COSO 2017 KURUMSAL RİSK YÖNETİMİ ÇERÇEVESİNE KONTROL ÖZ DEĞERLENDİRME YAKLAŞIMIYLA BAKIŞ VE BİR KURUM UYGULAMASI-II[1]

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

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, h edef 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*

1) Yazının 1. kısmı Denetişim Dergisinin 18. sayısında yayımlanmıştır.

*) İç Denetçi (CGAP), Düzce Üniversitesi, Orcid: 0000-0001-8439-9511, alptugguler@duzce.edu.tr

**) İç Denetçi (CGAP,CCSA), Düzce Üniversitesi, Orcid: 0000-0002-6826-0998, aliarkin@duzce.edu.tr

Yazı Gönderim Tarihi: 19.10.2018, Yazı Kabul Tarihi:31.10.2018

4. BİR UYGULAMA ÖRNEĞİ OLARAK DÜZCE ÜNİVERSİTESİ RİSK BELİRLEME ÇALIŞTAYI

Kurum çapında risk yönetimi süreçleri üzerinde üst yönetiminin liderliğinin olmaması, risk yönetimi değerlendirmelerinde ve iş birimlerinde risklere verilmesi gereken yanıtlarda kültürel farklılıklara ve kurum genelinde risk yönetimi uygulamalarında tutarsızlıklara yol açmaktadır. Kurumsal Risk Yönetimi üzerindeki üst düzey yönetici liderliği, kurumun risk felsefesi ve stratejisini risk yönetimine tutarlı bir şekilde tüm örgüt boyunca iletme ve entegre etme konusunda yardımcı olmaktadır (Beasley vd., 2008: 314). Düzce Üniversitesi'nde yürütülen Risk Belirleme Çalıştayının başlangıç aşamasında üst yönetimin desteği alınmış ve çalışma bu destekle yürütülerek tamamlanmıştır.

Temel yaklaşım olarak üniversitenin karşı karşıya olduğu veya olabileceği risklerin tespit edilmesi üzerine odaklanılmıştır. Çalıştay, üniversitenin misyon, vizyon ve temel değerleri doğrultusunda kurumsal hedeflerine ulaşmasına engel olabilecek risklerin belirlenmesiyle başlamış ve tespit edilen risklerin yönetilebilmesi için mevcut bulunan kontroller ve konulması gereken kontrol veya stratejilerin değerlendirilmesiyle devam etmiştir. Çalıştayın nihai hedefi, üniversitenin kurumsal hedefleri açısından mevcut risklerin belirlenmesi ve değerlendirilmesi olmuştur.

Düzce Üniversitesi İç Denetim Birimi olarak 2018 Yılı İç Denetim Programı'na "Düzce Üniversitesi Bünyesindeki Tüm Birimleri Kapsayan Risk Evreninin Belirlenmesi Faaliyeti- Kontrol Öz Değerlendirme" başlıklı Risk Temalı Çalıştay odaklı danışmanlık faaliyeti alınmıştır. Bu kapsamda bir takvim doğrultusunda 02 Temmuz 2018 tarihinde Cumhuriyet Konferans Salonunda yapılan genel sunum ile Düzce Üniversitesinin Teşkilat Şemasında tanımlı bulunan Genel Sekreterlik- İdari Birimler, Enstitüler, Koordinatörlükler, Bölümler, Fakülteler, Yüksekokullar, Meslek Yüksekokulları ve Araştırma ve Uygulama Merkezlerinden; her birimden ayrı ayrı olmak üzere; bir personelin birim yöneticisi pozisyonunda, diğer personelin ise Stratejik Planlama Kurulu Birim Temsilcisi (zorunlu) olduğu, en az üç personelin hazır bulunduğu Düzce Üniversitesi Risk Evreninin Belirlenmesi Çalıştayı başlamıştır.

Çalıştay öncesinde; 18-29.06.2018 tarihleri arasında çalışma grupları belirlenmiş ve 25.06.2018 tarihinde yapılacak olan çalışmanın genel şemasını da içeren bir Risk Yönetim Rehberi yayınlanmıştır.

Çalıştayın 2. aşamasında, 10-27.07.2018 tarihleri arasında ekip çalışması formatında, Üniversitenin 2 iç denetçisinin kolaylaştırıcı olarak görev aldığı Operasyonel Süreçlerin Belirlenmesi, Ana ve Alt Faaliyetler ile Yönetim Faaliyetlerinin Tespit Edilmesi ve Çalışma Gruplarıyla Birimler Temelinde Risk-Kontrol Çalışması faaliyetleri yerine getirilmiştir.

Çalıştayın 3. aşamasında, 01-09.08.2018 tarihleri arasında yine ekip çalışması formatında, Üniversitenin 2 iç denetçisinin kolaylaştırıcı olarak görev aldığı Risk Evreni Konsolidasyon Çalışması faaliyeti yerine getirilmiştir.

4.1. Risk Belirleme Çalıştayının Veri Toplama Aşamaları

02 Temmuz 2018 tarihinde Cumhuriyet Konferans Salonunda başlayan ve tüm gün süren Çalıştayın sunum içeriğini; Çalıştayın Düzenlenme Sebebi, Risk Yönetim - Risk Değerlendirmesi, Risk Yönetimi, Kurumsal Risk Yönetimi, İç Kontrol-Kontrol Öz Değerlendirme, İç Denetim, Süreç Yönetimi ve Risk Evrenini Belirme Çalışması-Örnek Uygulama konuları oluşturmuştur.

Çalıştayın 1. aşamasını oluşturan sunum bölümüne 99'u akademik ve 73'ü idari olmak üzere toplam 172 personel katılmıştır. Çalıştayın 2. ve 3. aşamalarına ise 69'u akademik ve 102'si idari olmak üzere toplam 171 personel katılmıştır.

