ISO 31000 VE COSO KURUMSAL RİSK YÖNETİMİ KARŞILAŞTIRMASI: ÇERÇEVELERİ ANLAMAK*

(COMPARISON OF ISO 31000 AND COSO ENTERPRISE RISK MANAGEMENT: UNDERSTANDING FRAMEWORKS)

Maşuk Cahit UYSAL**

ÖZ

Kurumsal risk yönetimi (KRY), bir örgütün karşılaştığı tüm riskleri bütünsel olarak yönetmek amacıyla risk yönetiminde yeni bir paradigma olarak ortaya çıkmıştır. Yine de örgütler riskleri hâlâ parça parça bir şekilde yönetmekte ve KRY'yi etkili bir şekilde uygulamak ve karmaşık stratejik riskleri yönetmek için mücadele etmektedir. Bu nedenle örgütler, çevresel faktörlerdeki yıkıcı değişiklikler ve sektörlerin dinamik doğası göz önüne alınarak, yeni risklere karşı güncel kalmalı ve KRY süreçlerini sürekli izlemelidirler. Her ne kadar KRY konusu literatürde geniş çapta araştırılmış olsa da, sadece birkaç çalışma olası uygulama sorunlarını vurgulamak için çerçevelerin analizine odaklanmıştır. Bu çalışmada, bu soruna bir çözüm olarak; riskleri, geri bildirim ve gecikmeleri içeren nedensel bir modelleme ortamına entegre etmeyi sağlayan bir sistem dinamiği yaklaşımı kullanarak KRY uygulaması önerilmektedir. Uygulama metodolojisi ISO 31000 Risk Yönetimi Standardı ve COSO KRY çerçevesi güncellemeleri kullanılarak tarif edilmektedir. Kullanıcıların değişikliklerin kapsamını anlamaları ve kuruluşlarının riski nasıl yönettikleri üzerindeki potansiyel etkisini belirlemeleri gerekir. Makale önemli yönetimsel sonuçları vurgulayarak konuya dair bilgilerin genişletilmesine katkıda bulunmayı amaçlamaktadır. Bu makalede ana hatlarıyla verilen kavramlar, yaklaşım ve rehberlik, KRY süreçlerinin uygulanması konusunda faydalı bilgiler sunmaktadır. Çalışma aynı zamanda sürekli iyileştirme çabaları, daha fazla bağlantı için fırsatları değerlendirme ve örgütlerin KRY faaliyetlerini strateji belirleme ve faaliyet süreçleri ile entegre etme noktasında çeşitli önerilere de yer vermektedir.

Anahtar Kelimeler: COSO Çerçevesi, ISO 31000 Standardı, Kurumsal Risk Yönetimi

JEL Kodları: M10

ABSTRACT

Enterprise risk management (ERM) has emerged as the new paradigm in risk management with the goal of holistically managing all risks facing an organization. Yet organizations still manage risks in a piece-meal fashion and struggle to effectively implement ERM and manage complex strategic risks. Therefore, given the devastating changes in environmental factors and the dynamic nature of the sectors, organizations must stay up-to-date with new risks and monitor ERM processes constantly. Although the issue of ERM has been extensively researched in the literature, only a few studies have focused on the analysis of frames to highlight potential implementation problems. İn this study proposes a solution to this problem; ERM implementation using a system dynamics approach, which enables integrating risks in a causal modeling environment that includes feedback and delays. The methodology of implementation is described using the ISO 31000 Risk Management Standard and COSO ERM Framework updates. Users need to understand the extent of the changes and identify their potential impact on how their organization manages risk. The article aims to contribute to the widening of the knowledge on the subject by emphasizing the important managerial results. The concepts, approach and guidance outlined in this article provide useful information on the implementation of ERM processes. The study also includes various suggestions for continuous improvement efforts, evaluating opportunities for more connectivity, and integrating organizations' ERM activities with strategy formulation and operational processes.

Keywords: *COSO Framework, ISO 31000 Standard, Enterprise Risk Management*

JEL Classification: *M10*

---

* Bu çalışma, 16.05.2020 tarihinde Sosyal Bilimler ve Eğitim Bilimleri Öğrenci Kongresinde sunulan tebliğin genişletilmiş hâlidir.

** Dr., CICP, ISO/IEC 27001 BD, Başmüfettiş, Türkiye Tarım Kredi Kooperatifleri, Ankara, Orcid. Id:0000-0001-8196-0764, muysal@tarimkredi.org.tr

Yazı Gönderim Tarihi: 19.11.2020, Yazı Kabul Tarihi: 13.12.2020

1. GİRİŞ

Örgütlerinin genelinde riskleri yönetmeye çalışmak isteyenlerin sayısı gün geçtikçe ciddi bir şekilde artmaktadır. Risk yönetimi ise kurumların vizyon ile misyonları çerçevesinde oluşturdukları hedeflerine varmalarına katkıda bulunan bir vasıtadır (Derici, Tüysüz & Sarı, 2007, s. 157). Örgütlerin belirsizlik dönemlerine ve krizlere karşı dayanıklı hâle gelebilmeleri için risk tanımlama faaliyetlerinin, örgütlerinin stratejilerinin belirlendiği planlama süreçlerine de entegreli olarak yürütülmesi gerekmektedir. Entegre bir KRY, yönetimin belirsizlikleri anlamasına ve yönetilmesine yardımcı olmak için bütüncül bir yaklaşım sağlamaktadır. KRY alanında farkındalığa sahip örgütler yönetişim konusunda iyi örnek uygulamaları vermektedir. KRY, örgütlerde karar alma süreçlerinin bir parçası hâline getirilmediği takdirde anlamsız yeni iş yükü oluşturmaktan öteye geçememektedir (Uysal, 2018, s. 43). Örgütlerin sürekliliğini sağlamaktan sorumlu yöneticiler ve denetçilere uygulamada nasıl yol izleyecekleri hakkında bir pratik rehbere ihtiyaç duymaktadırlar.

Kullanılan yaklaşım ne olursa olsun örgütler, günümüz iş dünyasında riskin dinamik doğasının getirdiği fırsatlara karşılaştıkça, KRY süreçleri sürekli olarak kendilerini geliştirmelidirler. KRY süreçlerini geliştirmeye çalışan organizasyonlar, büyük bir proje hedeflemektense yinelemeli somut adımlar tanımlamalıdırlar. KRY süreçlerini geliştirmek, yönetimin daha iyi kararlar verme ve strateji ile iş hedeflerine ulaşmalarına yardımcı olma rolünün net bir şekilde anlaşılmasıyla başlar. KRY, örgütlerin gerek strateji ve risk ilişkilerini konumlandırmalarına, gerekse strateji ve iş hedeflerine ulaşmalarına yardımcı olmaktadır. Bu iki husus sadece başarı için değil, aynı zamanda örgütlerin risk kültürünün oluşturulması ve yaygınlaşması için de önemlidir. Dolayısıyla KRY uygulamaları, faaliyetlerde karşılaşılacak engelleri önlemek ve sürdürülebilir bir örgütsel yapı sağlamak bakımından, yöneticilerin elindeki en önemli yönetim enstrümanları arasında yer alır.

KRY'nin uygulamaya konulması ve zamanla geçirdiği evrim, araştırmalara da konu olmaya başlar ve akademik bir risk yönetimi literatürünün gelişmesine neden olur. KRY'nin benimsenmesini etkileyen faktörleri inceleyen bir dizi makale yazılmıştır (örneğin, Kleffner, Lee & McGannon, 2003; Liebenberg & Hoyt, 2003). Diğer taraftan KRY'nin benimsenmesinin performans üzerindeki etkilerini ele alan makaleler de ortaya konulmuştur (örneğin, Beasley, Pagach & Warr, 2008; Gordon, Loeb & Tseng, 2009). Yine başka bir makale kümesi de, KRY'nin yıllar içindeki gelişiminin ve çerçevesinin karşılaştırmasını tartışmaktadır (örneğin, Mikes, 2009; Wahlström, 2009; Woods, 2009).

