

T.C.
AKSARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI

KURUMSAL RİSK YÖNETİMİ İÇİN WEB TABANLI RİSK ANALİZ PLATFORMU TASARIMI

YÜKSEK LİSANS TEZİ

MUHAMMED ÖZDEMİR

DANIŞMAN
DR. ÖĞR. ÜYESİ TARIK YILMAZ

AKSARAY 2019

AKSARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANA BİLİM DALI

KURUMSAL RİSK YÖNETİMİ İÇİN WEB TABANLI RİSK ANALİZ PLATFORMU TASARIMI

YÜKSEK LİSANS TEZİ

MUHAMMED ÖZDEMİR

DANIŞMAN
DR. ÖĞR. ÜYESİ TARIK YILMAZ

AKSARAY 2019

TELİF HAKKI VE TEZ FOTOKOPİ İZİN FORMU

Bu tezin tüm hakları saklıdır. Kaynak göstermek koşuluyla tezin teslim tarihinden itibaren 12(oniki) ay sonra tezden fotokopi çekilebilir.

YAZARIN

Adı : Muhammed

Soyadı : ÖZDEMİR

Bölümü : Yönetim Bilişim Sistemleri

İmza :

Teslim tarihi : 02.06.2019

TEZİN

Türkçe Adı : Kurumsal Risk Yönetimi İçin Web Tabanlı Risk Analiz Platformu Tasarımı

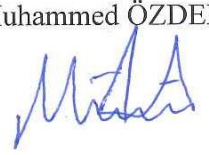
İngilizce Adı : Web Based Risk Analysis Platform Design for Enterprise Risk Management

ETİK İLKELERE UYGUNLUK BEYANI

Tez yazma sürecinde bilimsel ve etik ilkelere uyduğumu, yararlandığım tüm kaynakları kaynak gösterme ilkelerine uygun olarak kaynakçada belirttiğimi ve bu bölümler dışındaki tüm ifadelerin şahsıma ait olduğunu beyan ederim.

Yazar Adı Soyadı : Muhammed ÖZDEMİR

İmza :



T.C.

AKSARAY ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

JÜRİ ONAY SAYFASI

Muhammed ÖZDEMİR tarafından hazırlanan "KURUMSAL RİSK YÖNETİMİ İÇİN WEB TABANLI RİSK ANALİZ PLATFORMU TASARIMI" başlıklı tez çalışması aşağıdaki jüri tarafından oy birliği / oy çokluğu ile Aksaray Üniversitesi Yönetim Bilişim Sistemleri Anabilim Dalı'nda Yüksek Lisans tezi olarak kabul edilmiştir.

İMZA

Danışman: Dr. Öğr. Üyesi Tarık YILMAZ

Yönetim Bilişim Sistemleri ABD, Aksaray Üniversitesi ……

Üye: Doç Dr. İsmail KINACI

Aktüerya ABD / Selçuk Üniversitesi ……

Üye: Dr. Öğr. Üyesi Selçuk KILIÇ

Yönetim Bilişim Sistemleri ABD / Aksaray Üniversitesi ……

Tez Savunma Tarihi: 13/06/2019

Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun 04/07/2019 tarih ve 2019/27-12 sayılı kararı ile onaylanmıştır.

Öğrencinin

Muhammed ÖZDEMİR

İmza

Sosyal Bilimler Enstitüsü Müdürü

Doç. Dr. Sevilay USLU DİVANOĞLU

İmza

Annem ve Babama

TEŞEKKÜR

Tez çalışmam esnasında desteğini ve çayımı hiç eksik etmeyen değerli eşim Ayşe ÖZDEMİR, her daim desteklerini esirgemeyen kıymetli aile büyüklerim ve araştırmalarıma manen destek olan arkadaşlarıma ayrı ayrı teşekkür ederim. Ayrıca uzun yıllardır birlikte projeler geliştirdiğimiz saygıdeğer hocam Dr. Öğr. Üyesi Tarık YILMAZ'a teşekkür ederim.

AKSARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

KURUMSAL RİSK YÖNETİMİ İÇİN WEB TABANLI RİSK ANALİZ PLATFORMU TASARIMI

YÜKSEK LİSANS TEZİ

MUHAMMED ÖZDEMİR

AKSARAY 2019

ÖZET

Günümüzde insanlar yaşadıkları olaylar karşısında bilgi, beceri ve tecrübelerine göre tutum sergileyerek en az zarar, en fazla fayda ile olayları yönetmeye çalışmaktadır. Benzer şekilde kurumlar da faaliyetlerinde çeşitli risklere maruz kalmakta ve bunların yönetimi için farklı türde yöntemler kullanmaktadırlar. Sürekli gelişim ve değişim içerisinde olan piyasa şartlarına adapte olabilme, olası riskleri tamamen ortadan kaldırma ya da zararlarını en aza indirebilme ve risklerden kazanımlar elde edebilmeye yönelik kurumsal risk yönetim sistemlerinin kullanımı gün geçtikçe artmaktadır.

Geleneksel kurumsal risk yönetim sistemlerinde matbu formlar üzerinde faaliyetler yürütülmektedir. Bir veri tabanı kullanılmadan elektronik ya da kâğıt çıktısı formlar ile yapılan çalışmalarda zaman ilerledikçe geriye dönük veri ve bilgilerden yararlanmak zorlaşmaktadır. Risklerin artması verinin artmasına, verinin artması hesaplama zorluğuna buda riskler konusunda yanlış kararlar alınmasına sebep olmaktadır.

Bu çalışmada, kurumların risk süreçlerini her yerden yönetebileceği web tabanlı bir uygulama geliştirilmiştir. Geliştirilen uygulama ile kurumsal risk yönetim sisteminde, kurum yöneticilerinin oluşabilecek riskler için anlık kararlar verebilecekleri bir karar destek sistemi oluşturulmuştur. Risk yönetim faaliyetlerinde işlemler hızlandırılarak kolaylaştırılmıştır. Uygulama kurumlara göre esnek bir yapıda dizayn edilebilmektedir. Geliştirilen uygulama ile olayların risklerinin hesaplaması için kullanılan yöntemler, algoritmalar ve parametreler kullanıcı tarafından değiştirilebilmektedir. Bu sayede kurumun işleyiş yapısına uygun hesaplama modeliyle risk analizi yapılabilmektedir. Geçmiş verilere istenildiğinde ulaşılabilmekte ayrıca bu verilerden yararlanılarak gelecekte oluşabilecek risklerin şiddet ve olasılıkları hesaplanabilmektedir.

Bilim Kodu : 114606

Anahtar Kelimeler : Kurumsal Risk Yönetimi, Risk Analizi, Risk Yönetimi Karar Destek Sistemi

Sayfa Adedi : 127

Danışman : Dr. Öğr. Üyesi Tarık YILMAZ

AKSARAY UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES

WEB BASED RISK ANALYSIS PLATFORM DESIGN FOR ENTERPRISE RISK MANAGEMENT

M.S. THESIS

MUHAMMED ÖZDEMİR

AKSARAY 2019

ABSTRACT

Nowadays, people try to manage the events with the least harm and the most benefit by exhibiting their attitudes according to their knowledge, skills and experiences. Similarly, organizations are exposed to various risks in their activities and use different types of methods to manage them. Corporate risk management systems usage increasing day by day from the instutions, to adapt to market conditions that are constantly developing and changing, to eliminate potential risks completely or to minimize losses and to achieve gains from risks.

Activities are carried out on printed forms in traditional corporate risk management systems. In studies with electronic or paper print forms without the use of a database, it becomes difficult to benefit from retrospective data and information as time goes on. Increasing risks leads to increase in data, and increasing datas leads to increase difficulty in computation, which are leads to wrong decisions about risks.

In this study, a web-based application has been developed in which organizations can manage their risk processes from anywhere. With the application developed, a decision support system has been established in the corporate risk management system where corporate executives can make instant decisions for the risks that may occur. In risk management activities, transactions are accelerated and facilitated. The application can be designed in a flexible structure according to the institutions. With the developed application, the methods, algorithms and parameters used to calculate the risks of the events can be

changed by the user. In this way, risk analysis can be performed with the calculation model appropriate to the operational structure of the organization. Historical data can be accessed at any time and by using these data, the severity and probability of future risks can be calculated.

Science Code : 114606

Key Words : Enterprise Risk Management, Web Based Risk Analysis, Risk Management Decision Support System

Page Number : 127

Supervisor : Asst. Prof. Tarık YILMAZ

İÇİNDEKİLER

TELİF HAKKI VE TEZ FOTOKOPİ İZİN FORMU ... **Hata! Yer işareti tanımlanmamış.**

ETİK İLKELERE UYGUNLUK BEYANI..... **Hata! Yer işareti tanımlanmamış.**

TEŞEKKÜR.....v

ÖZET vi

ABSTRACT..... viii

İÇİNDEKİLER x

TABLOLAR LİSTESİ.....xvii

ŞEKİLLER LİSTESİ xix

SİMGELER VE KISALTMALAR LİSTESİ xx

GİRİŞ 1

1. BÖLÜM 3

RİSK ve İLGİLİ TANIMLAR.....3

1.1. Risk İle İlgili Temel Kavramlar 5

1.1.1. Belirsizlik ve Risk 6

1.1.2. Fırsat ve Risk.....6

1.1.3. Tehdit ve Risk 6

1.1.4. Risk Algısı.....7

1.1.5. Risk Zekası.....7

1.1.6. Risk Toleransı 8

1.1.7. Risk İştahı.....8

1.1.8. Risk Kütüğü.....9

1.2. Risk Türleri 10
1.2.1. Stratejik Riskler 11
1.2.2. Finansal Riskler 12
1.2.3. Operasyonel Riskler 12
1.2.4. Dış Çevre Riskleri 13
1.3. Diğer Risk Sınıflandırma Türleri 13
1.3.1. Sistematik Risk 13
1.3.2. Sistematik Olmayan Risk 13
1.3.3. Yönetilebilir Riskler 14
1.3.4. Yönetilemez Riskler 14
2. BÖLÜM 16
RİSK YÖNETİMİ 16
2.1. Riskin Erken Saptanması Ve Yönetimi 18
2.2. Risk Yönetiminin Faydaları 18
2.3. Risk Yönetim Sisteminin Gelişim Süreci 20
2.4. Geleneksel Risk Yönetimi Ve Kurumsal Risk Yönetimine Geçiş 22
2.5. Geleneksel Risk Yönetimi ile Kurumsal Risk Yönetimi Arasındaki Farklar 24
3. BÖLÜM 27
KURUMSAL RİSK YÖNETİMİ 27
3.1. Kurumsal Risk Yönetimi Kapsamı 31
3.2. Kurumsal Risk Yönetiminin Faydaları 31
3.2.1. Risk Yönetimine Kurumsal Yaklaşım 32
3.2.2. Risk Raporlama 32
3.2.3. İç Denetim Fonksiyonunun Geliştirilmesi 33
3.2.4. Kurumsal Verimlilik 33
3.2.5. Performans Artışı 34

3.2.6. Risk Yönetimine Proaktif Yaklaşım 34
3.2.7. Kurumsal Yönetim Anlayışı 35
3.3. KRY'nin Kurum Başarısına Etkisi 35
3.3.1. Risk İştahının Doğru Belirlenmesi 36
3.3.2. Risk, Büyüme Ve Karlılık İlişkisinin Belirlenmesi 36
3.3.3. Risklere Verilecek Karşılığın Kararlarını Belirleme 36
3.3.4. Risklerin Kurum Genelinde Tanımlanıp Yönetilmesi 37
3.3.5. Risklere Karşı Ortak Aksiyon Alınabilmesi 37
3.3.6. Karşılaşılabilecek Fırsatların Yakalanması 37
3.3.7. Kaynakların Doğru Yönetimi 37
3.4. Kurumsal Risk Yönetiminin Sınırlılıkları 38
4. BÖLÜM 39
KURUMSAL RİSK YÖNETİMİ BİLEŞENLERİ 39
4.1. COSO Kurumsal Risk Yönetim Modelinin Gelişimi 40
4.2. COSO Kurumsal Risk Yönetim Sistemi 41
4.2.1. İç Çevre 41
4.2.1.1. Risk Yönetim Felsefesi 43
4.2.1.2. Risk İştahı 45
4.2.1.3. Risk Toleransı 46
4.2.1.4. Yönetim Kurulunun Tutumu 46
4.2.1.5. Dürüstlük ve Etik Değerler 47
4.2.1.6. Yetenek Yükümlülüğü 47
4.2.1.7. Kurumsal Yapı 48
4.2.1.8. Yetki ve Sorumluluk Belirleme 49
4.2.1.9. İnsan Kaynakları Standartları 49
4.2.2. Hedeflerin Belirlenmesi 50

4.2.2.1. Stratejik Hedefler 51
4.2.2.2. Faaliyet Hedefleri 51
4.2.2.3. Raporlama Hedefleri 52
4.2.2.4. Uygunluk Hedefleri 52
4.2.3. Olayların Tanımlanması 52
4.2.3.1. Olay Tanımlama Teknikleri 54
4.2.3.1.1. Olay Envanteri Oluşturma 54
4.2.3.1.2. İç Analiz Yapma 55
4.2.3.1.3. Yükseliş ya da Başlangıç (Threshold) Tetikleyicileri 55
4.2.3.1.4. Atölye Çalışmaları ve Görüşmeler 55
4.2.3.1.5. Süreç Akış Analizi 55
4.2.3.1.6. Önemli Olay Göstergeleri 55
4.2.3.1.7. Kayıp Olay Veri Yöntemi 56
4.2.4. Risk Değerlendirme 56
4.2.4.1. Risk Tanımlama 58
4.2.4.1.1. Risk Tanımlamada Kullanılan Teknikler 60
4.2.4.2. Risk Değerlendirmede Kurumun Risk İştahı 64
4.2.4.3. Olasılık ve Etki Tahmini 64
4.2.4.4. Risklerin Analiz Edilmesi ve Ölçülmesi 66
4.2.4.5. Değerlendirme Teknikleri 67
4.2.4.5.1. Risk Haritası 69
4.2.4.5.2. Ön Tehlike Analizi (PHA) 69
4.2.4.5.3. İş Güvenlik Analizi (JSA) 70
4.2.4.5.4. Olursa Ne Olur? Analizi (What if?) 72
4.2.4.5.5. Kontrol Listesi Kullanarak Birincil Risk Analizi (Checklists CLA) 72

4.2.4.5.6. Birincil Risk Analizi (PRA) 74
4.2.4.5.7. Risk Analizi Karar Matrisi 75
4.2.4.5.8. Tehlike ve İşletilebilme Çalışması (HAZOP) 81
4.2.4.5.9. Hata Ağacı Analizi (FTA) 82
4.2.4.5.10. Olası Hata Türleri ve Etki Analizi (FMEA) 84
4.2.4.5.11. Güvenlik Fonksiyon Analizi (SFA) 86
4.2.4.5.12. Olay Ağacı Analizi (ETA) 86
4.2.4.5.13. Neden Sonuç Analizi (CCA) 87
4.2.4.5.14. Fine-Kinney Risk Analizi 88
4.2.5. Risk Tutumu 90
4.2.5.1. Riski Azaltma 91
4.2.5.2. Riski Paylaşma 91
4.2.5.3. Riski Kabul Etme 91
4.2.5.4. Riskten Kaçınma 92
4.2.6. Kontrol Faaliyetleri 92
4.2.6.1. Önleyici kontrol 93
4.2.6.2. Yönlendirici kontrol 93
4.2.6.3. Düzeltici kontrol 93
4.2.6.4. Denetleyici kontrol 93
4.2.7. Bilgi ve İletişim 94
4.2.8. İzleme 96
5. BÖLÜM 99
ARAŞTIRMANIN YÖNTEMİ 99
5.1. Sunucu Özellikleri 100
5.2. Platformun Belirlenmesi 100
5.3. Uygulama Geliştirme Dili 100

5.4. Veri Tabanı Özellikleri 101
5.5. Uygulamada Olması Gereken Modüller 101
6. BÖLÜM 102
KURUMSAL RİSK YÖNETİM UYGULAMASI 102
6.1. Uygulamanın Algoritması 102
6.1.1. Tehlikenin Tanımlanması 103
6.1.2. Tehlikenin Değerlendirilmesi 103
6.1.3. Tehlikenin Kapatılması 103
6.1.4. Tehlikenin Gerekli Görülmesi 103
6.1.5. Risklerin Tanımlanıp Hesaplanması 103
6.1.6. Olası Risklerin Değerlendirilmesi 104
6.1.7. Risklerin Kapatılması 104
6.1.8. Risk Azaltıcı Faaliyet Değerlendirmesi 104
6.1.9. Risk Azaltma Faaliyeti Yapılmadan Kapatılması 104
6.1.10. Riski Azaltma Faaliyeti Tanımı 104
6.1.11. Risk Azaltma Faaliyetinin Değerlendirilmesi 105
6.1.12. Risk Azaltma Faaliyetlerinin Yapılması 105
6.1.13. Yapılan Faaliyetlerin Değerlendirilmesi 105
6.1.14. Riskin Son Durumunu Tanımlama 106
6.1.15. Sürecin Sonlandırılması 106
6.2. Uygulamanın Modülleri 106
6.2.1. Risk Yönetimi 106
6.2.2. Şablonlar 107
6.2.2.1. Kurum Bilgileri 107
6.2.2.2. Tesis Listesi 107
6.2.2.3. Birim Listesi 107

6.2.2.4. Sorumlu Ekip Lideri Listesi 107
6.2.2.5. Risk Türleri 108
6.2.2.6. Risk Olasılıkları 108
6.2.2.7. Risk Şiddetleri 108
6.2.2.8. Risk Frekansları 108
6.2.2.9. Risk Dereceleri 108
6.2.3. Kullanıcılar 109
6.2.3.1. Sistem Yöneticisi 109
6.2.3.2. Risk Yöneticisi 110
6.2.3.3. Birim Amiri 111
6.2.3.4. Kurum Çalışanı 112
6.2.4. Raporlar 112
6.2.5. Mesajlar 112
6.2.6. Ajanda 113
6.2.7. İstek / Hata / Geliştirme 113
SONUÇ 114
KAYNAKÇA 116
ÖZGEÇMİŞ 127

TABLOLAR LİSTESİ

Tablo 1.1: Örnek Risk Kütüğü Formu 9

Tablo 1.2: Risklerin Sınıflandırılması 11

Tablo 1.3: Risk Sınıflandırma Matrisi 15

Tablo 2.1: Eski ve Yeni Risk Yönetimi Yaklaşımlarının Karşılaştırması 23

Tablo 2.2: Geleneksel Risk Yönetimiyle Yeni Risk Yönetim Yaklaşımı Kıyaslaması 24

Tablo 2.3: Risk Odaklı Yaklaşım, Geleneksel Risk Yönetimi ve Kurumsal Risk Yönetimi Karşılaştırılması 26

