OPUS
Uluslararası Toplum Araştırmaları Dergisi
International Journal of Society Researches

ISSN:2528-9527
E-ISSN : 2528-9535
Yıl *Year* : 8
Cilt *Volume*:9
Sayı *Issue* :16
Aralık *December* 2018
Makalenin Geliş Tarihi*Received Date*:06/11/2018
Makalenin Kabul Tarihi *Accepted Date*: 03/12/2018

Kurumsal Risk Yönetim Sisteminde Risk Değerlendirme Raporlarının Hazırlanması[1]

DOI: 10.26466/opus.479277

*

Özlem Usman*

* Araştırma Görevlisi Dr., Yalova Üniversitesi, İİBF Fakültesi, Yalova / Türkiye
E-Posta: sozlemozmen@hotmail.com **ORCID:**0000-0002-1745-889X

Öz

Bu çalışmada işletmelerde risk değerlendirme raporlarının hazırlanmasında izlenmesi gereken adımlar ve her bir adımda yürütülecek faaliyetler açıklanmıştır. Çalışmanın temel amacı kurumsal risk yönetim sisteminin bir parçasını oluşturan ve çok çeşitli durumlarda işletmede hazırlanan risk değerlendirme raporlarının nasıl hazırlanması gerektiği konusunda bilgi vererek işletmelerin kurumsal risk yönetim sistemlerinin işlerlik kazanmasına katkı sağlamaktır. Bu amaca yönelik olarak öncelikle kurumsal risk yönetim kavramından bahsedilmiştir. COSO'nun 2004 yılında yayınladığı kurumsal risk yönetimi raporunda yer verilen sekiz adet kurumsal risk yönetim bileşeni ve bileşenlerin ne ifade ettiği kısaca açıklanmıştır. Daha sonra Bursa ilinde faaliyet gösteren ve kurumsal risk yönetim çalışmaları yürüten bir işletmenin belirli dönemlerde hazırladığı risk değerlendirme raporları detaylı şekilde incelenmiştir. Yapılan İncelemenin ardından kurumsal risk yönetim sistemlerinin bir parçası olarak görülmesi gereken risk değerlendirme raporlarının hazırlanmasında izlenmesi gereken adımlar oluşturulmuştur. Her bir adım çalışmada alt başlık haline getirilmiş ve adım faaliyetlerinde kullanılabilecek örnek formlar geliştirilmiştir. Geliştirilen örnek formların tablo şeklinde ilgili alt başlıkların altında sunulması ile çalışma tamamlanmıştır.

Anahtar Kelimeler:*Kurumsal Risk Yönetimi, Kurumsal Risk Yönetimi Bileşenleri, Risk Değerlendirme Raporları.*

[1] *Bu makale, yazarın "İşletmelerde Kurumsal Risk Yönetim Süreci ve Bir Uygulama" isimli doktora tezinden türetilmiştir.*

OPUS
Uluslararası Toplum Araştırmaları Dergisi
International Journal of Society Researches

ISSN:2528-9527
E-ISSN : 2528-9535
Yıl *Year* : 8
Cilt *Volume*:9
Sayı *Issue* :16
Aralık *December* 2018
Makalenin Geliş Tarihi*Received Date*:06/11/2018
Makalenin Kabul Tarihi *Accepted Date*: 03/12/2018

Preparation of Risk Assessment Reports In Enterprise Risk Management System

*

Abstract

In this study, steps to be followed in the preparation of risk assessment reports and the activities to be carried out in each step are explained. The main purpose of the study is to contribute acquiring functionality on the enterprise risk management systems by providing knowledge on how to prepare risk assessment reports which are a part of the enterprise risk management systems and prepared in the enterprise in a wide variety of situations. For this purpose, first of all, the concept of enterprise risk management is mentioned. Eight enterprise risk management components which included in the COSO's enterprise risk management report published in 2004 and the meaning of the components are briefly explained. Then, the risk assessment reports prepared in certain periods by an enterprise operating in the province of Bursa and carrying out enterprise risk management studies are examined in detail. After review the steps to be followed in preparing the risk assessment reports that should be seen as part of the enterprise risk management systems have been composed. Each step has been developed into sub-titles and developed sample forms that can be used in step activities. The study was completed by presenting the sample forms under the subheadings in the form of tables.

Keywords: *Enterprise Risk Management, Enterprise Risk Management Components, Risk Assessment Reports.*

Giriş

Günümüzde geleneksel risk yönetim sistemleri hızla değişen çevresel, hukuksal ve ekonomik koşullar nedeniyle giderek yerini kurumsal risk yönetim sistemlerine bırakmaktadır. İşletmelerin kurumsal risk yönetim sistemlerini kurarak etkin şekilde sürdürmeleri ve bu sayede iç ve dış çevre kaynaklı risklerini yönetmeleri rekabet ortamı ile başa çıkabilmeleri ve başarılı olabilmeleri adına hayati önem taşımaktadır. İşletmeler her ne kadar güçlü bir stratejiye, yetenekli ve yeterli işgücüne, etkin işleyen iş süreçlerine ve ileri bir teknolojiye sahip olsalar da zamanla bir takım risklere karşı savunmasız hale gelme olasılıkları her zaman söz konusudur. Bu nedenle etkin işleyen kurumsal risk yönetim sistemlerinin varlığına tüm işletmeler ihtiyaç duymaktadır.

Amerika Birleşik Devletleri'nin önde gelen beş kontrol ve muhasebe kuruluşu (Amerikan Kamu Muhasebecileri Birliği (The American Institute of Certified Public Accountants - AICPA), Amerikan Muhasebeciler Birliği (The American Accounting Association - AAA), Finansal Yöneticiler Enstitüsü (The Financial Executives Institute – FEI), İç Denetçiler Enstitüsü (The Institute of Internal Auditors – IIA) ve Ulusal Muhasebeciler Birliği (The National Association of Accountants) katılımı ile 1985 yılında Committee of Sponsoring Organizations of Treadway Commission (COSO)kurulmuştur. COSO' nun en önemli amacı; finansal raporlarda oluşabilecek hata ve hilelerin olma olasılığını azaltmaktır. Söz konusu amaca yönelik olarak 1992 yılında "COSO I: İç Kontrol-Bütünleşik Çerçeve" (Internal Control-Integrated Framework) raporunu yayınlamıştır. Raporda ideal bir iç kontrol yapısının temelini oluşturma konusuna yer verilmiştir. 2004 yılında gelindiğinde ise, ikinci bir rapor olan "COSO Kurumsal Risk Yönetimi" (Enterprise Risk Management Integrated Framework) isimli raporu yayınlamıştır. Bu raporda, kurumsal risk yönetimi hakkında detaylı bilgiler verilmiş ve kurumsal risk yönetim bileşenleri adı altında sekiz adet bileşen açıklanmıştır.

COSO kurumsal risk yönetimi raporunda bahsi geçen ve detaylı şekilde ele alınan kurumsal risk yönetim bileşenlerinden birisi de "risk değerlendirme" bileşenidir. Risk değerlendirme, diğer tüm bileşenler içinde kilit bir bileşen olma özelliğini taşımaktadır. Çünkü bu kavram temel olarak risklerin analiz edilmesi anlamına gelmektedir ve işletmel-

