COSO 2017 KURUMSAL RİSK YÖNETİMİ ÇERÇEVESİNE KONTROL ÖZ DEĞERLENDİRME YAKLAŞIMIYLA BAKIŞ VE BİR KURUM UYGULAMASI-I

(OVERVIEW THROUGH CONTROL SELF-ASSESSMENT APPROACH TO COSO 2017 ENTERPRISE RISK MANAGEMENT FRAMEWORK AND APPLICATION OF AN ORGANIZATION-I)

Alptuğ GÜLER* / Ali Kasım ARKIN**

ÖZ

Dünyadaki sosyal ve teknik değişim hiç olmadığı kadar ivme kazanmış durumdadır. Bu değişime bağlı olarak da belirsizlikler ve riskler hem nicelik, hem de nitelik olarak artmakta, kurumları ve çalışanları kontrol edilemez bir yöne taşımaktadır. Kurumlar, riskleri kontrol edebildiği sürece sürdürülebilirliklerini sağlayabilmektedir. Kontrol Öz Değerlendirme sürdürülebilirlik ve risklere karşı öngörülebilecek kontrol araçlarını geliştirmek için etkin bir bakış açısı sağlamakta ve Kurumsal Risk Yönetimi için sağlam bir zemin oluşturma potansiyeli taşımaktadır. COSO (The Committee of Sponsoring Organizations of the Treadway Commission) 2017 yılında mevcut çerçevesini güncelleyerek Kurumsal Risk Yönetiminin kurumun tüm süreçlerine entegre edilmesinin önemini vurgulamıştır. Bu entegrasyon; örgütün yönetişim, strateji, hedef belirleme ve günlük operasyonlarına ilişkin karar alma süreçlerini iyileştirecek, performansı artıracak ve örgütsel sürdürülebilirliğe katkı sağlayacaktır. Yenilenen COSO çerçevesinin kurum bünyesinde içsellik kazanması için örgütlerin yapması gereken ilk adım, belirsizliklerini ve risklerini tespit etmesidir. Bunun en etkin yolu örgüt bünyesinde bir risk çalıştayı yapıp, çalıştay sonuçlarını Kurumsal Risk Yönetimi için yol haritası yapmaktan geçmektedir.

Bu makalede, Kontrol Öz Değerlendirme yöntemleri ile yenilenen COSO Kurumsal Risk Yönetim Çerçevesi açıklanmış ve Düzce Üniversitesi Risk Evreninin Belirlenmesi Çalıştayı örneğiyle kuruma sağlayacağı katkılar değerlendirilmiştir. Bir vaka analizi olarak Çalıştay, Kontrol Öz Değerlendirmenin kurum genelinde risk-kontrol ve hedef için bir farkındalık oluşturma kapasitesini göstermektedir.

Anahtar Kelimeler: Kurumsal Risk Yönetimi, Risk Çalıştayı, Kontrol Öz Değerlendirme, COSO KRY 2017 Çerçevesi

JEL Kodlaması: G32, L21, M12, M42

ABSTRACT

Social and technical change in the world has gained more momentum than ever before. Due to this change, uncertainties and risks increase in both quantity and quality and carry the institutions and employees to an uncontrollable direction. Institutions can ensure their sustainability as long as they can control the risks. Control Self-Assessment provides an effective perspective for developing control tools that can be predicted for sustainability and risks, and has the potential to be a solid ground for enterprise risk management. In 2017, COSO (The Committee of Sponsoring Organizations of the Treadway Commission) updated its existing framework and emphasized the importance of integrating enterprise risk management into all processes of the organization. This integration will improve the decision-making processes of the organization's governance, strategy, goal setting and daily operations, improve performance and contribute to organizational sustainability. The first step that organizations need to make for the internalization of the renewed COSO framework within the organization is to identify the uncertainties and risks. The most effective way to do this is to carry out a risk workshop within the organization and make the results of the workshop a roadmap for enterprise risk management.

In this article, Control Self-Assessment methods and renewed COSO Enterprise Risk Management Framework are explained, and the contributions to be provided to the organization by the example of Düzce University Risk Universe Workshop were evaluated. As a case study, the Workshop demonstrates the capacity of the Control Self-Assessment to establish an awareness for the risk-control and objective across the organization.

Keywords: *Entreprise Risk Managemeent, Risk Workshop, Control Self Assessment, COSO ERM 2017 Framework*

JEL Classification: *G32, L21, M12, M42*

*) İç Denetçi (CGAP), Düzce Üniversitesi, Düzce, alptugguler@duzce.edu.tr, Orcid:0000-0001-8439-9511
**) İç Denetçi (CGAP,CCSA), Düzce Üniversitesi, Düzce, aliarkin@duzce.edu.tr, Orcid:0000-0002-6826-0998
Yazı Gönderim Tarihi: 19.10.2018, Yazı Kabul Tarihi: 31.10.2018.

1. GİRİŞ

6 Temmuz 1988 tarihinde Piper Alpha denizaşırı petrol platformunda meydana gelen patlama ve yangın sonucu 167 kişi öldü. 2001 yılında iflas eden enerji şirketi Enron'un 90,75 dolar olan şirket hisseleri kısa bir sürede 0,67 dolara gerileyerek on binlerce yatırımcısı mağdur oldu. Piper Alpha teknolojik felaket olarak tarihte yerini alırken, Enron ise bir mali skandal olarak tarihte yerini aldı. 26 Nisan 1986 tarihinde Çernobil Reaktöründe meydana gelen patlama sonucu, ardında sayısı hala kestiremeyen oranda insanın ölümünü ve radyasyon kaynaklı yüzbinlerce hasta ve sakat insan bıraktı. 15 Eylül 2008 tarihinde Amerika Birleşik Devletleri'nin en büyük yatırım bankalarından biri olan Lehman Brothers firması iflas etti. Çernobil kıtalararası insani bir yıkımı tetikleyerek tarihte yerini alırken, Lehman Brothers ise ciddi bir ekonomik krizi tetikleyerek tarihte yerini aldı. 1929 Dünya Ekonomik Bunalımından Challenger Uzay Mekiğinin infilakına, Fukuşima Nükleer Santralı kazasına ve Titanik Faciasına bunlara benzeyen ya da benzemeyen uzak veya yakın tarihten verilebilecek binlerce kriz, skandal ve felaket örneği… Bu olayların ağır sonuçları oldu; insanlar hayatlarını kaybetti, sağlıklarını bir daha eski yerine gelmedi, zihnen ve fiziken sakat kaldılar, işlerini kaybettiler, ekonomik refahlarını kaybettiler. Bu sonuçlar karşısında ister istemez insan hayatını olumsuz etkileyen krizlerin, skandalların ve felaketlerin önlenmesi, en azından şiddetlerinin azaltılması mümkün olamaz mı diye sorulabilir.

Yukarıda örneklenen birbirlerine çokta fazla benzemeyen ekonomi ve teknoloji odaklı kriz, skandal ve felaketlerin ortaya çıkmasında ortak bir nokta vardır. Bu nokta, belirsizliklere ve ön görülebilir durumlara bir yanıt şeklinde, herhangi bir örgütün iş görme biçiminden bağımsız olarak iç ve dış riskler ön planda olmak üzere, proaktif bir risk yönetim sistemi kurması, kurum içinde içselleştirmesi ve sürdürülebilir kılması ile yakından ilgilidir. Bütün bu yaşanmışlıkların bize öğrettiği; birbirinden farklı amaç ve değerlerle faaliyet gösteren kurumların üretimlerini ve stratejik amaç ve hedeflerini gerçekleştirmesini etkileyebilecek olay veya durumların bütünsel bir bakış açısı ile belirlenmesi, ölçülmesi, önceliklendirilmesi sayesinde; yukarıda örneklenen olay veya durumların gerçekleşme ihtimalinin ve eğer gerçekleşecekse de ortaya çıkaracağı zararın etkisinin azaltılması ile ortaya çıkabilecek fırsatların etkin bir şekilde değerlendirilmesi için gerekli ve yeterli stratejilerin ve aksiyonların zamanında gerçekleştirilmesinin sağlanması için kapsamlı ve sistematik bir Kurumsal Risk Yönetimi yaklaşımına ihtiyaç bulunduğu gerçeğidir.

Çalışma, yukarıda anılan kriz, skandal ve felaketlere bir proaktif bakış açısı olarak yenilenen COSO[1] (The Committee of Sponsoring Organizations of the Treadway Commission) 2017 Çerçevesi temelinde Kurumsal Risk Yönetimi (KRY)[2]nin içeriğini ve bu içeriğin kurumsal bir uygulamasını tartışmaktadır. Çalışma üç bölümden oluşmaktadır. İlk bölümde yeni yayınlanan COSO 2017 Çerçevesi temelinde Kurumsal Risk Yönetiminin temel kavramları bir Kontrol Öz Değerlendirme Yöntemi olarak uygulanan Risk Temalı Çalıştay verileriyle açıklanmıştır. İkinci bölümde, Kontrol Öz Değerlendirmenin kavramsal içeriği ve bu içeriğin Kurumsal Risk Yönetimine sağlayacağı yöntem ve araçlar açıklanmıştır. Son olarak üçüncü bölümde Düzce Üniversitesinde gerçekleştirilen Çalıştayın temel yapısı ve verileri paylaşılmıştır.

2. KURUMSAL RİSK YÖNETİMİ

Risk kültürünün altında yatan temel etken gerçekte belirsizlikle beslenen bir korku kültürüdür. Bu yönüyle risk yönetimine, hem bir sosyolojik gerçeklik hem bir işletme / işletmecilik kavramı ve hem de sosyo-teknik bir ilişki yumağı olarak bakılabilmesi söz konusu olmaktadır. Sürekli değişim içinde hayatını idame ettirmek zorunda olan örgütler artan rekabet, ekonomik krizler, yasal yaptırımlar, teknolojinin artan ivmesi, yerelleşme, küreselleşme gibi etkenler için etkin bir yönetim arayışı ve anlayışı içinde olmaktadırlar. Bu nedenlerle risk yönetimi hiç olmadığı kadar çok önemli bir hale gelmiştir. Geleneksel anlayışla uygulanan risk yönetimi mevcut koşullarda yetersiz kalmaktadır. 20. yüzyılın sonlarına doğru ortaya çıkan "yönetişim" kavramı, başta hesap verebilirlik ve saydamlık olmak üzere Kurumsal Risk Yönetimi ol-

1) Treadway Komisyonu Sponsor Organizasyonlar Komitesi
2) Enterprise Risk Management (ERM)

gusunu da öncelemiş ve örgütlerin hayat bulduğu kaotik ve dinamik çevrenin hem riskleri arttırması ve hem de riskleri çeşitlendirmesi nedeniyle risklere karşı daha proaktif bir bakışı zorunlu kılmıştır. Bu durumun bir yansıması olarak, Kurumsal Risk Yönetimi birçok örgüt tarafından stratejik, operasyonel, finansal ve yasal faaliyetlerdeki tüm risklerin belirlenmesi, analiz edilmesi ve yönetilmesi için uygulamaya konulmaya başlanılmıştır.

Kurumlarda risk yönetiminin rolü konusunda her geçen yıl içinde çok büyük değişiklikler gözlemlenmiş ve günümüzde risk yönetimi örgütler için çok önemli bir hale gelmiştir. Günümüzde başarılı kurumlar belirsizlik ortamından kaçınma yollarını ararken aynı zamanda risklerden fırsatlar elde etmeye odaklanmaktadır. Bunun sonucu olarak da geleneksel bakış açısıyla uygulanan risk yönetimi mevcut koşullarda yetersiz kalmaktadır. Buradan hareketle kurumlar farklı risk türlerini de operasyonel ve stratejik riskler gibi dikkate almaya ve bunları aktif olarak yönetmeye başlamışlardır. Bir kurum mevcut risklerini yönetirken birbirinden tamamen farklı olan iki tür yol izleyebilir. **Birincisi** mevcut risklerini birer birer ele alıp yönetmek; **ikincisi** ise tüm risklerini sistemin bir parçası olarak görüp, onları bir risk yönetimi programı çerçevesinde bütün olarak yönetmektir. İkinci yöntem genel olarak Kurumsal Risk Yönetimi olarak adlandırılmaktadır. Kurumların Kurumsal Risk Yönetiminden beklenilen faydaları elde edebilmeleri iyi işleyen kurumsal risk yönetim yapısı ve kurum içerisinde içselleştirilmiş etkin kurumsal risk yönetim uygulamaları ile mümkündür (Akçakanat, 2012: 30-31).