Tablo 4.1: Olayları Etkileyen Dışsal ve İçsel Faktörler 53

Tablo 4.2: Risk Analizi ve Yönetim Modeli 66

Tablo 4.3: Ön Tehlike Analizi Risk Değerlendirme Seçim Matrisi 69

Tablo 4.4: JSA Tehlikenin Gerçekleşme Olasılığı 71

Tablo 4.5: JSA Tehlikenin Şiddeti 71

Tablo 4.6: JSA Risk Değerlendirme Seçim Matrisi 71

Tablo 4.7: Olursa Ne Olur? Analizi Form Örneği 72

Tablo 4.8: CLA Birincil Risk Değerlendirme Kontrol Listesi 73

Tablo 4.9: CLA Kontrol Listesi Kullanılarak Birincil Risk Analizi Temelli Risk Değerlendirme Formu 73

Tablo 4.10: PRA Riskin Şiddetiyle Etkisi Arasındaki İlişki 75

Tablo 4.11: L Tipi Matris Olasılık Tablosu 76

Tablo 4.12: L Tipi Matris Şiddet Tablosu 76

Tablo 4.13: L Tipi Matris Risk Skor Tablosu 77

Tablo 4.14: L Tipi Matris Risk Sonucu Değerlendirme Tablosu 77

Tablo 4.15: X Tipi Matris Olasılık Tablosu....78
Tablo 4.16: X Tipi Matris Kontrol Değerlendirme Tablosu....78
Tablo 4.17: X Tipi Matris Şiddet Tablosu....79
Tablo 4.18: X Tipi Matris Önceki Kazaların Sonucu....79
Tablo 4.19: X Tipi Derecelendirme Matrisi....80
Tablo 4.20: HAZOP Metodolojisi Uygulamasında Kullanılan Anahtar Kelimeler....81
Tablo 4.21: HAZOP Tehlike ve İşletilebilme Çalışma Formu....82
Tablo 4.22: FMEA Hatanın Gerçekleşme Olasılığı....84
Tablo 4.23: FMEA Şiddet Etki Sınıflaması....85
Tablo 4.24: FMEA Saptanabilme Olasılığı ve Derecelendirilmesi....85
Tablo 4.25: FMEA Risk Öncelik Değerleri ve Karar....86
Tablo 4.26: Fine-Kinney Zararın Gerçekleşme Olasılığı....88
Tablo 4.27: Fine-Kinney Tehlikenin Gerçekleşme Frekansı....89
Tablo 4.28: Etki/Zarar-Sonuç Tablosu....89
Tablo 4.29: Fine-Kinney Risk Düzeyine Göre Karar ve Eylem....89

ŞEKİLLER LİSTESİ

Şekil 2.1: Risk Yönetimimin Gelişimi.....21
Şekil 2.2: Risk Yönetiminde Zaman İçerisindeki Gelişmeler 22
Şekil 3.1: Kurumsal Risk Yönetim Sürücüleri 28
Şekil 3.2: Kurumsal Risk Yönetiminin Kurumsal Değere Etkisi 29
Şekil 3.3: Kurumsal Risk Yönetim Anlayışı.....30
Şekil 3.4: Kurumsal Risk Yönetiminin Kapsamı.....31
Şekil 4.1: Kurum Yönetiminin Hedefleri.....39
Şekil 4.2: COSO Kurumsal Risk Yönetim Küpü.....41
Şekil 4.3: İçsel Ortam 42
Şekil 4.4: İç ve Dış Kaynaklı Önemli Risk Faktörleri 62
Şekil 4.5: GZFT Analizi 63
Şekil 4.6: 3*3 Risk Matrisi 67
Şekil 4.7: İş Güvenliği Analizi Aşamaları 70
Şekil 4.8: Birincil Risk Analizi Frekans Çizelgesi 75
Şekil 4.9: X Tipi Matris Risk Değerlendirme Değişkenler Matrisi 80
Şekil 4.10: Hata Ağacı Analizi'nin 3 Temel Adımı ve Aşamaları.....83
Şekil 4.11: Hata Ağacı Oluşturma Aşamaları.....83
Şekil 4.12: Genel Bir Neden-Sonuç Temelli Risk Metodu Akış Diyagramı.....87
Şekil 4.13: Risk Tutum Matrisi.....92
Şekil 5.1: Uygulama Algoritması 102

SİMGELER VE KISALTMALAR LİSTESİ

AICPA: Amerikan Kamu Muhasebecileri Birliği (The American Institute of Certified Public Accountants),

AAA: Amerikan Muhasebeciler Birliği (The American Accounting Association),

COSO: Comittee of Sponsoring Organizations

ERM: Enterprise Risk Management(Kurumsal Risk Yönetimi)

FEI: Finansal Yöneticiler Enstitüsü (The Financial Executives Institute)

IIA: İç Denetçiler Enstitüsü (The Institute of Internal Auditors)

KRY: Kurumsal Risk Yönetimi

GİRİŞ

Risk, literatürde çok farklı şekillerde tanımlanmaktadır. Bu tanımlamaların çeşitliliği riskin değerlendirildiği alana göre değişmektedir. Dünyanın yaratılışından bugüne kadar insanoğlu sosyal, çalışma ve diğer bütün alanlarda yaşadığı olaylar sonucunda olumlu veya olumsuz durumlarla karşılaşmaktadır. Genel bir ifadeyle insanların karşılaştıkları bu durumların her birine risk denilebilir. Diğer bir ifadeyle risk, insanların sahip olduğu değerlerin karşılaşılan olaylar sonucunda zarar görme olasılığıdır (Klinke ve Renn, 2002: 1071). Örneğin Hz. Ademin elmayı ısırması bir riskti ve sonucunda daha fazla fayda elde edebilmek amacıyla bu riski kabullenmişti. Ancak her risk, sonucu itibariyle olumlu bir fırsat veya olumsuz bir tehlike içermektedir. Karşılaşılabilecek risk türlerinin çeşitliliği de risklerin tanımı kadar çok sayıdadır. Dolayısıyla insanlar karşılaşılan risklerin olası tehlikelerinden kaçınıp fırsatlar elde edebilmek amacıyla bu riskleri yönetmeye çalışmaktadır.

Çalışma hayatında kurum ve kuruluşlar genel bir sınıflamayla finansal, operasyonel, stratejik ve dış çevre risklerinden kaynaklanabilecek olumsuzlukları mümkünse yok etmek değilse azaltmak amacıyla bütün faaliyetlerinde risklerin yönetilmesine yönelik çalışmalar yapmaktadırlar. Kimi kurumlar risk yönetim birimleri kurarken kimileri de kurum dışında bağımsız denetçiler yardımıyla etkin bir risk yönetimi yapmayı amaçlamaktadırlar. Ancak dinamik bir yapıda olan çalışma hayatı sürekli olarak gelişip değişim göstermektedir. Bu nedenle geleneksel risk yönetim yaklaşımında riskleri yalnızca tehlike ve olumsuzluk olarak algılayarak yönetilmesi, elde edilmesi muhtemel fırsatların kaçmasına neden olmaktadır. Bu çerçevede kurum ve kuruluşlarda yürütülen faaliyetleri tekil olarak değerlendirip bireysel yönetmeye çalışmak yerine bütüncül bir yaklaşımla kurumun geneline hitap eden bir risk yönetim anlayışıyla riskleri yönetmenin göz ardı edilemeyecek derecede kuruma faydaları bulunmaktadır.

Kurumsal risk yönetimi, kurumların riskleri tanımlama, değerlendirme ve etkisinin makul bir düzeye indirilebilmesi için gereken kontrollerin uygulanması, gözden geçirilmesi ve raporlanmasını sağlayarak kurumun faaliyetlerinde ne kadar risk bulunduğunun belirlenmesi ve bu risklerin kabul edilebilir bir seviyeye çekilmesine yönelik süreçler bütünü olarak ifade

edilmektedir (Emhan, 2009: 213). Bu yönde geliştirilen çeşitli kurumsal risk yönetim politikaları bulunmaktadır. Çalışmada COSO (Comittee of Sponsoring Organizations) kurumsal risk yönetim anlayışı çerçevesinde risklerin yönetilmesi için gereken sekiz adım detaylı olarak incelenmiştir.

Kurumsal risk yönetiminin etkin bir şekilde yapılabilmesi için kâğıt ortamında yürütülen denetim ve yönetim çalışmaları teknolojinin yardımıyla bilgisayar ortamında yapılmaya başlanmıştır. Buna yönelik kurum ve kuruluşlar tarafından kullanılan çok sayıda kurumsal risk yönetimi yazılım bulunmaktadır. Bunların birçoğu kurum çalışanları tarafından yalnızca yerel bilgisayar üzerinde kullanılabilmektedir. Ancak kurumsal risk yönetiminin etkin bir şekilde yürütülebilmesi için risk tanımlamadan başlamak üzere riskleri değerlendirme ve sonuçlarının analiz edilip raporlanabilmesi için uygulamaya her yerden ve bütün cihazlardan erişilebilir olması gerekmektedir. Aynı zamanda kullanılan yazılımların birçoğu yalnızca belirli sektörlere yönelik geliştirildiğinden farklı sektörlerde bulunan kurumlarda risklerin yönetilmesine yönelik bir sınırlılıkta oluşturmaktadır.

Kurum ve kuruluşlar tarafından internet üzerinde her yerden erişilip kullanılabilmesi amacıyla bir sistem tasarlanmıştır. Uygulama internet üzerinde çalıştığından internet tarayıcıya sahip bütün cihazlar tarafından platform bağımsız olarak çalışabilecek şekilde tasarlanmıştır. Ayrıca uygulamanın kurum ve kuruluşların faaliyet gösterdikleri sektörle ilgili risklerin yönetilebilmesini sağlamak amacıyla dinamik bir altyapısı bulunmaktadır. Uygulama ister bir devlet kurumunda isterse de özel sektörde faaliyet gösteren bir firmada çalışacak şekilde tasarlanmıştır.

Uygulamanın geliştirilmesinde odak noktası, kurumsal risk yönetim çerçevesinde kurumlar risklerin yönetilmesi noktasında kurum hafızasını kullanmada yetersiz kaldığı düşünülmektedir. Kurum hafızasını bütün çalışanlar üzerinde etkili olacak şekilde, geçmiş tecrübelerden beslenip geliştirilerek kullanılmasını sağlamak risk yönetimi açısından büyük önem arz etmektedir. Bu çerçevede, tasarlanan algoritma ile geliştirilen uygulamada kaydedilen bütün riskler, risklere yönelik hesaplamalar, hesaplamalar sonucu alınan tedbirler ve bu tedbirlerin sonucunda riskin son durumu hakkında kurumun hafızasını canlı tutma amaçlanmıştır.

1. BÖLÜM

RİSK ve İLGİLİ TANIMLAR

Risk sadece bankacılık, iş yaşamı ya da belirli bir sektöre veya alana has bir olgu değildir. Günlük yaşamın her alanında her zaman var olan bir kavramdır. Bilimsel çalışmalar göstermektedir ki risk kavramsal olarak 14-15. Yüzyıllarda kullanılmaya başlanmıştır ve Rönesans döneminde bu konuda çeşitli çalışmalar yapıldığı görülmüştür. Kavramsal olarak belirli yıllarda çalışmalar yapılmasına karşın aslında risk, insanlık tarihinin var oluşundan beri hayatımızda yer almaktadır.

Başka bir deyişle risk, herhangi bir işlemle ilgili maddi bir kaybın oluşması ve beklenmedik bir giderin oluşması sonucu, bu işlemle alakalı ekonomik kazanımın azalması ihtimalidir (Ökdemir ve Çelenk, 2010).

Kurum ve kuruluşlarda yönetimsel anlamda risk, bilgilerin yetersiz edinilmesinden kaynaklı gelecek vizyonu açısından yanlış kararlar verme tehlikesi ile kurumun belirlediği hedefe ulaşamama ve hedeflerinden sapma olarak da tanımlanabilir (Şimşek, 2007).

İşletmeler açısından bir başka tanımda risk, işletmelerin önceden tahmin edemeyip kontrol altında tutamadığı parametreler içeren faktörlerdir (Bahtiyar, 2008: 5).

Yatırımcılar açısından risk, finansal bir araca yapılan yatırım sonrası belirlenmiş bir güven aralığında, yatırımcının bu finansal araçtan kaybedeceği en fazla değerdir. Daha genel anlamda ise yapılan bir işlemle ilgili herhangi bir kayıp ortaya çıkması durumunda veya bir giderin yahut zararın oluşması nedeniyle elde edilecek ekonomik faydada azalma olması ihtimaline risk denir (Babuşcu, 2005).

Banka sektörü perspektifinde bakılırsa risk, her iki tarafın da kabul ettiği yükümlülükleri yerine getirmemesi, beklenen faydanın geçekleşmemesi ya da beklenmeyen bir durumun oluşması sonucu zarar etme olarak ifade edilmiştir (Delikanlı, 2000).

Matematiksel olarak risk, herhangi bir getiriyle ilgili olasılık değerlerinin ortalama değer etrafında dağılımı olarak ifade edilmiştir (Wiener, 1999).

Teknik anlamda Risk, getirilere ilişkin olasılık değerlerinin ortalama değer etrafındaki dağılımı olarak ifade edilebilir, (Wiener, 1999).

İstatistiksel olarak risk İnal ve Günay (1993)'de

$X_1,\ldots,X_n$' nin $f(x,\theta),\theta\in\Omega$

Şeklinde olasılık yoğunluk fonksiyonuna sahip kitleden rasgele örneklem olduğu varsayılmaktadır. Ω parametre uzayı gerçek ekseni, δ Karar fonksiyonu, R^n den R' ye şeklinde tanımlanmış bir fonksiyondur. δ' nın $\delta(x_1,\ldots,x_n)$ değerine karar denir (İnal & Günay, 1993). $X_1,\ldots,X_n$ rasgele örneklemi verildiğinde, θ parametresinin tahminine yönelik kayıp fonksiyonu, θ ve δ' nın negatif olmayan bir fonksiyon olarak tanımlanmaktadır. Bu kayıp fonksiyonu,

$$L[\theta;\delta(X_1,\ldots,X_n)]=|\theta-\delta(X_1,\ldots,X_n)|$$

Ya da daha genel olarak;

$$L[\theta;\delta(X_1,\ldots,X_n)]=A(\theta)|\theta-\delta(X_1,\ldots,X_n)|^k,k>0$$

Biçiminde yazılmaktadır.

En çok kullanılan biçimi ise karesel kayıp fonksiyonudur, karesel kayıp fonksiyonu

$$L[\theta;\delta(X_1,\ldots,X_n)]=A(\theta)\,[\theta-\delta(X_1,\ldots,X_n)]^2$$

Şekildedir.

$L(\theta,\delta)$ Kayıp fonksiyonuna karşılık gelen $R(\theta,\delta)$ risk fonksiyonu, kayıp fonksiyonunun beklenen değeridir. Bu durum

$$R(\theta,\delta)=E[L[\theta;\delta(X_1,\ldots,X_n)]]$$
$$=\int_{\infty}^{+\infty}\ldots\int_{\infty}^{+\infty}L[\theta;\delta(x_1,\ldots,x_n)]f(x_1;\theta)\ldots f(x_n;\theta)dx_1\ldots dx_n$$

Şeklinde yazılabilir.

Bu tanımlara göre, $\delta=\delta(x_1,\ldots,x_n)$ kararı θ'nın tahmini olarak varsayılabilmektedir. Eğer δ_1,δ_2 gibi iki karar fonksiyonu için $R(\theta,\delta_1)<R(\theta,\delta_2)$ise δ_1 θ

'nın tahmini olarak tercih edilmelidir. θ Parametresinin tahmin edicisini bulmak için minimaks veya bayes yöntemi kullanılabilir.

Minimaks yönteminde, θ parametresi için önerilen $\delta_1(x_1,\ldots,x_n), \delta_2(x_1,\ldots,x_n)\ldots, \delta_m(x_1,\ldots,x_n)$ gibi tahmin edicilerden θ'ya göre en büyük risk için en küçük tahmin edici seçilir. A_δ, θ için tahmin edicilerin bir kümesi ve $\delta \in A_\delta$ olmak üzere eğer $\forall \delta^* \in A_\delta$ olan herhangi bir δ^* tahmin edicisi için,

$$\sup[R(\theta;\delta);\theta \in \Omega] \leq \sup[R(\theta;\delta^*);\theta \in \Omega]$$

ise, δ tahmin edicisine minimaks tahmin edicisi denilmektedir.

$\Omega \subset R$ olsun ve θ parametresinin $\lambda(\theta)$ önsel olasılık yoğunluk fonksiyonuna sahip bir rastlantı değişkeni olduğu varsayıldığında,

$$R(\delta) = E[R(\theta;\delta)] = \int_{\theta \in \Omega} R(\theta;\delta)\lambda(\theta)d\theta$$

yazılabilir. Görüldüğü gibi, burada $R(\delta)$, tüm Ω parametre uzayında ortalama risktir (Chorafas, 1997), (İnal & Günay, 1993).

$\delta \in A_\delta$ olmak üzere eğer $\forall \delta^* \in A_\delta$ için $R(\delta) \leq R(\delta^*)$ ise, δ tahmin edicisine Bayes tahmin edicisi denir. Bayes tahmin edicisini, klasik tahmin edicilerden ayıran en önemli özelliği tahmin edilmek istenen θ parametresine, $\lambda(\theta)$ gibi bir önsel olasılık yoğunluk fonksiyona sahip bir rasgele değişken gözü ile bakılmasıdır. Burada θ için $\lambda(\theta)$ önsel olasılık yoğunluk fonksiyonunun seçimi önemlidir (İnal & Günay, 1993).

Yukarıda yapılan açıklamalardan da anlaşılacağı gibi tek bir risk tanımı yoktur. Bu tanımlamalar daha da artırılabilir lakin genel bir ifade ile riskin tanımını toparlayacak olursak en basit tanımı ile Risk, belirli bir amaç veya hedefe ulaşmak için kullanılan para, zaman, itibar, iş gücü vb. değerlerin kaybedilme tehlikesinin ortaya çıkma ihtimalidir.

1.1. **Risk İle İlgili Temel Kavramlar**

Riske ait faklı bakış açılarının verilmesinin ardından bu başlığın altında risk kavramı ile doğrudan ilgili olan bazı kavramlardan bahsedilecektir.

1.1.1. **Belirsizlik ve Risk**

Belirsizlik, bir durumun gelecekte olup olmayacağı ile ilgili bilgi yetersizliğinden dolayı oluşan şüphe durumudur (Vaughan ve Vaughan, 2007: 3). Bu doğrultuda belirsizliğin kaynağı, oluşması beklenen olay ve sonuçların gerçekleşme ihtimalinin tam olarak belirlenememesidir (Yılmaz, 2007: 33).