Çalıştay öncesi yayınlanan Risk Yönetimi Rehberinde kurumsal yönetimin temel bileşenlerinden olan risk yönetimi için temel bilgiler verilmiş ve rehberin temel amacı Düzce Üniversitesi bünyesindeki tüm birimleri kapsayan risklerin tespit edilerek Üniversitenin Risk Evreninin belirlenmesi olarak ifade edilmiştir. Bu temel amacın dışındaki ikincil amaçlar;

- Düzce Üniversitesi genelinde risk kültürünün oluşturulması,
- Düzce Üniversitesi çalışanlarına Kontrol Öz Değerlendirme yönteminin tanıtılması,

- Üniversitenin tüm faaliyet alanlarında görülebilecek Stratejik, Operasyonel, İtibar, Finansal, Yasal (Uygunluk), Bilgi Sistemleri, Raporlamalar ve Sağlık ve Güvenlik risklerinin kategorik olarak belirlenmesi,
- Üniversitenin stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek öncelikli risklerin belirlenmesi,
- Risklerin analiz edilmesi, değerlendirilmesi, sınıflandırılması ve önceliklendirilmesi,
- Risklere yönelik stratejilerin ve uygulanacak kontrol faaliyetlerinin belirlenmesi,
- Risklerin hem birimlerce ve hem de İç Denetim Birimi tarafından izlenmesi ve raporlanması,
- Üniversitesinin Kurumsal Risk Yönetiminde rol ve sorumlulukları bulunan yöneticiler ve çalışanlar için temel bir farkındalık ve paylaşım kanalının oluşturulması,
- Üniversitenin risk yönetimi, iç kontrol ve iç denetim üçgenin etkin bir şekilde oluşturulması

olmuştur.

Üniversitenin risk evrenini belirlemek amacıyla ilgili birimlerden verileri toplamak ve ekip çalışmalarında kullanmak üzere Microsoft Office Excel programından faydalanılmıştır. Ekip üyelerinin rahatlıkla kullanabileceği birbirine entegre 3 sayfadan meydana gelen bir excel dosya formu tasarlanmıştır. Formun içeriğini aşağıda belirtilen üç ana başlık oluşturmaktadır:

- Risk Belirleme
- Risk Analizi
- Risk Yönetimi

Formun doldurulması yukarıda belirtilen sıra dahilinde olmuştur. İş tekrarını önlemek amacıyla bazı veriler sayfalar arasında otomatik olarak aktarılmıştır. Üniversite birimleri, tüm çalışanların katılımını ve riskin etkin yönetimini sağlamak amacıyla aşağıda örneği bulunan Birim Risk Profil Kartını (Şekil 6) kendi çalışanlarına dağıtarak Çalıştaya doğrudan katılmayanlardanda gerekli verileri toplayabilmişlerdir.

4.1.1. Risk Belirleme Sayfası

Risk belirlemesi, kontrol listelerinin tamamlanması, risklerin tanımlanması için toplantılar yapılması ve arşivlenmiş belgelerin analiz edilmesi ile sağlanır (Dinu, 2012: 68). Çalışmada kullanılan Risk Belirleme sayfası 4 ana başlık (sütun) içermektedir (Şekil 7). Risk No sütununa, riski kolayca tanımlamak için

Şekil 6. Birim Risk Profil Kartı

Birim Adı	
Anahtar Risk Göstergesi	
Detaylı Risk Açıklaması	
Risk Kategorisi (Türü)	Stratejik operasyonel (faaliyet), finansal (mali), yasal (uygunluk), itibar, bilgi sistemleri, raporlama ve sağlık - güvenlik
Risk Etki Değerlendirmesi	Çok yüksek, yüksek, orta, düşük ve çok düşük
Risk Olasılık Değerlendirmesi	Çok yüksek, yoksek, orta, düşük ve çok düşük
Risk Oranı (risk etki ve olasılık sıralaması, 5*5 matris)	Önem derecesi çok yüksek, yüksek, orta ve düşük
Risk Yönetimi Stratejisi	Kabul et, kontrol geliştir, transfer et, kaçın, faydalan
Kontrol Faaliyeti / Strateji Açıklaması	Riske karşı oluşturulan kontrol faaliyetinin / stratejisinin açıklanması
Risk Sorumlusu	
Riskin Ait Olduğu Süreç / Faaliyet	
Riskin Ait Olduğu Alt Süreç /Alt Faaliyet	
Riskin Kontrolüne Ait Mevzuat ve/ veya Politika Belgesi	

(Yazarlar tarafından oluşturulmuştur.)

manuel olarak risk numarası girişi yapılmıştır. Anahtar Risk Göstergesi sütununa, manuel olarak kısaca risk olayının spesifik göstergesi tanımlanmıştır. Detaylı Risk Açıklaması sütunu için, manuel olarak risk olayını (mevcut veya olabilecek bir durumu) ve olası olumsuz sonuçları açıklayan ayrıntılı bir açıklama yapılması istenmiştir. Son olarak Risk Kategorisi sütunu ile açılır listeden, Tablo 2'de verilen skalaya uygun olacak şekilde, riskin içeriğini taşıyan uygun bir risk kategorisi seçimi sağlanmıştır.