Kurumsal Risk Yönetimi esas olarak, işe özgü riskler için genel bir risk yönetimi yaklaşımının en son ismidir. Kurumsal Risk Yönetimine gelmeden önce bu dönemin öncüleri arasında Kurumsal Risk Yönetimi, iş riski yönetimi, bütünsel risk yönetimi, stratejik risk yönetimi ve entegre risk yönetimi yer almıştır. Her ne kadar bu kavramların her biri birbirinden az çok farklı bir odak noktasına sahip olsa da, her bir kavram ilk ortaya çıktığı zaman kurumların birincil endişesi olan risk unsurları tarafından desteklenmiş ve içerek olarak genelde benzer olguları taşımışlardır (D'Archy, 2001: 2).

Kurum bünyesinde sistematik bir risk yönetimi planının eksikliğini gidermek için, 2004 yılında COSO bir Kurumsal Risk Yönetimi çerçevesi (COSO-KRY) oluşturmuştur. COSO-KRY, Kurumsal Risk Yönetimini "kurum hedeflerine ulaşılması konusunda makul bir güvence sağlamak" için tasarlanmış bir kurumsal risk değerlendirme ve yönetim süreci olarak tanımlamaktadır. Risk yönetiminin benimsenmesi, organizasyonel risk düzeyini spesifik olarak değiştiremese de, muhtemelen risklerin gerçek ölçümünü ve kurum genelinde izlenmesini etkilemektedir (Callahan ve Soileau, 2017: 122-123).

Kurumsal Risk Yönetimi, bir kurumun hedeflerine ulaşmasını etkileyebilecek potansiyel olayları tanımlayan, risk alma istekliliği sınırları içinde yöneten ve kurum hedeflerinin başarılması konusunda makul derecede güvence sağlayan, kurum genelinde yapılandırılmış ve kurum yönetim kurulundan, yönetimden ve diğer çalışanlardan etkilenen bir süreçtir (COSO, 2004, III).

Kurumsal Risk Yönetimi son yirmi yılda popüler hale geldikçe, kurumlar, tüm paydaşlarını "risk yönetimi hakkına sahip olduklarından" memnun edecek bir program uygulamaya çalışmaktadırlar. Ancak burada temel bir sorun vardır, Kurumsal Risk Yönetiminin bir program olmadığıdır. Aslında o ne bir bölüm ne de bir süreç değildir. Kurumsal Risk Yönetimi veya daha genel olarak "risk yönetimi" karar vermenin ayrılmaz bir parçasıdır. Tek başına ayakta durmayan, ancak bir örgütün yaptığı her şeyin bir parçası olan yetenekler, yaklaşımlar, yetkinlikler, araçlar, kültür ve bunların daha fazlasıdır. Ne yazık ki, birçok kuruluş risk yönetimini iyi yürütememekte ve sonuçlarından zarar görmektedir (Anderson, 2017: 38).

Kurumsal Risk Yönetiminin ortaya çıkış gerekçesi risklerin de ortaya çıkış gerekçesi olan kurumun başarmayı hedeflediği stratejileri ve amaçlarıdır. Kurumsal Risk Yönetiminin temel amacı, risklerin yönetilmesi sağlanarak kurum amaçlarına ulaşmak olarak ifade edilebilir. Etkin bir şekilde çalışan ve amaçlarına ulaşan Kurumsal Risk Yönetimi sistemi de ancak etkin işleyen Kurumsal Risk Yönetimi temelli bir örgütsel yapılanmanın varlığı halinde mümkündür. Kurumsal Risk Yönetiminin etkin çalışabilmesi ancak sistemin etkinliğinin denetlenmesi, eksikliklerin ve aksayan yönlerin tespiti ve düzeltilmesi ile mümkündür. Kurumsal Risk Yönetimi için öne çıkan temel öğeleri aşağıdaki gibi sıralanabilir (COSO, 2004):

- Sürekli ve akışkan bir süreçtir. Kurumsal Risk Yönetimi bir olay veya durumdan oluşan bir etkinlik değil kurum faaliyetlerinin içinde yer alan bir eylemler serisidir.
- Kurumun her seviyesindeki çalışanlardan etkilenir. Yönetim kurulu Kurumsal Risk Yönetiminin en önemli öğelerinden birisidir. Ayrıca stratejileri, işlemleri ve politikaları onaylayan yöneticilerin de Kurumsal Risk Yönetimi üzerinde etkinlikleri fazladır.
- Kurumun her seviyesinde uygulanır. Kurumsal Risk Yönetimi kurum genelindeki faaliyetlerle ilgilidir. Bu faaliyetler kurum tepe yönetimi faaliyetleri, stratejik planlama ve kaynak tahsisi olabileceği gibi bölüm temelli faaliyetler de, pazarlama ve insan kaynakları da olabilir.
- Risklerin tamamıyla giderilmesine gerek yoktur. Riskler risk alma istekliliği sınırları içinde yönetilir. Risk alma istekliliği, basit olarak, niteliksel (yüksek, orta ve düşük sınıflandırması şeklinde) veya niceliksel (büyüme ile ilgili hedeflerin yansıtılması) olarak düşünülebilir.
- Kurumsal Risk Yönetimi, kurum hedeflerinin başarılacağına ilişkin makul düzeyde güvence sağlar.

COSO tarafından yayınlanan iki çerçeve vardır. İlk çerçeve 1992 yılında yayınlanan ve 2013 yılında revize edilen İç Kontrol- Entegre Çerçevesi (Internal Control-Integrated Framework), diğer çerçeve ise, 2004 yılında yayınlanan "Kurumsal Risk Yönetimi-Entegre Çerçevesi"dir (Enterprise Risk Management – Integrated Framework). COSO, Kurumsal Risk Yönetimi Çerçevesinde de bir revizyona giderek 2017 yılında, "Kurumsal Risk Yönetimi-Riskin Strateji ve Performansla Uyumlaştırılması" (Enterprise Risk Management—Aligning Risk with Strategy and Performance) çerçevesini yayınlanmıştır.

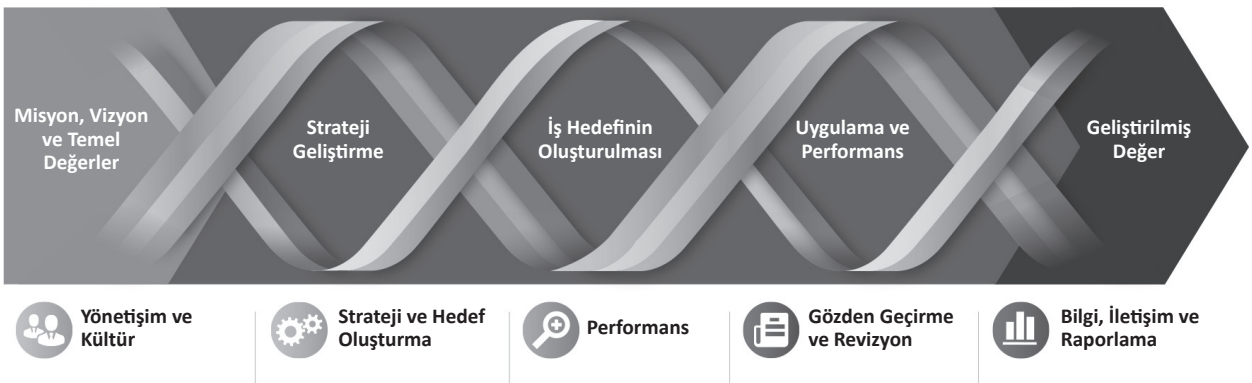
Yeni risklerin ortaya çıkması, mevcut risklerin daha karmaşık hale gelmesi, örgüt ve onun paydaşları arasında risk yönetimine yönelik farkındalığın artması ve Kurumsal Risk Yönetimi olgusundaki gelişmelerin mevcut çerçeveyi revize edilmesi (Şekil 1) ihtiyacını doğurmuştur.

COSO 2017 Kurumsal Risk Yönetimi Çerçevesinde dikkatini çeken ilk farkındalık modelin simgesinin 2004 Çerçevesinden farklı olduğudur. Yeni çerçeve beş bileşen ve 20 ilke içermektedir. Ancak, basit 2004 Kurumsal Risk Yönetimi küpünün aksine yeni modelin ana simgesi gizil ve soyut formdadır. Şekil 1'de gösterildiği gibi yeni Kurumsal Risk Yönetiminin simgesi çeşitli renkli şeritlerin kesişimleri arasında konumlandırılmış beş terimi içermektedir. Ana resmin (ama yine de modelin bir parçası) altında, ilgili terimlerle (farklı) beş mini ikon vardır. Bu terimler ile şeritler arasındaki ilişki ve şeritler içindeki terimler hemen anlaşılmaz bir yapıdadır (Prewett ve Terry, 2018: 17-19).

Yeniden güncellenen şematik yapılanma ile kübik yerini sarmal (helezon) bir düzleme (Şekil 1) bırakmıştır. Yenilenen modelde (Gleim CPA, 2018: 1; Kurt ve Uysal, 2018: 23-33);

- Yeni yapılanmada risk yönetiminin strateji belirleme ve performansla bütünleşmesine daha fazla önem verilmiştir.

Şekil 1. COSO 2017 Kurumsal Risk Yönetimi



Kaynak: COSO, 2017: 6

- "Kurumsal Risk Yönetimi" ve "risk" terimleri yeniden tanımlanmıştır. Kurumsal Risk Yönetimi tanımı basitleştirilmiştir.
- Entegre bir risk yönetimi üzerine odaklanılmıştır.
- Risk yönetimi örgüt geneline yayılmıştır.
- Örgüt kültürü ön plana çıkmıştır.
- Bilgi teknolojisinin değişen rolü vurgulanmıştır.
- "Risk profili" ve "portföy görünümü" terimleri yönetim sistemine dahil edilmiştir
- Sekiz bileşen yerini beş yeni bileşene (şeride) bırakmıştır. Risk yönetimi ve iş modeli arasındaki ilişkiyi gösteren yeni kavramsal grafikler oluşturulmuştur.
- Bu beş bileşenli yapıda, bileşenler arasında 20 ilke dağıtılarak temel şekil oluşturulmuştur.