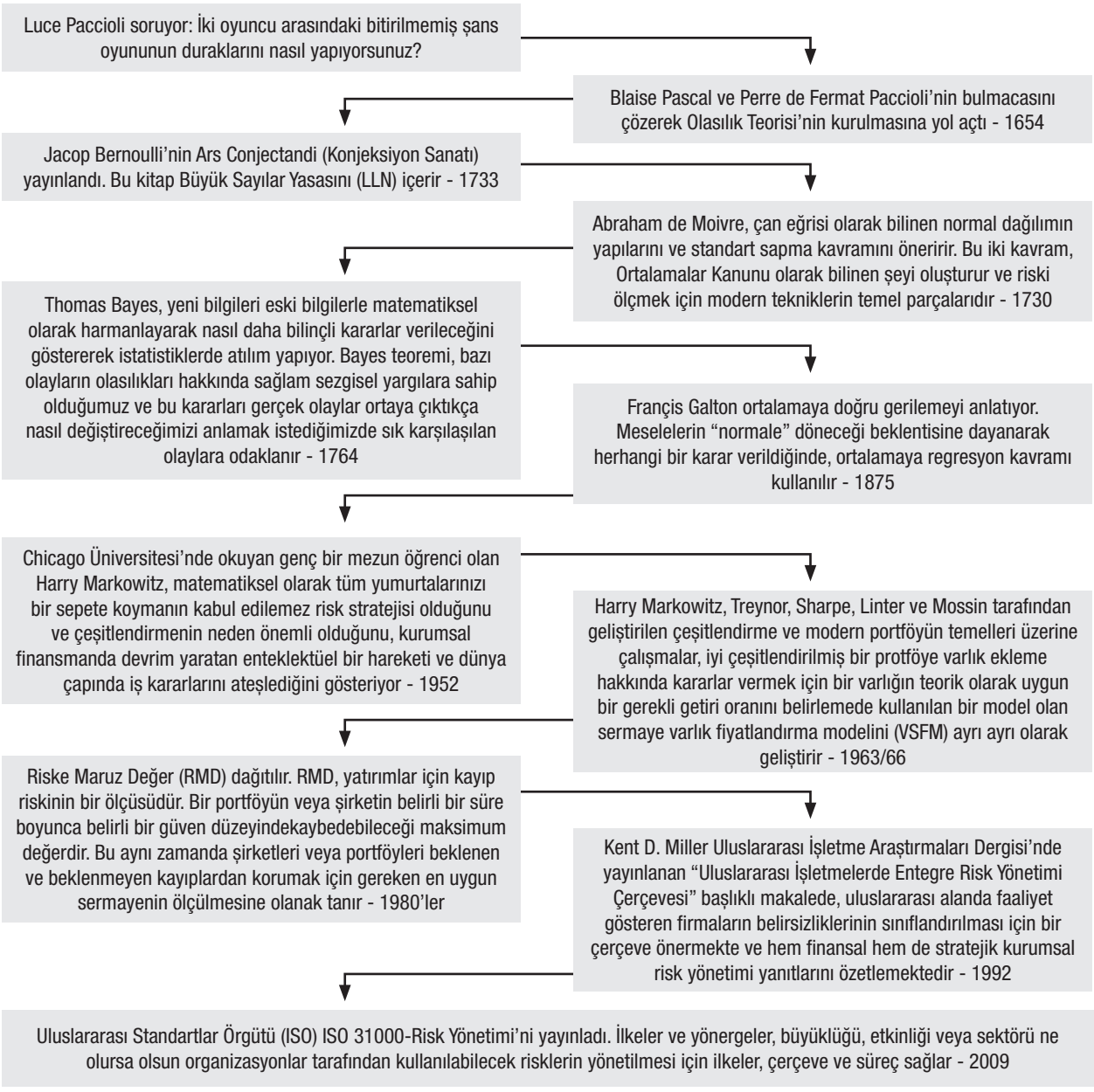
2. KURUMSAL RİSK YÖNETİMİ NEDİR?

Geçmişte risk kavramı günümüzdeki kadar yönetilmemiştir. Aşağıdaki şekil, risk kavramını anlamamıza, risk yönetimi metodolojilerinin geliştirilmesine ve günümüzde riskleri algılama ve tedavi etme şeklimize yol açan önemli kilometre taşlarından bazılarını göstermektedir. Risk yönetimi, 15. yüzyılda İtalyan bir matematikçinin yarattığı matematiksel bir bulmaca ile başlar ve bu incelemenin ana konusu olan ISO 31000'in yayınlanmasıyla bugünkü hâlini alır.

Daha proaktif ve daha entegre risk yönetimi ihtiyacına cevap vermek için KRY ortaya çıkmıştır. Günümüz örgütlerine baktığımız zaman, bu anlayışı benimseyip etkin bir şekilde uygulayanların çok daha başarılı olduklarını uygulamalarda görmekteyiz (Öksüz, 2015, ss. 109-116). KRY alanında, çeşitli düzenlemeler olmakla birlikte tüm dünyada, yaygın olarak kullanılan **iki çerçeve** vardır. Bunlar; **Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi (COSO)** ve **Uluslararası Standardizasyon Örgütü (ISO)** tarafından yayımlanan rehberlerdir.

KRY'nin ana hedefi, risk yönetimi süreci ile var olan yönetim sürecini kaynaştırmak, pozitif veya negatif etkisi olabilecek gelecekteki olayları tanımlamak, örgütlerin bu olaylardan ne kadar etkileneceğini gösteren olaylara maruz kalma oranını belirleyip yönetmek için etkili stratejiler geliştirmektir (Arslan, 2008, s. 7). KRY'nin arkasındaki dayanak, her örgütün paydaşlarına değer katmak için varoluşudur. Bütün örgütler belirsizliklerle karşılaşmaktadır. Bu durumda yönetimin yapması gereken, paydaş değerini artırmaya çalışırken, ne kadar bir belirsizliği karşılayabileceğine karar vermek olmalıdır.

Şekil 1. Risk Yönetiminin Kısa Tarihi



(Lachapelle, Aliu & Emini, 2018)

Sorumluluk olarak yönetimin merkezinde KRY vardır. Her birim KRY ile direk ilişki hâlinde kendi risklerini belirlemektedir ve önlemleri kendisi almaktadır (KİDDER, 2013, s. 6). Dolayısıyla örgütün tamamı KRY'den haberdardır. KRY'nin en büyük itici etkeni yönetime yeni sorumluluklar yüklemesidir.

KRY, strateji ve performansı optimize etmek için mümkün olan en iyi çerçeveye sağlamaktadır. KRY'yi örgüt geneline entegre eden kuruluşlar, fırsat çeşitliliğini artırmak, örgüt çapında risk belirleme ve yönetme, olumsuz sürprizleri azaltırken olumlu sonuçları ve avantajı artırmak, performans değişkenliğini azaltma, kaynak dağıtımını iyileştirme, örgüt esnekliğinin artırılması gibi faydalar elde etmektedirler (Saka & Uğural, 2008, s. 19). Bu faydaların elde edilmesi doğru KRY yapısının tesis edilmesi ve etkin KRY uygulamaları ile mümkündür (Seuamsothabandith, 2004, s. 4).

COSO, hileli finansal raporlamanın önlenmesi, iç kontrol, risk yönetimi, yönetişim ve suiistimali önleme alanlarında kapsamlı rehberler hazırlamak suretiyle fikir önderliği yapmak amacıyla, Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü, Amerikan Muhasebe Birliği, Finansal Yöneticiler Enstitüsü, İç Denetçiler Enstitüsü ve Yönetim Muhasebecileri Enstitüsü sponsorluğunda 1985 yılında kurulmuştur. COSO kurumların hedeflerine ulaşmasına yardımcı olmak doğrultusunda ilk versiyonu 1992 yılında yayımlanmıştır. Zamanla risk tanımlama ve değerlendirme ile ilgili ortak bir süreç ve yaygın olarak kabul gören ilkeler bulunmaması nedenleriyle örgütlere kapsamlı bir rehberliğe ihtiyaç duyulmuştur. Böylece COSO, 2001 yılında Pricewaterhouse Coopers firmasıyla beraber çalışmaya başlayarak iki çerçeve yayınlamıştır (Bulut, 2015, s. 4-6). COSO, strateji belirlemede çok boyutlu bir odak sağlar ve stratejiye yönelik riskin stratejik olarak dikkate alınması gereken tek risk boyutu olmadığını vurgular.

ISO, 162 ulusal standart bağı ile bağımsız, sivil toplum kuruluşudur. Üyeleri aracılığıyla ISO, gönüllülüğü geliştirmek, konsensüs tabanlı innovasyonu destekleyen uluslararası pazar standartları hakkında bilgi paylaşmak ve küresel zorluklara çözüm sağlamak için uzmanları bir araya getirmektedir. ISO 31000, ISO'nun risk yönetimi üzerine teknik komitesi ISO/TC 262 tarafından, risk yönetimi ile ilgili tüm operasyonlara en iyi uygulama yapısını sağlamak amacıyla geliştirilmiştir. Standart, 20'den fazla ülkeden teknik danışmanları içeren bir çalışma grubu tarafından oluşturulmuştur. Birkaç yıl içinde altı toplantıdan oluşan grup, AS/NZS 4360-Risk Yönetimi standardını, herhangi bir ülkedeki karmaşıklık, boyut veya türden bağımsız olarak çalışan çok çeşitli örgütler tarafından kullanılabilecek bir standart oluşturmak üzere revize etmiştir. Standart; riskleri yöneterek, kararlar vererek ve performansı geliştirerek kuruluşlarda değer yaratan insanları hedeflemektedir (Gjerdrum & Peter, 2011, s. 8). Standart, bir dizi ilke, kapsamlı bir risk yönetimi çerçevesi ve bir risk yönetimi sürecini içermektedir. ISO portföyündeki 31000'i destekleyen diğer standartlar, ISO/TR 31004 Teknik Raporunu, ISO 31000 uygulaması için Risk Yönetimi Rehberini ve ISO/IEC 31010 Risk Yönetimi-Risk Değerlendirme Teknikleri Standardını içermektedir (ISO, 2018a, s. 4).

