşen sonuçlar örgütün değerinin yaratılmasını ve korunmasına yardımcı olabilecektir. Bu noktada çerçevede tanımlanan ikinci bileşenin bir taraftan örgütteki kurumsal risk yönetiminin strateji seçiminin bir parçası olmasını sağlamakta, diğer taraftan da strateji belirlendikten sonra örgütün riskleri yönetmesine yardımcı olmaktadır. Bu da bizi çerçevede tanımlanan üçüncü bileşene yani performansa götürmektedir.

Gerek örgütün temel amaçları gerekse de risk iştahı temelinde geliştirilen ikinci bileşen yani stratejiye dayalı risk profilinin oluşturulması sonraki adımda performansın ölçülmesine uyumlaştırılmaktadır. Çünkü temelinde örgütün stratejisi ve amaçlarına ulaştırılması riskin önceliklendirilmesine ve varsayılan risk portföyüne bağlı olarak etkin bir şekilde çalışmaktadır. Uygulama sürecinde örgütlerin karşılaştıkları en büyük sorunlardan biri "risk iştahı" ve "risk profilleri" gibi terimlerin çok soyut nitelikte kalmasıdır. Çerçevede özellikle bu durumu önleyebilmek amacıyla örgüt içerisindeki risk sorununu performans hedefleri ve performansta kabul edilebilir farklılıkları belirleme gibi daha somut süreçler ile uyumlaştırıldığı dikkat çekmektedir. Bu noktada çerçevede önerilen risk yönetiminin performansın bir parçası olarak düşülmesi gerektiği ifade edilmekte ve örgüt genelinde daha çok risk hakkında konuşmayı ve tartışmayı esas alan hatta farkında olan bir kültüre teşvik etmektedir. Bu açıklamaları çerçevenin yönetici özetinde sıklıkla risk ile ilgili konuşmaları günlük karar alma süreçleri ile ilişkilendirme şeklinde yer verildiği görülmektedir. Böylelikle geleneksel risk yönetiminin sağladığı faydalardan daha fazla fayda ve değer yaratmayı hedeflemektedir.

Dördüncü bileşen olan inceleme ve gözden geçirmede, örgütün gerçekleştirdiği faaliyetleri yani kurumsal risk yönetiminin tüm bileşenlerinin işleyişini inceleyerek, belirli periyotlar ile gözden geçirme üzerinde durulmaktadır. Böylelikle işletmenin iç kontrol sistemine de bir anlamda referans gösterilmektedir. Güncellenen çerçevede 2013 yılında güncellenen COSO – İç Kontrol Bütünleşik Çerçevesine doğrudan atıf yapılmakta ve örgütün iç kontrol faaliyetlerinin kurumsal risk yönetimi ile entegreli bir şekilde sürdürülmesi gerektiği açıkça belirtilmektedir (http://www.radicalcompliance.com). Çünkü bir örgütte iç kontrol ve risk yönetimi, performans temelli ortak bakış açısı ile sürdürülen ancak odak noktaları farklı olan faaliyetlerdir. İç kontrol faaliyetler, uyumluluk ve raporlama ile ilgili örgütün amaçları konusunda güvence sağlarken, kurumsal risk yönetimi yöneticilere stratejik planlama, kaynak dağılımı ve riske cevap verme kararlarında güvence vermektedir. Bu noktada örgüt içerisinde yürütülen kurumsal risk yönetiminin yüksek riskli kararlara kritik anlayışlar sunmak için periyodik risk ve süreçler seviyesinde yürütüldüğünü ve iç kontrol tanımlamasının ötesine geçtiğini söylemek de mümkündür. Sonuçta çerçevede özellikle üzerinde durulan konu etkili iç kontrol sisteminin, başarılı kurumsal risk yönetimi ve performansı için kritik ve temel önem taşıdığıdır. Ancak etkili bir iç kontrol sistemi örgütün tek başına stratejik sonuçlar doğurması anlamına gelmemekte olup, etkin bir iç kontrol temeline dayandırılmayan kurumsal risk yönetimi de, yalnızca performansı engellemekle kalmamakta, aynı zamanda örgütü risklere karşı korumaya da engel olmaktadır (https://www.pwc.com; COSO ERM – Yönetici Özeti, 2017). Bu nedenle güncellenen çerçevedeki dördüncü bileşen özellikle önceki bileşenlerden performansı optimal seviyede

örgütte mümkün kılmak adına son derece önem taşımaktadır.