Yeni modelde COSO'nun iletişim kurmaya çalıştığı kavram, şeritlerin altındaki beş terimin modelin bileşenleri olması ve her bileşenin simgesinin renginin bu renk şeridi tarafından temsil edilmesi anlamına gelmesidir. Renkli şeritler sırayla beş bileşenin her birinin şeritler içinde tarif edilen işlemler boyunca birbiriyle temasını ifade etmektedir. Bir başka deyişle,

Tablo 1. COSO 2004 ve 2017 Kurumsal Risk Yönetimi Çerçevelerinin Karşılaştırılması

2017 Çerçevesi Bileşenleri	#	2017 İlkeleri	2004 Çerçevesinde var mı?	2004 Çerçevesi Bileşenleri
Yönetişim ve Kültür	1	Yönetim Kurulunun (Yönetimin) Riskin Gözetimini Yapması	✔	İç Ortam
	2	Operasyonel (Çalışma)Yapının Oluşturulması	✔	
	3	Arzu Edilen Kültürün (Örgüt Kültürünün) Tanımlanması	✔	
	4	Temel (Çekirdek) Değerlere Bağlılık Gösterilmesi	✔	
	5	Yetenekli Personeli (Örgüte) Çekme, Gelişimini Sağlama ve Elinde Tutma	✔	
Strateji ve Hedef Belirleme	6	İş Ortamını (İçeriğini) Analiz Etme	✔	Hedef Belirleme
	7	Risk İştahını Tanımlama	✔	
	8	Alternatif Stratejileri Değerlendirme	X	
	9	İş Hedeflerini Oluşturma	≠	
Performans	10	Riski Tanımlama	✔	Olay Tanımlama
	11	Riskin Şiddetini Değerlendirme	≠	Risk değerlendirmesi
	12	Riskleri Önceliklendirme	✔	
	13	Riske (Gerekli ve Uygun) Yanıtlarını Uygulama	✔	Riske Karşılık Verme ve Kontrol Faaliyetleri
	14	Portföy Bakışını Geliştirme	✔	Riske Karşılık Verme
Gözden Geçirme ve Revizyon	15	Önemli Değişimi Değerlendirme	✔	İzleme
	16	Riski ve Performansı Gözden Geçirme	✔	
	17	Kurumsal Risk Yönetimindeki İyileştirmeyi İzleme	✔	
Bilgi, İletişim ve Raporlama	18	Bilgi ve Teknolojiden Yararlanma	✔	Bilgi ve İletişim
	19	Risk Bilgisinin İletişimi Yapma	✔	
	20	Risk, Kültür ve Performans Hakkında Raporlama Yapma	✔	

LEJANT		
	✔	Konuyu içermektedir
	≠	Bazı anahtar kavramlar eksiktir
	X	Çoğu anahtar kavram eksiktir

Kaynak: Prewett ve Terry, 2018: 19

beş bileşen (Yönetişim ve Kültür, Strateji ve Hedef Belirleme, Performans, Gözden Geçirme ve Revizyon ve Bilgi, İletişim ve Raporlama) misyon, vizyon ve temel değerler, strateji geliştirme, iş hedefinin oluşturulması, uygulama ve performansın oluşturulmasını etkilemektedir. Son olarak tüm bu faktörler "geliştirilmiş değer" ile sonuçlandırılmıştır. COSO bu beş bileşenin her birine gömülü olan kavramları açıklığa kavuşturmak için 20 ilke belirlemiştir (Prewett ve Terry: 19). İlkelerin ve ilgili bileşenlerin başlığı Tablo 1'de sunulmuştur. COSO 2017 ile iç kontrol bileşeninin yeniden yorumlanmış ilkeleri, ana hatlarıyla 2004 Çerçevesinin içerdiği kavramlarla benzerlik ve paralellik göstermektedir. Temel olarak, 2004 Çerçevesinde ele alınmayan bir ilke çerçeveye yeni olarak giriş yapmış (8 no.lu ilke-Alternatif Stratejileri Değerlendirme) ve iki ilke ise güncellenerek (9 no.lu İş Hedeflerini Oluşturma ve 11 no.lu Riskin Şiddetini Değerlendirme) yeni çerçevede yer bulmuştur.

2017 Çerçevesi, her çeşit kurumda risk yönetiminin rolünün anlaşılmasında teknolojik değişimlerini ve büyümeyi yansıtacak şekilde güncellenmiştir. 2017 Çerçevesinde en göze batan, ilk iki ilke olan Yönetişim ve Kültür ve Strateji ve Hedef Belirlemeye yapılan vurgulamadır. Bu iki ilke, Kurumsal Risk Yönetimi sorumluluğunu en üst düzeydeki yönetim seviyesine taşıyarak ve Kurumsal Risk Yönetimi tarafından yerleşik ve bilgilendirilmiş örgüt çapında bir kültür oluşturarak, Kurumsal Risk Yönetimi kavramını teşvik etmektedir (Prewett ve Terry: 20).

Yeni çerçevedeki sarmal yapı beş şeritten ve ikili bağlamdan oluşurken, bu beşli yapının ilk bağlamındaki Yönetişim ve Kültür ile Bilgi, İletişim ve Raporlama şeritleri Kurumsal Risk Yönetiminin yatay ve dikey hatları olarak destek hattını oluşturmakta ve diğer bağlamdaki Strateji ve Hedef Belirleme, Performans ve Gözden Geçirme ve Revizyon şeritleri ana iskeleti meydana getiren örgütün temel süreçlerini oluşturmaktadır.

Çalışmanın bundan sonraki bölümünde bir Kontrol Öz Değerlendirme çalışması olarak yapılan Risk Temalı Çalıştay verilerinden faydalanılarak, yeni 20 ilke için risk odaklı örneklemeler yapılarak bunların ışığında değerlendirilmelerde bulunulacaktır.

2.1. COSO 2017 Kurumsal Risk Yönetimi-Yönetişim ve Kültür Bileşeni

Yönetişim, kurumun risk yönetimini belirler, Kurumsal Risk Yönetiminin önemini güçlendirir ve gözetim sorumluluklarını belirler. Kültür, etik değerlere, istenen davranışlara ve kurumdaki risk anlayışına ilişkindir (COSO, 2017: 6). Kurumsal yönetim, şirketin yönetiminin, yönetim kurulunun, hissedarların ve şirketin hedeflerinin belirlendiği yapıyı sağlayan diğer paydaşlar arasındaki ilişkidir. Etkin yönetişim, şirketin hedeflerini oluşturmak için gereken uygun gözetim, yapı ve kültür seviyesini sağlar, bu hedefleri takip etme ve bu arayışla ilişkili riskleri anlama araçlarını devreye sokar. Esasen yönetişim, kararların alınma biçimini ve bu kararların nasıl yürütüldüğünü belirler (ERM, 2018: 15). Bu ilk sarmal beş demet bileşene sahiptir.

2.1.1. Yönetim Kurulu (Yönetim) Riskin Gözetimini Yapar

Yönetim Kurulu (Yönetim)[3], kurumun mevcut risklerini kendi onayladığı şekilde yönetebilecek bir iç kontrol sisteminin etkin olmasını sağlamalıdır. Etkin ve güçlü bir iç kontrol sisteminin var olup olmadığının değerlendirilmesinde ise kurumun karşı karşıya kalabileceği risklerin şiddetini ve doğasının göz önünde bulundurulması gerekir. Kurumun katlanmayı göze alacağı risklerin doğası ve boyutu, olası risklerin gerçekleşme olasılığını, gerçekleşebilecek risklerin kurum faaliyetlerine olan etkilerinin azaltılabilme becerisinin göz önünde bulundurması gerekir (Turnbull Report, 2005: 12). Çalıştayda elde edilen veri setleri içerisinden yönetimin riskin gözetimini yaparak; risklerin kontrolünü ele alması**,** örgütün stratejisini ve iş hedeflerini gerçekleştirmesini desteklemek amacıyla, stratejinin izlenmesi ve yönetişime dair yükümlülüklerini yerine getirmesini içinde barındıran tipik bir örnek olarak A Merkezi'nde "*Operasyonel*" risk kategorisinde "*Yüksek*" risk değerlendirmesine sahip "*Pnömatik sistem arızalarından dolayı, hasta numunelerinin yanlış birimlere düşmesi, durumun geç fark edilmesi, kan laboratuvara ulaşmadığı için çalışılmaması..*" riski verilebilir. Riskin göze-

3) Her ne kadar COSO 2017 Kurumsal Risk Yönetiminin 1.prensibi "Yönetim Kurulu Riskin Gözetimini Yapar" olsa da makalemizde örneklerine başvurduğumuz Üniversite özelinde Yönetim Kurulu yerine Yönetim kavramını kullanmak örgütün doğası gereği daha doğru olacaktır.

timi için geliştirilebilecek kontrol faaliyeti (stratejisi); "*Numune gönderiminde pnömatik sisteme giriş çıkışın kayıt altına alınabileceği bir mekanizmanın oluşturulması*" olmuştur.

2.1.2. Operasyonel (Çalışma) Yapı Oluşturulur

Kurum, strateji ve iş hedefleri doğrultusunda gerekli operasyonel (işletme, çalışma) yapılarını kurar (ERM, 2018: 15). A Yüksekokulu'nda "*Operasyonel*" risk kategorisinde "*Yüksek*" risk değerlendirmesine sahip "Ön *lisans ve lisans öğrencilerinin akademik yılın başlangıcında yapılan İngilizce I-II dersi muafiyet sınavından haberdar olmaması nedeniyle muafiyet sınavına girememeleri*" riski örgüt, stratejisini ve iş hedeflerini gerçekleştirmek amacıyla operasyonel temelde gerekli yapıyı oluşturması için verili bir riski göstermektedir. Operasyonel yapı oluşumu için önerilen kontrol faaliyeti (stratejisi); "*Tüm birimlerde fiziki ortamlarda ve internet sayfalarında duyuruların paylaşılması*" olmuştur.

2.1.3. Arzu Edilen Kültür (Örgüt Kültürü) Tanımlanır

Kültür yönetimi süreci mevcut kurum kültürünün tanımlanmasıyla başlar. Bunlar, kurumun müşterileri gibi belirli kilit boyutlara ilişkin mevcut güncel değerlerini içerir. Bir sonraki adımda örgütün ideal veya arzu edilen kültürü formüle edilir. Bunlar kültürün gerçekte ne olduğu ya da ne olması istendiğidir. Buna ek olarak, bu istenen kültür, kurumun genel stratejik gelişimini desteklemesi amaçlandığından, kurumun "stratejik kültürü" olarak görülebilir (Flamholtz, 2001: 270). Fakülteler kısmında "*Operasyonel ve Yasal*" risk kategorisinde "Çok *Yüksek*" risk değerlendirmesine sahip "Şifrelerin çalışanlar arasında paylaşılmasından ve uygunsuz yetki paylaşımından dolayı *suiistimal riski*" örgütün, kurum bünyesinde bilgi güvenliğini içselleştiren bir kültürü karakterize edecek, arzu edilen davranışlarına referans olan bir riski işaret etmektedir. Arzu edilen örgüt kültürü için önerilen kontrol faaliyeti (stratejisi); "Öğrenci otomasyon işlemlerinde *password (*şifre*)* güvenliğine önem verilmesi ve görevler ayrılığı ilkesine uygun olarak işlem yapılması. Personel*, şifrelerin gizliliği hakkında bilgilendirilmeli ve gizlilik kurallarına uymaları sağlanmalı, mail adreslerin giriş şifresi ile not giriş şifresinin birbirinden farklı olması sağlanmalı.*" şeklinde tanımlanabilir.

2.1.4. Temel (Çekirdek) Değerlere Bağlılık Gösterir

Güçlü bir kültüre sahip olmak için, bir örgütün çok güçlü değerler olması gerekmez. Kritik olan, bu değerlerin örgüt içerinde geniş bir biçimde paylaşılması ve güçlü bir şekilde tutulmasıdır (O'Reilly, 1989:14). Örgüt, kurumca kabul edilmiş temel değerlere bağlılığını göstermesi gerekir. A Fakültesi'nde "*Operasyonel*" risk kategorisinde *"Çok Yüksek"* risk değerlendirmesine sahip "Öğretim elemanları arasında işbirliği ve iletişim eksikliği sonucu ortaya çıkan kurum psikolojik iklimi ile kültürünün olumsuz etkilenmesi" riski örgütün temel değerlere bağlılığını sınayacak bir riski göstermektedir. Temel değerlere bağlılığın sağlanması için önerilen kontrol faaliyeti (stratejisi); "*Bölümler arasında çatışmalara yol açan sorumluluk alanlarının açık şekilde belirlenmesi. Üst yönetim tarafından öğretim elemanlarını bir araya getirecek mekanizmaların oluşturulması"* olmuştur.