3. ISO VE COSO RİSK YÖNETİMİ ÇERÇEVELERİ

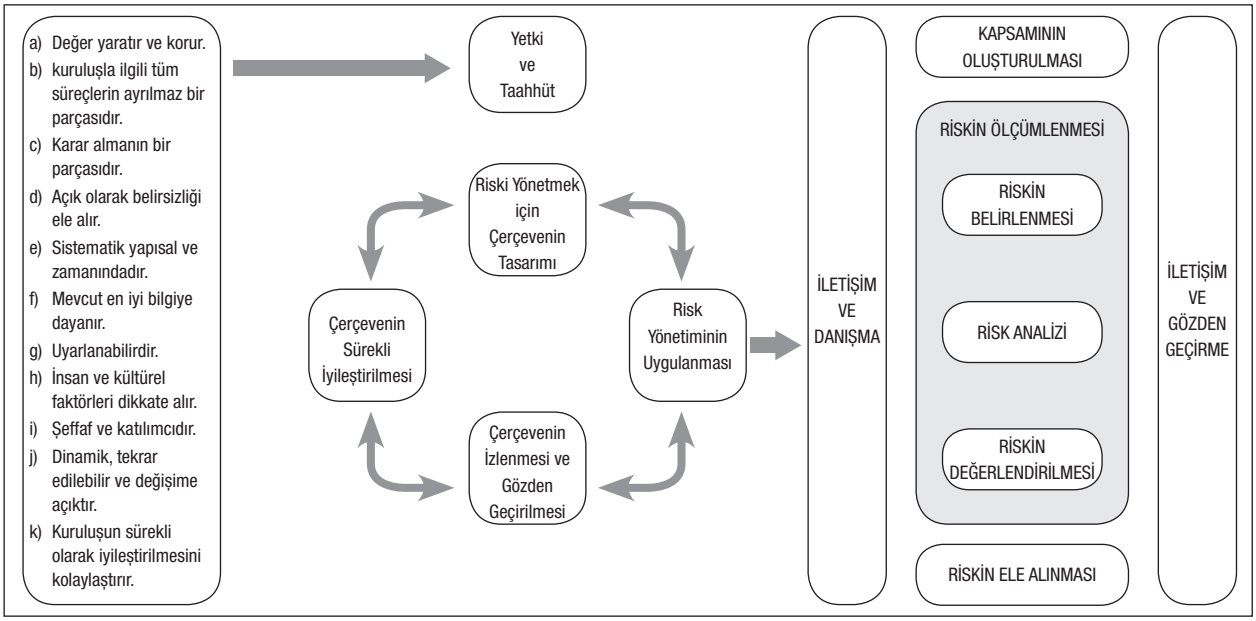
Tüm örgütler katma değer yaratmak için strateji belirlemeli ve dönemsel olarak güncellemelidirler. Bunun için örgütler sürekli değişen fırsatlardan ve zorluklardan daima haberdar olmalıdır. Çerçevelerde, bileşenler sırayla gösterilse de risk yönetiminin tam olarak sıralı bir süreç olmadığı, ancak her bir bileşenin diğerini sırayla bağımsız olarak etkileyebildiği etkileşimli ve çok yönlü bir süreç olduğu unutulmamalıdır.

3.1. Yeni ISO 31000 Risk Yönetimi Güncellemesini Anlamak

Tüm ISO standartları beş yılda bir gözden geçirilmekte ve ardından gerekirse revize edilmektedir. Bu, örgütleri güncel kalmaya ve pazar için yararlı araçlar sunaya yardımcı olmaktadır. Uluslararası örgütler için ekonomik sistemlerin artan karmaşıklığı ve dijital para birimi gibi günümüzün yeni tehditleriyle başa çıkmak için risk yönetimi yetersiz kalmıştır. Bu doğrultuda gözden geçirilmiş ISO 31000 sürümü, standardın ilk 2009 yılında sürüldüğü günden bu yana pazarın gelişimi ve karşılaştığı yeni zorluklar dikkate alınarak ISO 31000-Risk Yönetimi Rehberi adıyla, 15 Şubat 2018 tarihinde iş dünyası ve örgütler için yayınlanmıştır (Tranchard, 2018, s. 2).

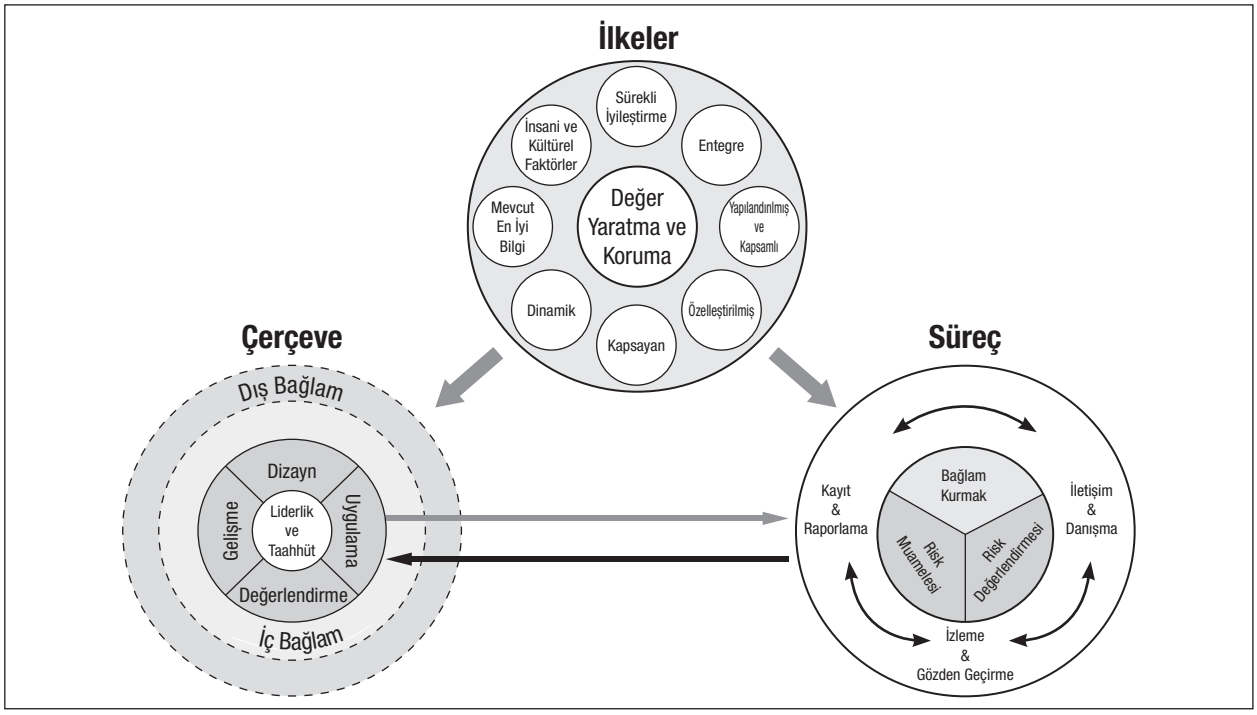
Standardın her bölümü, anlamayı kolaylaştırmak ve tüm paydaşlar tarafından erişilebilir hâle getirmek için daha basit bir dil kullanılarak, açıklık ruhu içinde gözden geçirilmiştir. Standardın yeni versiyonu, örgütlerde değer yaratan ve koruyanların kararlar vermek, hedefler belirlemek ve ulaşmak, performansı artırmak suretiyle riskleri yönetmelerine rehber sunmayı amaçlamaktadır (ISO, 2018b, s. v). Gelecekte riski yönetme şekline yeni bir anlam vererek risk yöneticilerine ISO 31000: 2018, şartlar yerine rehberlik sağlar. Bu, yöneticilere standardı örgütlerinin ihtiyaçlarına ve hedeflerine uygun şekilde uygulama esnekliği sağlamaktadır. 2009 ve 2018 rehberlerinde yer alan kısımların arasındaki ilişki aşağıda gösterilmiştir.