Tablo 2. Risk Kategorisi

Risk Kategorisi	Açıklama
Stratejik Risk	Stratejik riskler iş hedeflerinin peşinde - ya fırsatlardan yararlanarak ve/veya tehditleri azaltarak - ortaya çıkmaktadır (Emblemsvåg ve Kjølstad, 2002: 847). Üniversitenin belirlemiş olduğu amaç ve hedefleri doğrudan olumsuz etkileyebilecek risklerdir.
Operasyonel Risk (Faaliyet Riski)	Operasyonel risk gibi kategoriler, düzenleyici ve yönetsel bir vizyon sürecinde önemli bir rol oynar, uygulamaların yeniden düzenlenmesi için geçici haritalar ve örgüt seviyesinde değişim ajanları için yeni diller ve fikirler sağlar (Power, 2005: 578). Üniversitenin yetersiz sistemlerinden, süreçlerinden, çalışanlarından, faaliyetlerinden ya da dış etmenlerden kaynaklanabilecek kayıplar ve işleyişi aksatabilecek risklerdir.
Finansal (Mali) Risk	Örgüt genelinde finansal risk yönetiminin büyüme faaliyetinin her geçen gün arttığı ve daha önemli bir hale geldiği finansal riske ait sorulabilecek temel sorulardan biri; finansal risk değerlendirmelerinin kurumun genel stratejik planına entegre edilmiş ve genel merkezden mi yönetildiği, yoksa bireysel işletim birimleri tarafından merkezi olmayan bir şekilde mi yönetildiğidir (Dolde, 1993: 33). Üniversite bünyesinde mali boyutta bir kayba neden olabilecek potansiyel olay, koşul ya da durumlardan kaynaklaan risklerdir.
Yasal / Uygunluk Riski	Herhangi bir kriz meydana geldiğinde, örgütler için potansiyel olarak halkla ilişkiler ve hukuki anlamda bazı sonuçlar meydana gelir. Krizlerle yüzleşen kurumlar, hem maddi menfaat sahipleri güvenilirliğini yitirirken hem de kötü eylemler iddiasıyla yasal yükümlülük altına girme riskini de taşımaktadırlar (Fitzpatrick, 1995: 33). Üniversitenin yasal mevzuattan ve mevzuatın değişmesinden kaynaklanabilecek yükümlülükleri yerine getirememesi, zamanında yerine getirememesi, eksik olarak yerine getirmesi veya mevzuatın yanlış yorumlanmasından dolayı meydana gelebilecek risklerdir.
İtibar Riski	İtibar riskleri, yalnızca insan yapımı bir toplumsal etkileşim ve iletişim ürünü olmaları bakımından diğer risk türlerinden farklıdır (Power, Scheytt, Soin ve Sahlin, 2011: 316). Üniversitenin iç ve dış paydaşları ya da genel kamuoyu nezdinde imajına zarar verebilecek risklerdir.
Bilgi Sistemleri Riski	Çalışanların günlük işlerinde bilgi kaynaklarıyla çalışmaları durumunda oluşabilecek kurum içi güvenlik tehditlerine daha fazla önem verilmesi durumunda, personel tarafından bilgi sistemleri güvenlik ihlallerinin oluşması azaltılabilir. Bilgi sistemleri güvenliğini yönetmeye yönelik organizasyonel çabaların tipik olarak çalışanlar, politikalar, süreçler ve kültür gibi diğer zayıflık kaynaklarını yönetme yerine donanım, yazılım ve ağ gibi teknolojik varlıklardaki güvenlik açıklarına odaklanma eğilimi vardır (Spears ve Barki, 2010 :503). Kullanıcılar bilgi sistemlerinin güvenlik risklerini yönetmede değerli bir kaynak olabilmektedir (Spears ve Barki, 2010: 504). Üniversitenin sahip olduğu bilgi teknolojilerinin kullanıma bağlı olarak herhangi bir kayba neden olabilecek potansiyel olay, koşul ya da durumlardır.
Raporlamalar Riski	Maddi olarak yanlış beyan edilen finansal tabloların olasılığının, yöneticilerin iş dışı davranışları ile sezgisel ve ilgi çekici bir şekilde değişime uğradığı ve finansal raporlama riskine ilişkin çeşitli kanıtlar mevcuttur (Davidson, Dey ve Smith,2015: 25).Üniversitenin ürettiği raporlara bağlı olarak iç ve dış paydaşları ya da genel kamuoyu nezdinde üniversitenin imajına zarar verebilecek risklerdir.

Sağlık ve Güvenlik Riski	Sağlık ve güvenlik risklerinin doğasını ve büyüklüğünü bilmek, önceliklerin belirlenmesinde ve aynı zamanda rekreasyonel faaliyetlerin, işlerin ve günlük yaşamın diğer yönlerinin takip edilmesiyle ilgili kararlar vermede yardımcı olacaktır. "Risk-risk" durumları riskli alternatifler arasından seçim yapılmasını gerektirir. "Ne kadar güvenli" durumlar, daha fazla güvenlik için diğer istenen faaliyetlerin ne kadarının feda edilmesi konusunda daha genel bir seçim gerektirir. "Ne kadar güvenli" durumların yönetilmesi doğal olarak daha zordur, çünkü bunlar bulanık düşünme ve retoriğe tabidir. Mevcut tahminlerin büyük belirsizlikleri, mantıklı kararlara varmak için açıkça iletilmelidir (Lave, 1987: 291). Üniversite bünyesinde iş sağlığı ve güvenliği kurallarına uyulmaması nedeniyle iç ve dış paydaşların maruz kalabileceği risklerdir.
Operasyonel ve Yasal Risk	Üniversitenin hem yetersiz sistemlerinden, süreçlerinden, çalışanlarından, faaliyetlerinden ya da dış etmenlerden kaynaklanabilecek kayıplar ve işleyişi aksatabilecek operasonel riski ve hem de üniversitenin yasal mevzuattan ve mevzuatın değişmesinden kaynaklanabilecek yükümlülükleri yerine getirememesi, zamanında yerine getirememesi, eksik olarak yerine getirilmesi veya mevzuatın yanlış yorumlanmasından dolayı meydana gelebilecek yasal risklerdir.
Operasyonel ve Finansal Risk	Üniversitenin hem yetersiz sistemlerinden, süreçlerinden, çalışanlarından, faaliyetlerinden ya da dış etmenlerden kaynaklanabilecek kayıplar ve işleyişi aksatabilecek operasyonel riskleri ve hem de üniversite bünyesinde mali boyutta bir kayba neden olabilecek potansiyel olay, koşul ya da durumlardan kaynaklanan finansal risklerdir.
Karma Risk	Yukarıda bahsedilen risk kategorilerden aynı anda iki veya daha fazla başlık altında değerlendirilebilecek risklerdir (Örneğin, operasyonel, yasal ve itibar riskinin aynı anda mevcut olma durumu).

(Yazarlar tarafından oluşturulmuştur.)

Risk Belirlemesinde, üniversite birimlerinin hassas görevler değerlendirmeleri, stratejik plana yönelik yapılan çalışmalar, birimlerin uymakla yükümlü olduğu yasal mevzuat, birimlerin iş akış şemaları, sunmakta oldukları faaliyet alanları ile ilgili hizmetler göz önünde bulundurulmuştur. Birimlerin faaliyetleri, çevresel yapıları, sunduğu hizmetleri, maruz kalabileceği risklerin kaynağı için bir temel oluşturmaktadır.