Genel olarak belirsizlik riski kapsar bunun yanında belirsizliğin iki boyutu vardır, ilki bilgisizlik(ignorance) ikincisi ise sürpriz-şok(surprise-shock)'tur. Risk, belirli bir tehlikenin oluşması ihtimalinin olasılık hesabıyla öngörülebilmesi ve riske maruz değerin edineceği zarara karşı belirli bir maliyetle önlem alınabilmesidir. Buna karşın belirsizlik ise, bir şok ile ortaya çıktığında bir anlamı olmaktadır. Belirsizliğin riskten en belirgin iki farkı öngörülememesi ve önceden önlem alınamamasıdır. Bilgisizlik, belirsizlikteki ikinci boyut olarak yoksunluğu açısından önemli bir etken olmasına karşın riskte bilgi olduğu için bu tam tersidir. Bunun yanında bilgisizlik beraberinde öngörememe ve ölçememe gibi iki unsuru da beraberinde getirmektedir (Yalçınkaya, 2004: 9-10).

1.1.2. **Fırsat ve Risk**

Kurum ve kuruluşlar gösterdikleri faaliyetlerde yalnız olumsuz riskleri(tehditler) göz önünde bulundurup olumlu riskleri(fırsatlar) göz ardı etmeleri veya gözden kaçırmaları halinde belirledikleri hedeflere ulaşabilme, büyümeyi ve gelişmeyi sürdürebilme adına geride kalma veya sapma yaşayabilirler (Chapman, 2006: 5). Risklerin her ikisini de olumlu ve olumsuz olanları birlikte değerlendirmeleri fırsatları yakalayabilme açısından önem arz etmektedir. Fırsat başka bir tanımda, riskin olumlu yanı ve oluşturacağı olası kazanç olarak ifade edilmektedir (Maliye Bakanlığı, 2013).

1.1.3. **Tehdit ve Risk**

Tehdit genel bir ifadeyle riskin olumsuz yanı ve meydana getireceği olası kayıp olarak ifade edilmektedir (Maliye Bakanlığı, 2013). Risk meydana gelmemiş bir olasılık olarak kabul gördüğünden insanlar gündelik yaşamlarında bunu kabullenerek hayatlarını sürdürmektedir. Buna örnek olarak insanlar elindeki bıçağı yanlış kullanma sonucu yaralanma ihtimaline karşın diğer elindeki elmayı soymak için kullanmaktadır.

Kurum ve kuruluşların yönetimlerinin mevcut yetenekleri, herhangi bir olayın risk mi tehdit mi olduğunu belirlemede çok önemli bir etkendir. Herhangi bir durumun risk yahut tehdit olarak görülmesi, bu durumun kendine haiz özelliklerinin haricinde bu durumla karşılaşan

kurum, kuruluş veya insanların sahip oldukları yetenek veya güce göre değişebilir. Örneğin yönetimi güçlü olan bir kuruma göre risk olarak görülen bir durum daha zayıf yönetimi olan bir kuruma göre tehdit olarak görülebilir (Küçükşahin, 2006: 18-19).

1.1.4. **Risk Algısı**

Risk algısı, riskin doğasına ve insanların geçmiş tecrübelerine göre farklılık gösterebilmektedir (Cohrssen ve Covello, 1989: 9). İnsanlar için geçerli olan bu durum kurum ve kuruluşlar açısından da geçerliliğini sürdürmektedir. Yapısal değişikliklerine bağlı olarak bazı kurum ve kuruluşlar büyük oranda riskleri üstlenebilirken bazıları ise küçük oranda risklerden dahi imtina edebilir. Risk algısı tam bu noktada ortaya çıkmaktadır. Campbell (1992: 2) çalışmasında, kendi kendine hiçbir şeyin risk olamayacağını ve gerçekte riskin var olmadığından buna karşın her şeyin de risk olarak değerlendirilebileceğinden bahseder. Bu bakış açısıyla herhangi bir durumun risk olup olmadığı bu durumun nasıl algılandığıyla ve tehlike arz eden durumun nasıl analiz edildiğine bağlı olarak değişkenlik göstermektedir. Dolayısıyla kurum ve kuruluşlarda riskin nasıl algılandığı, risk kapsamının belirlenmesinde doğrudan ilintili olduğu gibi önemli bir yere sahiptir.

1.1.5. **Risk Zekası**

Haksöz (2013) maklesinde, "Boğaziçi Cambazı" diye isimlendirdiği bir metaforla risk zekasını özetlemiştir. Bu metafor, risk zekası için kurum, kuruluş ve insanların sahip olması gereken dört temel rolü ve davranışsal boyutu açıklayan I-Quartet Modeli üzerine kurulmuştur. Rollerin, modelde ana fikirleri aşağıdaki şekilde belirtilmiştir (Haksöz, 2013: 85):

Bütünleyici (Integrator): Sahip olduğu tüm yetenek, kabiliyet ve tecrübelerini akışın mükemmelliğini sağlayacak biçimde destekleyici bir unsur olarak iç ve dış koşulların gereklerine göre kullanma.

İrdeleyici (Inquirer): Yapılan hatalardan, geçirilen tehlikelerden ve neredeyse olmak üzere olan olaylardan ders almaya açık olma, gelecekte oluşması muhtemel değişiklikleri öngörebilme. Kurum ve kuruluşlarda oluşan geçmişleri sayesinde geçmiş tecrübelerine dayanarak bu modeli kullanabilirler. İrdeleyici model belirli bir tarihçesi oluşmamış kurum ve kuruluşlarda tecrübe eksikliğinden dolayı kullanılması pek mümkün değildir.

Doğaçlayıcı (Improviser): Direnç, esneklik ve dayanıklılığı artırmak için mevcut olanaklardan optimum düzeyde yararlanabilmektir. Bunun yanında karşılaşılacak olağandışı

durumlara karşı etkin ve anında reaksiyon verebilmedir.

Marifetli (Ingenious): Riskleri akılcı bir perspektifle üstlenirken işleri keyif verici fırsat aksiyonlarını oluşturabilme.

Kurum, kuruluş ve insanların yukarıda belirtilen dört rolü, doğru bir zamanlama ve yerde uygun bir şekilde uygulamaları risk zekâlarının yükselişine önemli bir katkıda bulunacaktır. Yaşadığımız dünyanın belirsizliklerle dolu olması sebebiyle, riski üstlenenlerin ayakta kalabilmeleri ve ilerleyebilmeleri risk zekâlarını arttırabilmeleriyle mümkün olabilecektir (Haksöz, 2013: 85).

Risk zekasına sahip olan kurum ve kuruluşların elde edeceği faydalar bir başka çalışmada şu şekilde maddeler halinde özetlenmiştir (Tekgül, 2007).

- Kritik risk sorunlarını oluşmadan önce önlenebilir. Kurum ve kuruluşlarda yönetimin yetkinliğini geliştirebilmek için herhangi bir sorun ortaya çıktığı anda gerekli olan düzeltme ve düzenlemelerin yapılması önem arz etmektedir.
- Alınan aksiyonlarda risk yönetiminin yükü hafifletilebilmesi için risk yönetim prensiplerinin standardizasyonu etkili bir önlemdir.
- Risk yönetim maliyetlerinin azaltabilmesi, kurum ve kuruluşların genelinde risk bilgilerinin ortak kullanılabilmesi ve halihazırdaki risk yönetimi fonksiyonlarına bu bilgilerin entegre edilebilmesiyle mümkündür.
- Kurum ve kuruluşların yönetim katında bütün risklerin doğru anlaşılıp yönetildiği hususunda hissedarlar ve paydaşlar açısından bir güven ortamı oluşturulabilir.

1.1.6. **Risk Toleransı**

Genel bir tanımla bir hedefe ulaşabilmek için kabul edilebilir risk seviyesidir. Risk toleransı Kurum ve kuruluşların hedefleri doğrultusunda belirledikleri risk aralığıdır. Risk iştahı ve risk toleransı kavramları genel olarak risk alma sınırlarını ifade eder. Bununla birlikte risk iştahı risk toleransından daha geniş bir kapsamı olduğu ifade edilebilir (Arslan, 2008: 8).

Kurum ve kuruluşların risk toleransı ile aksiyon almaları risk iştahı sınırında kalmalarını sağlayacaktır (Yılmaz, 2007: 52).

1.1.7. **Risk İştahı**

Risk iştahı, genel anlamda bir hedefe ulaşabilmek için alınması kabul edilen risk oranı olarak ifade edilebilir. Kurum ve kuruluşların risk yönetim felsefesini yansıtan risk iştahı aynı

zamanda kültürünü ve yönetim stilini de etkilemektedir (PWC, 2006: 20). Risk iştahının bir diğer tanımı ise misyon, vizyon, amaç ve hedeflere ulaşma noktasında herhangi bir zamanda kurum ve kuruluşların kabullenmeye hazır olduğu risk miktarıdır (Maliye Bakanlığı, 2013). Kurum ve kuruluşlarda risk değerlendirilmesine başlamadan önce üst yönetimin kontrolünde risk iştahının tespit edilmesi gereklidir.

Kurum ve kuruluşların yönetimi üç yolla ya da bunların birleşimleri dikkate alınarak risk iştahı düzeyine karar verebilirler. İlki, yönetim tüm risklerin ayrı ayrı değerlendirilip her birine risk iştahı düzeyi belirlenebilir. İkincisi, kurum ve kuruluşların stratejik hedef veya amaçlarının her birine önemine göre belirlenebilir. Üçüncü olarak da, kurum ve kuruluşların geneline yayılacak şekilde bir risk iştah düzeyine karar verebilir. Risk iştah düzeyi belirlenirken yönetimin dikkat etmesi gereken bazı noktalar bulunmaktadır bunlar, risklerle mücadele ederken oluşacak bütçe, personel ve zaman ihtiyaçlarıdır (Derici, 2015: 44).

1.1.8. **Risk Kütüğü**

Bir belge olan risk kütüğü dinamik bir yapısı bulunmakla birlikte içerisinde aşağıdaki unsurları barındırmaktadır;

- Kurum ve kuruluşlarda bulunan temel riskler
- Risklerin etki ve olasılık seviyeleri
- Risk yetkilileri ve sorumluları
- Risklerin yönetimi ve kontrolleri sonrasında oluşan durum değerlendirmeleri

Standart bir risk kütüğü bulunmamakla beraber her kurum ve kuruluş ihtiyacına ve yapısına göre kendine uygun bir biçim belirleyebilir. Tablo 1.1.'de Sayıştay'ın risk yönetiminde kullandığı örnek bir risk kütüğü formatı sunulmaktadır (Derici vd., 2007: 166).

Tablo 1.1: Örnek Risk Kütüğü Formu

SAYIŞTAY RİSK KÜTÜĞÜ						
TEMEL RİSKLER	**Mevcut Durum**			**Risk Sorumluları**	**Kontrol Faaliyetleri**	**Değerlendirme**
	İhtimal	**Etki**	**Önem Düzeyi**			
1. …. İlişkin Riskler	**Risk Yetkilisi : ……..**					

Kaynak: Derici vd., 2007: 166

1.2. **Risk Türleri**

Risk; kurum ve kuruluşların bütün faaliyetlerinde karşılaşabilme ihtimali olan bir durumdur. Geçmişten bugüne giderek daha karmaşık bir yapıda faaliyetlerde bulunmaya başlayan kurum ve kuruluşların karşılaştığı risklerin çeşitleri de artmaktadır. Şekil, şiddet ve zaman bakımında çeşitlilik arz eden risklerin belirli bir sınıflandırma yapılması da gerekmektedir. Bununla birlikte risk tanımlarında bulunan çeşitlilik bu risklerin sınıflandırılmasında da karşımıza çıkmaktadır (Kızıldağ, 2011: 21).

Gündelik yaşamda kurum ve kuruluşlar ile bireylerin sonucu tahmin edilen durumlar ile gerçekleşen farklılık gösterebilir. Tahmin edilen ile gerçekleşen sonuçların farklı olmasını etkileyen birden çok nedeni olabilir. Bir ülkede savaş durumunun oluşması, iklim koşullarının öngörülememesi veya beklenmeyen ani bir değişim göstermesi, doğal afetlerin meydana gelmesi, döviz kurlarında ani değişiklikler olması, kurum veya kuruluşların olağandışı kar ya da zarar açıklamaları gibi durumlar risk unsuru oluşturabilecek olaylara örnek olarak gösterilebilir. Olması öngörülen sonuçlarla gerçekleşenlerin birbirinden farklı olmasına sebep olan olayların çeşitliliği ile risk faktörlerinin sayısındaki çeşitlilik nedeniyle bunların tasnif edilmesi zorlaşmakta ve genel geçer herkesin üzerinde anlaşmaya varabildiği bir ortak tanım olmamasına neden olmaktadır (Bolak, 2004: 3). Bu sebeple araştırmacılar çalışmalarında riskleri birbirinden farklı bakış açısıyla sınıflandırmışlardır. Kızıldağ (2011) da çalışmasında temel risk kaynaklarını göz önünde bulundurarak dört ana başlık altında riskleri sınıflandırmıştır. Bu sınıflama aşağıdaki şekilde verilmiştir.

- Finansal Riskler
- Operasyonel Riskler
- Stratejik riskler
- Dış Çevre Riskleri

Risklerin yukarıdaki gibi tasniflenmesi birçok araştırmada karşımıza çıkmaktadır ancak bu ana başlıkları daha detaylı bir şekilde açıklayan araştırmacılar vardır. Moeller (2011); araştırmasında riskleri Tablo 1.2.'deki gibi sınıflandırmıştır.

Tablo 1.2: Risklerin Sınıflandırılması

STRATEJİK RİSKLER	
DIŞ FAKTÖR RİSKLERİ	**İÇ FAKTÖR RİSKLERİ**
• Endüstri riski • Ekonomi riski • Rekabetçi riski • Hukuki ve yasal düzenlemeler riski • Müşteri ihtiyaç ve beklentilerinden kaynaklı risk	• İtibar riski • Stratejik odak riski • Ana şirket destek riski • Ticari marka koruma riski

OPERASYONEL RİSKLER		
SÜREÇ RİSKLERİ	**UYGUNLUK RİSKLERİ**	**İNSAN RİSKLERİ**
• Tedarik zinciri riski • Müşteri memnuniyeti riski • Devir süresi riski • Süreç yürütme riski	• Çevresel risk • Düzenleyici risk • Politik ve prosedür riski • Dava riski	• İnsan kaynakları riski • İşten ayrılma riski • İş gören devir hızı riski • Performans teşvik riski • Çalışan yetiştirme riski

FİNANS RİSKLERİ		
MALİ RİSKLER	**KREDİ RİSKLERİ**	**TİCARET RİSKLERİ**
• Faiz oranı riski • Döviz kuru riski • Sermaye yeterliliği riski	• Kapasite riski • Teminat riski • Yoğunlaşma riski • Temerrüt riski • Ödeme riski	• Emtia fiyat riski • Süreklilik riski • Ölçüm riski

BİLGİ RİSKLERİ		
FİNANSAL RİSKLER	**OPERASYONEL RİSKLER**	**TEKNOLOJİK RİSKLER**
• Muhasebe standartları riski • Bütçeleme riski • Finansal raporlama riski • Vergilendirme riski • Düzenleyici raporlama riski	• Fiyatlandırma riski • Performans ölçüm riski • İşçi güvenliği riski	• Bilgi erişim riski • İş sürekliliği riski • Uygunluk riski • Altyapı riski

Kaynak: Moeller, Robert R., COSO Enterprise Risk Management, 2011, s.25.

Birçok araştırmacı tarafından dört ana başlıkta tasniflenen risklerin kısa bir şekilde tanımları aşağıdaki şekilde verilmiştir.

1.2.1. **Stratejik Riskler**

Bu tarz riskler, yönetimsel anlamda yanlış alınmış kararlardan veya alınan kararların yanlış uygulanmasından kaynaklı yaşanabilecek sermaye ve kazanç kayıplarını ifade etmektedir (Thomas, 2007:4). Bir diğer araştırmada Usul ve Mizrahi (2016: 13), rekabet koşullarının değişmesiyle birlikte sanayide meydana gelen değişimle beraber müşterilerin taleplerinde meydana gelen değişime bağlı olarak işletmelerin müşteri portföyündeki meydana gelen değişimleri ifade etmişlerdir.

Stratejik riskleri kurum ve kuruluşların belirledikleri hedeflerine ulaşmasına engel

oluşturacak yapısal riskler olarak tanımlamak mümkün. Bu kapsama girecek riskleri şu şekilde örneklenebilir; Planlama, yönetişim, iş modeli oluşturma gibi riskler stratejik riskler olarak tanımlanabilir (COSO, 2004a: s.12.)

1.2.2. **Finansal Riskler**

Kurum ve kuruluşlarda finansal olarak problemler oluşturabilecek riskler olarak tanımlanabilir (Usul ve Mizrahi, 2016: 12). Ekonomik gelişmeler sonucu piyasalarda yaşanan değişkenlikler kurum ve kuruluşların finansal planlarına çok farklı etkiler meydana getirebilmektedir bunlar da finansal açıdan riskler olarak değerlendirilmektedir. Bu duruma örnek olarak döviz kurlarındaki beklenmeyen değişiklikler, faiz oranları, kredi ve emtia fiyatlarında meydana gelen değişimler gösterilebilir verilebilir (Gacar, 2017: 125).

1.2.3. **Operasyonel Riskler**

Bu risk türü en genel tanımıyla, finansal risklerin haricinde kalan tümü olarak tanımlanmaktadır. Ancak bu tanımlamanın geniş bir kapsamda olması ve daha ziyade neyi kapsamadığını ifade nedeniyle bu risk türünün yönetilebilmesi açısından çok fazla bir anlam içermemektedir. Bankacılık sektörü tarafından aldığı kararları genel kabul gören Basel Komitesi 1994 yılında yaptığı bir tanımda operasyonel risk; "*Bilgi sistemlerinin veya iç kontrollerin yetersizliği nedeniyle beklenmeyen zararlara uğrama riski*" olarak tanımlanmıştır.

Bir diğer tanımla operasyonel riskler kurum ve kuruluşların ana faaliyetlerini yerine getirmesine engel teşkil edecek risklerdir. Bu riskler; "*İç kontrollerdeki aksamalar sonucu, hata ve usulsüzlüklerin gözden kaçmasından, üst yönetim ve diğer personel tarafından zaman ve koşullara uygun hareket edilmemesinden, yönetimden kaynaklanan hatalardan, bilgi teknolojisi sistemlerindeki hata ve aksamalar ile deprem, yangın, sel gibi felaketlerden kaynaklanabilecek kayıpları ya da zarara uğrama ihtimalini ifade etmektedir.*" (Risk Management and Control Guidance For Securities Firms and Their Supervisors, 1998: 5).

Bu tanımlara ek olarak operasyonel riskler diğer risk türlerinin doğrudan içinde olmakla birlikte ayrı bir risk olarak da değerlendirilmektedir.