Şekil 2. ISO 31000: 2009 – Risk Yönetimi Prensipleri, Çerçeve ve Süreç Arasındaki İlişkiler



(Karadeniz, 2017, s. 47)

Şekil 3. ISO 31000: 2018 – Risk Yönetimi Prensipleri, Çerçeve ve Süreç Arasındaki İlişkiler



(ISO, 2018b, s. v)

Yukarıdaki şekiller, ISO 31000 standardın 2018 sürümünün bileşenlerini özetlemektedir. Görüldüğü üzere ISO 31000 standardı kuruluşlara, risk yönetme sürecinde, kuruluşun genel yönetişimine, stratejisine, planlamasına, yönetimine, raporlama süreçlerine, politikalarına, değerlerine ve kültürüne entegre bir çerçeve geliştirmelerini, uygulamalarını ve sürekli iyileştirmelerini tavsiye eder.

İtibara ve markaya verilen zararlar, siber suçlar, politik riskler ve terörizm, dünyadaki her tür ve büyüklük-

teki özel ve kamu kuruluşlarının artan sıklıkta karşı karşıya kaldığı risklerden bazılarıdır. Artan risklerle oluşan belirsizliği yönetmeye yardımcı olmak üzere, ISO 31000 standartlar ailesinin en son sürümü ortaya çıkmıştır. Rehberin üç ana kısmı ve bu kısımlarda yapılan temel değişikler şunlardır (CGE, 2018):

- Başarısı için anahtar kriterler olan risk yönetimi ilkelerinin gözden geçirilmesi,
- Risk yönetiminin örgütlerin yönetişiminden başlayarak tüm organizasyonel faaliyetlere entegre edilmesini sağlayacak üst yönetimin liderliğine odaklanma,
- Risk yönetiminin yinelemeli niteliği, yeni deneyimlerden yararlanma, sürecin her aşamasında süreç unsurlarının, eylemlerin ve kontrollerin revizyonu için bilgi ve analiz,
- İçeriğin, dış ortamıyla düzenli olarak geri bildirim alışverişinde bulunan ve birden fazla ihtiyaca ve bağlama uyacak şekilde açık sistem modelini sürdürmeye daha fazla odaklanarak düzene konulması.

Bu değişiklikler, aşağıdaki tabloda da görüldüğü gibi ISO 31000 modelinin de revizyonuna yol açtı. Prensiplerin, etkin ve verimli bir risk yönetiminin, nitelikleri, amaç ve hedefleri hakkında rehberlik sağladığı ifade edilmiştir. Bunların, organizasyonların risk yönetimi çerçevesi ve süreçleri oluşturulurken dikkate alınması gereken esaslar olduğu belirtilmiştir (ISO, 2018b, s. 2). Prensiplerin sayısı, yeni versiyonda 11'den 8'e indirilmiştir. Bununla birlikte, yeni versiyondaki prensiplerin, eski versiyonda yer alan prensiplerin aynısı olduğu, sadece ifade ediliş şeklinde küçük değişiklikler yapıldığı görülmektedir.

Tablo 1. ISO Rehberlerinin Karşılaştırılması

ISO 31000:2009		ISO 31000:2018
Prensipler	Değer oluşturur	Entegre
	Organizasyonel süreçlere entegre	Yapılandırılmış ve geniş kapsamlı
	Karar almanın parçası	Özelleştirilmiş
	Belirsizliği net bir şekilde dikkate alan	Kapsayan
	Sistematik, yapılandırılmış ve zamanlamalı	Dinamik
	Var olan en iyi bilgiye dayanan	Var olan en iyi bilgi
	İhtiyaca ve duruma uygun hale getirilmiş	İnsani ve kültürel faktörler
	İnsani ve kültürel faktörleri hesaba katan	Sürekli iyileştirme
	Şeffaf ve kapsayan	
	Dinamik, yinelenen, değişimlere cevap veren	
	Organizasyonun sürekli iyileşme ve gelişimini kolaylaştıran	
Çerçeve	Emir/yetki ve adanma	Liderlik ve adanma
	Çerçevenin tasarımı	Tasarım
	Risk yönetiminin uygulaması	Uygulama
	Çerçevenin takip ve gözden geçirmesi	Değerlendirme
	Çerçevenin sürekli iyileştirmesi	İyileştirme
		Entegrasyon
Süreç	Bağlamın kurulması	Bağlamın kurulması
	Risk değerlendirmesi	Risk değerlendirmesi
	Risk tedavisi	Risk tedavisi
	İzleme ve Gözden geçirme	İzleme ve Gözden geçirme
	İletişim ve Danışma	İletişim ve Danışma
		Kayıt ve Raporlama

(Burca, 2018'den faydalanarak oluşturulmuştur.)

Çerçeve kısmında, risk yönetiminin, örgütlerin önemli aktivite ve fonksiyonlarının içerisine nasıl entegre edileceği açıklamaktadır. Risk yönetiminin başarısının, bu entegrasyonun başarısına bağlı olduğu ifade edilmiştir. Risk yönetiminin, örgütlerin tüm aktivitelerinin içerisine entegre olabilmesinde, üst yönetimin bu konuyu sahiplenmesi ve desteğinin kritik olduğu vurgulanmaktadır (Anderson & Frigo, 2020, s. 4). 2009 versiyonunda çerçeve kısmında yer alan beş husus, 2018 versiyonunda, entegrasyon da ilave edilerek, altıya çıkarılmıştır.

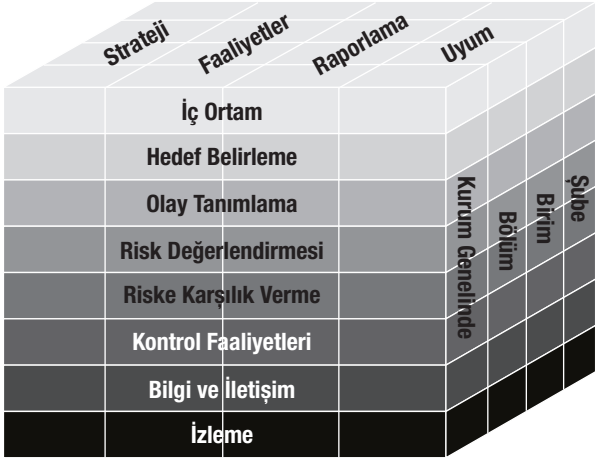
Süreç kısmı, iletişim ve danışma, ortamın oluşturulması, değerlendirme, cevap verme, gözden geçirme, kayıt ve raporlamayı kapsar. Eski ve yeni versiyon arasında içerik olarak önemli bir farklılık görülmemektedir. Yeni versiyonda kayıt ve raporlama sürece ilave edilmiştir. Eski versiyondaki, ortamın oluşturulması yeni versiyonda kapsam, ortam, kriter şeklinde ifade edilmiştir.

ISO 31000'in revize edilmiş versiyonu, organizasyonla entegrasyona, liderlerin rolü ve sorumluluklarına odaklanmaktadır. Risk uygulayıcıları genellikle örgütsel yönetimin sınırlarındadır. Bu vurgu, risk yönetiminin işin ayrılmaz bir parçası olduğunu göstermelerine yardımcı olmaktadır. 2018 sürümü, risk yönetiminin temel itici gücü olarak değer yaratmaya daha fazla odaklanır ve korumaya daha fazla odaklanmakta ve sürekli iyileştirme, paydaşların dâhil edilmesi, organizasyonla özelleştirme, insan ve kültürel faktörlerin düşünülmesi değerlendirilmesi gibi diğer ilgili ilkeleri içermektedir. Yeni versiyon ile risk, olayların veya koşulların eksik bilgisinin bir örgütün karar verme sürecine etkisi üzerine odaklanan "belirsizliğin hedefler üzerindeki etkisi" olarak tanımlanmaktadır (ISO, 2018b, s. 1). Bu tanımla birlikte standardın en önemli faydası, geleneksel risk anlayışında bir değişiklik yapılmasını gerektirmesi ve organizasyonları risk yönetimi ihtiyaçlarına ve hedeflerine göre uyarlamaya zorlamasıdır. ISO 31000, örgütlerin tüm düzeylerinde karar verme de dâhil olmak üzere tüm faaliyetleri destekleyen bir risk yönetimi çerçevesi sağlamaktadır. ISO 31000 çerçevesi ve süreçleri, örgütlerin tüm alanlarında yönetim kontrolünün tutarlılığını ve etkinliğini sağlamak için yönetim sistemleri ile entegre edilmesi gerektiğini belirtmektedir. Bu, strateji ve planlama, örgütsel esneklik, bilişim teknolojileri, yönetişim, insan kaynakları, uyum, kalite, sağlık ve güvenlik, iş sürekliliği, kriz yönetimi ve güvenliğini içermektedir.

3.2. Yeni COSO Kurumsal Risk Yönetimi Çerçevesi Güncellemelerini Anlamak

Zaman içerisinde risklerin tanımlanması, değerlendirilmesi ve yönetilmesine dair bir gereksinim doğurmuştur. Risk yönetiminde yaşanan skandalların zorunlu kılmasıyla da 2004 yılında yayınlanan COSO KRY Entegre Çerçevesi yayınlanmıştır. 2004 çerçevesinde sekiz adet bileşen vardır ve bunların altında prensipler şeklinde bir yapı bulunmamaktadır. Çerçeve aşağıda görüleceği gibi 3 boyutlu bir matrisle gösterilen COSO küpü ile temsil edilmektedir. Matrisin üstünde, faaliyetlerin etkinliği ve etkililiği, bilgilerin güvenirliği ve mevzuata uygunluğu kapsayan hedefler; ön yüzünde iç kontrol bileşenleri; yan yüzeyinde ise, birimler ve yürüttükleri faaliyetleri kapsayan örgütsel yapı bulunmaktadır.