Şekil 7. Risk Belirleme Sayfası

(Ekran görüntüsü)

4.1.2. Risk Analizi Sayfası

Modern dünyada karşı karşıya kalınan riskler üç temel yolla ele alınmaktadır. Duygular olarak ele alınan risk, tehlikeye yönelik hızlı, içgüdüsel ve sezgisel tepkilere işaret eder. Analiz olarak ele alınan risk, mantıksal nedene dayanır ve bilimsel yönetimin tehlike yönetimine katılmasını sağlar (Slovic vd., 2004: 311). Çalışmada Risk Analizi sayfası 6 ana başlık (sütun) içermektedir (Şekil 8). Sayfanın ilk üç sütun bilgisi Risk Belirleme sayfasından otomatik olarak gelmektedir. Etki sütununda, riskin neden olduğu yaklaşık etki çok düşük- düşük-orta- yüksek ve çok yüksek olmak üzere 5'li likert ölçeğinden uygun seçeneğin seçilmesini sağlayacak şekilde açılır listeden seçim yapılmaktadır. Olasılık sütununda da etki sütununa benzer bir biçimde, oluşan riskin yaklaşık olasılığı çok düşük-düşük-orta-yüksek ve çok yüksek olmak üzere 5'li likert ölçeğinden uygun seçeneğin seçilmesini sağlayacak şekilde açılır listeden seçim yapılmaktadır. Son olarak Risk Oranı sütununa, seçilen etki ve olasılık değerlerine göre düşük-orta-yüksek ve çok yüksek olmak üzere Excel hesaplama yapmakta ve veri girişi otomatik gerçekleşmektedir.

Şekil 8. Risk Analizi Sayfası

	A	B	C	E	G	I
1	RİSK ANALİZİ					
2	RİSK NO	Detaylı Risk Açıklaması	Risk Kategorisi	Etki	Olasılık	Risk Oranı
3	Otomatik	Otomatik	Otomatik	Açılır Liste	Açılır Liste	Otomatik
15						
16						
17						
18						
19						
20						

Risk Evreni Çalışması | Risk - Belirleme | Risk - Analizi | Risk - Yönetimi

(Ekran görüntüsü)

4.1.3. Risk Yönetimi Sayfası

Geleneksel olarak kurumlar, stratejik öğeler için birden çok kaynak kullanarak ve güvenlik stoğu tutarak, çevrelerindeki mevcut risklere karşı tampon oluşturan stratejiler benimsiyorlardı. Bu tamponlar operasyonel performansları kısıtlayabilmekte ve rekabet avantajını olumsuz yönde etkileyebilmektedir. Yeni yaklaşımlar, potansiyel kayıpları tanımlamayı, potansiyel kayıpların olasılığını anlama ve bu kayıplara önem vermeyi içeren resmi bir süreç olan risk yönetimini içermektedir (Giunipero ve Eltantawy, 2004: 699). Çalışmanın Risk Yönetimi sayfası 12 ana başlık (sütun) içermektedir (Şekil 9). Sayfanın ilk üç sütun bilgisi Risk Belirleme sayfasından otomatik olarak gelmektedir. Risk Yönetimi Stratejisi sütununa, belirlenen risk için uygun cevap ölçüsü (Kabul et, Kontrol geliştir, Transfer et, Kaçın, Faydalan) açılır listeden seçilmektedir. Kontrol Faaliyeti / Strateji Açıklaması sütununa, belirlenen riske karşı oluşturulan / oluşturulabilecek kontrol faaliyetinin / stratejisinin açıklaması yapılmıştır. Risk Sorumlusu sütununa, tanımlanan risk için ilgili birim risk sorumlusu girilebilmektedir. Riskin Ait Olduğu Süreç / Faaliyet sütununa, Birim bazında riskin ait olduğu süreç veya faaliyet yazılmaktadır. Riskin Ait Olduğu Alt Süreç / Alt Faaliyet sütununa, Birim bazında varsa riskin ait olduğu alt süreç veya alt faaliyet yazılmaktadır. Risk kontrolüne ait Mevzuat ve / veya Politika Belgesi sütununa,

Riskin kontrolü için kullanılan mevzuat, rehber, plan, politika belgesi, akış şeması gibi dokümanlar yazılmaktadır. Kontrol Önlemleri Sonrası Risk Değerlendirmesi Grubunda bulunan etki, olasılık ve risk oranı için sırasıyla; etki sütununa, seçilen müdahale eylemi / stratejisi hesaplanarak riskin neden olduğu yaklaşık etki çok düşük-düşük-orta-yüksek ve çok yüksek olmak üzere 5'li likert ölçeğinden uygun seçeneğin seçilmesini sağlayacak şekilde açılır listeden seçim yapılmaktadır. Olasılık sütununa, seçilen müdahale eylemi / stratejisi hesaplanarak, oluşan riskin yaklaşık olasılığı çok düşük- düşük-orta-yüksek ve çok yüksek olmak üzere 5'li likert ölçeğinden uygun seçeneğin seçilmesini sağlayacak şekilde açılır listeden seçim yapılmaktadır. Son olarak Risk Oranı sütununa, seçilen etki ve olasılık değerlerine göre düşük- orta- yüksek ve çok yüksek olmak üzere Excel hesaplama yapmaktadır. (Otomatik veri yerleşimi yaptığından herhangi bir veri bulunmamaktadır.)

Şekil 9. Risk Analizi Sayfası

A	B	C	D	E	F	G	H	I	K	M	O
RİSK YÖNETİMİ											
RİSK NO	Anahtar Risk Göstergesi	Risk Kategorisi	Risk Yönetimi Stratejisi	Kontrol Faaliyeti / Strateji Açıklaması	Risk Sorumlusu	Riskin Ait Olduğu Süreç /Faaliyet	Riskin Ait Olduğu Alt Süreç / Alt Faaliyet	Riske ait Mevzuat ve/veya Politika Belgesi	Kontrol Önlemleri Sonrası Risk Değerlendirmesi		
									Etki	Olasılık	Risk Oranı
Otomatik	Otomatik	Otomatik	Açılır Liste	Manuel	Manuel	Manuel	Manuel	Manuel	Açılır Liste	Açılır Liste	Otomatik

(Ekran görüntüsü)