2.1.5. Yetenekli Personeli (Örgüte) Çeker, Gelişimini Sağlar ve Elinde Tutar

İnsan Kaynaklarının üstleneceği en büyük stratejik görevlerden biri, yetenekli çalışanları kurumlarına çekmek ve kurumda tutmak için gerekli olan çekici, motive edici ve bağdaştırıcı kültürü geliştirmeye yardımcı olmaktır. Böylesi bir kültürde, yetkin bireylerdeki potansiyel ve tam işleyen ağlar, birbirine bağlı eylemlere dönüştürülebilir. Kurumlar, günümüz çalışanları arasındaki sadakatin ölü olduğu fikrini reddetmeli ve örgüte bağlı kalmaları için insanları çekecek ve enerjik bir ortam yaratmanın zorluğunu kabul etmelidir (Bartlett ve Ghoshal, 2002: 34). Örgüt, sahip olduğu misyon ve vizyonu referans alan, strateji ve iş hedefleri ile uyumlu olarak üretken ve etkin bir insan kaynağını inşa etmeye ve bunu sürdürülebilir kılmaya büyük önem vermelidir. A Fakültesi'nde "*Stratejik*" risk kategorisinde "*Yüksek*" risk değerlendirmesine sahip "*Alanında uzman olmayan öğretim üyelerinin derse girmesinden dolayı öğretim niteliğinin düşmesi*" etkin bir insan kaynakları politikası ile personel kaynağının oluşturulması ve geliştirilmesi için temel bir riske işaret etmektedir. Yetenekli personelin çekilmesi ve geliştirilmesi için önerilen kontrol faaliyeti (stratejisi); "*Ders görevlendirmelerinin uzmanlık alanlarına (yalnızca doktora ve doçentlik alanlarına) göre yapılması"* olmuştur.

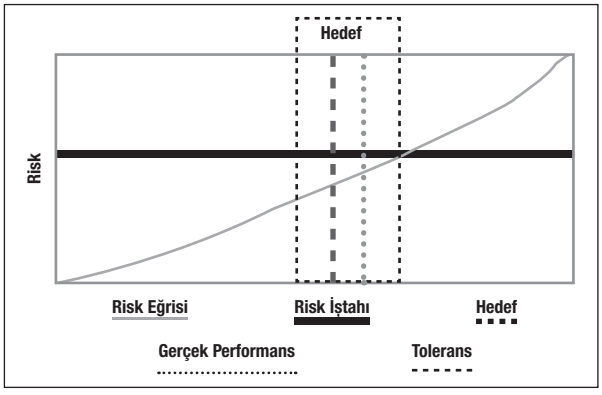
2.2. COSO 2017 Kurumsal Risk Yönetimi-Strateji ve Hedef Belirleme Bileşeni

Kurumsal Risk Yönetimi, strateji ve hedef belirleme, stratejik planlama sürecinde birlikte çalışır. Örgütün stratejisiyle uyumlu bir risk iştahı belirlenir. İş hedefleri; stratejiyi uygulamaya sokarken, riskleri tanımlamak, değerlendirmek ve yanıtlamak için bir dayanak noktası olarak hizmet verir (COSO 2017: 6). Etkin yönetişim, kuruluşun Kurumsal Risk Yönetimi faaliyetlerinin temelini oluştursa da, iş ortamına ve stratejisine güçlü bir anlayış ve bakış açısı, risk yönetimi için bir çapa görevi görür. Kurumda bir değeri yaratmak için bir örgütün stratejisi ve iş hedefleri belirlenir. Bu değer, finansal yapının ötesinde, toplumsal, insani ve ilişkisel, doğal, entelektüel ve üretilmiş sermayeyi kapsayacak şekilde, birbiriyle bağlantılı çoklu sermaye türlerine dayanmaktadır. İç ve dış iş bağlamındaki değişiklikler, kurumun değer oluşturma veya koruma yeteneğini doğrudan etkiler (ERM, 2018: 33). İkinci sarmal dört demet bileşene sahiptir.

2.2.1. İş Ortamını (İçeriğini) Analiz Eder

Örgüt, faaliyet alanı bulduğu iş ortamının, risk profili üzerindeki muhtemel (potansiyel) etkilerini bir analize tabi tutar. Risk profili (Şekil 2), belirli bir strateji veya iş hedefi ile ilgili risklerin çeşitleri, şiddeti ve bağımlılıkları ile bunların performans üzerindeki etkileri hakkında birleşik bir bakış açısıdır. Bir risk profili, örgütün herhangi bir seviyesinde (örneğin, varlık, bölüm, operasyon birimi veya fonksiyon) veya görünümünde (örneğin, ürün, hizmet veya coğrafya) oluşturulabilir (Gleim CPA: 2).

Şekil 2. Risk Profili



Kaynak: Gleim CPA, 2018:3

A Koordinatörlüğü'nde "İtibar" risk kategorisinde "*Yüksek*" risk değerlendirmesine sahip "*Amaca yönelik üretilen ürünlerin beklenen etkiyi karşılamaması (örneğin ağrı kesici özelliği olduğu iddia edilen bitki ekstratları ile hazırlanan kremin ağrı kesici etki göstermemesi)*" riski potansiyel bir etkiyi göstermektedir. İş ortamının analizi sonucu ortaya çıkan kontrol faaliyeti (stratejisi); "*Literatürde söz konusu bitkilerin etkileri hakkında yeterince bilgi varsa dikkatlice okunmadan yola çıkılmaması ve ürün denemelerinin yapılması"* olmuştur.

2.2.2. Risk İştahını Tanımlar

Kurumlar, önceden hedef risk iştahı ile tutarlı bir artık risk oluşturan kontrolleri ve azaltımları tasarlayarak, gerektiğinde geri bildirim ayarlaması yaparak ve tüm süreci izleyerek; tüm maddi riskleri hedeflerine ve alt hedeflerine göre tanımlamaya çalışmalıdır (Power, 2009: 849). Risk iştahı, örgütün amaçları ve hedefleri doğrultusunda razı olduğu (tolere edebileceği / maruz kalmaya kabul edeceği / önlem almayı planlamadığı / aksiyon hazırlamadığı) en yüksek risk düzeyi olarak tanımlanır. Risk iştahı kavramı, örgüt tarafından belirlenen bu seviyenin üzerindeki risklerin herhangi bir şekilde kabul edilemeyeceği ve aksiyon alınması (önlem alınması) gerekliliğini tanımlar. Örgüt, risk iştahını, kurumsal bir değer oluşturma, muhafaza etme ve gerçekleştirme temelinde tanımlar.

Risk iştahını karakterize edebilecek bir örnek, A Merkezi'nde "*Sağlık ve güvenlik*" risk kategorisinde "*Yüksek*" risk değerlendirmesine sahip "*Ameliyathanede kullanılan görüntüleme cihazlarından kaynaklanan radyasyon*" riski verilebilir. Risk iştahına karşı geliştirilen kontrol faaliyeti (stratejisi); "*Ehliyetli radyoloji teknisyeninin çalışması.* Çalışanlara dozimetre verilmesi" olmuştur.

2.2.3. Alternatif Stratejileri Değerlendirir

Üst yönetim bilinçli olarak örgüt içinde bir tartışma formu oluşturmalı ve kurumlarını tehdit edici konular hakkında örgüt çalışanlarının konuşmalarına izin vererek, yeni çözümleri ortaya çıkarmaları için zaman ayırmalarını teşvik etmelidir. Çevresel fırsatlar veya tehditler ele alınan alternatif stratejiler ile genişletilmelidir. Üretilen alternatif stratejiler değerlendi-

rilmeli ve örgüt için seçilen strateji en iyi alternatif olmalıdır (Schwenk, 1984: 120-124). Örgüt, alternatif stratejileri gösterge olarak risk profili üzerindeki etkilerini değerlendirmeye almalıdır. Alternatif strateji üretilmesi gereken tipik bir risk, A Merkezi'nde "*Sağlık ve güvenlik*" risk kategorisinde "*Orta*" risk değerlendirmesine sahip "*Hepatit B ve Hepatit C'li hastaların kullandığı diyaliz makinalardan diğer hastalara bulaşma riski"*dir. Alternatif kontrol faaliyetleri (stratejileri):

"*1. Hepati B ve Hepatit C'li hastaların kullandığı makinaların ayrılması,*
2. İlk hasta kabulünde hepatit markerlerin bakılarak makinalara alınması,
3. Bütün hastaların 3 ayda bir kontrollerinin yapılması,
4. Düzenli aralıklarla hastalardan geri bildirim alınarak eğitim verilmesi,
5. Hepatit B ve Hepatit C odalarının ayrı olması,
6. Hastaların Hepatit B aşı programında olması."

2.2.4. İş Hedeflerini Oluşturur

Kurum stratejisi, kurumun iş hedeflerinin sunulmasını desteklemede olumlu bir etken olmaktadır. İş hedeflerinin oluşturulması, insanların çalışma şeklini ve işteki üretkenliğini etkilemekte ve çalışma şeklinden bağımsız olarak gerekli kültürel değişimi sağlamaktadır (Levin, 2008). Örgüt, işe ait hedeflerini oluştururken, temel stratejisiyle uyumlu ve ona destek verecek biçimde, kurum bazında hem yatay ve hem de dikey seviyede riskleri dikkate alır. B Fakültesi'nde "*Operasyonel ve Yasal*" risk kategorisinde "*Yüksek*" risk değerlendirmesine sahip "*Başvuru dosyalarında olan eksiklikler veya hatalar nedeniyle etik kurul kararlarının geç çıkarılması*" birim bazında göz önüne alınması gereken bir iş hedefinin içsel riskidir. Hedefe varmak için önerilen kontrol faaliyeti (stratejisi); "*Başvuran adayların etik kurul yönergelerine göre başvurulmasının sağlanması"* olmuştur.

2.3. COSO 2017 Kurumsal Risk Yönetimi-Performans Bileşeni

Strateji ve iş hedeflerine ulaşılmasını engelleyebilecek riskler belirlenip ve değerlendirilmelidir. Risk iştahı bağlamında riskler öncelik sırasına göre belli bir ölçekte önceliklendirilmelidir. Örgüt daha sonra riske vereceği yanıtları seçer ve üstlendiği risk miktarını portföy bakış açısıyla ele alır. Bu sürecin sonuçları kilit risk paydaşlarına raporlanır (COSO, 2017: 6). Etkin risk yönetimi, risk azaltma ve riskten faydalanma için kaynak harcamalarının sabit bir şekilde dengelenmesini gerektirir. Bu durumda yönetim, önceliklendirme ve kaynak paylaşımını desteklemek için risklerin potansiyel etkilerini ve şiddetini değerlendirir. Bu nedenle önceliklendirme hedefi; bir kurum için stratejik, finansal ve operasyonel faydayı maksimize etmek olacaktır (ERM, 2018: 65). Üçüncü sarmal beş demet bileşene sahiptir.

2.3.1. Riski Tanımlar

Risk tanımlama, risk yönetimi uygulamasında temel bir aşamadır. Riskler tanımlanarak, bir karar verici veya bir karar verici grubu için belirsizlik yaratan olaylar ya da olgular hakkında bilinçlenme sağlanır. Risk tanımlamasının ana odak noktası, bu olayları ya da olguları proaktif olarak yönetebilmek için gelecekteki belirsizlikleri tanımaktır (Hallikas vd., 2004: 52). Örgüt, stratejisinin ve iş hedeflerinin gerçekleştirilmesini etkileyen olası riskleri tanımlar. B Koordinatörlüğü'nde "*Operasyonel*" risk kategorisinde "*Orta*" risk değerlendirmesine sahip "*Bilgi edinme birimine gelen başvurularda, ilgili Üniversitemiz birimlerince verilen cevabın eksikliği, bundan dolayı sürecin uzaması veya zamanında cevap verilmemesi*" ve A İdari Biriminde "*Yasal / Uygunluk" risk kategorisinde "Yüksek" risk değerlendirmesine sahip "Avans ve kredilerin zamanında kapatılmaması*" gibi riskler örgütün, stratejisinin ve iş hedeflerinin gerçekleştirilmesini etkileyen riskleri belirleme faaliyetidir. Bu riskler için önerilen kontrol faaliyeti (stratejisi) ilk risk için; "*Resmi yazılarla birimlerin, işlem sürecinin nasıl yürütüleceği ve hangi süreler içerisinde cevap verilmesi gerektiğine ilişkin bilgilendirilmesi"* ve ikinci risk için "*Avans ve kredi süreçlerinin takibi için SMS / e posta bilgilendirmesi yapılması*" olmuştur.