Şekil 4. COSO Küpü



(COSO, 2012, s. 5)

Zamanla risk türleri, risklerin nedenleri, risklere karşılık yapılacak uygulamalar değer üretebilen mekanizmalar olmaktan uzaklaştırmıştır. COSO, KRY Çerçevesini 6 Eylül 2017 tarihinde revize etmiştir. Yenileme ile çerçevenin adı ve yapısı değiştirilmiştir.

Çerçevenin adında, strateji, risk ve performans arasındaki ilişkiye vurgu yapılmıştır. Aşağıda gösterildiği üzere, yeni gösterimde helezon şeklinde bir gösterim yapılmıştır. Yeni çerçevede 5 adet bileşen ve bunlara ilişkin 20 adet prensip belirlenmiştir. Yeni modelin ana simgesi soyut formdadır. Yeni KRY'nin simgesi çeşitli renkli şeritlerin kesişimler arasında konumlandırılmış beş terimi içermektedir. Ana resmin altında, ilgili terimlerle beş mini ikon vardır. Bu terimler ile şeritler arasındaki ilişki ve şeritler içindeki terimler hemen anlaşılmaz bir yapıdadır (Prewett & Terry, 2018, s. 17-19).

Şekil 5. COSO Sarmalı

Yönetişim ve Kültür

1. Yönetim Kurulunun Risk Gözetimini Uygulaması
2. Operasyonel Yapının Oluşturulması
3. İstenen Kültür Yapısının Tanımlanması
4. Temel Değerlere Olan Bağlılığı Gösterme
5. Kabiliyetli Personeli Kazanma, Geliştirme ve Elde Tutma

Strateji & Hedef Oluşturma

6. İş Ortamını Analiz Etme
7. Risk İştahının Tanımlanması
8. Alternatif Stratejileri Değerlendirme
9. İş Hedeflerini Oluşturma

Performans

10. Risklerin Tanımlanması
11. Risk Şiddetlerinin Değerlendirilmesi
12. Risklerin Derecelendirilmesi
13. Risk Yanıtlarının Uygulanması
14. Bütüncül Bir Akış Açısının Geliştirilmesi

Gözden Geçirme & Revizyon

15. Yapısal Değişiklikleri Değerlendirme
16. Risk ve Performansı Gözden Geçirme
17. Kurumsal Risk Yönetimi ile İlgili Gelişmeleri Takip Etme

Bilgi, İletişim ve Raporlama

18. Bilgi Yönetim Sisteminin Güçlendirilmesi
19. Riske İlişkin Bilginin Paylaşılması
20. Risk, Risk Kültürü ve Performans ile İlgili Raporlama

(COSO, 2017, s. 6)

Bu yeni şekilde, KRY'nin bileşenlerinin, örgütlerin misyon, vizyon ve temel değerleriyle ilişkisi gösterilmektedir. Diyagramın üç şeridi örgüt boyunca akan genel süreçleri temsil ettiği, diğer iki şeridin ise KRY'nin destekleyici unsurlarını temsil ettiği ifade edilmiştir (COSO, 2017, s. 5). Yeni gösterime göre, KRY, strateji geliştirme, iş hedeflerinin oluşturulması ve uygulanması ve performansla entegre edildiğinde, bunun örgütlerin değerini artıracağı ifade edilmektedir. KRY'nin statik olmadığı, günlük alınan kararlar vasıtasıyla strateji geliştirme, iş hedeflerinin oluşturulması ve bu hedeflerin uygulanmasına entegre olduğu belirtilmiştir (Anderson & Frigo, 2020, s. 2).

Unsurlar ve bunlara ilişkin prensiplerin belirlenmesi, çerçevenin kullanım kolaylığı ve daha iyi anlaşılması bakımından uygun olmuştur. Küp şeklinde gösterimden vazgeçilmesi COSO iç kontrol küpü ile karıştırılmasını önlemek ve KRY'nin örgütlerin tüm süreçlerine entegre olduğunu göstermek açısından faydalı olmuştur (Kurt & Uçma Uysal, 2018, s. 23).

Güncellenen çerçevede KRY'nin tanımı değiştirilmiştir. 2004 çerçevesinde KRY, "bir örgütlerin yönetim kurulu, yöneticileri ve tüm çalışanlarından etkilenen, stratejinin belirlenmesinde ve kurum genelinde uygulanan, kurumu etkileme potansiyeli olan olayları belirleme ve risk iştahı çerçevesinde riskin yönetilmesi amacıyla dizayn edilen, örgütlerin hedeflerini başarması için makul güvence sağlayan bir süreçtir" şeklinde tanımlanmıştır (COSO, 2004, s. iii). Güncellenen çerçevede ise KRY, "organizasyonun değer

yaratma, koruma ve realize etmede, riski yönetmek için güvenebilecekleri, stratejinin belirlenmesi ve yürütülmesine entegre edilen, kültür, imkan ve uygulamalardır" şeklinde tanımlanmıştır (Anderson & Frigo, 2020, s. 2). Oluşturulan **yeni KRY çerçevesinde KRY'nin statik olmadığı**, tüm seviyelerdeki yönetim ve risk süreçlerine uygulanabileceği belirtilmiştir.

Yeni tanımda risk yönetimin temel amacının değer oluşturmak, korumak ve realize etmek olduğu, stratejinin belirlenmesi ve yürütülmesine entegre edilmesi gerektiği ifade edilmektedir. KRY'nin örgütlerin tüm aktivite ve süreçlerine entegre edilmesinin organizasyonun yönetişim, strateji, hedef belirleme ve günlük operasyonlarına ilişkin karar alma süreçlerini iyileştireceği, performansı artıracağı ve değerin oluşturulması, korunması ve sürdürülmesine katkı sağlayacağı ifade edilmiştir (COSO, 2017, s. 5). KRY'nin bir fonksiyon, bölüm veya risklerin listelenmesinden ibaret olmadığı, yönetimin, riskleri aktif bir şekilde yönetmek için kullandıkları uygulamaları kapsadığı ifade edilmiştir. Sarmal ile tasarlanan bu **bileşenler**, aşağıda aktarıldığı gibidir:

***Yönetişim ve Kültür**:* KRY'nin diğer unsurlarının temelini oluşturur. Yönetişim, tüm aktörlerin yönetime katılmasını ve yönetişimin bir parçası olmasını ifade etmektedir (Okçu, 2011, s. 45). Dolayısıyla yönetişim kavramı, birlikte karar alma ilkesinin kabul edilmesini gerekli kılmaktadır. Kültür ise, etik değerler, istenen davranışlar ve risk anlayışı ile doğrudan ilişkilidir (COSO, 2017, s. 6). Örgüt kültürü, kurumda çalışan tüm bireyleri içermektedir. Örgüt içerisinde yerleşik davranışlar tümünü kapsayan kültür, 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.

- *Yönetim Kurulunun risk gözetimini uygulaması.* Yönetim Kurulu, yönetimin strateji ve iş hedeflerini gerçekleştirmesini desteklemek amacıyla, stratejinin gözetimi ve yönetişim sorumluluklarını yerine getirir.
- *Operasyonel yapının oluşturulması.* Örgütler, strateji ve iş hedeflerini gerçekleştirmek amacıyla operasyonel yapıyı oluşturur.
- *İstenen kültür yapısının tanımlanması.* Organizasyon, örgütlerin kültürünü karakterize eden, arzu edilen davranışları tanımlar.
- *Temel değerlere olan bağlılığı gösterme.* Organizasyon, örgütün temel değerlerine bağlılığını gösterir.
- *Kabiliyetli personeli kazanma, geliştirme ve elde tutma.* Organizasyon, strateji ve iş hedefleri ile uyumlu olarak beşeri sermayesini inşa etmeye büyük önem verir.

***Strateji ve Hedef Oluşturma**:* KRY, strateji ve hedeflerin oluşturulması, strateji planlama süreçlerinin temel noktalarıdır ve bu unsurlar birlikte hareket etmektedirler. Bu düzenlemeyle iş ortamı ile stratejilerin belirlenmesi arasındaki temel ilişki irdelenmiştir. Bileşenin alt bileşenleri şu şekildedir:

- *İş ortamını analiz etme.* Organizasyon, bulunduğu iş ortamının, risk profili üzerine potansiyel etkilerini analiz eder.
- *Risk iştahının tanımlanması.* Organizasyon, risk iştahını, değer oluşturma, koruma ve realize etme bağlamında tanımlar.
- *Alternatif stratejileri değerlendirme.* Organizasyon, alternatif stratejilerin risk profili üzerine etkilerini değerlendirir.
- *İş hedeflerini oluşturma.* Organizasyon, iş hedeflerini oluştururken, stratejiyle uyumlu ve onu destekleyecek şekilde, çeşitli seviyelerdeki riskleri dikkate alır.