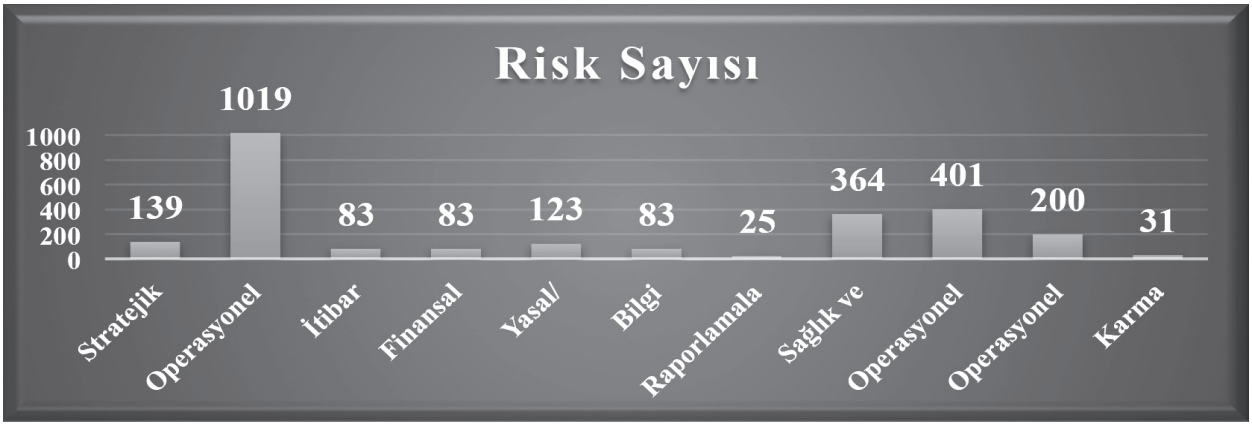
4.2. Risk Belirleme Çalıştayının Raporlama Aşaması ve Sonuçları

Çalıştayın raporlama aşamasında Fakülteler, Yüksekokullar, Enstitüler, Bölümler, İdari Birimler, Araştırma ve Uygulama Hastanesi, Koordinatörlükler ve Araştırma ve Uygulama Merkezlerinden gelen veriler konsolide edilmiş ve bu konsolidasyon sonrası Üniversitesi Genel Risk Raporu, Kısımlar Bazında Risk Raporu, Isı (Risk) Haritası, Risk Kategorileri Bazında Risk Raporu ve Çalıştay Metriklerini de kapsayan Düzce Üniversitesi Risk Evreninin Belirlenmesi Çalıştayı Raporu hazırlanmıştır.

Düzce Üniversitesi Risk Evreninin Belirlenmesi Çalıştayı sonucunda 69 üniversite biriminden; 139 adet Stratejik, 1019 adet Operasyonel, 83 adet İtibar, 83 adet Finansal, 123 adet Yasal / Uygunluk, 83 adet Bilgi Sistemleri, 25 adet Raporlamalar, 364 adet Sağlık ve Güvenlik, 401 adet Operasyonel ve Yasal, 200 adet Operasyonel ve Finansal ve 31 adet Karma risk kategorisinde toplam 2551 adet risk raporlanmıştır (Grafik 1).

Üniversite bünyesinde Operasyonel Risklerin baskın bir ağırlığının bulunması, birimlerin faaliyet alanla-

Grafik 1. Kategorilerine Göre Risk Sayısı

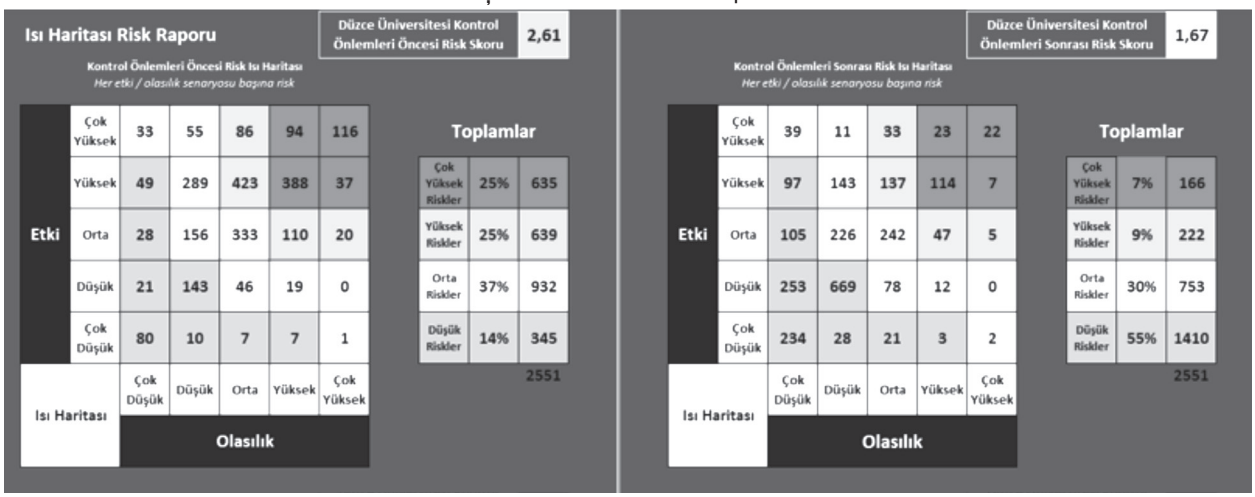


(Ekran görüntüsü)

rına daha fazla odaklanması ihtiyacını gün yüzüne çıkarmış ve risk yönetiminin omurgasının Operasyonel Riskler ağırlıklı olarak kurgulanması ihtiyacını doğurmuştur. Sağlık ve güvenlik risklerinin belirgin ağırlığı; bir taraftan İş Sağlığı ve Güvenliği (İSG) konusunda üniversite genelinde bir farkındalığın oluştuğunu göstermekte ve diğer yandan 6331 sayılı İş Sağlığı ve Güvenliği Kanunu temelinde, kurumsal bakış açısını yansıtan İSG yapılanma ihtiyacını işaret etmektedir.

Çalıştayın ikinci önemli sonucu olarak; toplanan veriler ışığında kontrol önlemleri öncesi ve sonrası durumu gösteren 2 adet ısı haritası risk raporu (Şekil 10) hazırlanmıştır. Bu haritalara göre; Düzce Üniversitesi Kontrol Önlemleri Öncesi Risk Skoru 2,61 değeri ile "*Yüksek*" ve Düzce Üniversitesi Kontrol Önlemleri Sonrası Risk Skoru 1,67 değeri ile "*Orta*" olmuştur. Çalıştay katılımcıları risklere karşı mevcut ve alınacak aksiyonlar (kontrol önlemleri) sonucunda yaklaşık 1 puanlık bir risk değer azaltımı öngörmüşlerdir.