Çerçevedeki son bileşen ise bilgi, iletişim ve raporlamadır. Kurumsal risk yönetimi sürekli bir süreç içerisinde gerekli bilginin elde edilmesi ve paylaşılmasını gerektirmektedir. Hem örgüt içindeki hem de dışındaki kaynaklardan elde edilen bilgilerin kurumsal risk yönetimi süresince aşağıdan yukarıya ya da tam tersi ya da yatay bir şekilde aktarılması yani iletişiminin sağlanması ve raporlama sürecine getirilmesi güncellenen çerçeve yönetici özetinde beşinci bileşeni ifade etmektedir. Açıklamalar doğrultusunda, güncellenen kurumsal risk yönetiminin değişen görünümü ve bütünleşik çerçevenin görünümü aşağıdadır.

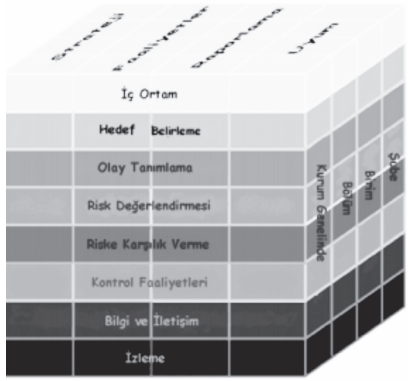


2017 COSO ERM

Kurumsal risk yönetiminin birbiri ile bağlantılı beş bileşenin yer aldığı yatay sunumda, riskin işletmedeki misyon, vizyon ve değerler temelinde strateji seçimi ve işletme amaçları ile uyumlaştırılması böylelikle de performans ile ilişkilendirilerek tüm örgüt seviyesinde uygulanmasını içermektedir.

Şekil 4. Güncellenen COSO ERM Çerçevesi

Kaynak: COSO ERM – Executive Summary, 2017



2004 COSO ERM

Kurumsal risk yönetimi, 8 bileşen temelinde örgütün temel hedefleri olan strateji, faaliyetler, raporlama ve uyum süreçleri ile bağlantılı bir şekilde bölüm, şube, iş birimleri ve örgüt genelinde etkin bir şekilde uygulanmasını ifade etmektedir.

Şekil 5. 2004 COSO ERM Bütünleşik Çerçeve

Kaynak: Arslan, 2009: 29

Güncellenen çerçevede açıklanan bileşenlerin yatay görünümü, bütünleşik çerçevede benimsenen küpten önemli ölçüde farklılık göstermektedir. Çerçevede başlıkta benimsenen değişimlerin yeni kurumsal risk yönetimi çerçevesinin de sunumunu büyük ölçüde belirlediğini söylemek mümkündür. Yeni çerçevede değer kavramının kurumsal risk yönetimi sürecine gömülü hale getirildiği, risk tanımından başlayarak bileşenlerin belirlenmesi ve ilkelerin tanımlanmasına kadarki süreçte risk iştahı ve örgütün risk profili üzerinde durulduğu hatta risk yelpazesi adı verilen tüm örgütteki riskin durumunu ifade eden bir kavram ile desteklendiği görülmektedir. Böylelikle güncellenen çervedeki yeni sunumda, kurumsal risk yönetimi statik bir faaliyet olmaktan çıkarılmakta ve örgütteki günlük karar alma süreçlerinde de aktif olarak yer alarak strateji geliştirme ve performansın ölçümüne uyumlaştırıldığı söylenebilir. Yine yeni çerçevede benimsenen yatay görünüm, bütünleşik çerçevede küp şeklinde yapılan sunumu daha anlaşılır hale getirmekte ve 2013 yılında güncellenen iç kontrol bütünleşik çerçevesindeki iç kontrol küpü ile karıştırılmasını önlemektedir.