2.3.2. Riskin Şiddetini Değerlendirir

Örgütsel felsefenin içine yerleştirilmiş bir disiplin olarak Kurumsal Risk Yönetimi, işle ilgili risk faktörlerini tanımlamak, şiddetini değerlendirmek, ölçmek ve hafifletmek ile üst düzey fırsatlardan yararlanmak

anlamına gelmektedir (Wu ve Olson, 2009: 4923). Örgüt, olası risklerin şiddetini değerlendirir. C Yüksekokulu'nda "*Operasyonel ve Yasal*" risk kategorisinde ,"*Engelli kullanıcılar için fiziksel yapının yetersiz olması*" anahtar risk göstergeli "*Engelli kullanıcılar için, asansör, rampa, wc vb. ihtiyaçlarını ve ulaşımlarını sağlayabilecekleri fiziksel donatıların olmayışı, engelli bireylerin hareket kabiliyetini sınırlaması, temel ihtiyaçlarını gidememesi*" riski "Çok Yüksek" etki ve "Çok Yüksek" olasılık değerlerine bağlı olarak "Çok Yüksek" risk oranında değerlendirilmiştir.

2.3.3. Riskleri Önceliklendirir

Risk analizinden sonra, duruma uygun yönetim eylemlerini seçebilmek için riskleri değerlendirmek ve önceliklendirmek önemlidir. Yaygın bir yöntem, olasılıkları ve sonuçlarını değerlendirerek olayları karşılaştırmak ve bunları bir risk haritası / matrisine koymaktır (Norrman ve Jansson, 2004: 438). Örgüt, risklere vereceği uygun aksiyona (cevaba) bir temel oluşturmak üzere, riskleri belli bir ölçekte derecelendirir ve önceliklendirir. C Yüksekokulu'nda "*Sağlık ve Güvenlik*" risk kategorisinde, " *Torna tezgâhında iş kazası olma riski*" anahtar risk göstergeli,

"*1- Ayna anahtarının ayna üzerinden fırlaması tehlikesi,*

2- İş parçasının ayna ayaklarından fırlaması tehlikesi,

3- Talaş kaldırma işlemi sırasında çıkan talaşın çalışan kişiye zarar vermesi tehlikesi,

4- Herhangi bir iş kazasında torna tezgahı aynalarının aniden durmaması,

5- Torna tezgahlarında ayna sensörünün bulunmaması tehlikesi,

6- Torna tezgahları otomatik operasyon noktaları,(ana mil, talaş mili) uygun şekil ve nitelikte koruyucu içinde olmaması tehlikesi,

7- Öğrencilerin aynayı tutarak elle fren yapmaları önlenememesi." riskleri "*Yüksek*" etki ve "*Orta*" olasılık değerlerine bağlı olarak "*Yüksek*" risk oranında değerlendirilmiş ve önceliklendirilmiştir.

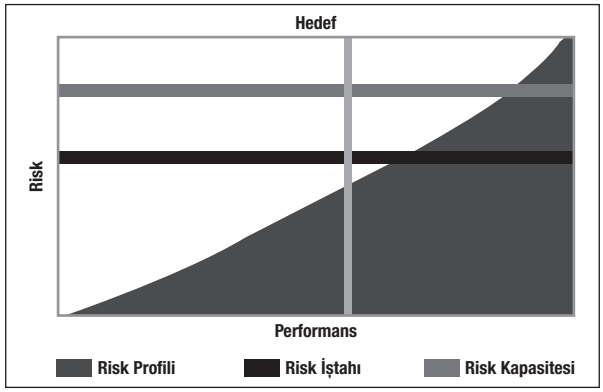
2.3.4. Riske (Gerekli ve Uygun) Yanıtlarını Uygular

Risklere yanıt olarak risk yönetim sisteminin kontrolünü arttırmanın bir yolu daha yapısal ve entegre risk yönetimi sağlamaktır. Kurumsal Risk Yönetimi (risklere verdiği yanıtlar ile) örgüt için birçok yönden bir itici güç oluşturmuştur (Lundqvist, 2015: 442). Örgüt, risklere vereceği uygun aksiyonları (cevapları) belirler ve seçer. Bu cevaplar bir dizi kontrol faaliyeti ve / veya kontrol stratejisi şeklinde olur. A Merkezi'nde "*Yasal / Uygunluk*" risk kategorisinde "*Yüksek*" risk değerlendirmesine sahip "*Adli konularda bilgi eksikliği. Bilgi güvenliğinin sağlanamaması. Hasta ve çalışan hakları konusunda mevzuat, kanun ve yönetmeliklerin eksik bilinmesi*" riskine uygun bir yanıt verilmelidir. Riske verilebilecek yanıt olarak geliştirilebilecek kontrol faaliyeti (stratejisi); "Çalışanların adli eğitim almasının sağlanması. *Bu eğitimin düzenli aralıklarla yenilenmesi.*" olmuştur.

2.3.5. Portföy Bakışını Geliştirir

Örgüt, risklere ve belirsizliklere ilişkin bir portföy bakış doğrultusu geliştirir ve değerlendirir. Portföy bakışı, bir risk profiline (Şekil 3) benzer. Aradaki fark, kurum çapında strateji ve iş hedefleriyle ilişkili risklerin ve bunların kurum performansı üzerindeki etkilerinin birleşik bir bakışıdır (Gleim CPA: 3). C ve D Fakültelerinde "*Stratejik*" risk kategorisinde "*Yüksek*" risk değerlendirmesine sahip "*Akademik personelin ders yükü fazlalığı nedeniyle bilimsel çalışmalara yeterince zaman ayıramaması*" riski kurum performansı üzerinde bileşik bir risk baskısı oluşturacaktır. Örgütün kurum çapında strateji ve iş hedeflerini doğrudan etkileyebilecek bu tipik risk için geliştirebileceği portföy bakışı için önerilen kontrol faaliyeti (stratejisi); "*Ders yükü planlamasının tüm öğretim üyeleri / elemanları arasında eşit dağılımının sağlanması, öğretim elemanı talebinin yapılması"* olmuştur.

Şekil 3. Risk Profili ve Performans



Kaynak: Phinicharomna, 2018, i

2.4. COSO 2017 Kurumsal Risk Yönetimi-Gözden Geçirme ve Revizyon Bileşeni

Kurum performansı incelendiğinde, örgütün risk yönetimi bileşenlerinin zaman içinde ve önemli değişiklikler ışığında ne kadar iyi işlediği ve hangi revizyonlara ihtiyaç duyduğu değerlendirebilir (COSO, 2017: 6). Risk yönetimi "tek ve bitmiş" bir etkinlik değildir. Hem bireysel risklerin hem de Kurumsal Risk Yönetimi sürecinin genel olarak devam eden, yeniden gözden geçirilmesi ve revize edilmesini gerektiren dinamik bir süreçtir. Örgütün birçok sisteminde, bir kurumun iç kontrol ve risk yönetimi sürecinin etkinliğinin izlenmesi için bir düzenleme (örneğin bir yönerge) gereklidir (ERM, 2018: 111). Dördüncü sarmal üç demet bileşene sahiptir.

2.4.1. Önemli Değişimi Değerlendirir

Eğer yöneticiler, örgüt çevresinde önemli bir değişiklik olduğu düşünüldüğünde, yönetim modellerinde önemli değişiklikler yapamazsa, örgütsel gerileme ortaya çıkabilir Artık uygun olmayan bu yönetim modelleri, yöneticilerin problemleri algılamasını engelleyebilir, stratejide yapılması gereken değişiklikleri geciktirebilir ve yeni bir iş ortamında etkisiz olan örgütsel eylemlere yol açabilir (Barr vd., 1992: 18). Bu nedenle örgüt, stratejisini ve iş hedeflerini önemli bir biçimde etkileyen / etkileyebilecek değişimleri belirler, analiz eder ve değerlendirir. E ve F Fakülteleri ile D ve E Yüksekokullarında "*Karma*" risk kategorisinde "Çok *Yüksek*" risk değerlendirmesine sahip "*Akademik ve idari personelin emeklerinin karşılığını zamanında almamaları, kurumsal şikâyetlerin artması*" riski örgüt bünyesinde önemli bir değişim ihtiyacını göstermekte ve örgüt sosyolojisinin strateji ve iş hedeflerini etkileme potansiyelini yansıtmaktadır.

2.4.2. Riski ve Performansı Gözden Geçirir

Risk yöneticileri, kurumdaki riskleri ve bu risklere verilen yanıtları ölçmek ve incelemek için genellikle bir ölçüm kartı[4] kullanırlar. Bir ölçüm kartı, yönetime risk yönetiminin etkinliği hakkında bilgi vermek ve kurumun risk profilinin revizyonunun, değerlendirmesinin veya risk yanıtının gerekip gerekmediğini belirlemek için tasarlanmıştır. ÇSY[5] (çevresel, sosyal ve yönetişim) ile ilgili risklerin gözden geçirilmesi ve revize edilmesi genellikle risk sahipleri ve sürdürülebilirlik yöneticileri tarafından gerçekleştirilir. Örgütün risk sahipleri, risk performansının gözden geçirilmesinden, risklerin gözden geçirilmesinden ve performansın izlenmesi için göstergeler geliştirmekten sorumludurlar (ERM, 2018: 112). Örgüt, kurum bünyesinde riski ve performans sonuçlarını gözden geçirir ve buna bağlı bir değerlendirme yapar. G Fakültesi'nde "*Operasyonel ve Yasal*" risk kategorisinde "*Yüksek*" risk değerlendirmesine sahip "Öğrencilerin mezun oldukları bölümle ilgili mesleklerini yapabilecekleri bir iş bulamaması" kurum için temel bir performans sonuç riskini ifade etmektedir. Örgütün etkin performansı için önerilen kontrol faaliyeti (stratejisi); "İlgili bölümler için kontenjanın dar tutulması ve ikinci öğretim yapılmaması" olmuştur.

2.4.3. Kurumsal Risk Yönetimindeki İyileştirmeyi İzler

Kurumlar, Kurumsal Risk Yönetimin olgunluğunu izlemeli ve risk ve uyum konusundaki tepkilerini geliştirmelidir (Abrams vd., 2007: 222). Örgüt, Kurumsal Risk Yönetimindeki iyileştirmeleri sistematik olarak izler. D ve G Fakültelerinde "*Yasal / Uygunluk*" risk kategorisinde "*Yüksek*" risk değerlendirmesine sahip "Öğrencilerin sınav esnasındaki sorumluluklarını bilmemeleri nedeniyle sınav düzenine uygun olmayan davranışlar sergilemeleri" riski örgütün, Kurumsal Risk Yönetiminde takip etmesi gereken temel bir risk öğesidir. Bu konuda yapılan veya yapılabilecek iyileştirmelere sistematik olarak izlemelidir. Sistematik izleme için önerilen kontrol faaliyeti (stratejisi); "*Sınavda uyulması gereken kuralların yazılı hale getirilerek sınav salon kapılarına asılmasının sağlanması*" olmuştur.