Şekil 10. Isı Haritası Risk Raporu



(Ekran görüntüsü)

Isı haritasındaki riskler kendi aralarında konsolide edildiğinde üniversite genelindeki riskler; kontrol önlemleri öncesi 346 adet Düşük, 931 adet Orta, 639 adet Yüksek ve 635 adet Çok Yüksek risk oranlarına (Grafik 2) sahip olmuştur. Bu riskler için geliştirilecek kontrol önlemleri ve stratejiler sonucunda mevcut risk dağılımı 1410 adet Düşük, 753 adet Orta, 222 adet Yüksek ve 166 adet Çok Yüksek risk (Grafik 3) olacaktır. Isı haritasının etki ve olasılık sağ-üst hattındaki yoğunluk kontrol önlemleri sonra belirgin bir şekilde sol-alt hatta konumlanmaktadır.

Son yorum olarak risklere karşı geliştirilmesi gereken risk yönetimi stratejisinde ağırlıklı oran, Kontrol Geliştir seçeneği (Grafik 4) olmuştur. Özellikle "Çok Yüksek" ve "Yüksek" riskler öncelikli olarak odaklanılması gereken bir risk portföyünü oluşturmaktadır. Woods'a (2009: 74) göre; "Çok Yüksek" ve "Yüksek" riskler, iş hedeflerinin karşılanması ve hizmet sunumunun sağlanması için acil bir kontrol iyileştirmesinin yapılması gereken bir durum olarak tanımlanır. Yüksek ve çok yüksek etki veya yüksek olasılıklı tüm riskler çok yüksek olarak sınıflandırılır ve bu riskler ve ilgili kontroller hakkındaki bilgiler organizasyonel hiyerarşide bir sonraki seviyeye kadar otomatik olarak yükselir. Diğer bir deyişle, bir birim yöneticisi bir faaliyette ciddi bir risk görüyorsa, bu durum daha sonra, riski azaltmak için eylem planlarının tasarlanmasını sağlama sorumluluğunu üstlenen bir üst yönetici tarafından bilinecektir. "Çok Yüksek" ve "Yüksek" riskler, ilgili birim bünyesinde haftalık toplantıların ve eylem planlarının konusu olmalıdır. Eylem planları, mevcut kontrollerin etkinliği, hangi ilave kontrollerin gerekli olduğu ve bunlardan kimin sorumlu olduğu hakkında yorumlar içermelidir.

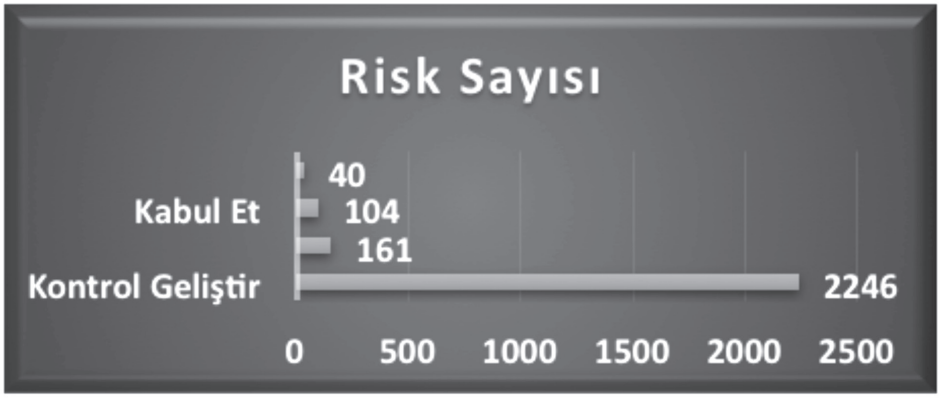
Grafik 2. Kontrol Önlemleri Öncesi Risk Oranı

(Ekran görüntüsü)

Grafik 3. Kontrol Önlemleri Sonrası Risk Oranı

(Ekran görüntüsü)

Grafik 4. Risk Yönetimi Stratejisine Göre Risk Sayısı



(Ekran görüntüsü)

5. SONUÇ

Örgüt varlık bulduğu habitatta sürekliliğini korumak zorundadır. Örgütün sürekliliği, belirsizlikler ve risklerle dolu dünyada eylemlerinin ne kadar etkin olduğuna bağlıdır. Çalışmada bu etkin eylemler için örgütün risk, kontrol ve hedef formasyonunu odağına alan Kontrol Öz Değerlendirme yaklaşımı ele alınmıştır. Bu yaklaşım ile örgütün risklerini belirlemesi, belirlenen risklerin etkin kontrolünün sağlanması ve bunlara bağlı olarak örgütsel hedeflere ulaşması için kurum bünyesinde oluşturulabilecek yol haritalarının içeriklerinin belirlenmesi sağlanmıştır. Kontrol Öz Değerlendirme yöntemi örgüt içinde ister dikey isterse yatay olarak kurulabilecek ağlar vasıtasıyla ve kurumsal negatif entropi üretme kapasitesiyle hem iş görenler ve hem de yönetim kademsinde bulunanlar için etkin bir kurumsal yönetme gücü sağlayabilmektedir. Ancak bu gücün örgütün sahip olduğu kültür kadar olacağı unutulmamalıdır. Örgüt kültürünün hedef-risk-kontrol formülasyonun kurulumu için Kontrol Öz Değerlendirme anlayışını bünyesinde içselleştirmesi gerekmektedir.

Kontrol Öz Değerlendirme sağladığı bakış açısı ile Kurumsal Risk Yönetimi için proaktif bir yönetim potansiyeli taşımaktadır. Örgütlerin etkin bir Kurumsal Risk Yönetimi için COSO güçlü bir çerçeve sağlamaktadır. Bu çerçeve COSO küpündeki paradigma değişimi sonucunda Kurumsal Risk Yönetimini daha uyarlanabilir bir yapıyı gösteren sarmal boyuta taşınmış ve bu boyut artık strateji, risk ve performans arasında daha kuvvetli bir bağ oluşturmuştur.