erde risk yönetim süreci ile ilgili yapılacak faaliyetlere de yön vermektedir. Bu gerçeklikten hareketle yapılan bu çalışmanın temel amacı kurumsal risk yönetim sisteminin bir parçasını oluşturan risk değerlendirme raporlarının hazırlanmasına yönelik yürütülebilecek faaliyetler ve kullanılabilecek çeşitli formlar önermek suretiyle işletmelerin kurumsal risk yönetim sistemlerinin işlerlik kazanmasına katkı sağlamaktır. Bu amaç doğrultusunda çalışmada öncelikle kurumsal risk yönetimi tanımlanarak kavramın ne ifade ettiği açıklanmıştır. Ardından COSO' nun 2004 yılında yayınladığı kurumsal risk yönetimi raporu dikkate alınarak raporda bahsi geçen ve kurumsal risk yönetiminin ana bileşenlerini oluşturan sekiz adet bileşene ve açıklamalarına yer verilmiştir. Özellikle "risk değerlendirme" bileşeni üzerinde durularak Bursa ilinde faaliyette bulunan bir işletmenin çeşitli yönetimsel kararlar alma durumlarında kurumsal risk yöneticisi tarafından hazırlanarak yönetim kuruluna sunulan risk değerlendirme raporları detaylı şekilde incelenmiştir. İnceleme sürecinde işletmenin kurumsal risk yöneticisi ile görüşülmüş ve karşılıklı görüş alışverişinde bulunulmuştur. Yapılan detaylı risk değerlendirme rapor incelemesinin ve sağlanan görüş alışverişinin ardından bir risk değerlendirme raporunda hangi başlıkların bulunması gerektiğine dair bir çalışma yapılmıştır. Son olarak işletmelerin risk değerlendirme raporu hazırlamalarında izleyebilecekleri adımlar ve bu adımlarda yürütülebilecek faaliyetler önerilmiş ve kullanılabilecek örnek formlar hazırlanmıştır. Formlar ilgili başlıklar altında tablo halinde sunulmuştur.

Kurumsal Risk Yönetimi

Kurumsal risk yönetimi, en kabul görmüş tanımla "İşletme genelinde uygulanan; işletmenin yönetim kurulu, yönetimi ve diğer personelinden etkilenen; işletmenin hedeflerine ulaşmasına ilişkin makul bir güvence sağlamak için işletmeyi etkileyebilecek potansiyel olayları tanımlamak ve belirlenen risk iştahı sınırları içinde yönetmek amacıyla tasarlanmış bir süreçtir (COSO, 2004, s.4). Tanımda bahsi geçen makul düzeyde güvence, riskin gelecek ile ilgili olması ve geleceğin de belirsizlik içermesi sebebiyle önceden kesin ve net bir tahmin yapılamaması düşüncesini temel almaktadır. Makul düzeyde güvence ifadesi ile an-

latılmak istenen işletmelerde kurumsal risk yönetim sistemi ne kadar etkin ve sağlıklı şekilde kurulmuş olursa olsun karar verme süreçlerinde alınan risk değerleme ve tutumlarına dair insan doğasından kaynaklanabilecek bazı hatalar söz konusu olabileceği ya da yapılacak kontrollerin engellenebileceğidir. Dolayısıyla hiçbir kurumsal risk yönetim sistemi işletmelere yüzde yüz bir güvence vermemektedir (Moeller, 2005, s.111).

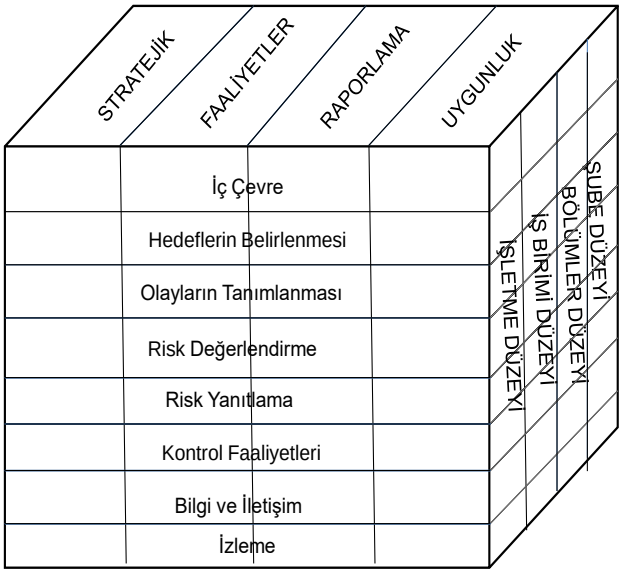
Kurumsal risk yönetimi birtakım temel unsurları da içerisinde barındırmaktadır. Buna göre kurumsal risk yönetimi (COSO, 2004, s.4),

- İşletmede devamlılık gösteren bir süreçtir.
- İşletmede yer alan her kademedeki çalışanlar tarafından etkilenmektedir.
- İşletmelerde stratejilerin belirlenmesinde kullanılmaktadır.
- İşletme genelinde her seviyede ve her birimde uygulanmaktadır.
- Gerçekleşmesi durumunda işletmeyi etkileyecek potansiyel olayları belirleyebilmek ve riski, saptanmış risk iştahı doğrultusunda yönetmek için tasarlanmıştır.
- İşletme yönetimine makul düzeyde güvence sağlamaktadır.
- İşletmede belirlenen hedeflere ulaşılabilmesi için bir araç olma niteliği taşımaktadır.
-

Geleneksel risk yönetim sistemlerinde işletmelerde risklerin birbirlerinden bağımsız ve ayrı olarak değerlendirildiği, sadece belirli risklere odaklanıldığı ve riskin sahiplenicilerinin bulunmadığı, riski daima azaltmaya yönelik bir risk yönetim anlayışının hakim olduğu göze çarparken, kurumsal risk yönetim sisteminde risklerin işletmenin geneli dikkate alınarak değerlendirildiği, kritik risklere odaklanmanın söz konusu olduğu, risklere yönelik stratejik olarak en uygun tepkinin belirlendiği ve işletmede risk yönetiminde tüm çalışanların sorumluluk sahibi olması gerektiği anlayışının hakim olduğunu söylemek mümkündür (Hall, 2007, s.4). Dolayısıyla kurumsal risk yönetim sisteminin işletmelerde, daha bilinçli kararlar alınması, daha fazla fikir birliği sağlanması ve yönetimle daha sağlıklı iletişim kurulması gibi konular da dahil olmak üzere işletme yönetiminin gelişimine de katkı sağladığı anlaşılmaktadır (Gates vd., 2012, s. 35).

COSO 2004 Kurumsal Risk Yönetimi Bileşenleri

COSO kurumsal risk yönetimi raporunda yer alan kurumsal risk yönetimi küpü, üç boyut olarak tasarlanmıştır. Bu üç boyut birbiriyle de ilişkilidir. Dolayısıyla küp bir bütün olarak ele alınıp incelenmelidir. Küpte Şekil 1'de yer aldığı gibi dikey sütunlar işletme hedeflerini göstermektedir. Yatay sütunlar ise, kurumsal risk yönetimini oluşturan sekiz adet bileşeni içermektedir. Küpün üçüncü boyutu ise işletme organizasyon yapısından oluşmaktadır. Söz konusu şekil bir işletmenin kurumsal risk yönetiminin bütününe veya hedef kategorisine, bileşenine, birimine veya herhangi bir alt kümesine odaklanma becerisini ifade etmektedir. Küpte yer alan sekiz bileşenin birbirini izler nitelikte olmalarından ziyade her bileşenin birbiriyle ilişkili olduğunu belirtmek daha doğrudur. Alt başlıklarda kurumsal risk yönetiminin sahip olduğu sekiz bileşen kısaca açıklanmaktadır.



Kaynak: COSO, 2004.
Şekil 1. COSO Kurumsal Risk Yönetimi Küpü

a. İç Çevre

Kurumsal risk yönetim bileşenlerinin temelinde rol oynayan iç çevre bileşeni, kurumsal risk yönetimi küpünde en üste yerleştirilmiştir. Risklerin işletme çalışanları tarafından nasıl algılanması ve karşılanması gerektiği hakkında bir temel oluşturmaktadır. Bununla birlikte iç çevre işletmenin risk iştahını, risk yönetim felsefesini ve işletme faaliyetlerinde yer alan etik değerleri de kapsamaktadır. İşletmenin faaliyet gösterdiği çevre de bu bileşen kapsamında ele alınmaktadır (COSO, 2004, s. 22).