4. SONUÇ VE DEĞERLENDİRME

2014 yılında kamuya açıklanan COSO güncelleme projesi; küresel ortamda iş yapmanın karmaşıklaşması, yeni risklerin geçmişten daha hızlı bir şekilde ortaya çıkmaya devam etmesi, tüketici davranışlarının değişmesi, öngörülemeyen bir küresel ekonomik durumun varlığı, teknolojik gelişmeler ve örgütün tüm paydaşları tarafından örgütten artan oranda şeffaflık beklenmesi gibi nedenler temelinde ortaya çıkmıştır. Sayılan nedenler örgütlerin stratejik planlama süreçlerini ve operasyonel yeteneklerini yönetmelerini zorlaştırmış, hatta bu zorlukların üstesinden gelebilmek ve riski yönetmek için yeni bir yaklaşım benimsemesini gerektirmiştir (www.pwc.blogs.com). Bu doğrultuda örgütlerin COSO ERM – Bütünleşik çerçevesinin 10 yıllık deneyimi gözden geçirilmiştir. Öncelikle taslak çerçeve hazırlanmış ve bir yorum dönemi belirlenerek kamuoyuna duyurulmuş ardından taslak çerçeveye geribildirimler alınmıştır. En son noktada ise güncelenen COSO Kurumsal Risk Yönetimi-Strateji ve Performans ile Entegrasyon (COSO Enterprise Risk Management–Integrating with Strategy and Performance) yayınlanmıştır.

Güncellenmiş çerçevenin ilk kısmı, gelişmekte olan bir iş ortamının taleplerini karşılamak için kurumsal risk yönetiminin güncel ve gelişen kavramları ile uygulamaları hakkında bir perspektif sunmaktadır (https://www.journalofaccountancy.com). Çerçeve, stratejileri ve karar vermeyi güçlendirmek için farklı bakış açılarına ve işletim yapılarına uyan beş kolay anlaşılır bileşen halinde organize edilmiştir. Böylelikle de örgütlerde şu anda ve gelecekte değer yaratmaya, korumaya ve gerçekleştirmeye yardımcı olacak nitelikte ilke temelli bir kurumsal risk yönetim anlayışı benimsenmiştir. Çervede özellikle kurumsal risk yönetimi, örgütün hedeflerini belirlemedeki riskleri yönetmekten daha fazlası olan stratejinin uygulamasının anlaşılması üzerinde durulmaktadır. Örgüt içerisinde bir stratejinin seçiminde yapısal karar alımı risk ve işletmenin misyonu ile vizyonu ile ilgili kaynakların yani örgüt değerinin analizini içermektedir (COSO ERM – Executive Summary, 2017).

Çalışmada sunulan detaylı açıklamalar ardından güncellenen çerçevedeki önemli değişimleri aşağıdaki başlıklar halinde özetlemek mümkündür (https://www.coso.org; http://www.pwc.blogs.com; https://ctmfile.com/story/changes-to-the-coso-erm-framework-unveiled):

- ***Yeni bir yapının getirilmesi:*** COSO'nun yayınladığı diğer çerçevelere benzer bir nitelikte bileşenler ve ilkelerden oluşan bir yapı benimsenmiştir. Sadece 5 bileşen ve iş döngüsüne uyumlu 20 ilke ile çerçevenin temel prensipleri yönetişimden gündelik faaliyetlere kadar olan süreçleri kapsayacak niteliğe dönüştürülmüştür.

Böylelikle büyüklüğü, türü veya sektörü farketmeden tüm işletmelere uygulanabilir bir hale getirilmiştir. Aynı zamanda çerçevede küp yerine, yeni anlayışın anlaşılmasını kolaylaştıran bir yatay grafik benimsenmiştir.

- ***Kurumsal Risk Yönetimi tanımının basitleştirilmesi:*** Çerçevede örgüt değerinin yaratılması, korunması ve anlaşılmasında riskin yönetimi amacıyla strateji belirleme ve strateji yürütme ile entegreli örgütün kültürü, yetenekleri ve pratikleri olarak kurumsal risk yönetimi tanımlanmaktadır. Böylelikle kurumsal risk yönetiminin farklı faydaları ön plana çıkarılmaktadır. Özellikle, kurumsal risk yönetimi uygulamalarını örgütün değeri ile ilgili fayda sağlanmasına yardımcı olmak için strateji belirleme ve performans yönetimi uygulamalarıyla bütünleştiren açık bir örnek uygulama sunmaktadır. Bu avantajlara odaklanmak, kurumsal risk yönetiminin işletmelerde neden önemli olduğu tartışmalarını da arttırıcı bir etki yaratabilmek amacı ile sıklıkla vurgulanmaktadır. Aynı zamanda da yönetim kurulu ile yönetim arasındaki risk hakkında daha fazla sayıda konuşmaya imkan tanımaktadır.