Sayısallaştırılamayan risklerin ölçümleri objektif olmaktan uzak olacağı gibi etkin bir şekilde yönetimlerinin sağlanamamasına da sebep olacaktır. Bununla birlikte sayısallaştırma sürecinde kurum ve kuruluşlar açısından çeşitli zorluklar bulunmaktadır; operasyonel risklerin sebep olabileceği kayıpların büyüklüğü, bu risklerin karşılaşılma sıklığı ve bu

bilgilerin nitelikli ve her yerden erişilebilen bir yapıda risk kütüğünün olmayışı gibi etkenler bu zorluklara birer örnek olarak verilebilir. Bu nedenlerden dolayı kurum ve kuruluşlarda öngörülen ya da karşılaşılan tüm operasyonel riskleri tespit etmek ve bunların net bir şekilde ölçümünü sağlayabilmek neredeyse mümkün olmamaktadır. (Özbilgin, 2012: 90). Buna rağmen gelişen teknolojinin yardımıyla internet üzerinden her yerden erişilebilen bir veri tabanı olması durumunda karşılaşılan bu zorlukları en aza indirebilmek mümkün kılınabilir.

1.2.4. **Dış Çevre Riskleri**

Kurum ve kuruluşların yaptıkları faaliyetlerden bağımsız bir şekilde karşılaşılan bu riskler, kurum ve kuruluşların tercih ettikleri yönetim şekline göre etki oluşturabilmektedir. Kanunlarda yapılan değişiklikler, siyasi erkin değişimi, sektördeki değişimler, müşteri veya paydaşların eğilimlerindeki değişimler, rakiplerin davranışlarındaki değişiklik gibi etmenler dış çevre risklerine örnek olarak gösterilebilir (COSO, 2004a: 12.).

1.3. **Diğer Risk Sınıflandırma Türleri**

Yukarıda yer alan farklı yazarların farklı sınıflandırmalarının yanı sıra risklerin, sistematik ve sistematik olmayan riskler (Altay, 2004); yönetilebilir ve yönetilemeyen riskler şeklinde de ayrımı yapılabilmektedir.

1.3.1. **Sistematik Risk**

Sistemden kaynaklanan riskler olarak tanımlanmaktadır (Demirtaş ve Güngör, 2004: 104). Bunun yanında sistematik risk, ekonomik, politik ve sosyal yapı ile bu yapılardaki değişikliklerden kaynaklanmakla birlikte mevcut piyasalarda ki tüm varlıklarla kurum ve kuruluşların tamamını aynı anda etkileyen bir risk türüdür. Bu tür riskler kurum ve kuruluşlarda yönetim katında alınan kararlar doğrultusunda kontrol edilmesi çok mümkün olmayan değişimler olarak ifade edilmektedir (Akgüç, 1994: 837). Ayrıca riskler çeşitlendirilemeyen risk olarak da adlandırılabilmektedir. Bununla birlikte bu risklerden korunmak mümkün olmakla birlikte tamamen yok etmek mümkün değildir (Mandacı, 2003: 70). Buna ek olarak bu risk türünü dış çevre riskleri olarak da görülebilmektedir.

1.3.2. **Sistematik Olmayan Risk**

Sistematik olmayan riskler, kurum ve kuruluşların kendilerinde veya bulundukları sektörle ilgili riskler olarak tanımlanabilmektedir. Yönetimdeki hatalar, reklam kampanyaları, müşteri veya paydaşların tercihlerindeki değişimler, yasalardaki uygulamalar, grevler gibi olaylar kazanımlarda değişkenliklere neden olabilir bu durum kurum ve kuruluşların

kendilerini veya sektörlerini ilgilendirdiğinden diğer sektörleri ve piyasaları etkileyen faktörlerden bağımsızdır. Bu durum da sistematik olmayan risklerin her kurum ve kuruluş için ayrı ayrı değerlendirilmesini gerektirmektedir. Bir diğer bakış açısıyla bu tarz riskler finansal, operasyonel ve stratejik risklere genel bir çerçeve gibi görülebilmektedir.

İki farklı risk türü tanımlamasının yanında bunlara ek olarak diğer bir risk türü tanımı da yönetilebilir ve yönetilemez riskler olarak görülmektedir.

1.3.3. **Yönetilebilir Riskler**

Risklerin belirli bir seviyeye kadar kurum ve kuruluşlar tarafından öngörülebilen ve çeşitli finansal araçlarla birlikte alınan önlemler sayesinde yönetilebilen riskler olarak ifade edilebilir. Bu risk türü aşağıdaki gibi dört başlıkta sınıflandırılabilmektedir (Eranti, 2008: 109).

- Piyasa riski
- Teknik riskler
- Kur riski
- Zamanlama riski

Risklerin yönetilebilir ve yönetilemez olarak sınıflandırılmasının kurum ve kuruluşların kendi bünyelerindeki riskler ve dış çevresel riskler olarak benzetilmesi genel bir kanı olmasına rağmen bu gibi bir sınıflandırma her zaman aynı olmamaktadır. Kurum ve kuruluşların dış çevresel riski olarak tanımlanan ürün fiyatlamasındaki değişkenlik, döviz kuru dalgalanmaları veya banka faiz oranlarındaki değişimler aslında belirli bir seviyeye kadar çeşitli finansal araçlar sayesinde yönetilebilme şansları bulunmaktadır (Bolak, 2004: 5). Bundan dolayı da kurum ve kuruluşların dışında kalan çevresel kaynaklı her risk, yönetilemez risk olma özelliği göstermemektedir.

1.3.4. **Yönetilemez Riskler**

Yönetilemez risk kavramı çeşitli kaynaklarda açık risk olarak ifade edilmektedir. Kurum ve kuruluşların alacağı yatırım kararlarında önemli bir role sahip olan bu risk türüne siyasi erkin riski yönetilemez bir risk olarak ifade edilmektedir (Eranti, 2008: 110). Aşağıdaki tabloda risklerin sistematik olup olmadıklarına ve yönetilebilir olup olmadıklarına göre bir sınıflandırma yapılmıştır.

Tablo 1.3: Risk Sınıflandırma Matrisi

	YÖNETİLEBİLİR RİSKLER	YÖNETİLEMEZ RİSKLER
SİSTEMATİK RİSKLER	• Faiz oranı riski • Kur riski • Piyasa riski	• Politik risk • Satın alma gücü riski
SİSTEMATİK OLMAYAN RİSKLER	• Faaliyet riski • Yönetim riski • Zamanlama riski	• İş ve endüstri riski

2. BÖLÜM

RİSK YÖNETİMİ

Risk yönetimi konusunda literatürde birçok tanım mevcuttur. Bunların en genel tanımı olarak Risk yönetimi esasında oluşması muhtemel bütün riskleri öngörme ve bu riskleri yok etme, kaçınma, transfer etme veya etkilerini azaltmaya yönelik tüm süreçleri kapsayan önleyici uygulamaları kapsamaktadır. Bu bağlamda risk yönetimi özünde bir öngörü ve tahmin yönetimi çalışmaları bütünüdür.

Risk yönetiminin yapılan işlerle ilgili gerekli görülen önleyici tedbirleri alarak risk ve tehlikenin yok edilmesi olarak tanımlanabileceği gibi; problemlerin gerçekleşmeden önlenmesi ile hedeflere ulaşmayı kolaylaştırma olarak da tanımlanabilir (Kuyucu, 2008).

Benzer şekilde risk yönetimi herhangi bir işletme ya da projede oluşması muhtemel bütün riskleri en aşağı düzeye çekme ve işletme performansını artırma uygulamalarının tamamı olarak ifade edilebilir (Ababneh, 2000: 23).

Kurum ve kuruluşlarda etkin bir şekilde risk yönetim kültürünü uygulamak demek, oluşması muhtemel kayıpları daha önceden öngörebilme ve bu risklere karşı proaktif bir yaklaşım sergileyebilmelerine olanak sağlayacaktır (Özkılıç, 2005).

Başka bir tanımda risk yönetimi, kişi ve kurumların finansal durumlarının ne oranda risk altında olduğu ve bu oranın risk toleransı sınırları içerisinde tutulmasıdır (Aybars, 1998).

Risk kavramının tanımlanmasında genellikle tehditler üzerine durulmuştur ancak risk kavramı yalnızca tehditlerden ve olumsuzluklardan oluşmamakta aynı zamanda fırsatları ve olumlu yönlerini de içerisinde barındırmaktadır. Çincede risk; tehdit ve fırsat anlamlarına gelen sembollerden oluşmaktadır (Damodaran, 2008: 6). Risk sadece tehlike, problem, tehdit veya kayıplar olarak tanımlanması klasik ve eski bir tanımlama olarak kabul görmektedir. Gelişen ve çeşitlenen risk yönetimi çerçevesinde risk tek taraflı değil hem olumlu hem de olumsuz olayları içerek bir olgu olarak tanımlanmaktadır (Ekici, 2015: 21). Bu nedenle

kurum ve kuruluşlar olumsuz olarak öngörülen olaylardan kaçınmanın yanı sıra olumlu olarak tahmin edilen durumları da değerlendirebilme de amaçlanmaktadır. Bir diğer deyişle; risk yönetimi sayesinde olumsuz sayılan durumlara karşı savunmanın yanında oluşabilecek fırsatlara karşı da hazırlı olabilmek mümkündür (Uzun, 2011: 1).

Risk yönetiminin amacını kısaca, kurum ve kuruluşların istikrarlı bir şekilde faaliyetlerini devam ettirebilmek için gerekli olan düzenlemeleri sağlamakla birlikte organizasyondaki paydaş ve müşterilerin korunması ile kazanımların korunmasıdır. Bir başka deyişle organizasyonda öngörülmeyen kayıpların minimum maliyetle kontrol altında tutulması için gereken kaynak ve aksiyonların planlanması ve yönetilmesi olarak tanımlanabilir (Çağırgan, 1997: 17).

Risk türleri açıklanırken belirtildiği üzere riskleri oluşturan çeşitli kaynaklar olduğu gibi bu risklerin gerçekleşmesi durumunda etkilediği alanlar da farklı farklıdır. Örneklemek gerekirse herhangi bir kurum ve kuruluşun marka itibarına ve finansal durumuna kalite, iş emniyeti ve çevre gibi faktörler arasındaki ilişkiler doğrudan etki etmektedir. Bu nedenle yönetim katında risk yönetimi çerçevesinde kararlar alınması kurum ve kuruluşlarda öngörü, proaktif yaklaşım ve sonuçların etkilerini istenilen bir seviyede kontrol altında tutabilme yetenekleri kazandıracaktır.

Kurum ve kuruluşların bir fırsat olarak veya olumlu etkileri olması öngörülen riskler, risk yönetiminin iyi bir şekilde yönetilememesinden kaynaklı olumsuz sonuçlar doğurabilir veya bir tehdide dönüşebilir. Örneğin bir restoranda aynı zaman için bir topluluk adına rezervasyon yaptıran iki farklı müşteri işletme tarafından daha fazla kazanç için bir fırsat olarak değerlendirilebilir. Ancak yetersiz yer, personel ve yiyecek sebebiyle müşterilerin taleplerini istenilen kalite ve zamanda sağlayamaması durumunda oluşabilecek müşteri kaybı ve işletme itibarının zedelenmesi gibi sonuçlar işletmeyi olumsuz yönde etkileyebilir. Böyle bir durumda ilk anda fırsat olarak değerlendirilen bir durum eğer iyi yönetilemezse çeşitli risklerin oluşmasına neden olan birer tehdit unsuru olabilmektedir (Ekici, 2015: 37).

Risk olgusu değerlendirilirken kayıp ve kazançlar aynı anda göz önünde bulundurulmalıdır. Olayların tek yönlü değerlendirilmesi, sadece olumlu bir risk fırsat veya olumsuz bir risk tehdit olarak ele alınması alınacak kararlar, belirlenmiş amaçlar veya yerine getirilen faaliyetler üzerinde beklenmedik ters bir etki oluşturabilir. Bu sebeple gerçekleşen sonuç bir kazanım olsa bile risk, içerisinde her zaman kayıpları barındırır ki bu durum da risklerin yönetilme nedenini meydana getirir (Yılmaz, 2007: 41).

2.1. **Riskin Erken Saptanması Ve Yönetimi**

Kurum ve kuruluşlarda başarılı bir yönetim için risk yönetiminin uygulanması bir gerekliliktir. Gündelik hayatta her yerde riskler bulunmaktadır ki bu risklerle başa çıkabilmek için gerçekleşmeden önce koşullar ne olursa olsun karşılanması için savunma mekanizması geliştirilmelidir. Bu sebeple kurum ve kuruluşlarda risk yönetiminin yapılmaması sonucu genellikle karşılaşılan diğer sorunların da çözülememesine neden olmaktadır (Derici vd., 2007: 154). Bu gerçek doğrultusunda, 6102 sayılı TTK"da, pay senetleri borsada işlem gören işletmelere "risklerin erken saptanması ve yönetimi" için uzman bir komite kurma zorunluluğu getirilmektedir. Getirilen bu zorunluluktaki hedeflenen, işletmelerin varlığını, devamlılığını ve gelişmelerini koruma altına alabilmektir. Bu doğrultuda yönetim kuruluna alanında yetkin kişilerden teşekkül edilecek bir komite kurulması, olaylar olmadan önce erken tespit yapabilen bir sistem oluşturulması ve oluşturulacak bu sistemin etkin bir şekilde çalıştırılması gibi sorumluluklar verilmektedir (Uzun, 2011: 3). Kurum ve kuruluşlar bahsedilen bu komiteyi çeşitli adlarla oluşturabilmektedir; örnek olarak "Risk Komitesi", "Risk Yönetim Komitesi" veya "Riskin Erken Saptanması ve Yönetimi Komitesi" gibi isimlendirmeler yapılabilmektedir. Ancak bu aşamada kritik önem arz eden nokta bu komitenin isminden ziyade faaliyetleri ve sorumluluklarını etkin bir şekilde yerine getirebilmesidir (Kaya, 2015: 317).

2.2. **Risk Yönetiminin Faydaları**

Risklerin kontrol altında tutulabilmesi için modern işletme teorisinin eriştiği en genel çözüm yollarından biri de risk yönetimi kavramıdır. Öyle ki risk yönetimi, kazanç, sermaye ve risk kavramlarını birbiriyle ilişkilendirirken bunlar arasında en uygun dengeyi sağlayan bir görüş ve yönetim tekniği olarak ifade edilmektedir (Üzer, 2002: 4). Bilhassa kazanımlara odaklanan risk yönetimi anlayışı kurum ve kuruluşlar için stratejik bir alan olarak görülmektedir. Risk yönetimi kurum ve kuruluşlarda risk toleransını belirleme, risk endeksli fiyatlama, portföy yönetimi, müşteri ve paydaşların karlılığı, kayıp tahmini yapma ve yapılan faaliyetleri iyileştirme gibi etkileri sebebiyle faydalıdır (Yüzbaşıoğlu, 2003). Bunun yanı sıra kurum ve kuruluşlardaki stratejik birliktelikler, maliyet ve tedarik zinciri yönetimi, verimlilik yönetimi, yenilikçi fikirler, işletmelerin birleşme veya satın alınmaları gibi kavramlar faaliyet gösterilen sektörde rekabet avantajı elde edebilmek ve olumsuz koşullardan sakınabilmenin yanında fırsatları değerlendirebilme gibi stratejik üstünlükleri sağlamasıyla risk yönetimi giderek daha da önem kazanmaktadır (Özsoy, 2012: 166).

Kar amacı gütsün veya gütmesin bütün kurum ve kuruluşlar faaliyetlerini bir belirsizlik ortamında devam ettirmektedir. Bu nedenle kurum ve kuruluşlarda kurulmuş ve iyi yönetilebilen bir risk yönetim sisteminin alınan aksiyonların kısa, orta ve uzun vadede sağlayacağı yararlar şüphesiz pek çoktur. Bunların bazıları aşağıdaki şekilde sıralanmıştır (Arslan, 2008: 20):

- İşletme tarafından belirlenen amaç ve hedeflenen sonuçlara ulaşabilmesine yönelik yaratılan ve artırılan güven hissi,
- İşletmenin karşılaşabileceği tehditleri yönetim tarafından belirlenen risk toleransı seviyesinde tutmaya yardımcı olması,
- Yönetim katında alınacak kararların, gerçekleşen olaylardan sonra ortaya çıkan fırsatlardan işletmenin yararına olabilecek şekilde alınması,
- İşletme paydaşlarının yönetime ve yönetim tarafından alınan kararların doğruluğuna dair güvenlerini tesis etme ve bu güveni giderek artırma.

Risk yönetimi, Kurum ve kuruluşlarda beklenen kazançlardaki olumlu ya da olumsuz istenmeyen değişimlerin azalmasına veya belirlenmiş risk toleransı sınırlarında tutulmasına yardımcı olur. Buna ek olarak etkin bir şekilde risk yönetimi yapabilen kurum ve kuruluşların kazanımlarını aşağı şekilde ifade edilebilmektedir mümkündür (Argüden, 2006).

- Etkin ve istikrarlı işleyen bir kurumsal yönetim yapısı kurabilmek,
- Yenilikçilikten ödün vermeden riskleri bilinçli bir şekilde alabilmek,
- Tutarlı bilgiler sunabilmek,
- Paydaşlar ve kurum arasındaki iletişim faaliyetlerinde güven oluşturabilmek,
- Kurumsal itibarın yüksek olmasını sağlamak,
- Oluşabilecek riskler sebebiyle belirlenmiş stratejik hedeflerden sapmamayı sağlamak,
- Kurum ve kuruluşlarda oluşturulan değerlerin daha uzun vadeli olabilmesini sağlamak.

Risk yönetimi kavramının sadece risklerin kontrolü, transferi, azaltılması veya kaçınma faaliyetleri olarak görülmemelidir. Çünkü gündelik yaşamımızda kurum ve kuruluşlarla beraber bireyler de herhangi bir faaliyette bulunurken risk almaktadır, bu amaçla belirli kaynaklar ayırmakta ve sonuç olarak da bu riskleri alırken bazı kazançlar beklenmektedir.

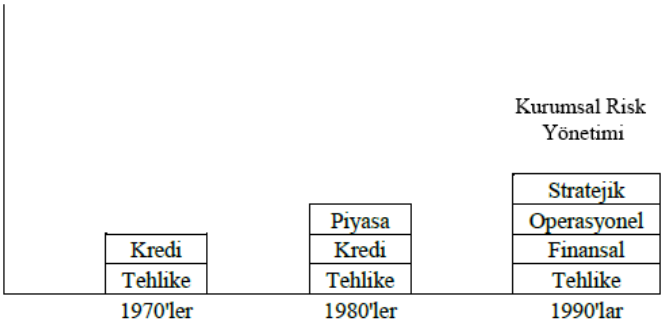
Tam da bu noktada alınan risklerle ilgili doğru karar alınıp alınmadığı, ayrılan kaynakların elde edilecek kazançlara değip değmeyeceğine gibi durumların doğru bir şekilde analizinin yapılabilmesi risk yönetimiyle mümkün olabilmekte ve beklenen kazancın elde edilebilmesi açısından karşılaşılan risklerin yönetilmesi önem arz etmektedir (Üzer, 2002: 4).