Performans: Örgütlerin hedefleri ile doğrudan ilgili olan riskler, tanımlanmak ve değerlendirilmek zorundadır. Bu nedenle riskler, risk iştahı haritası kapsamında şiddetleri ve dereceleri bakımından sınıflandırılmalıdır. Bileşenin 5 alt bileşeni bulunmaktadır.

- *Risklerin tanımlanması.* Örgütler strateji ve iş hedeflerinin yerine getirilmesini etkileyen riskleri belirler.
- *Risklerin şiddetlerinin değerlendirilmesi.* Örgütler risklerin şiddetini değerlendirir.
- *Risklerin derecelendirilmesi.* Örgütler risklere vereceği cevaba esas oluşturmak üzere, riskleri derecelendirir.

- *Risk yanıtlarının uygulanması*. Örgütler risklere vereceği cevapları belirler ve seçer.
- *Bütüncül bir bakış açısının geliştirilmesi*. Örgütler risklere ilişkin bütüncül bakış açısı geliştirir ve değerlendirir.

***Gözden Geçirme ve Revizyon**:* Örgütler ilgili birimlerin performanslarını gözden geçirme suretiyle KRY'nin temel bileşenlerinin işleyişlerini ve değer oluşturma sürecine yapacakları katkıları revize edebileceklerdir. Bu yolla doğabilecek yapısal değişimlere uyum konusunda ihtiyaç duyulacak güncellemeler belirlenebilecektir. Bu ana bileşen aşağıdaki alt bileşenden oluşmaktadır:

- *Yapısal değişiklikleri değerlendirme*. Örgütler starateji ve iş hedeflerini önemli şekilde etkileyen değişiklikleri belirler ve değerlendirir.
- *Risk ve performansı gözden geçirme*. Organizasyon örgütün performans sonuçlarını gözden geçirir ve riskleri ele alır.
- *KRY ile ilgili gelişmeleri takip etme*. Örgütler KRY'de gelişmeleri takip eder.

Bilgi, İletişim ve Raporlama: İletişim, "bilgilerin akla gelebilecek her türlü yolla başkalarına aktarılması, bildirişim, haberleşme, komünikasyon" anlamına gelmektedir (Parlatır, Gözaydın, & Zülfikar, 1998, s. 1067). Örgütlerde katma değer oluşturma süreçlerinde kullanılacak bilgilerin elde edilmesi, iletilmesi, paylaşılması ve raporlanması için, KRY yapısı oluşturulmalıdır. Söz konusu bilgiler iç ve dış kaynaklı olabilmektedir. Elde edilen bilgiler, kurum genelinde ilgili tüm birimlere de iletilmelidir. Ana bileşen 3 alt bileşenden oluşmaktadır:

- *Bilgi yönetim sisteminin güçlendirilmesi*. Örgütler KRY'yi desteklemek için, bilgi ve teknoloji sistemi avantajlarından yararlanır.
- *Riskle ilgili bilginin paylaşılması*. Örgütler KRY'yi desteklemek için iletişim kanallarını kullanır.
- *Risk, risk kültürü ve performans ile ilgili raporlama*. Örgütler teşkilat içi çeşitli düzeylerde risk, kültür ve performans hakkında raporlama yapar.

COSO, yeni KRY çerçevesinde kontrol faaliyetleri bileşenlerini belirtilmemiş, ancak bunlar hakkında COSO İç Kontrol Entegre Çerçevesinin birlikte kullanılmasını önermiştir (COSO, 2012, s. 160). Ayrıca, çerçevenin, sektör, büyüklük, coğrafyaya bağlı olmaksızın, tüm örgütler için uygulanabileceği belirtilmiştir (COSO, 2012, s. 1). Yenilenen çerçeve, örgütlerin gözetim, yönetim ve denetiminde bulunan tüm taraflar için, risk yönetimi uygulamalarının gözden geçirilmesi açısından önem arz etmektedir.

KRY faaliyetlerini uygulamak veya geliştirmek isteyen örgütler, KRY çalışmalarına başlamadan önce güçlü bir kavramsal temel oluşturmalıdırlar. Başarılı bir KRY faaliyeti için bazı unsurlar bulunmalıdır. Bu unsurlar KRY faaliyetlerini uygulayan veya geliştiren örgütler için başarının anahtarlarıdır. Bu başarının anahtarları, KRY faaliyetleri uygularken karşılaşılacak engelleri önlemek için yöneticilere yardımcı olmaktadır. Bu anahtarlar COSO tarafından 2020 Şubat bülteninde aşağıda değinildiği gibidir (Anderson & Frigo, 2020, s. 6):

- Yönetim Kurulu ve üst yönetimin desteğinin alınması,
- KRY'nin rolü ve amacının anlaşılması ve yerleştirilmesi,
- KRY'nin örgütlerinin kültürüne ve değerlerine entegre edilmesi,
- Başlangıç olarak örgütün temel strateji ve faaliyet hedeflerine odaklanmak,
- Ana stratejilerle ilgili olay ve sonuçlar kilit risklerdir,
- Basit eylemlerle başlanılması ve aşamalı olarak oluşturulması,
- Mevcut kaynaklardan ve risk yönetim faaliyetlerinden yararlanma.

COSO risk iştahı konusunda örgütlerin karar vermede kilit bir faktör olarak risk iştahını nasıl teşvik edebileceğine odaklanan **yeni bir bülten** yayınlamıştır. Bülten, risk iştahı hakkında hatırlanması gereken altı temel hususu içermektedir (Tysiac, 2020):

- *Risk iştahı ayrı bir çerçeve değildir.* Tek başına bir faaliyet değildir, ancak riskin yönetilmesinin yanı sıra örgütsel eylem ve iletişimin ayrılmaz bir parçası olmalıdır.

- *Risk iştahı ve risk toleransı farklıdır.* Bununla ilgili olsalar da, bunlar farklı fikirlerdir.
- *Risk iştahı, finansal hizmetler endüstrisinden daha fazlası için geçerlidir.* Tüm örgütlerin performansı daha etkili bir şekilde anlamalarına ve yönetmelerine yardımcı olabilir.
- *Risk iştahı karar vermenin merkezinde yer alır.* Ayrıca bir kararın bile gerekli olduğunu belirlemede önemlidir.
- *Risk iştahı bir metrikten çok daha fazlasıdır.* Her metriğe hedef iştah atanan bir yaklaşımın parçası olarak ele alınsa da daha iyi, ileriye dönük bir uygulama gelecekteki eylem için iştah ve stratejiyi birbirine bağlar.
- *Risk iştahı şeffaflığı artırmaya yardımcı olur.* Örgütlerin üstlenmek istediği risklerin yanı sıra sınırlamayı amaçladığı riskler konusunda farkındalık yaratabilir.

Yeni bültende "örgütlerin başarılı olma riski olduğu" belirtilmektedir. Ancak risk kontrol edilememektedir. Risk iştahını belirlemek ve anlamak örgütsel yönetim, stratejik planlama ve karar almanın önemli bir unsurudur. Bir performans merceğiyle iştahı belirlemek, yönetimini etkileyen ve etkili olması için bir örgütün kültürüne nüfuz eden derin tartışmalar gerektirir. Bu şekilde iştah, misyonu ve vizyonu yansıtır ve strateji ve hedeflerle değer katma hedefiyle bütünleşmektedir.

3.3. Çerçevelerin Karşılaştırılması

ISO 31000: 2018'i geliştirme süreci, 70'den fazla ülkeden üyelerin 5000'in üzerinde yorumuyla gerçekleştirilmiştir. COSO ise geliştirilirken 2017 güncellemesine katkıda bulunanların neredeyse tamamı Washington, D.C. ve New York City'de bulunmaktadır (Williams, 2019). Düzenleyici risk yönetimi, Avustralya'da uygulanmaktadır ve Birleşik Krallık, düzenleyici risk yönetimini yükseköğretim gözetim sürecinin temel bileşeni olarak kullanmaktadır. ABD'de KRY uygulaması, 2002 Sarbanes-Oxley Yasasını ilemeye dayalı olarak daha dolaylı ve isteğe bağlıdır (Padro, 2015, s. 1). Bununla birlikte, hem ISO 3100 kılavuzu hem de AS/NZS 4360 standardı, kuruluşlar arasında risk yönetiminin tekdüzeliğini teşvik etme niyetinde olmadıklarını açıkça belirtmektedir. Kanada'da ise kamu sektörüne hitap eden Risk Yönetimi Çerçevesi, kamu idaresinin organları ve belirli yönetim özelliklerine ilişkin bir dizi ilke ve kontrol listesi sağlamaktadır.