- ***Entegreli risk yönetimi üzerine odaklanma:*** Çerçeve, kurumsal risk yönetiminin daha iyi nasıl entegre edilebileceği konusunda rehberlik etmektedir. Strateji belirleme ve günlük faaliyetler ile risklerin ilişkilendirilmesi, örgütün kültürü, yetenekleri ve uygulamaları içerisine risklerin gömülü hale getirilmesi ve daha iyi karar alım sürecinin desteklenmesi gibi konulara vurgular yapılmakatdır.

- ***Çerçevede işletme perspektifi benimseme:*** Çerçevenin dili, kurumsal risk yönetimi uygulamalarını tasarlama, uygulama ve yürütme ile ilgili her seviyedeki yönetim mekanizmasının temel tanımlarını, bileşenlerini ve ilkelerini ortaya koyarak riskle ilgili ve evrensel nitelikte görüşmeler yapmaya imkan tanımaktadır. Bu noktada çerçevenin hazırlanmasında kullanılan dil içerisinde sıklıkla işletme perspektifi vurgulanmakta ve örgüt içerisinde risk tartışmalarını kolaylaştırmaktadır.

- ***Risk yönetimi ve iş modeli arasındaki ilişkiyi gösteren yeni kavramsal grafikler bulunması:*** Çerçevede yeni grafik seti benimsenmiştir. Özellikle sunulan yeni kavramsal grafikler risk yönetimi ve örgüt içerisinde benimsenen iş modeli arasındaki ilişkiyi yeniden canlandırmaktadır. Risk eğrileri gibi diğer grafiklerde risk, strateji ve performans arasındaki ilişkiler vurgulanarak günlük faaliyetlerin yerine getirilmesinde risk yönetimini derinlemesine ele almaktadır.

- ***Örgütün tüm seviyelerinde risk yönetimi:*** : Bir örgütün kuruluş aşamasından işleyiş aşamasına kadarki tüm süreçlerinde riskin nasıl tanımlanacağı, değerlendirileceği, stratejik olarak risklerdeki değişimlerin nasıl yönetileceği açıklanmakta ve araştırılmaktadır. Çerçeve aynı zamanda örgütün tüm seviyelerinde risk yönetimini gerektirmekte olup, risk iştahı ve portföyün risk durumu gibi konuları incelemekte ve daha derinlemesine bir kavrayış sağlayarak günümüzde var olan bazı yanlış anlamaları gidermektedir.

- ***Örgüt Kültürüne önem verilmesi:*** Çerçevede örgüt kültürü kavramına daha fazla önem verilmektedir. Özellikle kurumsal risk yönetimi uygulamalarının, bir örgütün kültürüne nasıl daha fazla şeffaflık ve risk bilincini aşılayabileceğini araştırmakta; bu kararların şekillendirilmesinde kültürün öneminin bilgi kullanıcılarının karar vermelerine nasıl yardımcı olduğunu ifade etmektedir.

- ***Bilgi teknolojisinin değişen rolüne değinilmesi:*** Çerçeve, verilerin çoğalması, yapay zeka ve otomasyon gibi iş eğilimlerinin bir

organizasyonun stratejisini, iş bağlamını ve risk yönetimini nasıl etkilediği üzerine ışık tutmaktadır.

Özetle COSO 2004 yılında kurumsal risk yönetimi bütünleşik çerçevesini yayınladıktan sonra geçen on yıllık süreç içerisinde küresel mega trendlerin ortaya çıkışı ve değişen paydaş beklentilerinin ışığında çerçeveyi güncelleme projesi başlatmıştır. Yenilenmiş yaklaşım ile çerçevede temel bileşenler rafine edilmekte ve örgütlerde risk yönetimi uygulamalarını destekleyici ilkeler belirlenmektedir. Çerçeve, risk, strateji ve performans arasındaki bağlantının önemini kabul etmekte olup, bütün örgütlerde kurumsal risk yönetiminin mevcut ve gelişmekte olan kavramları ve uygulamaları hakkında perspektif sunmaktadır. Sonuçta mevcut olan kurumsal risk yönetimi uygulamalarının yeni çerçevedeki formunda sağlayabileceği yeni avantajları tüm yararlanıcılara sunmaktadır.