2.3. **Risk Yönetim Sisteminin Gelişim Süreci**

Yenilikçi düşünceye sahip bir grup sigorta profesörü tarafından risk yönetimi alanında 1950'li yıllarda ilk çalışmaların yapıldığı görülmektedir. Bunun yanında "Risk Management and Business Enterprise" isimli bir yayını Robert I. Mehr ve Bob Hedge 1963 yılında yayımlamışlardır. Bu çalışmada risk yönetimi yapılmasındaki temel amacın işletmedeki üretici etkinliğin en yüksek düzeye çıkarmak olduğu belirtilmiştir. Belirtilen bu amaçtan da anlaşılacağı üzere yapılan çalışmada üzerinde durulan temel nokta, risklerden yalnızca sigortalanarak korunmanın yanı sıra bunların yönetilmesi gerekliliği belirtilmiştir (D'Arcy, 2001: 3).

Dünya var olduğundan bu yana risk insanların yaşamında yer almaktadır. Faaliyetlerin yer aldığı sektör ne ise risklerin çeşitleri de ona göre değişmektedir. Geçmiş yıllarda tarım toplumunda faaliyet gösterilirken en kritik risk unsurunu hava koşulları olurken küresel çapta yaşanan gelişmelerden dolayı sanayi toplumuna geçişle beraber hava koşulları kritik risk unsuru olmaktan çıkıp yalnızca bir risk unsuru olarak değişime uğramıştır. Bu değişime ek olarak küreselleşme ile birlikte sınırların ortadan kalkıp iletişimin yayınlaşmasından dolayı döviz kurları, ürün fiyatlamalarında meydana gelen ani değişimler ve benzeri yeni ve kritik risk unsurları her geçen gün artarak kurum ve kuruluşların karşılarına çıkmıştır. Kurum ve kuruluşlar artarak devam eden ve birbirini etkileyen risk unsurlarının çeşitliliği içerisinde faaliyetlerini devam ettirmek durumundadır. Yönetim katında alınan kararlarda stratejik, operasyonel, finansal ve dış çevre riskleri göz önünde bulundurulması ve gerçekleşme ihtimallerine karşı alınacak önlemler ve bu önlemler için harcanan kaynakların yeterlilik düzeyiyle birlikte elde edilecek kazanımlara değip değmeyeceği önem arz etmektedir. Bu noktada kurum ve kuruluşlar riskleri tanımlamanın yanında ölçüp yönetebilmesi, yerine getirmeleri gereken zorunlu bir faaliyet olarak karşımıza çıkmaktadır (Tüzün, 2002: 26). Bir diğer deyişle risk yönetimi, kurum ve kuruluşların faaliyetlerini gerçekleştirirken karşılaşacakları riskleri öngörebilmeleri ve bu riskleri göğüsleyebilmek için tedbirleri alabilmeleri ve risklerden en az zarar ile birlikte en yüksek faydayı elde etmelerini sağlayacaktır (Derici vd., 2007: 153).

Gelişen ve değişen risklerin yanında risk yönetimi de bu gelişimle beraber daha fazla önem kazanmıştır. Bu değişkenlik geleneksel risk yönetiminin uygulama ve tanımlamalarının yetersiz kalması nedeniyle daha gelişmiş ve yenilikçi bir tanıma ihtiyaç duymuştur. Risk yönetimi kavramı kapsamı ve yapısı itibariyle çeşitli değişimlere uğramıştır. Risk yönetiminin gelişim süreci Şekil 2.1.'de gösterildiği gibidir.



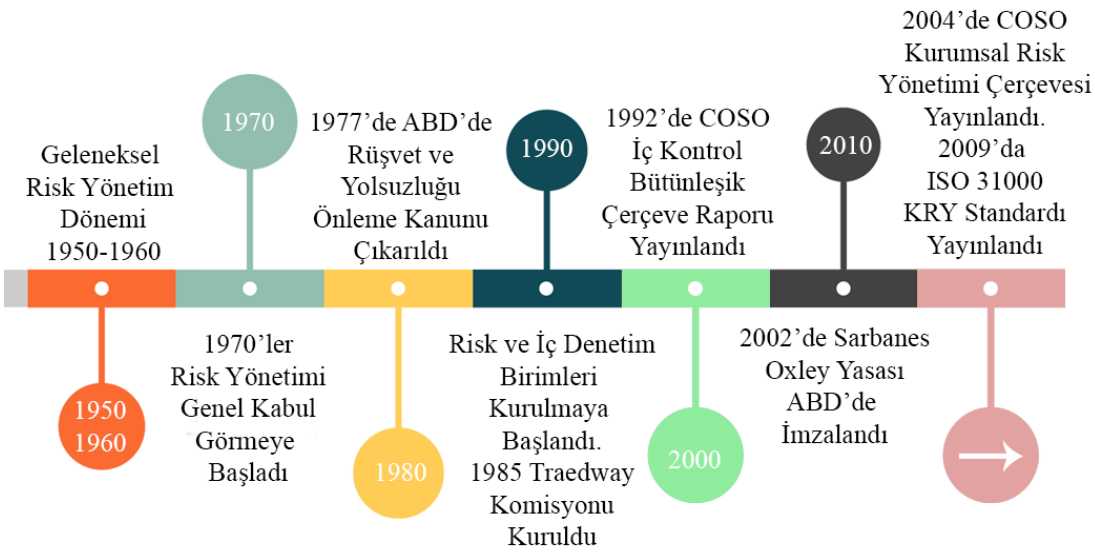
Şekil 2.1: Risk Yönetimimin Gelişimi
Kaynak: Shenkir, vd., 2002: 3.

Risk yönetimi şekil 2.1.'de de görüldüğü üzere ilk başlarda kapsamı ve risk olarak algılanan olgular açısından oldukça dar bir alanda kabul görmekteydi. Öyle ki yalnızca sigorta firmalarının sunduğu hizmetlerde ön görülen kredi ve tehlike olarak algılanmaktaydı. Yıllar içerisinde gelişen piyasa koşulları ve buna bağlı çeşitlenen riskler sebebiyle finansal, operasyonel ve stratejik alanlarda risk yönetimi anlayışına ihtiyaç duyulmuştur (Protiviti Inc., 2006). Günümüzde kurum ve kuruluşlar riskleri tanımlayabilmek ve risklerin yönetiminde alacakları kararların daha doğru olabilmesi için genel geçer bir risk dili oluşturma ihtiyacı duymuşlardır (Pricewaterhouse Coopers, 2006, s.11.). Bu yönde yeni risk tanımı olarak "Kurumsal Risk Yönetimi" ifade edilmektedir. Kurumsal risk yönetimindeki temel amaçlar; yönetim sistemine risk yönetiminin sistemini bütünleştirme, karşılaşılabilecek olayları öngörebilme, bu olaylar karşısında alınacak tedbirleri ve uygulanacak gerekli stratejileri yönetmek olarak sıralanabilir.

Risk yönetiminin tarihsel gelişimine bir başka açıdan daha detaylı bakabilmek için o dönemlerde yaşanan olaylara da değinmek gerekirse, 1970'li yıllarda karşılaşılan hammadde kriziyle birlikte petrol krizleri neticesinde yaşanan beklenmeyen iflaslar ve kayıplar şirketlerle beraber yatırımcıları çok zor duruma sokmuş ve bu nedenle risklere bakış açısını değiştirmiştir. Bu durum risk yönetiminin ne kadar önemli ve gerekli olduğunu ortaya çıkarmıştır. Derecelendirme kuruluşlarının tam da bu safhada temelleri atılmaya başlanmıştır. 1980'lerde risk kapsamında kredi, kayıp ve piyasa riskleri değerlendirilirken,

1990'lara gelindiğinde yönetim katmanında bulunanlar aldıkları kararlarda oluşması muhtemel riskler ve bu risklerin gerçekleşmeleri neticesinde beklenmedik sonuçlarıyla da ilgili daha fazla bilgiye ihtiyaç duymaya başlamışlardır. Geçmiş yıllarda edinilen tecrübelerle birlikte kurum ve kuruluşlar artık iflasla sonuçlanabilecek riskleri daha dikkatli bir şekilde ele almaya başlamışlardır. 1990'ların sonlarına doğru yapılan çalışmalar, kurum ve kuruluşların yönetmek amacıyla değerlendirmeye tabi tuttukları risklerin kapsamlarının genişlediğini ve çeşitlenerek arttığını ortaya koymuştur. Bu tespitler 2000'lere gelindiğinde risk yönetiminin kurumsal ölçekte bir risk yönetim felsefesinin gerekliliğini ortaya çıkarmış ve bu sayede riskin kapsamı daha da genişletilerek kurumsal risk yönetimi olarak değerlendirilmeye başlanmıştır. Bu sayede artık sadece finansal riskler değil, faaliyetlerden doğabilecek riskler yani operasyonel riskler ve yönetim kararlarından dolayı karşılaşılabilecek riskler yani stratejik riskler de göz önünde bulundurulmaya başlanmıştır. Sonuç olarak kurumun bütününü kapsayan bir risk yönetim anlayışı ortaya çıkmıştır.

Şekil 2.2.'de risk yönetiminde 1950'lerden günümüze meydana gelen gelişmeler izlenebilir;



Şekil 2.2: Risk Yönetiminde Zaman İçerisindeki Gelişmeler

2.4. Geleneksel Risk Yönetimi Ve Kurumsal Risk Yönetimine Geçiş

Geleneksel risk yönetimi, çağdaş risk yönetimi anlayışı ortaya çıkana kadar kurum ve kuruluşlar tarafından kullanılmaktaydı. Ancak geleneksel risk yönetimi statik yöntemlerle riski ölçmeyen ve kurumun tümünü kapsayacak şekilde bir risk planıyla yönetme anlayışı yerine her birimin riskini ayrı ayrı değerlendiren bir yönetim sistemi olarak bilinmektedir. Bu yönetim sisteminin aldığı en büyük eleştiri de birim bazlı değerlendirmelerde statik olmayan yöntemlerle riski ölçmediği için objektiflikten uzak genelde değerlendirmeyi

yapanların etkisi altında sübjektif değerlendirmeler ortaya koymasıdır.

Bir başka deyişle geleneksel risk yönetimi yaklaşımında kurum ve kuruluşlar risk yönetimini özel bir alana yönelmiş ve bazı etkilerden izole edilmiş bir faaliyet olarak görmektedir. Buna rağmen yeni anlayışla risk yönetimi belirli bir alandan ziyade kurumun her düzeyinde katılımcıyla yönetilmesi gerekliliğini ortaya koymaktadır (Barton vd., 2002: 4).

Ekonomik krizlerin yoğunlaştığı 1990'larda kurum ve kuruluşlarda artan risk algısı geleneksel risk yönetimi anlayışının kapsam ve etkinliği bakımından yetersiz kaldığı düşüncesi hakim olmuştur. Bu düşünce daha yeni, etkin ve kapsamı geniş bir risk yönetim anlayışının gerekliliğini ortaya çıkarmıştır. Bu nedenle kurumsal risk yönetimi anlayışı geçtiğimiz son 20 yılda stratejik, kurumun tamamını kapsayan, entegre ve sistematik bir yapıyla yönetim gibi özelliklerinden dolayı kurum ve kuruluşlar tarafından tercih edilmektedir.

Entegre risk yönetim kavramı 2000'li yıllarda Colquitt tarafından ortaya atılmış, daha sonrasında Dickinson 2001 yılında ilk defa Kurumsal Risk Yönetimi (KRY) kavramını literatüre kazandıran bilim adamı olmuştur. KRY, kurum ve kuruluşların, yaptıkları faaliyetlerde meydana gelebilecek riskleri, öngören, tasnifleyen, değerlendiren ve bütün riskleri sistematik ve koordineli bir şekilde yürütüldüğü çağdaş bir risk yönetim anlayışıdır.

Günümüzde kurum ve kuruluşlar artık risk yönetiminde parçalı, geçici ve dar kapsamlı yönetim anlayışı yerine bütünleyici, devamlı ve daha geniş kapsamı olan yönetim tarzına doğru yönelmişlerdir. Aşağıdaki tabloda görüldüğü üzere eski ve yeni yaklaşım karşılaştırmalı olarak verilmiştir.

Tablo 2.1: Eski ve Yeni Risk Yönetimi Yaklaşımlarının Karşılaştırması

YENİ RİSK YÖNETİM YAKLAŞIMININ TEMEL ÖZELLİKLERİ	
ESKİ YAKLAŞIM	**YENİ YAKLAŞIM**
• **Parçalılık (Bölümlülük):** Departman/Bölüm riski bağımsız olarak yönetir; muhasebe, maliye, iç denetim başlıca ilgi alanlarıdır.	• **Entegre (Bütünsel):** Risk yönetimi üst düzey gözetimi ile koordinelidir. İşletmedeki herkes risk yönetimini işinin bir parçası olarak görür.
• **Geçicilik:** Risk yönetimi, yöneticilerin gereklilik halinin olduğuna inandıkları zaman uygulanmaktadır.	• **Süreklilik:** Risk yönetim süreci işletmede süreklidir.
• **Dar Kapsamlılık:** Öncelikle sigortalanabilir ve finansal risklere odaklanma söz konusudur.	• **Geniş Kapsamlılık:** Tüm işletme riskleri ve **fırsatlar** göz önünde bulundurulur.

Kaynak: Barton vd., 2002: 5.

Yukarıdaki tablodan da anlaşılacağı üzere risk yönetiminde üç noktanın önem arz etmektedir. İlki risk yönetimi kurum ve kuruluşlarda sürekli olarak uygulanması gereken

kritik bir yönetim unsuru olarak değerlendirilmesidir. İkinci olarak yalnızca risklerin olumsuz yanları ve tehlikeleri yerine, doğru yönetilebildiğinde elde edilebilecek fırsatları da göz önünde bulundurulabilmesidir. Son olarak da bu anlayışın yalnız bir birime özel olmasından ziyade kurumun tümünde uygulanması ve kabullenilmesi gerekliliğinin anlaşılmasıdır. Buradan da görüleceği üzere risk yönetimi hala süreçlerin doğru bir anlayışla geliştirildiği bir yönde ilerlemektedir (Barett, 2003: 2).

Risk yönetimine geleneksel yaklaşımın yetersizlik ve olumsuzlukların sıyrılan ve daha doğru ölçümler içeren risk yönetimindeki yeni yaklaşım arasındaki farklar aşağıdaki şekilde biraz daha farklı bir şekilde ele alınmıştır;

Tablo 2.2: Geleneksel Risk Yönetimiyle Yeni Risk Yönetim Yaklaşımı Kıyaslaması

GELENEKSEL YAKLAŞIM	⇨	**YENİ YAKLAŞIM**
Risk kontrol edilmesi gereken olumsuz bir faktördür.	⇨	Risk bir fırsattır.
Risk organizasyonel silolarda yönetilir.	⇨	Risk bir bütün olarak kurum çapında yönetilir.
Risk yönetiminin sorumluluğu aşağı seviyelere delege edilir.	⇨	Risk herkesin sorumluluğundadır.
Risk ölçümü sübjektiftir.	⇨	Risk ölçülebilir.
Finansal kontrol esastır.	⇨	Stratejik ağırlıklıdır.
Risk azaltma sağlanır.	⇨	Risk optimizasyonu sağlanır.
Kurum değerini korumak esastır.	⇨	Kuruma değer katmak ve korumak esastır

Kaynak: (PWC, 2006).

2.5. **Geleneksel Risk Yönetimi ile Kurumsal Risk Yönetimi Arasındaki Farklar**

Geleneksel ve Kurumsal Risk Yönetimi arasındaki öne çıkan bazı önemli farklılıkları değerlendirmek gerekirse 6 maddede özetlenebilir. Bunlar;

1. Geleneksel risk yönetimi tekil riskler üzerinde duran ve risk odaklı bir yönetim anlayışına sahiptir. Kurumsal risk yönetiminde ise risklerin yalnız kurum içi ve tekil olduğuna değil, kurum dışındaki faktörlerin de risklerin oluşumuna etki edebileceğini aynı zamanda risklerin yalnızca tehdit gibi algılanmamasının yanı sıra fırsatlar doğurabileceğine odaklanmaktadır.
2. Geleneksel risk yönetimi, birimler arasında risklerin etkilerine ve sebeplerine bakmayıp birimleri ayrı ayrı değerlendirdiği için risklerin bütün olarak görmeyi engellemekte ve birimler arası entegrasyonu engelleyebilmektedir (Hoyt, Liebenberg, 2011) Yönetim katmanı tarafından alınan stratejik kararların birimler arası entegrasyon eksikliğinden dolayı işlevselliği azalır. Ayrıca Kurum faaliyetlerinde karşılaşılan risklerin fırsata çevrilememesinden dolayı verimsizlik

meydana gelir. Kurumsal risk yönetiminde bütüncül bir yaklaşımın yanında fırsatlar daima göz önündedir.

3. Geleneksel risk yönetim sisteminde kurum bazında risk değerlendirme raporu oluşturulması mümkün değildir çünkü birimlere ve çalışanlara sorumluluk yüklenmesiyle her birim için ayrı ayrı risk değerlendirmesi yapılmaktadır. Kurumsal risk yönetiminde ise risk değerlendirme raporları KRY komitesine yapıldığından kurumun tamamına ait risk değerlendirme raporu bu komite tarafından hazırlanıp kurumun tüm birimlerine gönderilerek bütüncül yaklaşım korunmaktadır. Bu sayede risk yönetim sorumluluğu üst yönetim katmanında bulunması sağlanır.
4. Geleneksel yönetimde kurumun tümünü bağlamayan şekilde birim bazında hazırlanan risk raporlamaları sonucu analizlerin nasıl değerlendirileceği belli değildir. KRY sisteminde ise belirli risklere odaklanmak yerine, riski yüksek alanlar belirlenip bu alanlar odak noktasına alınarak değerlendirmeler raporlanır ve sonuçlar toparlanıp kurumun geneli için bir risk toleransı ve iştahı belirlenir böylece her birim için ortak bir risk tutumu ortaya konulur.
5. Geleneksel risk yönetiminin odağında finansal riskler vardır ancak KRY yalnız finansal risklere değil kurumun genelini ilgilendiren iç ve dış tüm risklerle ilgilenir. Stratejik riskler, operasyonel riskler ve dış çevre riskleriyle birlikte finansal riskler değerlendirilir.
6. Geleneksel risk yönetiminde sorumlulukların çalışanlara bireysel olarak dağıtılması, sorumluluk verilmemiş kişilerin risk yönetimine katılamamasına neden olur. Ancak KRY' de ise kurumun tümünü ilgilendiren bütüncül bir yaklaşımla risk yönetim çalışması yapıldığından ortaya çıkan risk değerlendirmeleri kurumun tümünü kapsayıp kişilerin kayıtsız kalmamasını sağlar.