Tablo 2. Temel KRY Çerçevelerinin Karşılaştırılması

Çerçeveler	Amaç ve Kapsam	Risk Yönetim Süreci
COSO KRY 2017	2004 yayınına yönelik bu güncelleme, kurumsal risk yönetiminin gelişimini ve organizasyonların gelişen iş ortamının taleplerini karşılamak için risk yönetimi yaklaşımlarını geliştirme ihtiyacını ele almaktadır. Yönetim ve paydaş güvenini artırmak için herhangi bir organizasyonda kurumsal risk yönetimini uygulamaya yönelik özlü bir çerçevedir. Güncellenen belge, hem strateji belirleme sürecinde hem de uygulama performansında riski göz önünde bulundurmanın önemini vurgulamaktadır.	1) Yönetişim ve Kültür 2) Strateji ve Hedef Belirleme 3) Performans 4) İnceleme ve Revizyon 5) Bilgi, İletişim ve Raporlama
ISO 31000: 2018	Bu uluslararası standart, kuruluşların, riski yönetme sürecini kuruluşun genel yönetişimine, stratejisine ve planlamasına, yönetimine, raporlama süreçlerine, politikalarına, değerlerine ve kültürüne entegre etmek olan bir çerçeve geliştirmelerini, uygulamalarını ve sürekli iyileştirmelerini tavsiye eder. Risk yönetimi, herhangi bir zamanda birçok alanda ve düzeyde tüm bir kuruluşa ve ayrıca belirli işlevlere, projelere ve faaliyetlere uygulanabilir. Bu standart, sistematik, şeffaf ve güvenilir bir şekilde ve herhangi bir kapsam ve bağlamda her türlü riskin yönetilmesine yönelik ilkeleri ve yönergeleri sağlar. Standart, kuruluşlar arasında risk yönetiminin tekdüzeliğini teşvik etmeyi amaçlamaz.	1) Bağlamın kurulması 2) Risk değerlendirmesi 3) Risk tedavisi 4) İzleme ve Gözden geçirme 5) İletişim ve Danışma 6) Kayıt ve Raporlama

(Rubino, 2018, s. 205-207 faydalanarak oluşturulmuştur.)

Bu çerçeveler, dünya çapında uygulanan diğer daha küçük çerçevelere kıyasla daha yapılandırılmıştır. Analiz edilen iki çerçevede de risk, tehdit ve fırsatlar açısından tanımlanır. Tablo 2'de gösterildiği gibi, amaç ve kapsam açısından, çerçeveler güçlü bir benzerlik göstermektedir. Çerçeveler, risk yönetimi faaliyetlerinin etkili ve verimli bir şekilde uygulanmasını ve geliştirilmesini teşvik eden ve kolaylaştıran yönergeler ve genel ilkeler sağlar. Bu yönergeler, yalnızca bireysel projelere değil, kamu veya özel kuruluşların tüm faaliyetlerine uygulanabilen çok çeşitli kuruluşlar için geçerlidir. Tabloda belirtildiği gibi risk yönetimi sürecindeki farklılıklar, temelde terminolojinin kullanımındaki değişikliklere veya bazı faaliyetlerin açık veya örtük tahminine bağlıdır. Risk yönetimi çerçevelerinin yönetim kontrol araçlarından büyük ölçüde kopuk göründüğü anlaşılmaktadır. Yönergeler genellikle, kurumsal kontrolün klasik araçlarına alternatif olarak düşünülemeyecek bir metodolojiyi yansıtır. Çerçeveler, çeşitli düzeylerde kurumsal kontrol araçlarına değinmelidir ancak bunların kurumsal kontrol vizyonundan kopuk olduğu görünmektedir. Ek olarak, tüm risk çerçeveleri bilgi ve iletişim bileşenini içerir ancak bilgi sistemleri ile entegrasyon prosedürleri sağlamaz.

3.4. Örgütsel Etki

Bir örgütün bu revizyonlara dayanarak değişiklik yapması gerekecek düzey, mevcut risk yönetimi uygulamalarının mevcut entegrasyon seviyesine ve olgunluğuna bağlıdır. Risk süreçlerini ve tekniklerini karar verme ve strateji belirlemeye dâhil eden örgütleri için çok az değişiklik gerekebilmektedir. Ancak, paydaşlar KRY'nin örgütlerin misyonunu ilerletmek için çevresel olarak bağlantılı başka bir faaliyet olduğuna inanırlarsa, riski yönetme amacını ve yaklaşımını değiştirerek daha güçlü ve daha yetenekli bir organizasyon oluşturma fırsatı olabilir. Bu revizyonlar aşağıdakilerle ilgili bir sorgulama başlatmak için kullanılabilir (Fox, 2018, s. 4):

- *Güncel uygulamalar*. Risk yönetimini temel bir yetkinlik mi yoksa periyodik bir egzersiz olarak mı değerlendiriliyor?
- *Paydaş değerlendirmeleri*. Riski yönetmekten sorumlu olanlar yapılmakta olanın değer kattığına inanıyor mu?
- *GAP analizi*. Revize edilen belgelerin hangi yönleri örgüt içindeki risk yönetimi yeteneklerini geliştirmek için kullanılabilir?

Bu rehber, belgelerde aktarılan risk yönetiminin gelişimi, risk yönetiminin nasıl görüldüğü ve entegre edileceği konusunda mevcut değişikliği değiştirebilir. Risk uzmanları ve örgütleri, değişiklikleri stratejik hedeflere daha etkin bir şekilde ulaştırmayı örgütlerini güçlendirmek için bir fırsat olarak görmelidir.

4. SONUÇ ve DEĞERLENDİRME

Risk yönetiminin uygulanması, kontrol, örgüt kültürü, iyi tanımlanmış bir organizasyon yapısının varlığı, uygun prosedürlerin sağlanması ve şirket politikaları, varlığı açısından bir dizi unsura dayanarak örgütten örgüte değişen karmaşık bir faaliyettir (Agarwal & Kallapur, 2018, s. 329). Bu nedenle, tüm bu unsurların ve diğerlerinin analizi, özellikle ana KRY çerçeveleri gibi çok küçük veya sınırlıysa, basit bir kılavuzda yer alamaz. Gözlemlendiği gibi, en iyi ve yaygın olarak kullanılan kılavuz, diğerleri gibi bazı sınırlamalar getiren COSO KRY'dir. Risk yönetimi faaliyetlerinin etkili şekilde uygulanması, COSO KRY veya ISO 31000 kılavuzları gibi güvenilir bir standart dikkate alınarak gerçekleştirilebilir. Standartların derinlik seviyesi incelendiğinde, 254 sayfalık COSO KRY'nin ilkeler ve odak noktaları ile ilgili daha fazla ayrıntılı olduğu söylenebilir.

Birkaç temel tanımın karşılaştırılması, ISO 31000 ve COSO KRY Çerçevesi arasındaki temel farkları gösterecektir. COSO KRY Çerçevesi, birçok örgütün uygulanması zor bulduğu karmaşık ve çok katmanlı bir rehberdir. ISO, özümsenmesi daha kolay ve daha akıcı bir yaklaşım sunmaktadır. ISO bir yönetim sürecine dayanmaktadır ve her örgüt için risk süreci uyarlayarak mevcut yönetime ve stratejik sisteme entegre olmaktadır. COSO modeli kontrol ve uyumluluğa dayanır. Bu, geleneksel risk yöneticileri tarafından uygulanması zordur. COSO bir örgütün iç denetim ekibi tarafından uygulanırsa, programın uygulayıcı-

larla aynı insanlar tarafından denetlenmesi sorunu bulunmaktadır. ISO ise bağımsız denetim fonksiyonunun izleme ve inceleme aşamasında yer almasına imkan vermektedir. COSO denetçiler, muhasebeciler ve finansal uzmanlar tarafından yazılmıştır; ISO ise risk yönetimi uygulayıcıları ve uluslararası standart uzmanlarınca yazılmıştır.

Çerçeveler arasında risk yönetim süreçlerinin ilk aşaması açısından büyük farklılık vardır. COSO yönetişim, stratejinin incelenmesi, uygulanması ve ilgili risklere vurgu yaparken, ISO 31000 içinde bulunması gereken tüm öğeleri içermeyen bağlamın oluşturulmasını tanımlamaktadır. Örneğin, yönetişim unsurlarının etik değerlerine, yönetim tarzına, davranış kurallarına, insan kaynağının becerileri ve yetki ve sorumluluk alanlarının tanımlanmasına ISO'da atıf yapılmamaktadır. Bununla birlikte, COSO, ISO standardına kıyasla dış bağlamın analizine daha fazla alan ayırmaktadır.