İç çevre, işletmede stratejilerin ve hedeflerin ne şekilde oluşturulması gerektiği, risk ile ilişkili olan faaliyetlerin nasıl yürütüldüğü, risklerin nasıl tanımlandığı, risklere karşı ne şekilde bir tavır sergilenerek yönlendirileceği konularında da etkili olmaktadır (Moeller, 2011, s. 56). Öte yandan iç çevre bileşeni birçok öğeden de etkilenmektedir. Bu öğelere, işletme yönetim felsefesi ve işletmenin çalışma biçimi, yönetim kurullarının ve bu kurullara bağlı komitelerin fonksiyonları, işletmede oluşturulan organizasyonel yapı ve bu yapıya bağlı olarak yetkilerin ve sorumlulukların dağılımı, işletme çalışanlarına karşı benimsenmiş olan politika ve prosedürler, iç denetim faaliyetlerini de kapsayan kontrol sistemleri örnek olarak verilebilir (İbiş ve Çatıkkaş, 2012, s.106).

b. Hedeflerin Belirlenmesi

Hedef belirleme bileşeni, işletmede belirlenen stratejik ve operasyonel hedefleri, işletmenin risk toleransı ile risk iştahını ve bunların her birinin işletmenin misyon ve vizyonu ile olan ilişkilerini içermektedir. Hedef belirleme sürecinde bu ilişkiler işletme tarafından da dikkate alınmalıdır (Schanfield vd., 2005, s.1).

İşletme başarısını etkileme olasılığı bulunan potansiyel olayların tanımlanması için öncelikle işletmede hedeflerin belirlenmiş olması gerekir. Kurumsal risk yönetimi, işletmenin risk alma eğilimini de göz önünde bulundurarak işletme misyon ve vizyonuna uygun olarak belirlenen hedeflerin işletme içinde sağlıklı bir şekilde gerçekleştirilmesine katkıda bulunmaktadır. Tüm işletmeler, iç ve dış kaynaklı olarak bir takım risklerle karşı karşıya kalmaktadır ve olay tanımlama, risk değerlendirme ve risk yanıtlama bileşenlerinin kurumsal risk yönetim sistem-

lerinde varlık gösterebilmesinin ön koşulu hedeflerin belirlenmesidir. Kurumsal risk yönetiminin işletmelerde söz konusu olabilmesi için ilk önce yönetimin operasyonel, raporlama ve uygunluk hedeflerini de kapsayacak şekilde stratejik hedeflerini belirlemiş olması gerekmektedir.

c. Olay Tanımlama

Olay tanımlama bileşenini "*risk tanımlama*" olarak da ele alan çalışmalar (Gacar, 2016; Güneş, 2009) mevcuttur (Pehlivanlı, 2010, s.74). Ancak COSO' nun raporunda yer alan kurumsal risk yönetim küpünde üçüncü bileşen olarak "Event Identification" kavramı ifade edilmiştir. Bu çalışmada kurumsal risk yönetimi bileşenleri bahsedilen rapor temel alınarak açıklandığından üçüncü bileşenin "Olay Tanımlama" olarak açıklanması daha uygun görülmüştür. Burada olay olarak tanımlanan kavram, esasında risktir.

İşletme yönetimi, işletmenin belirlediği hedeflerine ulaşılmasına etki edecek (engel olacak) olayları (ya da riskleri) saptamalıdır. Bu anlamda risk, belirlenen hedeflere ulaşılmasında etkisi olabilecek bir olayın olasılığıdır (Matyjewicz ve D'arcangelo, 2004, s.7). Dolayısıyla yönetim, gerçekleşmesi halinde işletmeye etki edecek potansiyel olayları saptar ve söz konusu bu olayların fırsatları temsil edip etmediklerini ya da hedeflere ulaşılmasını negatif olarak etkileyip etkileyemeyeceklerini belirler. Negatif etki meydana getirecek olaylar, değerlendirme yapılmasının ardından bir tutum belirlenmesini zorunlu kılan riskleri temsil ederken pozitif etki meydana getirecek olaylar ise, fırsatları temsil etmektedir (COSO, 2004, s.41). Bu noktada işletmede sürdürülen kurumsal risk yönetimi faaliyetleri, işletmede negatif etkiye sahip olayların bu etkisini minimuma indirgemek ve pozitif etkiye sahip olayların etkisini de en üst seviyeye çıkarmak üzere işletmelere destek olmaktadır (Marchetti, 2012, s.38).

Olay tanımlamasında, belirsizliklerin her zaman söz konusu olduğu ve bir olayın meydana gelip gelmeyeceğinin, ne zaman olacağının ve gerçekleştiği takdirde etkisinin kesin olarak bilinemeyeceği gerçeği yönetim tarafından kabul edilmektedir. Bu nedenle yönetim, öncelikle etkinin pozitif mi negatif mi olduğuna odaklanmadan içsel ve dışsal faktör kaynaklı bir dizi muhtemel olayı değerlendirir. Böylelikle sadece negatif

etkiye sahip olan olayları değil aynı zamanda pozitif etkiye sahip olayları bir başka deyişle fırsatları da tanımlama şansı yakalar. Olayların tanımlanması aşamasında, işletme genelinde dikkate alınan ve olayları etkileyen içsel faktörleri, altyapı faktörleri, çalışanların faktörü, süreç ile ilgili faktörler, teknoloji faktörü olarak; dışsal faktörleri ise, ekonomik faktörler, doğal çevre faktörü, politik faktörler, sosyal ve teknolojik faktörler olarak sıralamak mümkündür (COSO, 2004, s.41-42). Görüldüğü gibi içsel faktörler işletmenin iç yapısı ve işleyişi ile ilgili olan faktörleri ifade etmektedir. Dışsal faktörler ise daha çok işletmenin dış çevresinden kaynaklanan faktörleri içermektedir.

d. Risk Değerlendirme

Risk değerlendirme bileşeni, işletmede risklerin ne şekilde yönetileceğini belirleyip bu yönde risk yanıtları geliştirebilmek adına risklerin olasılıklarını ve sonuçlarını göz önünde bulundurarak analiz edilmesini ifade etmektedir (Kalyoncu, 2013, s.118).

Risk değerlendirmenin, kurumsal risk yönetimi bileşenleri arasında de kilit bir rolü bulunduğunu söylemek mümkündür. Kurumsal risk yönetimi bileşenlerinden iç çevre, hedef belirleme ve olay tanımlama bileşenlerinin işletmede bilgi toplanmasına ve genel itibariyle bir çerçeve oluşturulmasına katkıda bulunduğu düşünülürse risk değerlendirme, risk yanıtlama, kontrol faaliyetleri, bilgi-iletişim ve izleme bileşenlerinin de risklere karşı daha ziyade bir faaliyet alanı olduğu düşünülebilir. Bu noktada risk değerlendirme sürecinin verileri söz konusu riskle ilgili faaliyetlere yön verecektir (Pehlivanlı, 2010, s. 78).

Risk değerlendirme sürecinin önemli bir parçası olarak yönetim, riskleri doğal (inherent) ve artık (residual) riskler olarak göz önünde bulundurmalıdır (Moeller, 2011, s. 71). Doğal risk, genel ifadeyle yönetimin riskin gerçekleşme olasılığını ya da etkisini değiştirmek için herhangi bir faaliyette bulunmadığı durumda meydana gelen risktir (COSO, 2004, s. 49). Doğal riskler, riski yönetmek adına herhangi bir faaliyet yürütülmediğinde söz konusu olmakta (The Orange Book, 2004, s. 49) ve dolayısıyla olayların doğasında bulunmaktadırlar. İşletme yönetimi riske ilişkin herhangi bir tedbir almadığında, kendi kendine meydana gelecek olan risklerdir (Ernst & Young, 2005). Artık risk ise,"*yönetimin, olumsuz*

bir olayın etkilerini ve gerçekleşme ihtimalini azaltmak amacıyla, riski gidermeye yönelik aldığı tedbirler veya hali hazırda uyguladığı mevcut iç kontrollere rağmen kalan risktir"[2] (İç Kontrol Temel Terimler Sözlüğü). Artık riskler, riski yönetmek için gerekli faaliyetlerin yürütülmesinin ardından yani yönetimin riske tepkisinin ardından kalan risklerdir (The Orange Book, 2004, s. 49). Her ne kadar bu risklere karşı işletme yönetiminin tepkileri ve önlemleri uygulansa da işletmede her zaman bir miktar artık risk söz konusu olacaktır (Moeller, 2011, s. 71). Doğal ve artık riskler çeşitli kaynaklarda, içsel ve kalıntı riskler (Ekici, 2015; Pehlivanlı, 2010; Ernst & Young, 2005) olarak da açıklanmıştır.