KAYNAKÇA

Arslan, I. (2009). Kurumsal Risk Yönetimi, Maliye Bakanlığı Stareteji Geliştirme Başkanlığı, http://www.sgb.gov.tr/MaliyeUzmYrdArasRaporlari/Maliye%20Uzmanlığı%20Araştırma%20Raporları/Kurumsal%20Risk%20Yönetimi%20Işıl da%20ARSLAN.pdf Erişim Tarihi: 08.09.2017

Brief, A. P., Dukerich J. M., Brown P.R. and Brett J. F. (1996). What's Wrong with the Treadway Commission Report? Experimental Analyses of the Effects of Personal Values and Codes of Conduct on Fraudulent Financial Reporting*, Journal of Business Ethics,* Volume: 15, pp. 183-198.

COSO ERM – Integrated Framework. (2004). https://www.coso.org Erişim Tarihi: 08.09.2017

COSO Enterprise Risk Management–Integrating with Strategy and Performance. (2017). Executive Summary, https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf Erişim Tarihi: 07.09.2017

COSO Enterprise Risk Management–Integrating with Strategy and Performance. (2017). Frequently Asked Questions, https://www.coso.org/Documents/COSO-ERM-FAQ-September-2017.pdf Erişim Tarihi: 07.09.2017

Deloitte - Risk Committee Resource Guide. (2014). https://www2.deloitte.com/governance-risk-compliance/ZA_Risk-CommitteeResourceGuideOnline2014_22052014.pdf Erişim Tarihi: 12.09.2017

Kurt, G. ve Uçma, T. (2013). COSO iç kontrol-bütünleşik çerçeve güncelleme projesinin yenilikleri*, Muhasebe Bilim Dünyası Dergisi*, Vol. 15 Issue 2, p99-109.

Kurt, G. ve Uçma Uysal, T. (2015). Siber Risk ve COSO İç Kontrol Bütünleşik Çerçevesi, *Muhasebe ve Denetime Bakış Dergisi,* Yıl: 15, Sayı: 46, p. 1-11.

Locklear, K. (2012). Toward a Theory of Everything? Exploring at the Edges of the ERM Construct. In Enterprise Risk Management Symposium.

Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable*. New York, NY: Random House.

http://www.bumko.gov.tr Erişim Tarihi: 12.09.2017

https://www.corporatecompliance.org/Portals/1/PDF/Resources/past_handouts/euroCEI/2017/602_slides_A4_2.pdf Erişim Tarihi: 12.09.2017

http://www.coso.org/aboutus.htm Erişim Tarihi: 12.09.2017

https://ctmfile.com/story/changes-to-the-coso-erm-framework-unveiled Erişim Tarihi: 12.09.2017

http://www.dallasiia.org/wp-content/uploads/2017/04/PwC-COSO-ERM-and-FRMG-for-UTD-Fraud-Summit-March-31-2017-Final.pdf Erişim Tarihi: 12.09.2017

https://www2.deloitte.com/bg/en/pages/risk/articles/coso-erm-update.html#top Erişim Tarihi: 16.09.2017

https://www.journalofaccountancy.com/news/2017/sep/coso-erm-framework-201717164.html Erişim Tarihi: 15.09.2017

http://www.kpmg.com/TR/tr/Issues-And-Insights/Haberler-ve-Etkinlikler/Documents/Fider-BT-S%C3%BCrec-Denetimi-Sunumu-7-Haziran-2012.pdf Erişim Tarihi: 23.09.2017

http://markets.businessinsider.com/news/stocks/COSO-Issues-Important-Update-to-ERM-Framework-1002345634 Erişim Tarihi: 12.09.2017

http://pwc.blogs.com/resilience/2017/09/the-top-changes-to-the-coso-erm-framework-you-need-to-know-now.html Erişim Tarihi: 13.09.2017

https://www.pwc.com/gx/en/services/advisory/consulting/risk/resilience/publications/COSOframework-keychanges.html Erişim Tarihi: 10. 09.2017

https://www.pwc.com/us/en/press-releases/2016/pwc-coso-erm-framework-press-release.html Erişim Tarihi: 12.09.2017

https://www.protiviti.com/US-en/insights/bulletin-vol-6-issue-2 Erişim Tarihi: 12.09.2017

http://www.radicalcompliance.com/2017/05/03/update-coso-erm-framework-update/ Erişim Tarihi: 07.09.2017