COSO yenilenen çerçevesi ile günümüz çalışma dünyasına daha esnek bir yapılanma biçimine bürünmüş, ağaç şeklindeki bir metaforik bakışla Kurumsal Risk Yönetiminin köklerine yönetişim ve kültür kavramlarını oturtmuştur. Bu metaforda ağacın gövdesini; strateji ve hedef belirleme (örgütün hedeflerinin risk iştahı ile stratejiyle uyumlu ve onu destekleyecek şekilde kurgulanması, örgütün her seviyesindeki risklerinin göz önünde bulundurulması), performans (risklerin belirlenmesi, şiddetinin değerlendirilip önceliklendirilmesi ve buna bağlı olarak risk yanıtlarıyla portföy bakış açısının oluşturulması), gözden geçirme ve revize etme (örgütün, önemli değişimler ışığında, hedeflerine göre performansını nasıl sonuçlandırdığı, kurumsal yönetim uygulamalarının etkin ve verimli çalışıp çalışmadığı, kuruma ne kadar değer kattığı ve değer katmaya süreklilik kazandırıp kazandırmadığı ve düzeltilmesi gereken faaliyetler bulunup bulunmadığı) oluşturmaktadır. COSO Kurumsal Risk Yönetimin dallarını ise bilgi, iletişim ve raporlama oluşturmuştur. Bu dallar aracılığıyla örgüt içinden ve dışından bilgi elde edilip, kurum içinde gerekli paylaşım sağlanmaktadır. Örgüt bilgi ve veriyi faaliyetlerinde kullanmakta, işlemekte, bilgi sistemlerinden faydalanmakta ve bunu bir süreç mantığıyla işletmektedir. Son olarak örgüt yönetişim, risk, kültür ve performansa ait raporlama yapmakta ve bunu paylaşmaktadır. COSO'nun yeni çerçevesinin örgüt bünyesinde işlerliğinin sağlanması için ilk adım olarak örgütün bir risk envanterinin elde hazır bulunması gerekmektedir.

Risk envanterini çıkarmak için için en kullanışlı yol, örgüt bünyesinde bir risk çalıştayı düzenlemek olmaktadır. Bu çalıştay aracılığıyla; örgütsel hedeflerin gerçekleştirilmesini engelleyen riskler belirlenip bir listesi oluşturulabilmekte, belirlenen risklerin nasıl yönetilebileceğine veya uygun şekilde yönetilip yönetilmediğine karar verilebilmesi için kontrol süreçleri izlenebilmekte veya tasarlanabilmektedir. Çalıştay yalnızca örgütün maruz kaldığı riskleri tespit etmekle kalmamakta ayrıca örgüt kültürünün risk ve kontrol kavramlarıyla tanışmasına aracılık etmekte ve buna bağlı olarak örgüt iklimini riske-kontrole-yönetişime odaklı bir yapıya çevirebilmektedir. 2018 yılı içinde gerçekleştirilen Düzce Üniversitesi Risk Evreninin Belirlenmesi Çalıştayı ile örgüt hem Kontrol Öz Değerlendirme ve hem de risk-kontrol-hedef bütünlüğü kavramlarıyla tanışmış oldu. Kurumun insan kaynaklarının yapısı ve teknik altyapısının yeterliliğine, faaliyetlerinin karmaşıklık düzeyine, stratejik hedeflerinin değişkenliğine bağlı olarak farklı birimlerden çok farklı iş pozisyonlarından katılımın sağlandığı Çalıştay sonucunda, uzun soluklu bir çalışma olarak risk evreni ortaya çıkarılmış ve böylece Kurumsal Risk Yönetiminin geliştirilmesi için ilk kök kazanılmıştır. Özgün bir uygulama olduğu düşünülen söz konusu Çalıştayın, Düzce Üniversitesinde risk yönetimi konusunda bundan sonra yapılacak çalışmalara yön vermesi ve diğer kurumlara da örneklik oluşturması beklenmektedir.

Kaynakça

Abrams C., Von kanel J., Muller S., Pfitzmann B., ve Ruschka-Taylor S., (2007) "Optimized Enterprise Risk Management", *IBM Systems Journal*, 46(2), 219–234.

Anderson D., (2017, Ekim) "COSO ERM Getting Risk Management Right", *Internal Auditor*, 38-43.

Akçakanat Ö., (2012) "Kurumsal Risk Yönetimi ve Kurumsal Risk Yönetim Süreci", *Süleyman Demirel Üniversitesi Vizyoner Dergisi,* 4(7), 30-46.

Barr P. S., Stımpert J. L. ve Huff A. S., (1992) "Cognitive Change, Strategic Action, and Organizational Renewal" *Strategic Management Journal*, 13(S1), 15–36.

Bartlett C. A. ve Ghoshal S., (2002) "Building Competitive Advantage Through People: Human, Not Financial, Capital Must Be The Starting Point and Ongoing Foundation of A Successful Strategy", *MIT Sloan Management Review*, 43(2), 34+.

Beasley M., Pagach D., ve Warr R., (2008) "Information Conveyed in Hiring Announcements of Senior Executives Overseeing Enterprise-Wide Risk Management Processes", *Journal of Accounting, Auditing & Finance*, 23(3), 311–332.

Bhatt G. D. ve Grover V., (2005) "Types of Information Technology Capabilities and Their Role in Competitive Advantage: An Empirical Study", *Journal of Management Information Systems*, 22(2), 253–277.

Callahan C. ve Soıleau J., (2017) "Does Enterprise Risk Management Enhance Operating Performance?", *Advances in Accounting*, 37, 122-139.

COSO, (2004) *Enterprise Risk Management Framework*, http://www.coso.org/documents/COSO_ERM_Execut iveSumm ary.pdf. Erişim Tarihi: 01.08.2016.

COSO, (2017) *Integrating with Strategy and Performance Executive Summary*, https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf Erişim Tarihi: 12.09.2018.

D'arcy, S. P., (2001) "Enterprise Risk Management", *Journal of Risk Management of Korea*. 12(1).

Davıdson R., Dey A. ve Smıth A., (2015) "Executives' "Off-The-Job" Behavior, Corporate Culture, and Financial Reporting Risk", *Journal of Financial Economics*, 117(1), 5-28.

Dınu A. M., (2012) "Modern Methods of Risk Identification in Risk Management", *International Journal of Academic Research in Economics and Management Sciences*, 1(6), 67-71.

Dolde W., (1993) "The Trajectory of Corporate Fınancial Risk Management", *Journal of Applied Corporate Finance*, 6(3), 33–41.

Emblemsvåg J. ve Kjølstad L.E. ,(2002) "Strategic Risk Analysis – A Field Version", *Management Decision*, 40(9), 842-852.