Risk değerlendirmesi, işletmede olaylara ilişkin potansiyel risklerin hedeflere ulaşma üzerindeki etki derecelerinin değerlendirilmesine olanak sağlar. Bu anlamda riskler, gerçekleşme ihtimali (olasılık) ve potansiyel etkisi (etki) olmak üzere iki perspektiften değerlendirilir (Moeller, 2011, s. 71). Belirlenen potansiyel risklerin gerçekleşme ihtimallerini ve gerçekleştikleri takdirde olası etkilerinin tahmin edilmesi ve buna göre bir sınıflandırma yapılarak öncelik verilmesi risk değerlendirme sürecinde yer alır (Derici, 2015, s. 19). İşletme yönetimi, söz konusu değerlendirme sürecinde nitel ve nicel tekniklerden yararlanabilir.

İşletmenin risk değerlendirme metodolojisi, hem nitel hem de nicel tekniklerden oluşan bir kombinasyonu içerebilmektedir. Risk değerlendirme için kullanılan teknikler, değerlendirmenin kapsamına ve risk faktörleriyle ilgili bilgilerin özelliklerine bağlı olarak farklılık gösterebilir (Kumaş ve Birgören, 2010, s. 32).

Nitel teknikleri yönetim, genellikle niceliksel değerlendirmeler için gerekli olan güvenilir verilerin mevcut olmadığı ya da verilerin elde edilmesinin ve analizinin fazla maliyetli olduğu durumlarda kullanmaktadır (COSO, 2004, s. 52). Bununla birlikte işletmede daha detaylı analiz yapılmasını gerektiren risklerin belirlenebilmesi için hazırlık çalışmaları esnasında ve bazı durumlarda değerlendirmeye tabi riskin yapısal özellikleri itibariyle de nitel tekniklerden yararlanma yoluna gidilebilir (TÜSİAD, 2008, s. 56). Riskleri derecelerini dikkate alarak kolaylıkla bir sıralamaya tabi tutabilmesi ve acil iyileştirilmesi gereken alanları tanımlaya-

[2] http://webdosya.csb.gov.tr/db/strateji/editordosya/TEMEL_TERIMLER_SOZLUGU.pdf.

bilmesi nitel tekniklerin avantajları olarak değerlendirilebilir (Kumaş ve Birgören, 2010, s. 32).

Nicel teknikler ise, veri kaynaklarını kullanarak gerçekleşme olasılığı ve potansiyel etki tahminlerini rakamsal değerler kullanarak açıklamayı amaçlamaktadır. Nicel tekniklerden elde edilen sonuçların kalitesi teknikte kullanılan verilerin doğruluğuna ve bütünlüğüne ve şüphesiz teknikte kullanılan modelin geçerliliğine bağlı olmaktadır (TÜSİAD, 2008, s. 57). Nicel teknikler ile daha hassas sonuçlar elde edilmektedir ve daha karmaşık ve ileri düzey faaliyetlerin söz konusu olduğu durumlarda nitel teknikleri desteklemek için kullanılmaktadır. Çünkü nicel değerlendirme teknikleri genelde matematiksel modeller kullanarak yüksek derecede çaba ve titizlik gerektirmektedir (COSO, 2004, s. 52).

Her ne kadar nicel teknikler bilgisayar destekli matematiksel modellere ve rakamsal değerlere dayandığından göreli olarak nitel tekniklere kıyasla daha objektif bir teknik olma özelliği gösterse de özellikle kurumsal risk yönetim sisteminin kurulması ve risk değerlendirilme sürecinin başlangıç aşamalarında nitel tekniklerden yararlanılması önerilmektedir (Merna ve Al-Thani, 2008, s. 68).

e. Risk Yanıtlama

Risk değerlendirme bileşeninde risklerin analizlerinin yapılmasının ardından risk yanıtlama bileşeni ele alınmaktadır. Risklerin yanıtlanması kavramı, risk yönetiminin riskler karşısındaki faaliyet alanını oluşturmaktadır (Ekici, 2015, s. 107). Risklerin değerlendirilmesi sonucu elde edilen verilerin işletmede risk alma istekliliği ile karşılaştırılması suretiyle acil önlem alınması gereken riskler belirlenir. Ardından seçenekler arasından risk yanıtları (tutumları) tercih edilir (Pehlivanlı, 2010, s. 84).

İşletme tarafından tercih edilebilecek risk yanıtları; kaçınma, azaltma, paylaşma ve kabul etme olarak sıralanabilir. Bunlardan kaçınma stratejisi riske neden olan iş birimini satmak, endişe veren bir coğrafi bölgeden çıkmak ya da bir ürün grubunu bırakmak gibi faaliyetler yoluyla işletmenin riskten uzak durma durumudur. Esasen işletme çok düşük risk iştahına sahip olmadıkça, diğer bütün koşullar hali hazırda yolundayken sadece gelecekteki potansiyel risk temeline dayanarak bir faaliyet

alanından çıkması ya da ürün grubundan uzaklaşması oldukça zordur. Öte yandan eğer herhangi bir yatırım gelecekte daha büyük bir riski önlemeye yarayacak bir alana girmek için yapılıyorsa bu defa kaçınma tutumu potansiyel olarak daha maliyetli bir strateji olacaktır (Moeller, 2011, s. 74). Ancak işletme yönetimi, riskin olasılığını ve etkisini kabul edilebilir bir düzeye indirgeyecek seçeneği belirleyemezse, riske karşı uygun risk tutumu olarak kaçınma seçeneği seçilmelidir (Marchetti, 2012, s. 42).

Diğer bir risk yanıtı olan azaltma stratejisi ise risk olasılığını, etkisini veya her ikisini de azaltmak için harekete geçilmesini ifade etmektedir. Gerekli ve uygun kontroller ile risklerin olumsuz etkilerinin gerçekleşme olasılıklarının azaltılmasına ya da risklerin olumsuz etkilerinin derecesinin azaltılmasına yönelik gerçekleştirilen faaliyetlerdir (TÜSİAD, 2008, s. 60).

Paylaşma (transfer etme) stratejisini konu alan risk yanıtı ise riski bir varlıktan diğerine taşımayı içermektedir **(**Marchetti, 2012, s. 29). Paylaşma stratejisinde riskin tümünün ya da bir kısmının başka bir tarafça üstlenilmesi durumu söz konusudur (TÜSİAD, 2008, s. 60). Hemen hemen tüm işletmeler düzenli olarak risklerinden korunmak ya da risklerini paylaşmak için örneğin sigorta yaptırma yolunu tercih ederler. Bu risk yanıtında sigorta yaptırma yönteminden başka çeşitli farklı teknikler de mevcuttur (Moeller, 2011, s. 75). Bu paylaşım teknikleri içinde çeşitli anlaşmaların kullanılması, ortaklıklar kurma gibi yapılanmalar da sayılabilmektedir. Çoğunlukla riskin paylaşılması esnasında bir maliyet ortaya çıkacaktır. Bu sebeple riskin paylaşılması kararlarında fayda-maliyet analizi yönetim tarafından dikkatlice gerçekleştirilmelidir (TÜSİAD, 2008, s. 60-61).