Ayrıca Risk odaklı yaklaşım, geleneksel risk yönetimi ve kurumsal risk yönetimi arasındaki farklar karşılaştırmalı olarak Tablo11'de gösterilmektedir;

Tablo 2.3: Risk Odaklı Yaklaşım, Geleneksel Risk Yönetimi ve Kurumsal Risk Yönetimi Karşılaştırılması

FAKTÖR	RİSK ODAKLI FAALİYETLER	GELENEKSEL RİSK YÖNETİMİ	KURUMSAL RİSK YÖNETİMİ
PERSPEKTİF	Fiziksel Tehditler	Tüm Tehditler	Fırsatlar Ve Tehditler
ODAK	Özel Projeler	Özel Faaliyetler	Kurum Geneli Ve Kurum Ortakları Temelli
SORUMLULAR	Uzmanlar	Yöneticiler	Tüm Çalışanlar
AYRINTI DÜZEYİ	Karmaşık Analizler	Detaylı Analizler	Genel Değerlendirmeler
ZAMANLAMA	Bir Defa	Düzenli	Sürekli
DİL	Farklı Terimler	Benzer Terimler Fakat Farklı Açılar	Genel Dil Ve Perspektif
RAPORLAMA	Bir Defa Detaylı	Yüksek Seviyede Parçalanmış	Bütünleştirilmiş İşletme Raporları
KONTROL ODAĞI	Güvenlik Ve Olasılık Planlaması Temelli	Bireysel Kontrol Mekanizmaları Temelli	Kontrol Çerçeveleri Temelli
ARAÇLAR	Veri Analizi	Kontrol Risk Ve Öz Değerlendirme (KRÖD) Ve Anketler	(KRÖD), Anketler Ve KRY'nin İşletme Süreçleriyle Bütünleştirilmesine Yönelik Araçlar
AMAÇ	Düşük Seviyede Güvence	Risk Kayıtlaması İçin Risk Tanımlamaları Ve Yönetimi	Kurum Amaçlarına Ulaşılması
STANDARTLAR	Uzmana Bağımlı	Yöneticiye Bağımlı	Kurum Risk Politikasına Bağımlı
VİZYON	Kurum Kaynaklarının Korunması	Yönetim Kurulunun Ve Yöneticilerin Korunması	Bütünleştirilmiş Risk Yönetimi Çerçevesinin Oluşturulması Ve Kurum İtibarının İyileştirilmesi
SİSTEME YÖN VERENLER	Dış Tehditler	CEO Ve CFO	Pay Sahipleri, CEO Ve CFO

Kaynak: (Pehlivanlı D., 2008).

3. BÖLÜM

KURUMSAL RİSK YÖNETİMİ

Risk yönetiminin temel amacı olarak karşılaşılan risklerin tanımlanabilmesi, değerlendirilebilmesi, gereken aksiyonların alınabilmesi ve kontrol altında tutulabilmesi şeklide ifade edilebilir. Bu amaçlar kredi veya piyasa riskleri gibi dar kapsamlı risk türlerini yönetmek için olabileceği gibi kurumun genelini kapsayacak şekilde riskleri değerlendirirken tehditlerle birlikte yakalanabilecek fırsatların da göz önünde bulundurulması şeklinde de uygulanabilmektedir. Kurumsal risk yönetimi kurumun yönetim süreçlerinde sürekli bir gelişme sağlaması yönüyle de önem arz etmektedir.

Bir diğer ifadeyle kurum ve kuruluşlar var olan risklerini yönetmek için yapı ve kapsam olarak birbirinden ayrışan iki yol izleyebilir. İlki mevcut riskler tekil olarak ayrı ayrı değerlendirilip yönetme; diğeri ise bütün riskler kurum genelinde bir dağılımın parçası olarak görülüp genele hitap eden bir risk yönetim felsefesiyle bütüncül bir yaklaşımla yönetmektir. İkinci yöntem genel olarak Kurumsal Risk Yönetimi olarak adlandırılır (Tekgül, 2007).

Risk yönetiminde süreklilik ve tutarlılığın önemine vurgu yapılması bakımından Kurumsal risk yönetimi bir başka ifadeyle şu şekilde tanımlanmıştır. Kurum ve kuruluşların belirledikleri hedeflere ulaşabilmelerini etkileyebilecek risklerdeki tehditler ve süreç içerisinde karşılaşılabilecek fırsatların tespiti, değerlendirilmesi ve tanımlanması sonucunda risklere karşı alınacak aksiyonların kararlaştırılıp rapor edilerek kurumun tamamında uygulanmasını sağlayan, istikrarlı, tutarlı ve kesintisiz bir süreçtir (The IIA, 2009, s.2).

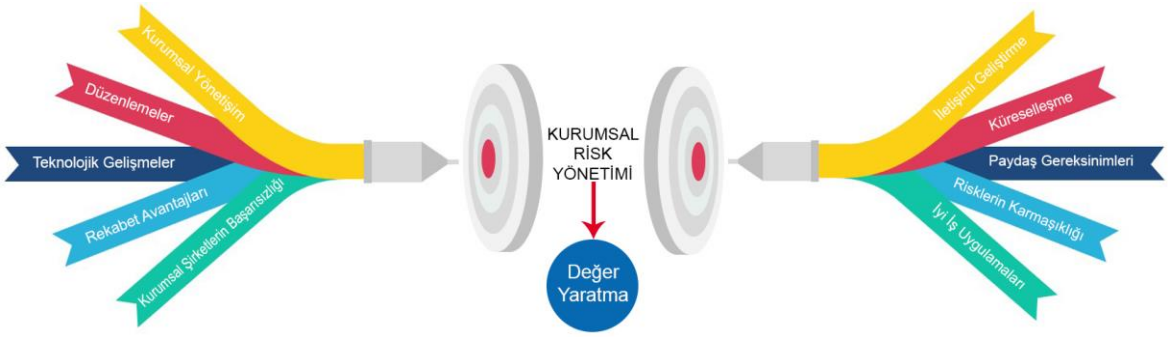
Kurum geneline hitap etmesi bir çalışmada şu şekilde ifade edilmiştir; Kurumsal risk yönetimi, bir kurumun yüzleştiği risklerin tamamının yönetimine entegre ve sistematik bir yönetim anlayışıdır (Dickinson, 2001: 360).

Kurumsal risk yönetiminin risklerin gerçekleşmesi durumunda karşılaşılacak olumlu ve olumsuz yönleri açısından şu şekilde ifade edilmiştir; “kurumlar tarafından belirlenen hedeflere ulaşabilme başarısını olumlu ve olumsuz yönde etkileyen belirsizlikleri yönetme

ve paydaşlarda aidiyet değeri oluşturmanın yanında bu değeri koruyup geliştirme amaçlı kurumun tamamında uygulanan bir girişimdir (Barton vd., 2002: 5).

Kapsayıcı özelliğine ait bir diğer tanımlama da şu şekilde ifade edilmiştir. Kurumsal risk yönetimi; kurum ve kuruluşların geneli için oluşturulmuş stratejileri uygulama, kurum içinde ve dışında ki paydaşları etkileyen ve onlardan etkilenen, hedeflere ulaşabilme amacıyla kuruma etkisi olan riskleri tanımlama ve kabul edilmiş risk kapasitesiyle kurumu yönlendiren bir anlayıştır (COSO, 2004a).

Kurumsal risk yönetimini etkileyen çeşitli faktörler bulunmaktadır. Bu faktörlerin gelişmeye zorladığı yönetim anlayışı, kuruma değer katmak amacıyla kurumun belirsizlikler karşısında strateji üretebilmesi ve bu strateji çerçevesinde teknoloji, insan ve süreçleri yönetebilmek amacıyla bu yeni yönetim yaklaşımını benimsemektedir. Bu yeni yönetim anlayışında istikrarlı, sürekli, değişime ayak uyduran ve kurumun tamamına nüfuz etmiş bir sistem olması tercih edilmesinde etkili olmaktadır. Sistemi etkileyen belli başlı bazı temel sürücüleri vardır (Manab, Hussin ve Kassim, 2010). Kurumsal risk yönetim sürücüleri şekil 3.1.'de gösterilmektedir.

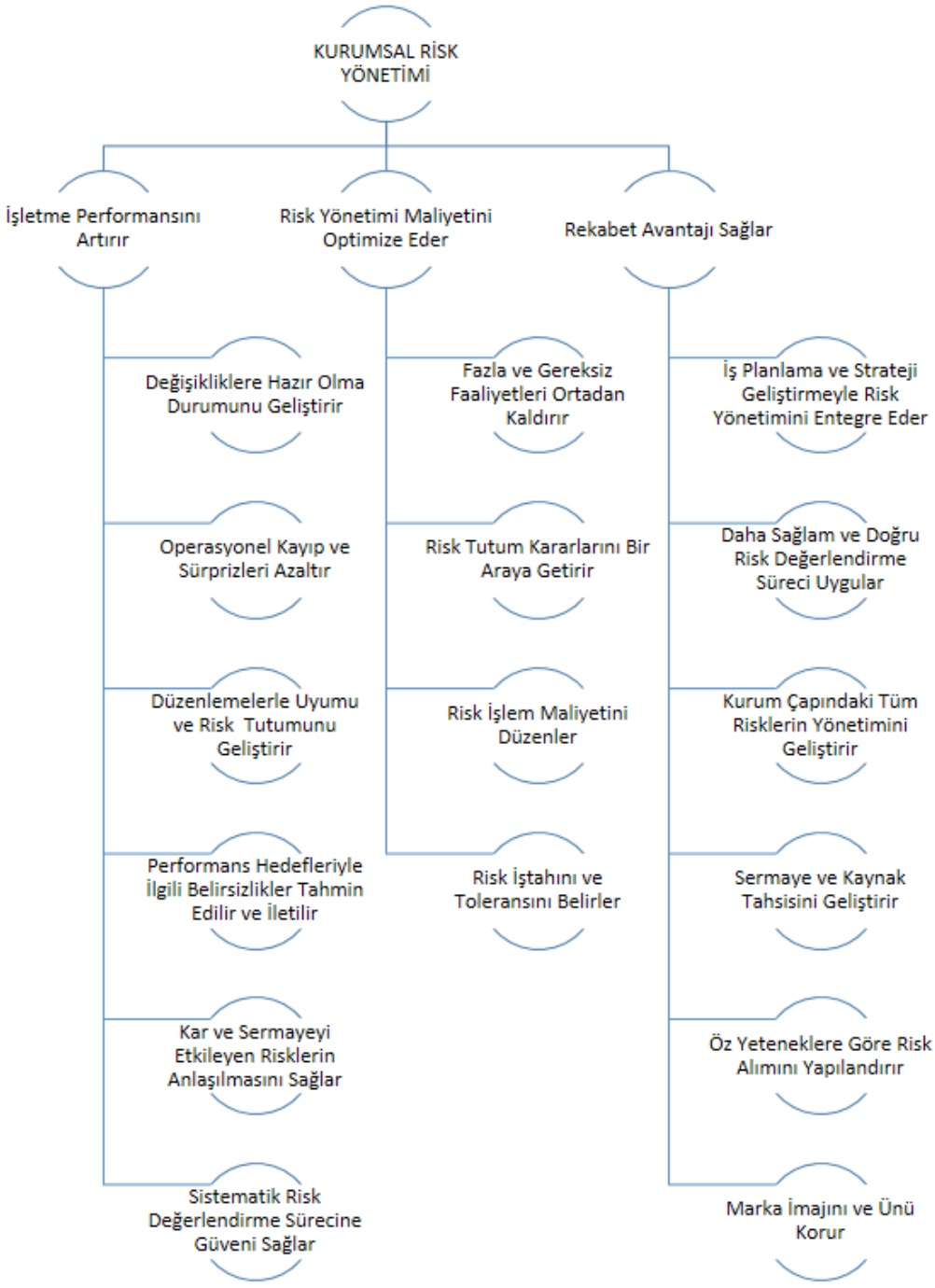


Şekil 3.1: Kurumsal Risk Yönetim Sürücüleri

Kurumsal değerin oluşturulması açısından bir diğer değerlendirme CAS (Casualty Actuarial Society) tarafından şu şekilde yapılmıştır; "Kurumsal risk yönetimi, herhangi bir işletmenin kısa ve uzun vadeli değerini olumlu yönde artırabilmek amacıyla bütün risklerin değerlendirilip kontrol edildiği, finanse edip izlediği bir bütüncül bir disiplindir." (CAS, 2003: 8). Kurumsal risk yönetimindeki odak noktası her kurumun paydaşlarına değer sağlamak için var olduğudur (Arslan, 2008)

Kapsam ve değer yönetimi açısından bir diğer görüş ise şu şekildedir. Kurumsal risk yönetimi, kurum ve kuruluşların değerini en üst düzeye çıkarabilmek için kredi, piyasa, operasyonel ve sermaye riskleriyle bu risklerin transferini yönetme amaçlı bütüncül ve kapsamlı bir çerçeveye sahiptir (Lam, 2003: 45).

Kurumsal risk yönetiminin kurumsal değer oluşturma ve bu değeri koruyup artırma amacı vardır. Dolayısıyla bu yönetim anlayışının değer üzerinde etkisi bulunmaktadır. Şekil 3.2.'de kurumsal risk yönetiminin performans, maliyet ve rekabet alanlarındaki etkileri gösterilmiştir. Şekil 3.2. incelendiğinde kurumun değerlerini koruyarak artmasını sağlayan kurumsal risk yönetiminin gerekliliği, önemi ve uygulanmasındaki amaçlar netlik kazanmaktadır.



Şekil 3.2: Kurumsal Risk Yönetiminin Kurumsal Değere Etkisi
Kaynak: (COSO, 2004b)

Kurum değerinin korunup artırılmasında kurumsal risk yönetiminde üç temel odak noktası bulunmaktadır bunlar;

- Rekabet avantajının sürdürülebilir olmasını sağlar
- Risk yönetim maliyetleri optimize edilir
- Kurumun performansının artırılması sağlanır.

Kurumsal risk yönetiminin başarılı bir şekilde uygulanmasında en temel düzeyde aşağıdaki kazanımlar elde edilebilir;

- Riskler arası bütün bağlantı ve ayrışan noktalar dikkate alınır,
- Faaliyetler gerçekleştirilirken tehdit ve fırsatlar birlikte değerlendirilir,
- Strateji geliştirilirken riskler göz önünde bulundurulur,
- Risklere portföy bakış açısıyla bakılır,
- Ortak bir risk dili oluşturulur ve bu iletişimi kolaylaştırır,
- Yönetimin şeffaflığını artırır,
- Kurumun performansını artırır.

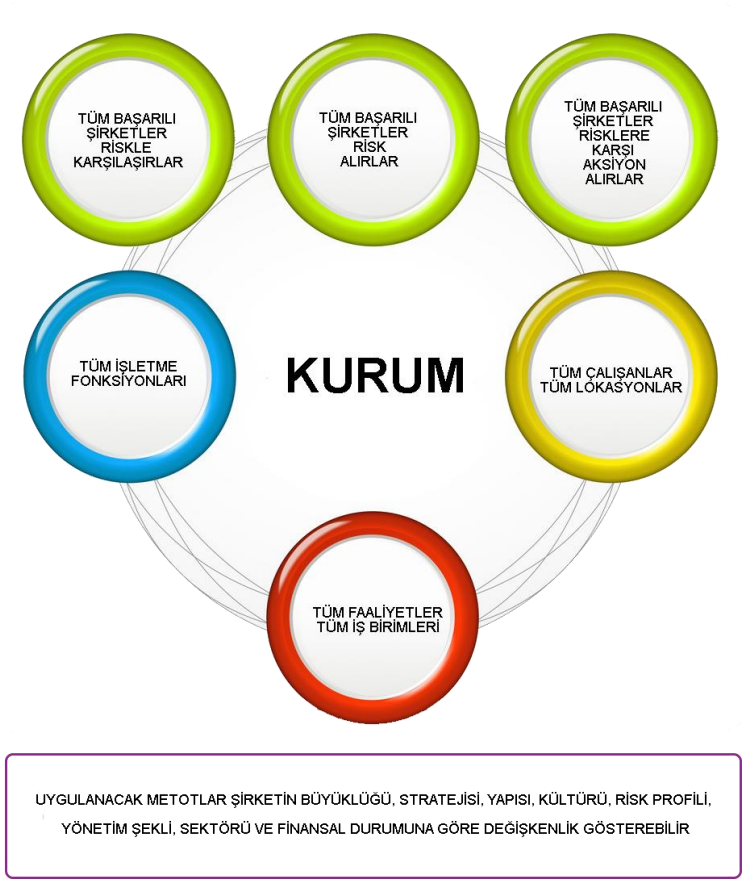


Şekil 3.3: Kurumsal Risk Yönetim Anlayışı

Genel bir ifadeyle yeni risk yönetim yaklaşımı olan kurumsal risk yönetiminde riskler, fırsat, belirsizlik ve tehlikelerden oluşur. Bununla birlikte bu anlayıştaki temel amaçlar yönetim süreci ile risk yönetim süreçlerini bütünleştirmek, kurumun karşılaşacağı risklerde olumsuz yönlerinin yanında olumlu yönlerini de keşfetmeye çalışmak ve etkin bir strateji geliştirip kurum değerini artırmaya çalışmak olarak özetlenebilir.

3.1. Kurumsal Risk Yönetimi Kapsamı

Kurumsal risk yönetimi kurumun bütün birimleri, çalışanları ve yöneticileri içine alan tüm paydaşları etkileyen entegre bir yönetim sürecidir. Şekil 3.4.'te kurumsal risk yönetiminin kapsamı içerisinde, bulunanların birbiriyle etkileşimi görülebilir.



Şekil 3.4: Kurumsal Risk Yönetiminin Kapsamı

3.2. Kurumsal Risk Yönetiminin Faydaları

Kurumsal risk yönetiminin uygulanmasıyla kurum ve kuruluşların sistematik ve disiplinli bir yapıyla yönetilmesini sağlayacağı gibi çeşitli faydaları da olacağı görülmektedir. Geleneksel risk yönetimi yaklaşımında finansal ve fiziksel varlıklar çevresinde görülen belirsizlikleri yönetme yaklaşımı baskındı, ancak kurumsal risk yönetimi bu çerçeveyi kurum geneline yayarak belirlenen hedeflere ulaşılması yolunda kapsam ve nitelik bakımından yönetim anlayışını üst seviyelere çıkartmıştır.