2.5. COSO 2017 Kurumsal Risk Yönetimi-Bilgi, İletişim ve Raporlama Bileşeni

Kurumsal Risk Yönetiminin, örgüt içinde yukarıdan aşağıya doğru akan iç ve dış kaynaklardan gerek-

4) scorecard
5) environmental, social and governance (ESG)

li bilgileri elde etme ve paylaşma konusunda sürekli bir sürece ihtiyacı vardır (COSO, 2017: 6). Kurumsal Risk Yönetimi sürecinin son aşaması, risk bilgilerinin paydaşlara iletilmesi ve raporlanmasıdır. Risk bilgisi, hem iç hem de dış paydaşlar tarafından yapılan birçok stratejik, operasyonel, yatırım veya satın alma kararının bir girdisi olarak hizmet eder. Kurumlar hedef kitlelere zamanında, ilgili ve kaliteli bilgi sağlamak için mevcut iletişim kanallarından faydalanmalıdır (ERM, 2018: 123). Bu son sarmal üç demet bileşene sahiptir.

2.5.1. Bilgi ve Teknolojiden Yararlanır

Bilgi Teknolojisinin (BT) kurum değerini yaratmadaki rolü verimlilik kavramıyla değerlendirilmektedir. Bilgi ve teknolojiden yararlanarak iş süreçlerine, kurumsal uygulamalara ve örgütsel yapılardaki gelişmelere yön verilmekte ve maddi olmayan bilgi teknolojisinin örgütsel faydaları ön plana çıkmaktadır. BT'nin yönetilmesi, örgüt için bir benzersizlik yaratabilecek ve kurumlara rekabet avantajı sağlayabilecek bir yetenek olduğu ağırlık kazanan bir görüştür (Bhatt ve Grover: 2005, 254-255). Örgüt, Kurumsal Risk Yönetimine destek sağlamak için, kurumun mevcut bilgi sistemlerinin sunduğu olanaklardan yararlanır. D Fakültesi'nde "*Stratejik*" risk kategorisinde "*Yüksek*" risk değerlendirmesine sahip "*Akademik personelin değişim programları hakkında yeterli bilgi sahibi olmaması nedeniyle öğrencilere değişim programları konusunda yeterli danışmanlık hizmeti sunamaması*" riski örgütün, Kurumsal Risk Yönetiminde bilgi teknolojisini kullanarak yönetebileceği bir riski göstermektedir. Bilişim teknolojisinin sunduğu kontrol faaliyeti (stratejisi); "*Erasmus ve Farabi komisyonları tarafından öğretim elemanlarına bilgilendirme maili atılması"* olmuştur.

2.5.2. Risk Bilgisinin İletişimi Yapılır

Daha büyük büyüme fırsatlarına sahip kurumlar, daha fazla belirsizlikle karşı karşıyadır ve sadece ortaya çıkan riskleri kontrol etmek için değil aynı zamanda çeşitli fırsatların kurum çapında risk üzerindeki etkisine bağlı olarak büyümeyi en iyi yönde yönlendirmek için daha iyi risk yönetimi gerektirmektedir. Bu kurumların Kurumsal Risk Yönetimine yatırım yapma konusunda daha fazla teşvikleri vardır ve bir risk yöneticisi[6] ataması daha olasıdır. Risk yöneticisi bir kurumu tehdit edebilecek olayları tanımlayan ve bunları hafifleten bir yöneticidir. Risk yöneticisinin rolünün önemli bir parçası, risk yönetiminin hedeflerini ve stratejilerini dış paydaşlara iletişimini yapmaktır (Liebenberg ve Hoyt, 2003: 43-44). Örgüt, Kurumsal Risk Yönetimine destek sağlamak için, çeşitli iletişim kanallarını kullanır. H Fakültesi'nde "*Operasyonel*" risk kategorisinde "*Orta*" risk değerlendirmesine sahip "İdari görevi bulunan personelin yıllık izin, sağlık problemi vs. gibi sebeplerle bulunamaması ve bu yüzden fakülte kurullarının işlevlerini yerine getirememesi ile hak kayıpları yaşanması", örgütün Kurumsal Risk Yönetimini desteklemek için, iletişim kanallarını kullanılarak yönetebileceği bir riski göstermektedir. İletişim kanalının sunabileceği kontrol faaliyeti (stratejisi); "*Vekalet sisteminin etkin işletilmesi, personel arasında etkin iletişim ağı kurulması"* olmuştur.

2.5.3. Risk, Kültür ve Performans Hakkında Raporlama Yapar

Yönetim Kurulu (Yönetim), karar alma ve yönetim faaliyetleri ile görevlendirilmiş üst yönetici ile kurumun uzun vadeli başarısından nihai olarak sorumludur. Üst yönetici bu sorumluluğu risk yönetiminin operasyonel faaliyetlerini yerine getiren yönetim komuta zincirindeki kurum yöneticilerine delege eder. Etkin yönetişim için yönetim kurulunun komitelerinden (yönetimin ilgili birimlerinden) etkili raporlama hatları oluşturulması gerekir (ERM, 2018: 22). Örgüt, kurum bünyesinde çeşitli seviye ve kademelerde, risk, yönetişim, kültür ve performans konularında raporlama yapar. F Yüksekokul'unda "*Stratejik*" risk kategorisinde "Çok Yüksek" risk değerlendirmesine sahip "*Kurumsallaşmaya yönelik çalışmaları arttıramamak*" ifadesi doğrudan örgütün risk, kültür ve performansını etkilemektedir. Yapılacak olan raporlamada önerilen kontrol faaliyeti (stratejisi); "*Kurum Kültürü Geliştirmek"* olmuştur.

---

6) Chief Risk Officer (CRO)

Kurumun faaliyet gösterdiği sektör ve büyüklüğünden bağımsız olarak kurum genelinde yürütülmek istenen bir Kurumsal Risk Yönetimi çalışmasında Kontrol Öz Değerlendirme yaklaşımı bir pusula görevi görecektir. Kurumların hedeflerine ulaşmasında etkin ve verimli iş süreçlerinin oluşturulması, çalışanların kontrolleri ve riskleri nasıl değerlendireceklerinin öğrendiği / öğrettiği ve dolayısıyla kurum yönetiminin ve yöneticilerinin problemlerin kök nedenlerine ulaşabileceği bir yaklaşım sunan Kontrol Öz Değerlendirme kavramı bir sonraki başlık altında değerlendirilmiştir.

3. KONTROL ÖZ DEĞERLENDİRME

Tehlikelere ve risklere maruz kalmak kurumları etkilemekte, hatta bunlardan bazıları kritik iş hedeflerine ulaşma yeteneğini önemli ölçüde etkilemekte ve kurumların sürdürülebilirliğini tehlikeye atmaktadır. Bir kurum için belirsizlik yaratan bu risklerin birçoğu bilinmeyen veya niteliksiz özelliktedir (Lyon ve Hollcroft, 2012: 28). Belirsizlik, bir kuruma iş hedeflerini karşılama açısından yüksek bir maliyete sahiptir. Belirsizliği azaltabilen kurumlar, riski ortadan kaldırarak veya azaltarak amaçlarına ve hedeflerine ulaşmak için daha iyi kararlar alabilecektir (Lyon ve Popov, 2016: 40). Risk değerlendirmesi, bir kurumun risklerini değerlendirmek için kullanılan önemli ve karmaşık bir süreçtir ve böylece riskleri kabul edilebilir bir düzeye indirebilir ve azaltabilir (Lyon ve Hollcroft: 28). Etkin bir risk değerlendirme ve risk yönetimi eyleminin verimli bir şekilde işlemesi ve hedeflenilen sonuçları vermesi için risk yönetimi faaliyetlerine gerekli destek ve katılım gösterilmelidir. Bu anlayış için yapısal bir döngü ihtiyacı vardır. Risklerin belirlenmesi, değerlendirilmesi, önceliklendirilmesi ve bunlara bağlı olarak yönetim-izleme sisteminin kurulması gerekmektedir. Bu yapısal döngünün işlevsel bir Kurumsal Risk Yönetimine evrilmesi için kurum bünyesinde uygulanabilir ve sürdürülebilir etkin bir araç setine ihtiyaç vardır. Günümüzde bahsedilen bu araç seti için kurumlarda Kontrol Öz Değerlendirme anlayışı ön plana çıkmaktadır.

Kontrol Öz Değerlendirme, iç kontrol etkinliğini ve iş süreçlerini değerlendirmek için bir araç olarak ilk olarak 1987 yılında Gulf Canada Resources Ltd. firmasının iç denetçiler ekibi tarafından geliştirilmiştir. O zamanlarda, Gulf Canada, hem şirket iç kontrollerini hem de geleneksel denetim değerlendirmeleri yoluyla petrol ve gaz ölçüm konularını çözme konusunda bazı güçlükleri rapor etmesini isteyen bir yasal zorunlulukla karşı karşıya kalmıştır. Gulf Canada'nın iç denetim grubu, iç kontrol sorunları veya süreçleri ile ilgili görüşmeler ve tartışmalar için yönetim ve personel toplanmasını içeren kolaylaştırılmış bir toplantı öz değerlendirme yaklaşımını başlattı. Süreç, resmi olmayan ya da yumuşak kontrollerin yanı sıra muhasebe bakiyeleri gibi daha geleneksel sabit kontrolleri değerlendiren bir mekanizma olan Kontrol Öz Değerlendirme haline gelmiştir (Moeller, 2015: 296).

İç Denetçiler, yumuşak kontrol zayıflıklarından kaynaklanan riskleri tespit etmeye çalışırken, iç denetimin tarafsızlığını bozmadan risklerin tanımlanmasını ve değerlendirilmesini kolaylaştırmak için Kontrol Öz Değerlendirmesini kullanabilirler. Kontrol Öz Değerlendirme süreçlerinin sağlamlığı, yalnızca bu riskleri ele almak için güçlü bir araç sağlamakla kalmaz, aynı zamanda iç denetim kaynaklarının gereksiz yere tükenmesine sebep olabilecek denetim bulgularının tekrarlanma olasılığını azaltmaya da yardımcı olabilir (Sadu, 2017: 58).

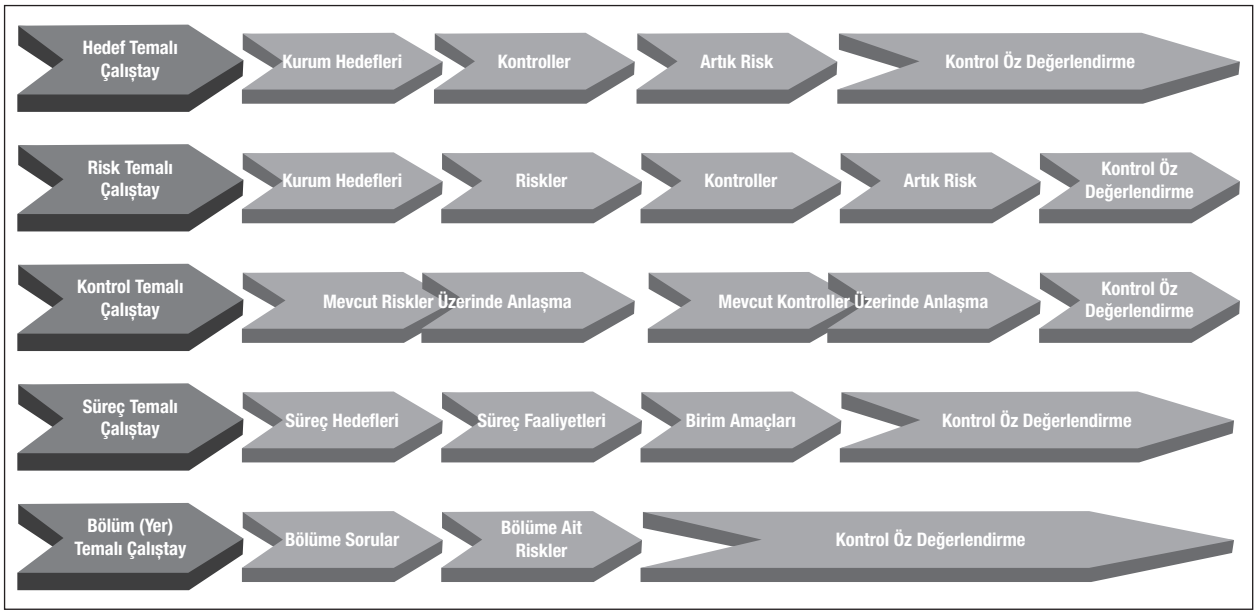
Kontrol Öz Değerlendirme yöntemi literatürde bazen Kontrol Risk Öz Değerlendirme (Control Risk Self-Assessment, CRSA) veya Risk Kontrol Öz Değerlendirme (Risk Control Self-Assessment, RCSA) olarak da anılmaktadır. Kontrol Öz Değerlendirme temel olarak iş hedeflerini gözden geçirme, hedefe ulaşmada engel olan riskler ile bu riskleri yönetmek için tasarlanmış kontrolleri değerlendiren bir anlayıştır ve bunu sağlamak için üç temel yöntemden yararlanmaktadır (Hubbard, 2000):

- Çalıştaylar,
- Anketler,
- Yönetim Özel Analizleri

3.1. Çalıştaylar Şeklinde Yapılan Kontrol Öz Değerlendirme Faaliyetleri

Çalıştaylar yöntemi beş farklı temaya (Şekil 4) dayanabilen ve ekiplerin Kontrol Öz Değerlendirme prosedürlerini yürütmek için oluşturulduğu basitleştirilmiş bir tekniktir.