ISO ve COSO'nun birlikte incelenmesi, KRY uygulayıcıları ve denetçiler için faaliyetleri bütünleştirmek ve güçlendirme yönünden fırsat sunmaktadır. Kuruluşların COSO ile ilgili görüş ve başarısına bağlı olarak, örgüt genelinde büyümeyi ve karlılığı hızlandırmak için daha etkili bir yol tasarlamada ISO'nun değerlendirilmesi farklı bir yaklaşım sağlayabilir.

Yapılan düzenlemelerde, risk değerlendirmesi konusunda genellikle COSO sistemine atıfta bulunulmaktadır. KRY ve iç kontrol konularındaki düzenlemelerde açık ve uygulama zorunluluğu getiren hükümler bulunmamaktadır. Dolayısıyla KRY farkındalığının oluşturulmasında ISO 31000–Risk Yönetimi gibi çerçevelerden faydalanılabilir. Nihayetinde ISO 31000 standardı, risk yönetimini bir örgütün başarısı için merkezi bir hâle getirecek bir araç ve planlama, yönetim ve yönetişim gibi önemli süreçlerin samimi bir parçasını sunmaktadır.

İki standart arasında tezatlık yerine daha fazla ortak nokta olduğu düşünülmektedir. Zayıflıkları tanındığı sürece COSO tamamen uygulanırsa, ISO'ya geçmeyi düşünmeye gerek olmayabilir. Öte yandan, eğer COSO'dan kullanışlı ve verimli bir uygulama elde edilemezse herhangi bir geçiş süreci kaybetmeden ISO'ya geçilebilir ve örgütler muhtemelen basitleştirip güçlenebilir.

Bununla birlikte, sadece ISO 31000'in uygulanması kötü iş kararlarını ve hatta başka bir küresel mali çöküşü engellemeyecektir. Yönetişim sorunlarının çözümünde tek yönlü bir model yerine belirtilen değerleri dengeleyen bir yaklaşımla hareket edilmesi doğru olacaktır. Ancak ISO 31000, örgütlere var olma nedenlerini anlama ve geleceklerindeki belirsizliği azaltmak için gerekli tedavileri tanımlama fırsatı sunmaya devam edecektir.

Kaynakça

Agarwal, R. & Kallapur, S. (2018). Cognitive risk culture and advanced roles of actors in risk Governance: a Case study. *The Journal of Risk Finance, 19*(4), 327-342.

Anderson, R. J. & Frigo, M. L. (2020). *Creating and Protecting Value: Understanding and Implementing enterprise risk management.* Lake Mary: COSO.

Arslan, I. (2008). *Kurumsal risk yönetimi* (Uzmanlık tezi). Ankara: Maliye Bakanlığı Strateji Geliştirme Başkanlığı.

Beasley, M., Pagach, D. & Warr, R. (2008). Information conveyed in hiring announcements of senior executives overseeing enterprise-Wide risk management processes. *Journal of Accounting, Auditing & Finance,* (23), 311-332.

Bulut, E. (2015). *COSO 2013 "Bataklığı kurutmak mı? Sinekleri öldürmek mi?* İstanbul: TİDE.

Burca, N. (2018, Şubat 27). *Yenilenen ISO 31000 Risk Yönetimi Rehberi.* Nazif Burca: https://nazifburca.com/2018/02/27/yenilenen-iso-31000-risk-yonetimi-rehberi/ adresinden alındı. (Erişim Tarihi, 15 Aralık 2020).

CGE. (2018, Temmuz). *Main changes in revised ISO 31000 Standard – Keep risk management simple.* CGE Risk Management Solutions: https://www.cgerisk.com/2018/07/main-changes-in-revised-iso-31000-standard-keep-risk-management-simple/ adresinden alındı. (Erişim Tarihi, 15 Haziran 2020).

COSO. (2004). *Enterprise Risk Management Framework.* Lake Mary: PwC.

COSO. (2012). *Internal control—Integrated Framework: Framework and appendices.* PwC.

COSO. (2017). *Enterprise risk management ıntegrating with strategy and performance executive summary.* Lake Mary: PwC.

Derici, O., Tüysüz, Z. & Sarı, A. (2007). Kurumsal risk yönetimi ve sayıştay uygulaması. *Sayıştay Dergisi,* (65), 151-172.

Fox, C. (2018). Understanding the New ISO and COSO Updates. *Risk Management, 65*(6), 1-5.

Gjerdrum, D. & Peter, M. (2011). The new ınternational standard on the practice of risk management – A Comparison of ISO 31000:2009 and the COSO ERM Framework. *Risk Management,* (21), 8-12.

Gordon, L. A., Loeb, M. P. & Tseng, C. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy,* (28), 301-327.

ISO. (2018a). *ISO 31000 Risk Management.* Cenova: ISO.

ISO. (2018b). *31000: Risk Management - Guidelines.* Cenova: BSI Standards Publication.

Karadeniz, I. (2017, Nisan 17). *Risk tabanlı proses yönetimi eğitimi TS EN ISO 9001: 2015.* TSE: https://slideplayer.biz.tr/slide/15159610/ adresinden alındı. (Erişim Tarihi, 11 Haziran 2020).

KİDDER. (2013). Kurumsal risk yönetiminin doğuşu. *Kurumsal risk yönetimi (ERM)*. İstanbul: Kamu İç Denetçileri Derneği.

Kleffner, A. E., Lee, R. B. & McGannon, B. (2003). The effect of corporate governance on the use of enterprise risk management: evidence from Canada. *Risk Management and Insurance Review,* (6), 53-73.

Kurt, G. & Uçma Uysal, T. (2018). COSO Kurumsal risk yönetimi çerçevesi güncelleme projesinin getirdiği yenilikler. *Muhasebe ve Denetime Bakış,* (54), 19-34.

Lachapelle, E., Aliu, F. & Emini, E (2018, Şubat 20). *ISO 31000:2018-Rısk Management Guıdelınes.* PECB: https://pecb.com/whitepaper/iso-310002018-risk-management-guidelines adresinden alındı. Erişim Tarihi, 16 Haziran 2020).

Liebenberg, A. P. & Hoyt, R. E. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk Management and Insurance Review,* (6), 37-52.

Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research,* (20), 18-40.

Okçu, M. (2011). *Değişen dünyayı anlamak için önemli bir kavram: Yönetişim.* Ankara: Ankara Sanayi Odası Yayını.

Öksüz, F. (2015). *Kamu İdarelerinde daha etkili bir yönetim için nasıl bir iç denetim.* R. Doğanay, & M. A. Meydanlı içinde (ss. 109-116). Ankara: TBMM Basımevi.

Padro, F. F. (2015). Which ıs better for embedding risk management ın higher education quality assurance: ISO 31000 or the COSO Framework? *Proceedings of the 18th QMOD-ICQSS International Conference on Quality and Service Sciences*, 1-39. Seoul.

Parlatır, İ., Gözaydın, N. & Zülfikar, H. (1998). *Türkçe Sözlük* (Cilt 1). Ankara: Türk Dil Kurumu.

Prewett, K. & Terry, A. (2018). COSO's Updated enterprise risk management framework—A Quest for depth and clarity. *Journal of Corporate Accounting & Finance, 3*(29), 16-23.

Rubino, M. (2018). A Comparison of the main ERM Frameworks: How limitations and weaknesses can be overcome ımplementing IT governance. *International Journal of Business and Management, 13*(12), 203-214.

Saka, T. & Uğural, A. (2008). Kurumsal risk yönetimi. TÜSİAD (Dü.), *Kurumsal risk yönetimi ve 2008 yılı risk öngörüleri* içinde (ss. 1-44). İstanbul.

Seuamsothabandith, S. (2004). *An Examination on enterprise risk management.* Macomb: Western Illinois University Press.

Tranchard, S. (2018). *The new ISO 31000 keeps risk management simple.* Cenova: ISO.

Tysiac, K. (2020, Mayıs 26). *COSO provides new guidance on risk appetite*. Journal of Accountancy: https://www.journalofaccountancy.com/news/2020/may/new-coso-guidance-risk-appetite.html adresinden alındı. (Erişim Tarihi, 16 Haziran 2020).

Uysal, M. C. (2018). Kamu kurumlarında kurumsal risk yönetimi ve risk odaklı iç denetim: İç denetçiler üzerine bir araştırma-II. *Denetişim Dergisi,* (18), 35-44.

Wahlström, G. (2009). Risk management versus operational action: Basel II in a Swedish context. *Management Accounting Research,* (20), 53-68.

Williams, C. (2019, Nisan 8). *ISO 31000 vs. COSO - Comparings and constrasting the World's leading risk management standarts*. ERM Insights: https://www.erminsightsbycarol.com/iso-31000-vs-coso/ adresinden alındı. (Erişim Tarihi, 17 Aralık 2020).

Woods, M. (2009). A contingency perspective on the risk management control system within Birmingham City Council. *Management Accounting Research,* (20), 69-81.