Son olarak işletme yönetimi, zaman zaman işletmede sürdürülen faaliyetlerin doğası gereği bir takım kaçınılmaz riskleri kabul etmek durumunda kalabilmektedir. Kimi durumlara yönelik fayda-maliyet analizi uygulandığında riski azaltmak için gereken maliyet, onu üstlenmek için gereken maliyetten daha yüksek olduğu tespit edildiği takdirde risk yanıtı olarak kabul etme stratejisi benimsenebilir (Marchetti, 2012, s. 29). Bu stratejide Kabul etme riskin gerçekleşme olasılığını ya da etkilerini önlemek adına herhangi bir faaliyette bulunulmaz (COSO, 2004, s. 55). İşletmeler belirlenen risk toleransı ışığında bir riskin olasılığına ve

etkisine bakmalı ve ardından bu riskin kabul edilip edilmemesi konusunda karar vermelidir. İşletmede var olan çeşitli riskler için birçok yanıt tercih edilebilirse de kabul etme yanıtı çoğu zaman bazı riskler için en uygun stratejidir (Moeller, 2011, s. 75). Şüphesiz yönetimin kabul ettiği bu riskler risk yönetimi sürecinde de izlenmelidir (Marchetti, 2012, s. 29).

f. Kontrol Faaliyetleri

Kontrol faaliyetleri bileşeni ile uygun risk yanıtlarının gerçekleştirilmesini sağlamaya destek veren politika ve prosedürler kastedilmektedir. Kontrol faaliyetleri, işletmede yer alan birimlerin her seviyesinde yer almaktadır (Cendrowski ve Mair, 2009, s. 95). İşletmede risk yanıtları seçildikten sonra, yönetim bu risk yanıtlarının doğru zamanda ve etkili bir şekilde gerçekleştirilmesini sağlamaya yönelik, gereken kontrol faaliyetlerini yürütmelidir (Moeller, 2011, s. 78).

En yaygın olarak kullanılan kontrol faaliyetlerini üst düzey raporlar, faaliyet yönetimi, bilgi işlemleri, fiziksel kontroller, performans göstergeleri ile görev ve sorumlulukların ayrıştırılması olarak sıralamak mümkündür. Söz konusu faaliyetler çeşitli organizasyonel düzeydeki personel tarafından yaygın olarak uygulanan ve işletmenin hedeflerine ulaşması için ilerlemesini sağlayan birçok prosedür arasında sadece birkaçıdır. İşletme yapılarına bağlı olarak kontrol faaliyetlerini de çeşitlendirmek mümkündür. Genellikle işletmeler tarafından ilgili risk yanıtları için birkaç kontrol faaliyetinin birleşiminden oluşan bir kombinasyon kullanılması tercih edilmektedir (COSO, 2004, s. 62).

Kontrol faaliyetlerinin belirlenmesinde üzerinde durulması gereken noktalardan birisi de işletmede optimum kontrol seviyesinin belirlenmesidir. Kontrol faaliyetleri işletmede devam eden günlük rutin işleyişi engellemeyecek şekilde esnek, fakat hedeflere ulaşma olasılığını ve yönetimi destekleyecek şekilde de sert olmalıdır (TÜSİAD, 2008, s. 37).

g. Bilgi ve İletişim

Tüm işletmeler iç ve dış olaylarla ve faaliyetlerle ilgili geniş ölçüde sayısız bilgi elde etmektedir. Bu bilgiler, çalışanlara kurumsal risk yöne-

timini ve diğer sorumluluklarını yerine getirmelerini sağlayan bir form ve zaman çerçevesinde personele iletilmelidir. (COSO, 2004, s. 67). Kurumsal risk yönetim sürecinin her aşamasında, tüm bileşenlerinde ve kontrol faaliyetlerinde bilgi ve iletişim bileşeni merkezi bir rol üstlenmektedir. (Cendrowski ve Mair, 2009, s. 95). Çünkü risklerin tanımlanması, değerlendirmesi, değerlendirilen risklere yanıt verilmesi faaliyetlerinin yürütülmesi ve belirlenen hedeflere ulaşabilmesi için işletmelerin her seviyesinde bilgi gereklidir. Bilgi sistemleri, gerek işletmede üretilen gerekse dışsal faktörlerden kaynaklı gelen bilgileri kullanarak, riskleri yönetmek ve hedeflere uygun bilinçli kararlar vermek için bilgi sağlamaktadır (COSO, 2004, s. 67).

İletişim ise, bilginin işletme içerisinde aşağı yönde, yukarı yönde ve yatay olarak dolaşmasıdır. Aşağı yönde iletişimden kasıt yönetimin planlarından çalışanların haberdar olması, üst kademeden alt kademeye doğru yapılan bilgi akışıdır. Yukarı yönde iletişim ise alt kademeden üst kademeye doğru olan iletişimdir. Çalışanların, üst yönetimi bilgilendirmesi bu yönde bir iletişime örnektir. Yatay iletişim ise, aynı düzeydeki birimler arasında var olan iletişimdir (Pehlivanlı, 2010, s. 87).

İşletmede sağlıklı bir kurumsal risk yönetim sisteminin kurulması ve sürdürülebilmesi için tedarikçilerle, müşterilerle, çalışanlar ve pay sahipleri ile bağlantı kuran risk izleme ve iletişim sistemlerinin geliştirilmesine ihtiyaç duyulmaktadır. Bu şartı gerçekleştirmek geçmişte oldukça güç bir süreç olsa da, günümüzde web tabanlı veritabanlarının kullanımı ve özellikle büyük işletmelerde birçok tedarikçi ve müşterinin işbirliğinde bulunmaları bu bilgi bağlantılarını daha ulaşılabilir hale getirmektedir (Moeller, 2011, s. 83).

Etkili iletişimde tüm çalışanlar, üst düzey yönetimden kurumsal risk yönetimi ile ilgili sorumluluklarının dikkatle yerine getirilmesi gerektiğine dair açık bir mesaj alır. Kurumsal risk yönetimi konusundaki hem kendi rollerini hem de bireysel faaliyetlerinin diğer çalışanların faaliyetleri ile nasıl ilişkili olduğu hakkında bilgi sahibi olurlar. İletişim etkili bir şekilde şu maddeleri aktarmalıdır (COSO, 2004, s. 71):

- Etkin kurumsal risk yönetiminin önemi
- İşletmenin hedefleri
- İşletmenin risk iştahı ve risk toleransları
- Ortak bir risk dili

- Kurumsal risk yönetimi bileşenlerini etkilemek ve desteklemek için personelin rolleri ve sorumlulukları

İşletmeler, gerek işletme içinde ve dışında etkin iletişim sistemi kurabilmek için açık iletişim kanallarını oluşturmalı ve devamlılığına olanak tanımalıdır. Üst yönetim, yönetimin sorunları dinlemeye, hızlı ve uygun bir şekilde sorunları çözmeye istekli olduğuna dair çalışanların inanmasını sağlamalıdır. Bu adımın tamamlanmasının ardından yönetim, risk yönetimini korumanın yeterli olup olmadığını belirlemek için iletişim tarzı, süreci ve etkililiğini destekleyici teknolojik gelişmeleri de takip etmelidir (Marchetti, 2012, s. 46).

h. İzleme

İzleme bileşeni, işletmede uygun kontrollerin bulunduğuna, prosedürlerin anlaşıldığına ve takip edildiğine dair bir güvence sağlamayı öngören bir süreci ifade etmektedir (Griffiths, 2005, s. 25).

Her işletme, kurduğu kurumsal risk yönetim sisteminin izleme sürecinde dikkatli olmalıdır. Yönetim, sürekli izleme sürecinde, işleyen sistemin etkinliğinin sürdürülüp sürdürülmeyeceğinin belirlenmesini kolaylaştıran bilgi edinmeyi sağlamalıdır (Marchetti, 2012, s. 6). Zira işletmelerde kurulan kurumsal risk yönetimi sistemleri zaman içerisinde değişime uğramaktadır. Geçmişte işletmede etkili olan bir risk yanıtı bir süre sonra geçerliliğini ya da etkisini kaybedebilir. Yine benzer şekilde kontrol faaliyetleri de zamanla daha az etkili hale gelebilir. Bu tür değişiklikler karşısında yönetim, kurumsal risk yönetim sisteminin işleyişinde etkinliğin sürdürülüp sürdürülemeyeceğini belirlemelidir. İzleme, yürütülen faaliyetler üzerinden ya da ayrı değerlendirmeler şeklinde iki yoldan yapılabilir. Kurumsal risk yönetim sistemleri genellikle bir dereceye kadar devamlı olarak kendilerini izlemek üzere yapılandırılmıştır. Bu izlemenin derece ve etkinliği ne kadar yüksek olursa, ayrı değerlendirmelere de daha az ihtiyaç duyulur. Yönetim, sürdürülen risk yönetiminin etkililiği konusunda makul bir güvenceye sahip olmak için gereken ayrı değerlendirmelerin sıklığına kendisi karar verir. Genellikle, devam eden izleme ve ayrı değerlendirmelerin bir kombinasyonu, kurumsal risk yönetiminin zaman içindeki etkinliğini sürdürmesini sağlamaktadır (COSO, 2004, s. 75).