Kurumsal risk yönetiminin fayda sağlayacağı noktalar maddeler halinde şu şekilde sıralanabilir;

- Risk yönetimine kurumsal yaklaşım,
- Risk raporlama,
- İç denetim fonksiyonunu geliştirme,
- Kurumsal verimlilik,
- Performans artırma,
- Proaktif yaklaşım,
- Kurumsal yönetim anlayışı

Bu faydaların elde edilebilmesi için doğru kurgulanmış bir kurumsal risk yönetim yapısı ve etkin bir uygulama ile mümkündür. Yukarıda belirtilen bu faydaları biraz daha detaylı ele almak gerekirse (Seuamsothabandith, 2004: 4):

3.2.1. Risk Yönetimine Kurumsal Yaklaşım

Kurumsal risk yönetiminin ilk faydası olarak risk yönetimine kurumsal bir yaklaşım sağlamasıdır. Geleneksel yaklaşımda birimlerin her birinin kendi stratejilerini oluşturup bireysel olarak riskleri ele alıp değerlendirmeleri ve buna göre alacakları aksiyonları belirlemeleri gerekiyordu (Barton vd., 2002: 51-53). Bu yaklaşım genel olarak silo yaklaşımı olarak adlandırılmaktaydı. Bu yaklaşım risklerin etkin yönetimi açısından yetersiz kalmaktaydı. Çünkü her bir risk kurum içerisinde veya dışında bulunan belirsizliklere etkisi olacağı için bu belirsizliklerin kurumun karşılaşacağı etkileşimli birer risk olarak görülememesi silo yaklaşımında yetersizlikleri ortaya koymaktadır (Seuamsothabandith, 2004: 5). Buna ek olarak risk yönetimine bir değerler toplamı yaklaşımıyla bakan kurumsal risk yönetimi, riskler arasındaki etkileşim ve iletişimi dikkate almaktadır (Chapman, 2003: 30-35). Kurum ve kuruluşlar bu sayede risklere bakış açısında daha geniş bir perspektif kazanabilecektir.

3.2.2. Risk Raporlama

Etkin bir risk yönetiminin olmazsa olmazları arasında hiç şüphesiz ki risklerin raporlanmaları olarak gösterilebilir. Bu yüzden hem geleneksel hem de kurumsal risk yönetim anlayışlarında risk raporlaması yapılmaktadır. Ancak geleneksel risk yönetimi anlayışında birimler ayrı ayrı kendi sorumluluk alanlarında risklerin raporlamalarını

yapmaktaydı ve bu durum raporlanan riskler arasında uyumsuzluk hatta çelişen değerlendirmelerin ortaya çıkmasına sebep olmaktaydı. Kurumsal risk yönetiminde hazırlanan raporlarda kurumsal çapta oluşabilecek toplam kayıplar, erken uyarı göstergeleri, istisna oluşturan yönetim politikaları ve birimler arası etkileşimli risk tanımlamaları gibi içerik ve seviye olarak kurumun genelini kapsayacak şekilde olması sağlanmaktadır. Bu sayede kurum genelinde risk algısının artırılmasının yanında risk şeffaflığı sağlanmakta ve üst yönetime özet ancak genel bir rapor hazırlanabilmektedir.

3.2.3. İç Denetim Fonksiyonunun Geliştirilmesi

Kurum ve kuruluşlarda kurumsal yönetim anlayışının gerekliliklerinden biri olan iç denetim fonksiyonu kurumsal risk yönetim anlayışında etkin bir işlevsellik kazanmaktadır. Bu kazanım kurumsal risk yönetimi uygulamaları sayesinde iç denetçilerde kurumun risk profiline daha şeffaf ve tanımları net bir şekilde görebilmelerinin yanı sıra kapsamı ölçülebilen ve etkin yönetilebilen bir risk anlayışına sahip olmalarını sağlamaktadır (Barton vd., 2002: 55). İç denetçilerin riskleri en iyi şekilde tanımlayabilmelerini sağlayacak yüksek kaliteli bilgi edinilmesini sağlayan kurumsal risk yönetimi, bu risklerin önceliklerinin belirlenebilmesi, sıralanabilmesi ve bu riskler için kuruma uygun planlar geliştirmelerini mümkün kılacaktır (Seuamsothabandith, 2004: 7).

İç denetim fonksiyonu kurumun genel risk tanımlama ve analizleriyle uğraşmak yerine kurum genelinde öngörülen risklerin durumlarını denetleme faaliyetleriyle uğraşmaları gerekmektedir. Kurumsal risk yönetimi uygulamalarında hazırlanan risk analizleri etkin bir denetim için iç denetçilerin faaliyetlerini kolaylaştırmakta ve bu faaliyetlere harcanan süreleri azaltmaktadır. Bu sayede iç denetçiler denetim faaliyetlerini gerçekleştirmeleri mümkün olmaktadır (Chapman, 2003: 30-32).

3.2.4. Kurumsal Verimlilik

Kurumsal risk yönetimi uygulanmayan kurum ve kuruluşlarda kurumsal risk yönetimi ve risk yönetimi fonksiyonları ayrı ayrı bulunmaktadır. Bu da kurumun fonksiyonları arsında entegrasyon ve iletişim eksikliğinden kaynaklanan verim kayıplarına neden olmaktadır. Kurumsal risk yönetimi bu fonksiyonları bütüncül bir yaklaşımla kurum genelinde etkinliği olacak biçimde kaynaşmasını sağlayarak koordineli bir yönetim ortamı oluşmasını sağlamaktadır. Bu sayede oluşturulacak olan kurumsal risk yönetim ekipleri daha geniş bir

perspektife sahip olacakları için risklerin tanımlanması ve riskler arasındaki ilişkilerin görülüp birlikte değerlendirilmesinde avantaj elde edeceklerdir.

3.2.5. **Performans Artışı**

Kurum ve kuruluşlar birimler arası entegrasyon, iletişim ve kaynakların ortak kullanılamamasından hem verimlilik hem de performans kaybı yaşamaktadır. Kurumsal risk yönetiminde, hizmet/ürün geliştirilmesinde kaynakların ortak kullanımı, risk tanımı ve analizlerine kurumun genelinde aynı perspektiften bakılmasını ve birimler arası iletişimin artırılmasını sağladığı için kurumun genel performansı artmaktadır. Tüm bu gelişmeler, risklerin portföy olarak görülmesi sonucunda meydana gelir.

3.2.6. **Risk Yönetimine Proaktif Yaklaşım**

Kurum ve kuruluşların hızlı büyüyen ve ani değişkenliklere sahip pazarda faaliyetlerini yerine getirirken potansiyel olarak kurumu tehdit eden veya kuruma kazandıracağı fırsatlar içeren çok çeşitli riskler bulunmaktadır. Proaktif tutum sayesinde kurumların karşılaşabilecekleri bu riskleri öngörüp tanımlayabilmek ve gerçekleşmeden önce olumsuz risklerini azaltmak için önleyici ve düzeltici faaliyetlerde bulunulmasına katkı sağlar (Seuamsothabandith, 2004: 6). Kurumsal risk yönetiminin kullanılması sayesinde kuruma etkin risk yönetimi için bu proaktif yaklaşım yeteneğini kazandırmaktadır.

İnsanlarda bulunan merkezi sinir sistemi, herhangi bir olayla karşılaşıldığında kişiye karşılaşılan olayın niteliğine göre farklı farklı tepkiler verebilmesini sağlamaktadır. Örneğin tehlike durumunda kaçmayı veya savunmaya geçmeyi, korku durumunda saklanmayı veya saldırmayı öngörerek tepki vermesini sağlar. Kurumsal risk yönetimi de kurum ve kuruluşlarda bir sinir sistemi oluşturur. Bu sistem önceden karşılaşılmış olaylarda risklere verilen tepkilerden çıkarılan dersler sonucu yeni risklerin sistematik bir şekilde tanımlanmasını sağlar ve oluşması muhtemel olaylarda uyarıcı olduğu gibi önleyici faaliyetlerle birlikte yeni öğrenimleri sağlar (Funston, 2003). Bu sayede proaktif yaklaşım sergileyen kurum ve kuruluşların risk farkındalığı ve bilgisi giderek artmasını ve bunun yanında alınan kararların kurumun amaçları doğrultusunda en iyi kararlar olmasını sağlayabilecektir (Seuamsothabandith, 2004: 7).

3.2.7. **Kurumsal Yönetim Anlayışı**

Günümüzde kurum ve kuruluşlarda paydaşlarına hesap verebilirlik ve şeffaf bir yönetim anlayışı önemli bir olgu haline gelmiştir. Kurumsal risk yönetimi sayesinde kurum ve kuruluşlarda yönetim anlayışı daha kurumsal bir yapıya kavuşabilecektir. Kurumsal yönetimle karşılaşılan veya oluşması muhtemel risklerin etkin bir şekilde yönetimi sağlanacağı için yönetimin paydaşlarına hesap verebilirliği artacaktır (Chapman, 2003: 33). Kurumsal risk yönetimi uygulanması yönetim katmanında hem yönetim becerileri hem de stratejik kararlarda ihtiyaç duyulan öngörüleri edinmede kolaylık sağlayacağı için bu sebeple bu yeni anlayışın uygulanmadığı kurumlarda yönetim kuruluna bu sistemin önerilmesi kurumsal yönetim anlayışının tesisi açısından en etkili yöntem olarak görülecektir (Seuamsothabandith, 2004: 8).

Kurumsal risk yönetiminin yukarıda saylan onca faydasına rağmen birçok kurum ve kuruluşta yöneticiler reaktif bir yaklaşımla herhangi bir kriz anında veya meydana gelen bir felaketi engellemek amacıyla harekete geçmektedir. Bu durum ise kurumsal risk yönetimi anlayışının proaktif yaklaşımıyla çelişmektedir. Hâlbuki risk yönetimine harcanan kaynak ve zaman kurumların ilerlemesini ya da gerilemesini önemli ölçüde değiştirmemektedir. Gelişmiş bir yönetim anlayışı olan kurumsal risk yönetimi çerçevesinde kurumlar daha rasyonel yatırım yapabilir ve proaktif bir yaklaşım sergilemeleri sayesinde risk profillerini optimize edebilirler. Gerileyen kurumlar ise yatırımlarını rasyonellikten uzak yaptıkları gibi reaktif bir tutumla risklere karşı aksiyon almaktadırlar ve bu yüzden bir krizden diğerine mücadeleyle performans ve verimliliklerini düşürmektedirler (Lam, 2003: 45-46).

3.3. **KRY'nin Kurum Başarısına Etkisi**

Riskin olmadığı bir çevreden söz etmek mümkün değildir, kurum ve kuruluşlar da faaliyetlerini bu ortamda gerçekleştirmek zorundadırlar. Kurumsal risk yönetimi bu şekilde bir çevre oluşturmaya çalışmaktan ziyade risklerle dolu bir ortamda faaliyetlerin etkin ve başarılı olması için gerekli tedbirlerin alınmasını sağlamaktadır. Kurumsal risk yönetimi çerçevesinde aşağıda belirtilen noktalarda kurumun başarısını olumlu yönden etkilemektedir (COSO, 2004b: 2-4);

- Risk iştahının doğru belirlenmesi
- Risk, büyüme ve karlılık ilişkisinin belirlenmesi

- Risklere verilecek karşılığın kararlarını belirleme
- Risklerin kurum genelinde tanımlanıp yönetilmesi
- Risklere karşı ortak aksiyon alınabilmesi
- Karşılaşılabilecek fırsatların yakalanması
- Kaynakların doğru yönetimi.

Bu olguları kısaca açıklamak gerekirse;

3.3.1. Risk İştahının Doğru Belirlenmesi

Bir kurum hedeflerine ulaşmak için risk almak zorundadır ancak kontrolsüzce fazla risk alırlarsa batmalarına sebep olur eğer riskleri daha az alırsa o zaman da oldukları yerde sayabilirler yani risk iştahı kurumların almaya istekli olduğu riskin derecesi olarak tanımlanmaktadır (Güneş, 2009). Kurum ve kuruluşlar kurumun risk iştahını belirlerken risk toleransı sınırlarını dikkate almaktadır. Böylece alınacak stratejik kararlar da risk iştahı göz önünde bulundurulduğunda kurum risk toleransı içerisinde kalarak etkili kararlar alabilir. Yanlış belirlenen risk iştahı kurumun başarısını etkilemesinin yanında sonunu getirebilecek çok kritik bir süreçtir.

3.3.2. Risk, Büyüme Ve Karlılık İlişkisinin Belirlenmesi

Kurum ve kuruluşlar mevcut değerlerini korumayla birlikte büyütmek amacıyla risk alırlar. Alınan risklerin karşılığında elbette kar beklentisi olmaktadır. Bununla birlikte kurumsal risk yönetimi hedeflenen kazanımların kurumun karşılaşması muhtemel risklerin belirlenmesi, değerlendirilmesi ve analizi için kuruma doğru yönetim kabiliyeti sağlayarak kabul edilebilir risk oranını belirlemesine yardımcı olur. Bu sayede kaynakların bu kabiliyetle yönetilerek istenilen düzeyde karlılık ve büyüme seviyesi yakalanabilir.

3.3.3. Risklere Verilecek Karşılığın Kararlarını Belirleme

Kurumsal risk yönetimi anlayışında kurum ve kuruluşlar risklerle karşılaşıldığında bu risklere ne şekilde yanıt vereceğini alacağı stratejik kararlarla önceden belirlemektedir. Bu yaklaşım proaktif özellikler içerdiği için riskler henüz gerçekleşmeden bunları önleme, azaltma, transfer etme ve sonunda kaçınması mümkün olmayanları kabul etme seçeneklerinden hangisini tercih edeceğine önceden karar verebilmesini sağlamaktadır. Bir örnekle açıklamak gerekirse; lojistik işi yapan bir firmada trafik kazaları riskine karşı

çalışanın eğitimi veya aracın gerekli bakımlarının zamanında yapılması gibi önlemler riskin oluşmadan önce önlenmesi ve azaltılması kararlarına birer örnek oluşturabilir.

3.3.4. Risklerin Kurum Genelinde Tanımlanıp Yönetilmesi

Kurumun geneli itibariyle geniş bir perspektif kazandıran kurumsal risk yönetimi anlayışında herhangi bir birimde meydana gelebilecek riskler sonucunda etkilenebilecek diğer birimlerin de önceden belirlenip alınacak tedbirlerde bu durumun göz önünde bulundurulması sağlanabilmektedir. Bu sayede riskler bütüncül bir yaklaşımla değerlendirilebilmekte böylece birimler arası entegrasyon ve iletişim artırılabilmektedir.

3.3.5. Risklere Karşı Ortak Aksiyon Alınabilmesi

Kurum ve kuruluşlar faaliyetlerinde çok yönlü risklerle karşılaşırlar. Kurumsal risk yönetimi bu risklerin kurumun belirlenen hedefleri doğrultusunda alınacak stratejik kararları diğer bütün risklere karşı alınacak aksiyonların tamamını kapsayacak şekilde bütüncül ortak bir yapıda olmasını sağlamaktadır.

3.3.6. Karşılaşılabilecek Fırsatların Yakalanması

Kurum ve kuruluşlara risklerin yalnızca tehdit olarak değerlendirilmesi yerine kurumsal risk yönetimi çerçevesinde her bir riskin yeni fırsatlar getireceği konusunda yönetim kabiliyeti kazandırılmaktadır. Bu sayede kurumların amaçları doğrultusunda riskleri birer fırsata çevirmesi, kurumsal başarıyı olumlu yönde hızla ivmelendirmesini sağlayacaktır. Örneğin pazarda meydana gelen bir değişiklik veya müşteri eğilimlerinde oluşacak bir değişim esasında bir risk olarak değerlendirilebilir. Ancak kurumlar bu gibi durumlara öngörü yeteneği kazanmış bir şekilde yaklaştıkları zaman rakiplerine karşı avantaj elde edecekleri için risklerini fırsata çevirmiş olacaklar böylece kurumun başarısı artacaktır.

3.3.7. Kaynakların Doğru Yönetimi

Risklerin doğru belirlenmesi kaynakların etkin kullanımında çok önemli bir rol oynamaktadır. Kurumsal risk yönetimi kurumun genelinde risk yönetimi yapılmasını olanaklı kıldığı için yapılan faaliyetlerde kaynakların birimler arası doğru paylaştırılması mümkün olmaktadır. Yanlış yönetilen kaynaklar da kurumun farklı risklere maruz kalmasının önünü açacaktır. Bu sebeple kurumun başarıya ulaşabilmek için kaynak israfını önleyip doğru yönetmesi büyük önem arz etmektedir.

3.4. **Kurumsal Risk Yönetiminin Sınırlılıkları**

Kurumsal risk yönetiminin uygulanmasıyla elde edilecek çok sayıda faydanın yanında bu sistemin başarıya ulaşabilmesi için bazı sınırlılıklar da bulunmaktadır. Kurumsal risk yönetiminin çok iyi kurgulanıp uygulanmasına rağmen kurumun amaçlarını başarıyla ulaşmasını garanti etmediği yönde görüşler de bulunmaktadır (Chapman, 2003: 30-35). Kurumun olması muhtemel başarısızlığını tamamen engelleyecek bir sistem olduğu anlayışı yanıltıcı olacaktır. Bu yönde kısıtlayıcı birçok durumla karşılaşılabilir bu durumlara birkaç örnek vermek gerekirse;

- Gelecek belirsizliktir ve risk gelecekle ilgilidir.
- Yönetim katmanında tüm olaylar öngörülüp çözülemeyebilir.
- Art niyetli veya dikkatsiz çalışanlar sistemi bozabilir.
- Belirlenen hedeflere kesinlik sağlayamayan bu anlayış makul oranda bir güvence sağlamaktadır.

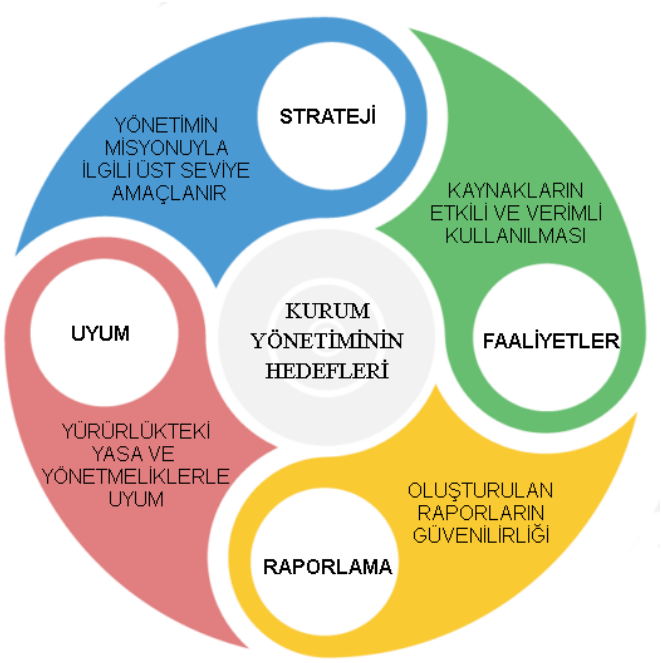
Gelecek kesin olarak kimse tarafından bilinemez bu yüzden genel itibariyle gelecek belirsizliklerle doludur. Riskleri yönetmeye çalışmak da zaten bu belirsizliklerin getireceği olumlu veya olumsuz gelişmeleri anlayıp gereken uygun aksiyonları almaya çalışmaktır. Stratejik kararlarla bu gibi durumlar önlenmeye çalışılmaktadır ancak yönetim katında da öngörülemeyecek ya da farklı çözüm önerileri getirilen risklerle karşılaşıldığında hiç beklenmedik bir sonuçla karşılaşılabilir. Bununla birlikte çalışanların dikkatsiz davranması veya art niyetli olarak bilinçli yanlışları yüzünden başarı sağlanamayabilir. Kurumsal risk yönetimi bu çerçevede kurumlara kesin başarıyı vadetmemekle beraber makul düzeyde gelecekte oluşması beklenen risklere karşı yönetim becerisi kazandırmaktadır.