ERM, (2018) *Applying Enterprise Risk Management to Environmental, Social and Governance-Related Risks*, https://www.coso.org/Documents/COSO-WBCSD-Release-New-Draft-Guidance-Printer-friendly.pdf Erişim Tarihi: 11.10.2018.

Fıtzpatrıck K. R., (1995, Summer) "Ten guidelines for reducing legal risks in crisis management", *Public Relations Quarterly*, 40(2), 33-38.

Flamholtz E., (2001) "Corporate Culture and the Bottom Line", *European Management Journal,* 19(3), 268–275.

Gıunıpero L.C. ve Eltantawy R.H., (2004) "Securing The Upstream Supply Chain: A Risk Management Approach", *International Journal of Physical Distribution & Logistics Management*, 34(9), 698-713.

GLEIM CPA REVIEW, (2018) *Updates to Business Environment and Concepts.*

Hallikas J., Karvonen I., Pulkkınen U., Vırolaınen V.M. ve Tuomınen M., (2004) "Risk Management Processes in Supplier Networks", *International Journal of Production Economics*, 90(1), 47–58.

Hamıd A.R.A., Majıd M.Z.A. ve Sıngh, (2008) "Causes of Accidents at Construction Sites", *Malaysian Journal of Civil Engineering*, 20(2) : 242 - 259.

Hubbard L., (2000) *Control Self-Assessment A Practical Guide*, the IIA.

Joseph G. ve Engle T., (2005) "The Use of Control Self-Assessment by Independent Auditors", *The CPA Journal*, 38-43.

Kıral H. ve Hatipoğplu İ.İ., (2017) "Risk Yönetiminde Kontrol Öz Değerlendirme Yaklaşımı ve Strateji Geliştirme Birimlerinin Bu Kapsamda Üstlenebilecekleri Roller", *Amme İdaresi Dergisi*, 50(4), 115-133.

KİDDER, (2014) *CCSA Sınavı Hazırlık Kursu Notları*, Ankara: Kamu İç Denetçiler Derneği.

Kurt G. ve UYSAL T.U., (2018) "COSO Kurumsal Risk Yönetimi Çerçevesi Güncelleme Projesinin Getirdiği Yenilikler", *Muhasebe ve Denetime Bakış*, 54, 19-34.

Lave L., (1987) "Health and safety risk analyses: information for better decisions", *Science*, 236(4799), 291–295.

Levın A.C., (2008) "Solving the Right Problem: A Strategic Approach to Designing Today's Workplace", *Building Design Strategy: Using Design to Achieve Key Business Objectives*, ed.: LOCKWOOD T. ve WALTON T., New York: Allworth Press.

Lıebenberg A. P. ve Hoyt R. E., (2003) "The Determinants of Enterprise Risk Management: Evidence From the Appointment of Chief Risk Officers", *Risk Management Insurance Review*, 6(1), 37–52.

Lundqvist S. A., (2015) "Why Firms Implement Risk Governance – Stepping Beyond Traditional Risk Management to Enterprise Risk Management", *Journal of Accounting and Public Policy*, 34(5), 441–466.

Lyon B.K. ve Hollcroft B., (2012, Aralık) "Risk assessments: Top 10 pitfalls and tips for improvement", *Professional Safety*, 57(12), 28-34.

Lyon B.K. ve Popov G., (2016, Mart) "The Art of Assessing Risk", *Professional Safety*, 61(3), 40-51.

Mcnally J., (2007) "Control Self-Assessment: Everybody Pitching in with Internal Controls", *Pennsylvania CPA Journal*, 78(3), 33-35.

Moeller R., (2015) *Brink's Modern Internal Auditing–A Common Body of Knowledge*, 8th Edition, New Jersey: John Wiley&Sons.

Norrman A. ve Jansson U., (2004) "Ericsson's Proactive Supply Chain Risk Management Approach After a Serious Sub-Supplier Accident", *International Journal of Physical Distribution & Logistics Management*, 34(5), 434–456.

O'reılly C., (1989) "Corporations, Culture, and Commitment: Motivation and Social Control in Organizations", *California Management Review*, 31(4), 9–25.

Phinicharomma S., (2018) *Risk Base Internal Controls & Audit: What's New under COSO-ERM 2017 Framework?*

Power M., (2005) "The Invention of Operational Risk", *Review of International Political Economy*, 12(4), 577-599.

Power M., (2009) "The Risk Management of Nothing", *Accounting, Organizations and Society*, 34(6-7), 849-855.

Power M., Scheytt T., Soın K. ve Sahlın K., (2011) "Reputational Risk as A Logic of Organising in Late Modernity", *Organisation Studies*, 30(2&3), 301–324.

Prewett, K. ve TerrY, A., (2018) "COSO's Updated Enterprise Risk Management Framework—A Quest for Depth and Clarity", *Journal of Corporate Accounting & Finance*, 29(3), 16-23.

Sadu I., (2017, Ekim) "Assessing Soft Controls", *Internal Auditor*, 57-60.

Schwenk C. R., (1984) "Cognitive Simplification Processes in Strategic Decision-Making" *Strategic Management Journal*, 5(2), 111–128.

Slovıc P., Fınucane M.L., Peters E. ve Macgregor D.G., (2004) "Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality", *Risk Analysis*, 24(2), 311-322.

Spears J. L. ve Barkı, H., (2010) "User Participation in Information Systems Security Risk Management", *MIS Quarterly*, 34(3), 503-522.

Touam Z., (2016, Aralık) "Control Self-Assessment, Techniques and Strategies", *IA Internal Auditor Middle East*, 18-20

TURNBULL REPORT, (2005) Internal Control - Revised Guidance for Directors on The Combined Code, London:Financial Reporting Council.

Türedi H. ve Karakaya G., (2015) "COSO İç Kontrol Modeli ve Kontrol Ortamı", *Finans Politik & Ekonomik Yorumlar*, 52(602), 67-76 .

Woods M., (2009) "A contingency theory perspective on the risk management control system within Birmingham City Council", *Management Accounting Research*, 20(1), 69-81.

Wu D. D. ve Olson D., (2009) "Enterprise Risk Management: a DEA VaR Approach in Vendor Selection", *International Journal of Production Research*, 48(16), 4919–4932.