Yöntem

Bu çalışmada yöntem olarak nitel araştırma tercih edilmiştir. Veri toplama yöntemi olarak doküman incelemesi ve yerinde gözlem yöntemi kullanılmıştır. Çalışmada Bursa ilinde faaliyette bulunan bir işletmenin çeşitli yönetimsel kararlar alma durumlarında kurumsal risk yöneticisi tarafından hazırlanarak yönetim kuruluna sunulan risk değerlendirme raporları detaylı şekilde incelenmiştir. İnceleme esnasında raporlarda eksik görülen hususlar işletmenin kurumsal risk yöneticisi ile görüşülmüş ve karşılıklı görüş alışverişinde bulunulmuştur. Yapılan detaylı incelemenin ve sağlanan görüş alışverişinin ardından bir risk değerlendirme raporu hazırlanırken hangi adımların uygulanması gerektiğine dair bir çalışma yapılmıştır. Adımların her biri alt başlık haline getirilmiş ve adımlarda yürütülmesi önerilen faaliyetler ilgili alt başlıklarda açıklanmıştır. Faaliyetler esnasında kullanılabilecek çeşitli formlar da geliştirilmiştir.

Kurumsal Risk Yönetiminin Bir Parçası Olarak Risk Değerlendirme Raporları

Kurumsal risk yönetimi bileşenleri hakkında ayrıntılı bilgilerin verilmesinin ardından bu başlıkta özellikle risk değerlendirme bileşeninden hareketle risk değerlendirme raporları üzerinde durulmuştur.

Risk değerlendirme raporları, alacakların yönetilmesi, tedarikçi seçimi, pazarlama uygulamaları gibi herhangi bir faaliyet, yatırım ya da ticaret yapma kararları alma vb.'ne ait çok çeşitli durumlarda ve gerekli görülmesi halinde işletme yöneticilerinin özel talepleri doğrultusunda da hazırlanabilen raporlardır. Bu tür risk değerlendirme raporları, işletmelerde hazırlanan özel raporlar kapsamında olmakla birlikte yapı itibariyle risk değerlendirme süreci açısından işletmede hazırlanan diğer rutin risk değerlendirme raporlarından herhangi bir farklılık göstermemektedirler.

Bu başlıkta doküman incelemesi ve yerinde gözlem yöntemleri kullanılarak uygulama yapılan işletmenin risk değerlendirme raporlarından hareketle risk değerlendirme raporları hazırlanırken uygulanması gerekli adımlar alt başlıklar haline getirilmiş ve yürütülecek

faaliyetler açıklanmıştır. Faaliyetler esnasında kullanılabilecek çeşitli formlar ilgili başlıkların altında yer almaktadır.

1. Risk Değerlendirme Raporunun Hazırlanmasına Esas Teşkil Eden Konunun Tanımlanması ve Durum Değerlendirmesinin Yapılması

Risk değerlendirme raporlarının hazırlanma sürecinde öncelikle raporun hazırlanmasına sebep teşkil eden konu ortaya konmalıdır. İçerik; yeni bir yatırım kararı alma, yeni bir tedarikçi ile anlaşma, yurtdışı ticareti, yeni bir projeye başlanması, üretim durdurma vb. gibi işletmeyi ilgilendiren herhangi bir konu olabilir ya da mevcut bir durumun gözden geçirilmesi maksadıyla işletme yöneticilerinin rapor hazırlanması hususunda özel bir talepleri söz konusu olabilir. Burada önemli olan nokta konunun net bir şekilde ortaya konmasıdır. Daha sonra mevcut konuya ilişkin durum değerlendirmesi yapılmalıdır. Durum değerlendirmesi için konunun niteliğine bağlı olarak beyin fırtınası yöntemi, geçmiş yıllara ait elde bulunan verilerin incelemesi, SWOT analizi, mali tablo analizleri, senaryo analizleri, duyarlılık analizleri, çalıştay düzenleme vb. gibi çeşitli tekniklerden biri ya da birkaçı kullanılabilir.

2. Mevcut Konunun İçerdiği Ana Risk Sınıflarının Belirlenmesi

Risk değerlendirme raporunun hazırlanmasına sebep teşkil eden konunun açıkça ortaya konulması ve konuya ilişkin durum değerlendirmesinin yapılmasının ardından konuyla bağlantılı işletmenin karşı karşıya kalabileceği tüm riskler belirlenebilecektir. Gerçekleştirilecek bir toplantı sayesinde durumla ilişkili belirlenen tüm riskler, ana risk sınıflarına ayrılmalıdır. Toplantıya Chief Risk Officer (CRO), riskin erken teşhisi ya da risk yönetim komitesi ve konuyla ilgili sorumlu çalışanların katılımı sağlanmalıdır.

3. Ana Risk Sınıflarının Alt Risk Sınıflarına Ayrılması

Bu adımı durum değerlendirmesi yapılmak suretiyle belirlenmiş ana risk sınıflarının detaylandırılarak daha alt risk sınıflarına ayrımının yapılması süreci oluşturmaktadır. Bu aşamada CRO ile riskin erken teşhisi ya da

risk yönetim komitesinde yer alan kişiler koordineli olarak çalışmalıdır. İhtiyaç duyulması halinde konuyla ilgili sorumlu çalışanların tekrar görüşlerine başvurulabilir. Risklerin niteliklerine bağlı olarak daha detaylı analiz çalışmaları gerçekleştirmek gerekli olabilir.

4. Her Alt Risk Sınıfına Ait Risklerin Tanımlanması

Alt risk sınıflarının belirlenmesinin ardından her bir alt risk sınıfı için konuya ait risk tanımlanmalıdır. Burada amaç risklerin anlaşılır nitelikte açık ve net olarak ortaya konmasını sağlamak olmalıdır. Risk tanımlarının yapılması sayesinde konuyla ilgili karar alacak kişilerin konuya ait riskler hakkında aynı bilgi düzeyine sahip olması ve riskleri aynı şekilde algılaması sağlanabilecektir. Raporun hazırlanmasına esas teşkil eden konunun niteliğine bağlı olarak ana ve alt risk sınıflarının çeşitleri şüphesiz işletmeden işletmeye farklılık gösterecektir. Ana ve alt risk sınıflarının belirlenmesi, bu sınıflandırmaya göre yapılacak risk tanımları için kullanılabilecek örnek bir form Tablo 1'de yer almaktadır.

Tablo 1. Risk Değerlendirme Rapor Konusuna Ait Risklerin Tanımlanması

Durumdan Kaynaklı Ortaya Çıkabilecek Ana Risk Sınıfları	**Alt Risk Sınıfları**	**Tanımlanan Risk**
Politik Riskler	• Savaş • Diplomatik Şartlar • Ekonomik Yaptırımlar • Ülke Riskleri	• ……
Yasal Riskler	• Vergiler • Kanunlar • Sınırlamalar (Kotalar) • …….	• ……
Sözleşmeden Kaynaklı Riskler	• ……	• …….
Finansal Riskler	• Kredi Riskleri • ……	• ……
Üretim Riskleri	• Kapasite Artışı Riskleri • İş Gücü Riskleri	• ….
Tedarikçi Riskleri	• ……..	• ……
Satış Riskleri	• …….	• …….
Teknoloji Riskleri	• ……..	• …….
Kalite Riskleri	• ……	• …….
İtibar Riski	• ……..	• …….
Stratejik Riskler	• ……	• …….
…..	• …..	• …….