Şekil 4. Kontrol Öz Değerlendirme Çalıştay Temaları



Kaynak: KİDDER, 2014: 63 kullanılarak yazarlar tarafından yeniden üretilmiştir.

Bu ekibin koordinasyonu iç denetim tarafından yürütülmektedir. Ekip, İç Denetim Departmanının iki üyesine ek olarak, biri koordinatör, diğeri ise takımın kabul ettiği bir yazıcı olmak üzere 6-15 arasında değişen kişiden oluşmaktadır. (Touam, 2016: 18).

3.1.1. Hedef Temalı Çalıştaylar

Bu çalıştaylar, doğru finansal raporlama gibi bir iş hedefine ulaşmanın en iyi yoluna odaklanmaktadır. Çalıştay, sistem hedeflerini desteklemek için mevcut kontrolleri tanımlayan ekiple başlar ve daha sonra kontroller çalışmadığı takdirde kalan riskleri belirler. Bu çalıştay formatının amacı, kontrol prosedürlerinin etkin bir şekilde çalışıp çalışmadığını ve kalan risklerin kabul edilebilir düzeyde olup olmadığına karar vermektir. Bu tür bir çalışma, aşağıda örneklenen kontrol ortamındaki bu alanları vurgulayarak kolaylaştırıcı tarafından katılımcılardan gruplarının kontrol ortamlarını belirlemelerini isteyerek başlayabilir (Moeller, 2015: 300):

- Kurumun kontrol bilinci
- Çalışanların doğru olanı yapmaya ne derece bağlı olduğu veya bunu ne ölçüde yapacağı
- Teknik yeterliliği ve etik bağlılığı kapsayan çok çeşitli faktörler
- Etkili iç kontrol için çoğunlukla gerekli olan somut olmayan faktörler

3.1.2. Risk Temalı Çalıştaylar

Bu çalıştaylar, iç kontrol hedeflerine ulaşmak için riskleri listeleyen Kontrol Öz Değerlendirme ekiplerine odaklanmaktadır. Çalıştay, bir hedefe ulaşmayı engelleyebilecek tüm bariyerleri, engelleri, tehditleri ve riskleri listeleyerek ve ardından belirlenen herhangi bir kilit riski yönetmek için yeterli olup olmadığını belirlemek için kontrol prosedürlerini inceleyerek başlar. Çalıştayın amacı önemli kalıntı risklerini belirlemektir. Bu format, çalışma ekibini gözden geçirilen öğeyi çevreleyen tüm hedefler, riskler ve denetimler kümesi aracılığıyla alır. Çalışma, ekiplerden risklerini aşağıdaki gibi sorularla sormaları istendiği risk temelli tartışmalarla devam eder (Moeller, 2015: 300-301):

- Ne yanlış gidebilir?
- Varlıklarımızı korumak için hangi araçlara ihtiyacımız var?
- Kuruma ait bir varlık bizden nasıl çalınabilir?
- En büyük yasal açmazımız nedir?

Çalışma sırasında yapılan oturumlarda bölüm, aktivite veya süreç seviyelerindeki önemli riskler tespit edilmeye çalışılır. Çalışma ekipleri, belirlenen her risk için meydana gelme olasılığı ve potansiyel etkiyi tartışmalıdır. Risk için, makul bir olasılığa sahip olma ve büyük bir potansiyel etki önemli bir faktör olarak tanımlanacaktır (Moeller, 2015: 301):

3.1.3. Kontrol Temalı Çalıştaylar

Bu çalıştaylar, yerinde kontrollerin ne kadar iyi çalıştığına odaklanır. Bu format, önceki iki çalıştaydan farklıdır. Çünkü kolaylaştırıcı, çalıştayın başlangıcından önce önemli riskleri ve kontrolleri tanımlamaktadır. Kontrol Öz Değerlendirme çalıştayı sırasında, çalışma ekibi kontrollerin riskleri ne kadar azalttığını ve hedeflere ulaşılmasını teşvik ettiğini değerlendirir. Çalıştayın amacı, kontrollerin nasıl çalıştığı ve yönetimin bu kontrollerin nasıl çalışmasını beklediği arasındaki farkın analizini yapmaktır (Moeller, 2015: 301).

3.1.4. Süreç (Proses) Temalı Çalıştaylar

Bu çalıştaylar, bir süreçler zincirinin öğeleri olan seçilmiş etkinliklere odaklanır. Süreçler, satın alma, ürün geliştirme veya gelir oluşturma gibi çeşitli adımlar içeren bir başlangıç noktası ile başlayan bir dizi ilgili faaliyet ile devam edip sona eren bir faaliyet zinciridir. Bu tip bir çalıştaylar genellikle tüm sürecin hedeflerinin ve çeşitli ara adımlarının tanımlanmasını kapsar. Çalıştayın amacı tüm süreci ve bileşen faaliyetlerini değerlendirmek, güncellemek, doğrulamak, iyileştirmek ve hatta hızlandırmaktır. Çalıştay formatı, süreç içinde birçok hedefi kapsayarak, yeniden yapılanma, kalite iyileştirme ve sürekli iyileştirme girişimleri gibi eş zamanlı yönetim çabalarını destekleyerek, kontrol temelli bir yaklaşımdan çok daha geniş bir analize sahip olabilir (Moeller, 2015: 301).

3.1.5. Bölüm (Yer) Temalı Çalıştaylar

Bu çalıştaylar, her bir iş merkezinin (bölümlerinin) ayrı ayrı ele alındığı basitleştirilmiş bir tekniktir. Çalıştay aracılığıyla, her bir iş merkezine iki soru sorulur ve cevaplandırılması gerekir (Touam, 2016: 19-20):

- Soru 1: Hedeflere ulaşılmasına katkıda bulunan faktörler nelerdir?
- Soru 2: Hedeflere ulaşmanın önünde duran engeller nelerdir?

Kolaylaştırıcı daha sonra bu sorulara verilen cevapları toplar ve özetlemesini yapar. Önemli engeller ele alınarak, olası çözümlere ulaşmak için çalıştay çalışmaları sırasında bunlar tartışılır (Touam, 2016: 20).

3.2. Anketler Şeklinde Yapılan Kontrol Öz Değerlendirme Faaliyetleri

Kontrol Öz Değerlendirme çalışmalarında genellikle çalıştaylar yöntemi, iç kontrol, risk ve süreç temalı olup olmamasına bağlı olmaksızın zaman alıcı ve zor olabilmektedir. Bu gibi birçok durumda bir anket yöntemi iç kontrol başta olmak üzere bilgilere ulaşmanın etkili bir yolu olmaktadır. Bunun için çalışma yapılacak ilgili süreci veya sistemi kapsayan bir anket hazırlanır ve daha sonra ilgili alandaki risk ve kontrollerin anlaşılması için seçilmiş bir paydaş grubuna dağıtılır. Anketler, odak gruplardan çıkacak olan keşif tipi (bulgu türünde) yorumlar vermeyecektir, ancak süreçlerin ve iç kontrollerin sağlamlığının genel bir değerlendirmesini verecektir. Bu temel yapı, Kontrol Öz değerlendirme sürecinde gerekli olan arka plan verilerini toplamak için etkili bir yoldur (Moeller, 2015: 302-303).

Anketler yöntemi, bir dizi evet-hayır sorusu içeren bir anket tasarlama yoluyla Kontrol Öz Değerlendirmenin yapılmasına dayanmaktadır. Anketin sonuçları daha sonra iç kontrolün gerekli değerlendirmesine ulaşmak için analiz edilir. Bu teknik tercihen aşağıdaki durumlarda kullanılır (Touam, 2016: 20):

- Örgütün kültürü açık diyaloğa dayanmadığında ekip üyeleri arasındaki çalıştaylarda yapılacak tartışmalar güvenilirlikten yoksun kalacaktır. Üyelerin kendilerine karşı alınabilecek herhangi bir idari yaptırımdan korkmaları nedeniyle, bu yöntem tercih edilir.
- Kontrol Öz Değerlendirme kapsamı geniş ve hızlı bilgi gerektirdiğinde büyük ölçekli kurumlarda çalıştay yapmak kolay bir yol olmayacaktır.
- İç Denetçiler çalıştaylar için koordinatör olarak

çalışmak için gerekli uzmanlık ve beceriden yoksun olduklarında, anket iyi bir çözüm olacaktır.
- Kurumlar zaman duyarlı olduğunda, çalıştaylara çok fazla zaman ayırmak istemeyeceklerdir.

Daha güvenilir sonuçlar elde etmek için ankete katılanların isimlerinin açıklanmasının tercih edilmeyeceği belirtilmelidir. Bu yöntemin en önemli avantajlarından biri geniş kapsama sahip olmasıdır. Aynı zamanda anketi cevaplayacak ilgili kişilerden az bir zaman istemekte ve çok fazla bir çaba veya toplantı / koordinasyon becerileri gerektirmemektedir. Bu yöntemin temel eksiklikleri ise, özellikle herhangi bir takip yokken, katılımcıların ciddiyet eksikliğini içermesidir. Anketleri yanıtlama oranı düşük olabilmekte ve verilen cevaplar bağlamında anketin hedeflediği soruların açıklığa kavuşturulması şansı düşük olabilmektedir (Touam, 2016: 20).

3.3. Yönetim Özel Analizleri Şeklinde Yapılan Kontrol Öz Değerlendirme Faaliyetleri

Çalıştay veya anket yöntemlerine bir diğer alternatif yöntem, kurum yönetimi tarafından üretilen özel yönetici analizleri, bir iç denetçinin gerçekleştirdiği denetim işlevine benzer bir yöntem olarak değerlendirilmektedir (Moeller, 2015: 303).

Bu yöntemde yönetim örgüt geneli için bir çalışma üretmektedir. Kontrol Öz Değerlendirme konusunda yetkin bir çalışan veya genellikle bir iç denetçi, kurum yönetimi için bu çalışmalarla yönetim çalışanları ve konuya hakim personelden gerekli verileri toplayıp bunların birleştirmesini yapmaktadır. Birleştirilen ve konsolide edilen bu veriler ışığında Kontrol Öz Değerlendirme görevlisi süreç sahiplerinin kullanmaları için bir analiz geliştirmektedir.