5. Tanımlanan Risklerin Değerlendirilmesi ve Önceliklendirilmesi

Risklerin sınıflandırılmasının ve her bir sınıfa ait risklerin tanımlarının yapılmasının ardından söz konusu riskler için değerlendirme ve önceliklendirme çalışmalarının yürütülmesi gerekmektedir. Değerlendirme çalışmalarında belirlenen risklerin ortaya çıkma olasılıkları ve ortaya çıktıklarında işletmenin karşı karşıya kalacağı olası sonuçlar incelenmelidir. Ana riskler ile ilgili belirlenmiş bir risk iştah seviyesi mevcut ise bu seviye de mutlaka göz önünde bulundurulmalıdır. Ayrıca risklerin değerlendirilmesinde anahtar risk göstergelerinden de yararlanılmalıdır. Önceliklendirme çalışmaları ise konuyla bağlantılı olarak risk değerlendirmelerinin yapılmasını ve en önemli ve acil müdahale edilmesi ya da kontrol altında tutulması gereken risklerin belirlenmesini kapsamaktadır. Risk değerlendirme rapor konusuna ait olan risklerin değerlendirilmesi sürecinde kullanılabilecek örnek bir form Tablo 2'de yer almaktadır.

Tablo 2. Risk Değerlendirme Rapor Konusuna Ait Risklerin Değerlendirilmesi

Risk Değerlendirme Raporunun Konusu					**Rapor No:**		
					Düzen. Tarihi:		
Rapora Ait Tanımlanan Risk (A)	Riskin Kaynağı (İç/Dış) (B)	Anahtar Risk Göstergesi(C)	Riskin GerçekleşmeOlasılığı (D)	Riskin Olası Etkisi (E)	Top. Risk Puanı (D x E)	Risk Seviyesi (Düşük/ Orta/ Yüksek)	Riskin Olası Sonucu
Düzenleyen Birim	**Risk Değerlendirmesini Gerçekleştirenin Adı Soyadı**				**Onaylayan Birim**		

6. Risklere Ait Eylem Planlarının Belirlenmesi

Değerlendirilmesi yapılan ve önceliklendirilen riskler için eylem planları oluşturulmalıdır. Eylem planları, riskleri kontrol altında tutabilmek ya da bertaraf edebilmek için işletme tarafından belirlenen planlardır. Riskler ve risklerden kaynaklı olası sonuçlar göz önünde bulundurularak bir eylem planlaması yapılmalıdır. Risklere ait eylem planlaması yapılırken bir takvim oluşturulması ve eylem planlarından sorumlu kişilerin atanması da gereklidir. Eylem planı belirlenmiş olan bir riskin kaynağının ve dayanak noktasının da kaydedilmesi, tanımlanan risk ile riske ait eylem planının uyumunun görülmesi yönünden fayda sağlayacaktır. Gerekli görüldüğü takdirde eylem planına ait önemli açıklamalara da yer verilmelidir. Bir risk değerlendirme raporunda eylem planlarının oluşturulması ve takibinin yürütülmesinde Tablo 3'te önerilen örnek form kullanılabilir.

Tablo 3. Risk Değerlendirme Rapor Konusuna Ait Eylem Planlarını Belirleme

Değerlendirilen Risk: ……			**Risk Kodu:** **Tarih:**	
Değerlendirilen Risk için Belirlenen Eylem Planı	Eylem Planı Sorumlusu	Plan. Tarihi	İzleme sorumlusu	Açıklama
Düzenleyen Birim			**Onaylayan Yönetim Temsilcisi**	

7. Risk Değerlendirme Raporunun Sunulması

Risk değerlendirme raporu hazırlanmasına yönelik faaliyetlerin son adımını hazırlanan risk değerlendirme raporunun sunulması oluşturmaktadır. Risk değerlendirme raporları, risk komitesi tarafından yöne-

tim kurulu başkanı ve genel koordinatöre raporlanmaktadır. Yönetim kuruluna sunulan risk değerlendirme raporları ile ilgili alınan kararlar, yönetim kurulu karar defterine işlenecektir.

Sonuç

Risklerin değerlendirilmesi, COSO' nun 2004 yılında yayınladığı kurumsal risk yönetimi raporundaki kurumsal risk yönetim küpünde bahsi geçen sekiz kurumsal risk yönetim bileşenlerinden bir tanesidir. Risk değerlendirme bileşeni genel olarak kurumsal risk yönetim sistemlerinde tanımlanan risklerin analizinin yapılmasını ifade etmektedir.

Kurumsal risk yönetim sistemlerinin işletmelerde işleyiş sürecinde önemli etkiye sahip olan risk değerlendirme aşaması işletmelerin karar alma süreçlerine dahil olan risklerin detaylı analizini yapmak suretiyle risk yönetimine yön vermektedir. Bu noktada en az risk değerlendirme aşamasında yapılan analizler kadar önemli olan ve işletmede gerekli görüldüğü takdirde üst yönetimin özel talebi doğrultusunda ya da herhangi bir faaliyet, yatırım ya da ticaret yapma kararları alma gibi durumlarda kurumsal risk yöneticisi tarafından hazırlanarak yönetim kuruluna sunulan risk değerlendirme raporlarının da kurumsal risk yönetim sistemlerinin işleyiş amaçlarına cevap verebilecek şekilde hazırlanması gereklidir.

Bu görüş doğrultusunda Bursa ilinde faaliyet gösteren ve kurumsal risk yönetim sistemine yönelik çeşitli faaliyetlerde bulunan bir işletmenin belirli dönemlerde hazırladığı ve yönetim kuruluna sunduğu risk değerlendirme raporları detaylı olarak incelenmiştir. İnceleme esnasında raporlarda eksik görülen hususlar işletmenin kurumsal risk yöneticisi ile görüşülmüş ve karşılıklı görüş alışverişinde bulunulmuştur. Yapılan detaylı incelemenin ve sağlanan görüş alışverişinin ardından bir risk değerlendirme raporunda hangi başlıkların bulunması gerektiğine dair bir çalışma yapılmıştır. İncelenen çok sayıda rapordan hareketle işletmelerin risk değerlendirme raporu hazırlamalarında izleyebilecekleri adımlar ve bu adımlarda yürütülebilecek faaliyetler önerilmiştir.

Çalışma neticesinde bir risk değerlendirme raporunda bulunması gereken ana başlıklar aşağıdaki şekilde sıralanmıştır;

- Raporu konusunun tanımlanması ve konuyla ilgili durum değerlendirmesinin yapılması,
- Mevcut konunun içerdiği ana risk sınıflarının belirlenmesi,
- Ana risk sınıflarının, alt risk sınıflarına ayrılarak detaylandırılması,
- Her alt risk sınıfına ait risklerin tanımlanması,
- Tanımlanan risklerin değerlendirilmesi ve önceliklendirilmesi,
- Risklere ait eylem planlarının belirlenmesi,
- Risk değerlendirme raporunun sunulması.

Şüphesiz kurumsal risk yönetim sistemlerinin her işletme için aynı şekilde kurgulanması ve sürece yönelik yürütülen faaliyetlerin aynı nitelikte olması mümkün değildir. Aynı şekilde işletmelerin bu süreçte hazırlayacağı risk değerlendirme raporlarının da gerek formatlarının gerekse içeriklerinin tüm işletmeler açısından aynı olmasını beklemek mümkün değildir. Ancak bu çalışmada kurumsal risk yönetim sistemini bünyesinde kurmak isteyen ve bu süreci hali hazırda yürüten işletmelerin çeşitli konularda hazırlayarak yönetim kurullarına sunacakları risk değerlendirme raporlarında bulunması gerekli ana başlıklar ve raporların hazırlanması sırasında yürütülmesi gereken faaliyetler ana hatlarıyla genel olarak tasarlanmıştır. Faaliyetlerin detaylandırılması ya da bazı faaliyet adımlarının atlanması elbette mümkündür. Ancak bu çalışmada bir risk değerlendirme raporunda olması gereken asgari temel konular üzerinde durulmuştur. Çalışmanın bundan sonraki kurumsal risk yönetim sistemleri kapsamında hazırlanacak risk değerlendirme raporlarının incelenmesini konu edinecek çalışmalara yol gösterici olması öngörülmektedir.

EXTENDED ABSTRACT

Preparation Of Risk Assessment Reports In Enterprise Risk Management System

*

Özlem Usman

Yalova University

Today, traditional risk management systems are increasingly replaced by enterprise risk management systems due to rapidly changing environmental, legal and economic conditions. The establishment of enterprise risk management systems and the effective management of the risks arising from the internal and external environment are vital for the companies to cope with the competitive environment and to be successful. Although businesses have a strong strategy, talented and competent workforce, efficient business processes and advanced technology, there is always the possibility of becoming vulnerable to a number of risks over time. Therefore, all enterprises need the existence of effective operational enterprise risk management systems.

The most important objective of the Committee of the Treadway Commission (COSO) was established in 1985; to reduce the possibility of errors and tricks in financial reports. In 2004, COSO published the "COSO Enterprise Risk Management Integrated Framework 2004". In this report, detailed information on enterprise risk management is given and eight components are described under the name of corporate risk management components.

One of the institutional risk management components mentioned in the COSO enterprise risk management report is the risk assessment risk component. Risk assessment is a key component among all other components. Because this concept basically refers to the analysis of the risks and directs the activities to be done about the risk management process in the enterprises. The main purpose of this study is to contribute to the operation of the enterprise risk management systems by proposing activities that can be carried out for the preparation of risk assessment reports

that form part of the corporate risk management system and various forms that can be used. For this purpose, firstly enterprise risk management is defined and the meaning of the concept is explained. After taking into consideration the enterprise risk management report published by COSO in 2004, eight components and explanations which are mentioned in the report and which constitute the main components of corporate risk management are given. In particular, the risk assessment report was prepared and the risk assessment reports prepared by the enterprise risk manager in various managerial decisions of an entity operating in the province of Bursa were examined in detail.

Methodology

Qualitative research was preferred as a method in the study. Document analysis and on-site observation method were used as data collection method. In the study, the risk assessment reports prepared by the enterprise risk manager and presented to the board of directors were examined in detail in various managerial decisions of an enterprise operating in the province of Bursa. Furthermore, during the review process, the Company's enterprise risk manager was interviewed and exchanged views. Following the detailed risk assessment report review and the exchange of views, a study was carried out on which headings should be found in a risk assessment report.

Findings & Discussion

As a result of the study, the steps that the enterprises can follow in preparing the risk assessment report and the activities that can be carried out in these steps were proposed and sample forms were prepared. The forms are presented in tabular form.

The main headings in a risk assessment report are listed as follows;

- Defining the subject of the report and conducting a situation assessment on the subject,
- Determination of the main risk classes included in the current issue,
- Detailing the main risk classes into sub-risk classes,

- Defining the risks of each sub-risk class,
- Evaluation and prioritization of identified risks,
- Determination of action plans for risks,
- Presentation of the risk assessment report.

Undoubtedly, it is not possible to establish enterprise risk management systems in the same way for each enterprise and to have the same nature of activities carried out. Likewise, it is not possible to expect that the risk assessment reports to be prepared by the enterprises in this process will be the same in terms of both their formats and their contents. However, in this study, the main headings and the activities that should be carried out during the preparation of the reports have been designed in general in order to prepare the enterprise risk management system within the body and prepare the companies that currently carry out this process on various subjects and present the risk assessment reports to be presented to the board of directors. It is of course possible to elaborate on activities or skip some of the operational steps. However, this study focuses on the minimum basic issues in a risk assessment report. It is foreseen that the study will guide the studies that will be examined about the risk assessment reports to be prepared within the scope of the corporate risk management systems.

Kaynakça/References

Cendrowski, H. ve Mair, W. C., (2009). *Enterprise risk management and COSO: A Guide for Directors, Executives and Practitioners*. New Jersey: John Wiley & Sons, Inc.

COSO, (2004). *Enterprise risk management- integrated framework*, Executive Summary Framework, COSO Publications, September.

Derici, O., (2015). *İç kontrol ve risk yönetimi*. Antalya: BEKAD Yayınları, Yayın No:21.

Ekici, H., (2015).*Kurumsal risk yönetimi*. Konya: Çizgi Kitabevi.

Ernst ve Young, (21 Nisan 2005). *Kurumsal yönetim ilkeleri doğrultusunda risk yönetimi ve muhasebe denetimi. 26 Nisan 2018 tarihinde https://www.slideserve.com/wyoming-potts/21-nisan-2005 adresinden alındı.*

Gacar A., (2016). *İşletmelerde kurumsal risk yönetimi varliğinin belirleyicileri.*Yayınlanmamış Doktora Tezi, Celal Bayar Üniversitesi, Sosyal Bilimler Enstitüsü, Manisa.

Gates S., Nicolas, J. L. ve Walker P.L., (2012). Enterprise risk management: A process for enhanced management and improved performance. *Management Accounting Quarterly*, 13(3), 28-38.

Griffiths, P., (2005). *Risk-based auditing*. England: Gower Publishing.

Güneş, Ş., (2009). *Kurumsal risk yönetimi ve Türkiye'de farkındalığına ilişkin bir uygulama.* Yayınlanmamış Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Hall, J., (2007) . Internal auditing and ERM: Fitting in and adding value., Esther R. Sawyer Scholarship Essay, 2007, https://global.-theiia.org/about/about-the-iia/Public%20Documents/Sawyer-_Award_2007.pdf, (01.09.2018).

İbiş, C., Çatıkkaş, Ö., (2012). İşletmelerde iç kontrol sistemine genel bakış. *Sayıştay Dergisi*, 85, 95-121.

İç Kontrol Temel Terimler Sözlüğü, 100 Kelimede İç Kontrol, http://webdosya.csb.gov.tr/db/strateji/editordosya/TEMEL_TERIMLER_SOZLUGU.pdf, (16.09.2018).

Kalyoncu, D., (2013). *Risksiz risk yönetiminin alternatif yolları.*Yayınlanmamış Yüksek Lisans Tezi, Okan Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Kumaş, E. ve Birgören, B., (2010). E-Devlet kapısı projesi bilgi güvenliği ve risk yönetimi: Türkiye uygulaması.*Bilişim Teknolojileri Dergisi*,3(2), 29-36.

Marchetti, A., (2012.). *Enterprise risk management best practices*. New Jersey: John Wiley & Sons.

Matyjewicz, G. ve D'arcangelo J.R., (2004). ERM based auditing. *Internal Auditor*, November/December, 4-18.

Merna, T. ve Al-Thani, F., (2008). *Corporate risk management*, Second Edition. England: John Wiley & Sons.

Moeller, R., (2005). *Brink's modern internal auditing*. New Jersey: John Wiley & Sons, Sixth Edition.

Moeller, R., (2011). *COSO enterprise risk management*, Second Edition. New Jersey: John Wiley & Sons.

Pehlivanlı D., (2010). *Modern iç denetim*, İstanbul: Beta Basım A.Ş. 1. Baskı.

Schanfield A., Miller M., Roth J., ve Espersen D. (2005). A sustainable approach to ERM", *Internal Auditor*, April, 62(2), 79-83.

TREASURY Her Majesty, (2004). *The orange book: Management of risk-principles and concepts*, London: HM Treasury.

TÜSİAD Risk Yönetimi Çalışma Grubu, (2008). *Kurumsal risk yönetimi*, Yayın No. TÜSİAD-T/2008-02/452.

Kaynakça Bilgisi / Citation Information

Usman, Ö. (2018). Kurumsal risk yönetim sisteminde risk değerlendirme raporlarının hazırlanması. *OPUS–Uluslararası Toplum Araştırmaları Dergisi, 9(16*), 1586-1612. DOI: 10.26466/opus.479277