Yönetim özel analizleri yöntemi, yönetimin kontrol durumu hakkında bilgi sağlandığı analizleri içerir. Bu yöntem, üçüncü bir Kontrol Öz Değerlendirme Yöntemi olarak en az kullanılan yöntemdir ve aşağıdakiler dahil olmak üzere bazı durumlarda kullanılır (Touam, 2016: 20):

- İç kontrol prosedürleri hakkında görüş bildirmek için yönetim tarafından geliştirilen anketler.
- Dış denetçiler tarafında istenilen yıllık raporları hazırlamak için kurum finans sorumluları arasında yapılan görüşmeler.
- Bir dolandırıcılığın nedenini ya da belli bir kontrolün başarısızlığını keşfetmek için yürütülen soruşturmalar.
- Yeni geliştirilen sistemlerde iç kontrol uygulamalarının değerlendirilmesi.

Yönetim özel analizleri her ne kadar İç Denetçiler Enstitüsü (The Institute of Internal Auditors, IIA) tarafından önerilen üç yöntemden biri olsa da, tipik bir kurum için yerine getirilmesi oldukça zor bir yöntem olarak görülmektedir. Kurumdaki bir çalışan tarafından neredeyse "akademik" bir inceleme yapılmasını ve buna müteakip analizler için bazı karşılaştırmalı araştırmalar izlemesi önerilmektedir. İç Denetçiler Enstitüsü, burada ele alınan tüm yöntemlerin kurumun kontrol yapısını güçlendirdiğine inanmaktadır. Kurum yukarıda anılan üç yöntem içinden en uygun olanı tercih edebilmek adına her örgüt kendi SWOT (güçlü ve zayıf yönler, fırsat ve tehdit durumları) analizini yaparak, buna göre bir değerlendirme seçimi yapmalıdır. Birçok Kontrol Öz Değerlendirme kullanıcısı, ihtiyaçlarını en iyi şekilde karşılamak için belirli bir çalıştay temasından yararlanmakta veya birbirinden farklı birkaç formatı birleştirerek kullanabilmektedir (Moeller, 2015: 303).

3.4. Kontrol Öz Değerlendirme Stratejisi

Kurumların risklerini etkin bir biçimde yöneterek hedeflerine ulaşmaları için, yönetişim ve kültür bileşeninin diğer bileşenler üzerinde yönlendirici bir etkisi vardır. Kurumların risklere karşı aksiyon üretme ve hedeflerine ulaşabilme kabiliyeti, yönetişim ve kültür ile performans bileşenlerini kurum içerisinde kurabilmesi ve işletebilmesi ile doğrudan ilgilidir. Kurumların iç kontrolünün kurulumunda Kontrol Öz Değerlendirme yaklaşımı çalışan, iç denetçi ve kurum arasında enerjik bir işbirliği sağlama potansiyeline sahiptir.

COSO iç kontrol modelinin yapısı birbirinden bağımsız olmayan zincir halkaları örneği gibi iç içe geçmiş beş bileşenden oluşmaktadır (Türedi ve Karakaya, 2015: 69). Bunlar;

- Kontrol Ortamı (Control Environment),
- Risk Değerleme (Risk Assessment),
- Kontrol Faaliyetleri (Control Activities),

- Bilgi ve İletişim (Information and Communication),
- İzleme / Gözlem (Monitoring)

olmak üzere beş bileşenden oluşmaktadır.

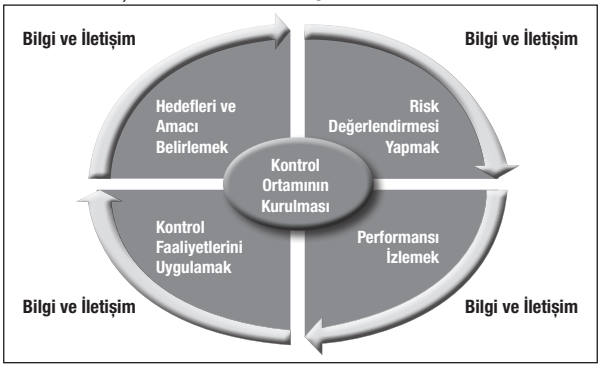
Kıral ve Hatipoğlu (2017: 126) Kontrol Öz Değerlendirmenin, Strateji Geliştirme Birimlerinin (SGB) kurumlarındaki diğer birimlere iç kontrol sisteminin geliştirilmesine destek olma konusunda kullanabileceği önemli bir araç olarak ifade etmektedir. Bu nedenle, SGB'lerin bu aşamada üstlenebilecekleri rol ve görevlerin netleştirilmesi kamu idarelerinde etkili bir iç kontrol ve risk yönetimi sisteminin hayata geçirilmesi bakımından önem kazanmaktadır. Bu kapsamda, SGB'lerin kontrol öz değerlendirme yaklaşımının risk yönetiminde uygulanması kapsamında üstlenebilecekleri ilk görev şüphesiz bilgilendirme görevi olacaktır.

Etkin bir iç kontrol ortamının kuruluşundan sonra ikinci sırada risk değerlemesi bileşeni gelmektedir. En genel ifadeyle risk değerlendirme, örgütlerin amaçlarına ulaşılırken karşılaşılabilecek risklerin tanımlanıp, değerlendirmesi ve bu risklerin nasıl yönetilmesi gerektiğine karar vermek için bir temel oluşturulmasıdır. Söz konusu risklerin tespiti adına yapılması gereken işlem, kurumların amaç ve hedeflerinin belirlenmesidir. Çünkü riskler bu hedeflere ulaşma noktasında kurumların karşısına çıkan bir durumdur (Türedi ve Karakaya, 2015: 75).

Kontrol Öz Değerlendirme, bir kurumdaki bölümlerin kendi iç kontrollerini değerlendirmelerine yardımcı olmak için tasarlanmış bir süreçtir. Birçok açıdan Kontrol Öz Değerlendirme yaklaşımı, yukarıda ikinci bölümde tartışıldığı gibi COSO çerçevesinde bulunan aynı kavramların bir kısmını kullanmaktadır. Kontrol Öz Değerlendirme modeli, bir kurumun etkili bir kontrol ortamına sahip olmak için güçlü kontrol hedefleri ve kontrol faaliyetlerini gerçekleştirmesi gerektiğini söylemektedir. Bu iki unsur iyi bir bilgi ve iletişim sistemi ile risk değerlendirme süreçleri ve performansın izlenmesiyle çevrelenmiştir (Moeller, 2015: 296-297). Belirtilen Kontrol Öz Değerlendirme modeli, Şekil 5'de gösterilmiştir

Kontrol Öz Değerlendirme, bir kalite geliştirme sisteminde açıklanan ve kullanılan yöntemlere benzer sürekli bir iyileştirme sürecidir. Sistemin kurulumu için öncelikle kontroller ile ilgili hedef ve hedefler belirlenerek, kontrol ortamının oluşturulup iyileştirilmesi için bir ekip kurulumu yapılır. Ardından belirlenen kontrol risklerini daha iyi anlamak için bir risk değerlendirmesi yapılır ve belirlenen riskleri azaltmak için kontrol faaliyetleri uygulamaya sokulur. Daha sonra bu geliştirilmiş kontrollerin performansı izlenir. Bu süreç, Kontrol Öz Değerlendirme ekibinin Şekil 5'de görülen Kontrol Öz Değerlendirme Sürecinin herhangi bir çeyreğinde başlayabileceği ve daha sonra bir sonraki aşamaya saat yönünde ilerleyebileceği sürekli bir süreçtir (Moeller, 2015: 297). Bu sürecin kurum genelinde etkin ve verimli işlemesi için temel bir **strateji akışına** ihtiyaç vardır.

Şekil 5. Kontrol Öz Değerlendirme Süreci



Kaynak: Moeller, 2015: 297 kullanılarak yazarlar tarafından yeniden üretilmiştir.

Aşağıda, Kontrol Öz Değerlendirmenin oluşturulmasında göz önünde bulundurulabilecek uzmanlık ve tecrübe ile seçilen önemli yedi adet strateji yer almaktadır (Hubbard, 2000):

- **Birinci Strateji:** Tüm iç denetçilerin eğitilmesi, daha sonra bu iç denetçilerden bir kısmına çalıştay koordinasyon yöntemleri üzerine eğitim verilmesi ve yapılacak olan ilk iki çalıştayı yönetmek için danışman / danışmanlar tutulması.
- **İkinci Strateji:** Bir pilot çalıştayın planlanması ve yönetilmesi için danışman / danışmanların işe alınması ve daha sonra kontrol ve çalıştay koordinasyon yöntemlerinin ana kavramları üzerine ikincil bir iç denetçi grubunun eğitimi.
- **Üçüncü Strateji:** Bilgisayar ve yazılımların satın alınması ve bu teknolojileri kullanmak için bir pilot çalıştay çalışması yapılması.

- **Dördüncü Strateji:** Tüm iç denetçilerin eğitilmesi, daha sonra bu iç denetçilerden bir kısmına çalıştay koordinasyon yöntemleri üzerine eğitim verilmesi ve ardından denetçilerin İç Denetim Birimi aracılığıyla çalıştayları yönetmesi için bu denetçilerin görevlendirilmesi.
- **Beşinci Strateji:** Kontrol Öz Değerlendirme ve koordinasyon becerileri ile ilgili temel kavramları içeren bir eğitim programına kurumdan belirli bir çalışanı gönderme ve daha sonra öz değerlendirme pilot çalıştaylarını yönetmesi için bu çalışanın görevlendirilmesi.
- **Altıncı Strateji:** Tüm iç denetçilerin eğitilmesi, daha sonra bu iç denetçilerden bir kısmına çalıştay koordinasyon yöntemleri üzerine eğitim verilmesi ve Kontrol Öz Değerlendirme çalıştayları düzenleyebilmesi için bu denetçileri eğitmek üzere danışman / danışmanlardan faydalanılması.
- **Yedinci Strateji:** Kontrol Öz Değerlendirme ve koordinasyon becerileri ile ilgili temel kavramları içeren bir eğitim programına kurumdan belirli bir çalışanı gönderme ve daha sonra bu çalışanın, bir çalıştay aracılığıyla, güncel olarak gerçekleştirilen son iki denetimin verilerini toplaması ve sonrasında Kontrol Öz Değerlendirme için bir pilot çalıştayı yönetmesi.

Kontrol Öz Değerlendirme, bazıları için COSO iç kontrol çerçevesinden veya COBIT[7] (Bilgi ve İlgili Teknoloji İçin Kontrol Hedefleri) modelinden daha kolay görülebilecek bir kontrol değerlendirme sürecidir. Konusunda uzman bazı çalışanlar bir COSO iç kontrol risk değerlendirme sürecine, çok yüksek düzeyde ve anlaşılması zor bir süreç olarak bakarken, Kontrol Öz Değerlendirme bir kurumdaki münferit bölümlerin kolaylaştırılmış bir grup biçiminde resmi olarak bir araya gelebildiği ve bireysel bölümleri veya işlevleri içindeki riskleri ve iç kontrolleri değerlendirebileceği bir yaklaşım özelliği taşımaktadır (Moeller, 2015: 297).

Kontrol Öz Değerlendirme bir model olarak, sistemin iş hedeflerini karşılayıp karşılamadığını belirlemek için iç kontrolün incelenmesini ve değerlendirilmesini yönetim ve süreç sahiplerine aktarır (McNally, 2007). Kontrol Öz Değerlendirme çeşitli yollarla uygulanabilir, ancak ayırt edici özelliği, risk değerlendirmelerinin ve iç kontrol değerlendirmelerinin, değerlendirilmekte olan alanda çalışan operasyonel çalışanlar veya hat yöneticileri tarafından yapılmasıdır (Joseph ve Engle, 2005). Çalışmanın bir sonraki bölümünde Düzce Üniversitesi bünyesinde risk temalı olarak gerçekleştirilen bir Kontrol Öz Değerlendirme faaliyeti olan Çalıştayın aşamaları ve sonuçları paylaşılacaktır.

Kaynakça

Yazının ikinci kısmıyla birlikte sonraki sayıda yer verilecektir.

7) Control Objectives for Information and Related Technology