Kurumsal risk yönetimi sisteminde tüm kurallara uyulup gerekenler yerine getirilse bile tamamen hatasız bir sistem değildir elbette, çünkü bu durumu etkileyecek de birçok risk mevcuttur. Bir diğer deyişle risk yönetiminin de riskleri her zaman bulunmaktadır.

4. BÖLÜM

KURUMSAL RİSK YÖNETİMİ BİLEŞENLERİ

Kurumsal risk yönetimi en genel tanımında bir kurumun belirlediği hedeflerine ulaşmasına engel oluşturabilecek belirsizliklerin yönetilebilmesi olduğuna göre bu risklerin doğru bir şekilde yönetilebilmesi kurumun hedeflerinin tam olarak anlaşılmasıyla mümkündür. Kurum vizyonu ve misyonu belirlenirken yönetim bu noktada hedefleri anlaşılır bir şekilde belirlemelidir ve bu hedefe ulaşabilmek için stratejiler kurgulanmalıdır.



Şekil 4.1: Kurum Yönetiminin Hedefleri

Kurum ve kuruluşların belirledikleri hedeflere ulaşma noktasında zaman içerisinde çok çeşitli yöntemler denenmiştir. Bu bağlamda günümüzde uluslararası bir standart olarak görülen Committee of Sponsoring Organizations of Treadway Commission (COSO) küpü 2004 yılında kurumsal risk yönetimi bütünleşik çerçevesini yayınlamıştır. Bu çerçevede kurumların temel olarak amaçladıkları belirlenen hedeflere ulaşma isteği kurumun geneline hitap edecek bir şekilde yaygınlaşabilmesi için COSO birbiriyle ilgili sekiz unsur tanımlamıştır. Bu sekiz unsur COSO ERM Küpünde gösterilmiştir.

4.1. COSO Kurumsal Risk Yönetim Modelinin Gelişimi

Amerika Birleşik Devletlerinde 1985 yılında kontrol ve muhasebe kuruluşlarından beş tanesinin katılımıyla kurulmuştur. Bu kuruluşlar;

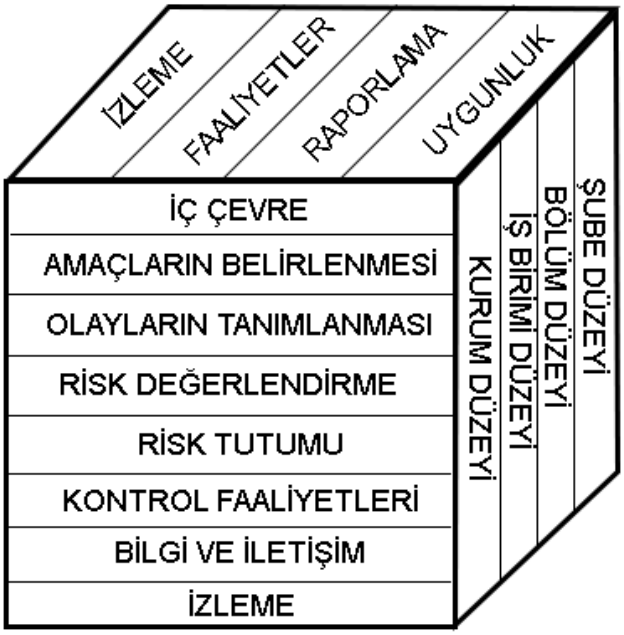
- Amerikan Kamu Muhasebecileri Birliği (The American Institute of Certified Public Accountants - AICPA),
- Amerikan Muhasebeciler Birliği (The American Accounting Association - AAA),
- Finansal Yöneticiler Enstitüsü (The Financial Executives Institute – FEI)
- İç Denetçiler Enstitüsü (The Institute of Internal Auditors – IIA)
- Ulusal Muhasebeciler Birliği (The National Association of Accountants)

COSO'nun kurulmasındaki temel amaç, finansal raporlarda bilinçli hilelerin veya yanlışlıkla yapılan hataların oluşmasını azaltmaktır. Bu amaca yönelik 1992 yılında COSO I: İç Kontrol Bütünleşik Çerçeve (Internal Control-Integrated Framework) raporu yayınlanmıştır. Bu raporda iç kontrol yapısının temelleri atılmıştır. 2004 yılında ikinci bir rapor olan COSO Kurumsal Risk Yönetimi (ERM- Enterprise Risk Management) isimli rapor yayınlanmıştır. Bu raporun çerçevesi de kurumsal risk yönetimi kavramı olmuştur. Raporda kurumsal risk yönetimi, işletmelerin hedeflerine ulaşabilmesi için kabul edilen düzeyde bir güvence oluşturmak amacıyla tasarlanmış bir süreç olarak tanımlanarak yapısal olarak dinamik olduğu belirtilmiştir. Ayrıca kurumsal risk yönetiminin başarılı bir şekilde uygulanabilmesi için işletmelerin risk alma eğilimini göz önünde bulundurarak strateji oluşturulması ve risk algısının işletmenin genelinde benimsenmesinin sağlanması belirtilmiştir (COSO, 2004a: 19). 2004'ten sonra gelişen ve değişen çevre şartlarına gereken uyumu sağlamak amacıyla 2017 yılında mevcut rapor güncellenerek Kurumsal Risk Yönetimi-Strateji ve Performans ile Entegrasyonu (Enterprise Risk Management-Integrating with Strategy and Performance) adıyla yayınlanmıştır. Bu raporda da kurumsal risk yönetiminin çerçevesi, yapısı ve adında bazı değişiklikler yapılmıştır (COSO, 2017).

İkinci rapor olarak 2004'te yayınlanan kurumsal risk yönetimi raporunda kurumsal risk yönetimi, işletmelerin belirledikleri hedeflere ulaşabilme amacıyla kabul edilebilir bir güvence oluşturmak için dinamik olarak tasarlanan bir süreç olarak tanımlanmıştır. Bu süreç içerisinde işletmenin etkilenebileceği olası olayların belirlenmesi ve bu olaylardan dolayı meydana gelebilecek risklerin işletmenin belirlediği risk iştahına göre yönetilmesi olarak ifade edilmiştir (Göğüş, 2015: 47).

4.2. **COSO Kurumsal Risk Yönetim Sistemi**

COSO kurumsal risk yönetimi küpü olarak bilinen üç boyutlu bir matris olarak tasarlanan küpte her bir yüzeyde belirtilen alanlar birbiriyle ilişkili olduğu için küp bir bütün olarak değerlendirilmelidir. Şekil 4.2.'de görüldüğü üzere işletme amaçlarını belirten dört ana kategori dikey sütunlar şeklinde verilmiş, Strateji, Faaliyetler, Raporlama ve Uygunluktur. Kurumsal risk yönetiminin çerçevesini oluşturan sekiz adet bileşen ise yatay satırlar olarak verilen, İç çevre, Amaçların Belirlenmesi, Olayların Tanımlanması, Risk Değerleme, Risk Yanıtlama, Kontrol Faaliyetleri, Bilgi ve İletişim ve son olarak İzlemedir (Staciokas ve Rupsys, 2005: 23). Küpün üçüncü boyutunda da İşletmenin organizasyon yapısını gösteren dört başlık ise, Şube Düzeyi, Bölümler Düzeyi, İş Birimi Düzeyi ve İşletme Düzeyidir. Küpte verilen üç boyutun her bir boyutu bir diğeriyle ilişkilidir ve hepsi etkili bir kurumsal risk yönetimi sisteminin nasıl olacağını göstermektedir (Kinney, 2003: 141).



Şekil 4.2: COSO Kurumsal Risk Yönetim Küpü
Kaynak: COSO, 2004a

4.2.1. **İç Çevre**

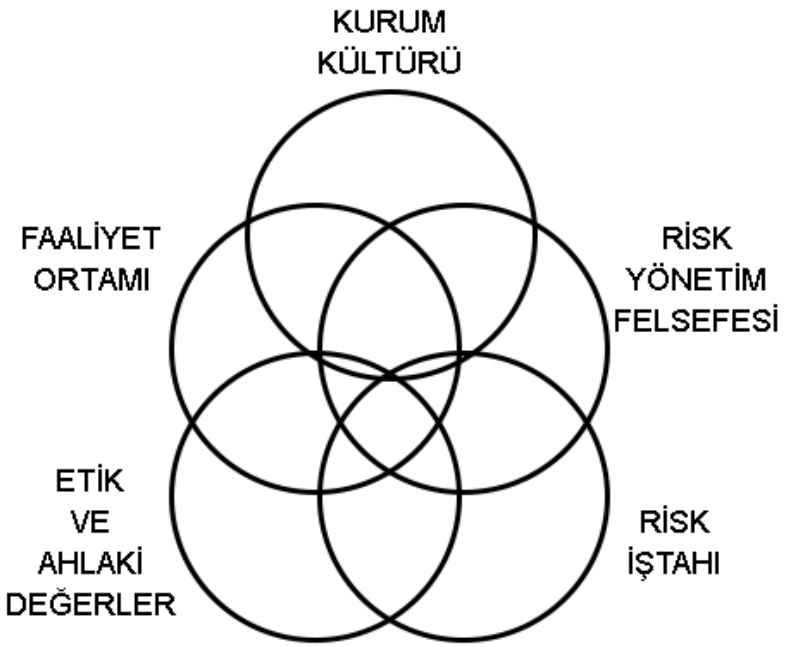
COSO Kurumsal Risk Yönetimi küpünde ilk sırada gelen iç çevre, kurumsal risk yönetiminin temelini oluşturmakla beraber bir disiplin ve altyapı sağlamaktadır. İç ortam olarak da adlandırılan bu adımda çizilecek çerçeve kurum ve kuruluşlar tarafından kurumsal strateji ve hedeflerin tespiti, faaliyetlerin yapılandırılması, risklerin belirlenmesi, değerlendirilip yönetilmesi aşamalarında büyük önem arz etmektedir. Kurumun tümünü kapsayan iç ortam, risk ve riske dair kontrollerin personel tarafından nasıl görüldüğü ve

değerlendirildiğine yönelik bir yaklaşım oluşturmaktadır. İç ortam kurumun tarihi ve kültürel gelişiminden etkilenmektedir. Bu sebeple kurumda oluşan etik değerler, personelin yeterlilik düzeyi ve gelişimi, risk yönetimindeki yönetim felsefesiyle beraber yetki ve sorumluluk devri süreçleri gibi unsurları içermektedir. Kurumlar arasında bu unsurların etkinlik düzeyi farklılık gösterebilmektedir (COSO, 2004b: 5).

Bir diğer deyişle iç ortamın kurumların yönetim katında kurumun hedeflerini belirleme, strateji oluşturma ve bu stratejilerin uygulanabilmesi için faaliyet planları oluşturmasına yarar. Bu aksiyonlar kurumsal risk yönetiminde iç ortam unsurlarını oluşturmakla birlikte geri kalan diğer unsurlar için bir çerçeve oluşturur (Kinney, 2003: 141).

Risk odaklı bir başka görüş ise; iç ortam, işletmelerde hedef ve buna bağlı stratejilerin ne şekilde oluşturulacağını, riskle ilgili faaliyetlerin hangi yöntemle yapılandırıldığının yanı sıra risklerin tanımlanması, risklere karşı verilecek tepkilerin ne olacağı ve risklerin nasıl yönetileceği konularında etkili olmaktadır (Moeller, 2011: 56).

Özetle iç ortam, kurumun tamamını kapsamakla birlikle personeldeki risk algısı ve değerlendirilmesine dair genel ilkeleri içermektedir. Bu sebeple kurumsal risk yönetimi bileşenlerinin en başında gelen iç ortam unsurları başlangıçta diğer unsurlardan önce belirlenmelidir. İç ortamın kapsamına ait bir görsel bir araştırmada aşağıdaki şekilde gösterilmiştir.



Şekil 4.3: İçsel Ortam
Kaynak: KIDDER, 2013b

İç ortam COSO'nun üzerinde önemle durduğu aşağıda belirtilen unsurları kapsamaktadır (Reding, vd., 2009: 4-6,7):

- Risk Yönetim Felsefesi ya da Yaklaşımı
- Risk İştahı
- Risk Toleransı
- Yönetim Kurulunun Tutumu
- Dürüstlük ve Etik Değerler
- Yetenek Yükümlülüğü
- Kurumsal Yapı
- Yetki ve Sorumluluk Belirleme
- İnsan Kaynakları Standartları

4.2.1.1. **Risk Yönetim Felsefesi**

Kurumsal risk yönetiminde risk yönetim felsefesinin en genel tanımı olarak; Kurum genelinde riskin nasıl algılandığı ve buna yönelik stratejilerin belirlenmesinin yanı sıra faaliyetlerde de bu yöndeki inanç ve tutumdur (COSO, 2004b: 5). Bu risk kültürü olarak da adlandırılmaktadır (COSO, 2004b: 6). Bir diğer deyişle risk yönetim felsefesi kurumun değerleri, kültürü ve çalışma şeklini yansıtmaktadır. Bunun yanında risklerin tanımlanması, risklerin kabul edilebilir seviyelerini belirleme ve daha genel bir ifadeyle risk yönetim şeklini ifade eder (COSO, 2004a: 27). Bir kurumda risk yönetim felsefesi, iç ortam ve kurum kültüründen doğrudan etkilenmektedir (COSO, 2004b: 6). Risk yönetim felsefesi belirlenirken kurumun belirlediği stratejik kararların göz önünde bulundurularak bunlara ters düşecek bir risk yönetim felsefesi belirlenmemelidir. Çünkü böyle bir hataya düşmek belirlenen stratejilerden sapmaya ve risk yönetim felsefesinin kurum içinde tutarlı bir yer edinememesine sebep olacaktır.

Risk yönetim felsefesi illaki kağıt üzerinde yazılı olmak zorunda değildir. Ancak kurum genelinde bütün personel tarafından sergilenen ortak bir tutum özelliği vardır. Bununla birlikte risk yönetim felsefesi ile risk iştahı arasında çok sıkı bir bağ bulunmaktadır (Cendrowski ve Mair, 2009: 92). Risk yönetim felsefesinin etkilediği alanlar bir araştırmada şu şekilde belirtilmiştir; kurum kültürünü etkileyen değerleri tanımlayan, kabul edilmiş risk iştahı seviyesinin yanında risklere karşı nasıl tepki verileceği konularını kapsayan risk yönetimindeki tüm unsurları etkileyen bir tutumdur (Arslan, 2008).

Risk yönetim felsefesinin kurumdan kuruma farklılık göstermesine örnek olarak bir kurum faaliyetlerinde herhangi bir riskle karşılaştığında yönetici ve diğer personeller tarafından kuruma katkısı olabilecek bir girişim olarak görülemeyeceği gibi bir diğer kurum benzer bir riski ilgi çekici bulup getiri oranını sorgulama yoluna gidebilir. Her iki durumda da verilen cevaplar yanlış olarak değerlendirilememektedir. Çünkü verilen cevapların çeşitliliği kurumun sahip olduğu felsefeye göre farklılık gösterebilmektedir. Bu noktada önemli olan, kurumların riskli girişimleri nasıl kabul edeceğine yönelik tutarlı bir risk yönetim felsefesine sahip olması ve buna uygun tutumlar geliştirmeye çalışmak olmalıdır (Moeller, 2011: 57).

Risk yönetimi anlayışının kurum kültüründe yer almasının kuruma birtakım faydalı bulunmaktadır bunlar (Griffiths, 2005: 21):

- Yönetim katında gereksiz olaylara zaman harcanması önlenip önemli konulara odaklanması sağlanır
- Karşılaşılabilecek olumsuz durumlar azaltılır
- Doğru işlerin doğru şekilde yapılarak kurumun hedeflerine ulaşabilmesi ihtimali artırılır
- Müşteri odaklı çalışma odak noktasına alınır ve böylece şikâyet oranı azaltılır
- Proje ve girişimlerden fayda elde etme oranı artırılır
- Risk alımında yüksek düzeyde bilinç sağlayarak yeniliklerin desteklenmesi sağlanır
- Sigorta maliyetlerinde düşüş elde edilir
- Kurumun itibarının korunması sağlanır

Sonuç olarak risk yönetim felsefesi iyi geliştirilip kurum personeli tarafından sahiplenilmesi sağlanabilirse kurum genelinde riskin fark edilmesi ve yönetilebilmesi kolaylaşacaktır. Aksi takdirde kurumsal risk yönetim uygulamasında istikrar sağlanamayabilir. Kurum genelinde iyi bir kurumsal risk yönetim sistemi geliştirilse bile birimler bazında oluşabilecek kültürel farklılıklar sistemin işlerliğinde farklı kararlar alınmasını sağlayabilir. Örneğin bazı yöneticiler riskler konusunda tutucu davranabilirken bazıları ise daha fazla risk üstlenmek isteyebilir. Dolayısıyla sistem; yönetim katında yapılan her şeyin içinde olmalı ve buna ek olarak kurum politikalarının beyanı, iletişim yollarında ve karar vermenin bir parçası olmalıdır. Bu felsefenin başarıya ulaşabilmesi için yönetim tarafından sadece sözle değil pratik olarak günlük uygulamalar tarafından desteklenmelidir (COSO, 2004a: 28).

4.2.1.2.**Risk İştahı**

Risk iştahını en genel tanımıyla kurum ve kuruluşların bir değeri elde etmek amacıyla üstlenmeyi kabul ettikleri risk oranı olarak ifade edilebilir. Risk iştahı kurumun risk yönetim felsefesini yansıtan bir ayna gibi olmakla birlikte kültürünü ve işletme tarzını da doğrudan etkilemektedir (PWC, 2006: 20). Bir diğer tanıma göre şirketler açısından paydaşlarına değer kazandırma ölçütlerini belirleme, makul bir büyüme sağlamak, risk ve kar oranı olarak görülmekle birlikte bunun yanında kar amacı gütmeyen kurumlar açısından ise paydaşlarının memnuniyetini artırabilmek ve değer kazandırma amacıyla kabul edebilecekleri risk seviyesi olarak ifade edilmektedir (COSO, 2004a: 40).

Kurum ve kuruluşlar risk yönetim sisteminin kapsamını geliştirmeye yönelik risk iştahı, risk kapasitesine fonksiyonellik ve risk yönetimine olgunluk kazandırmalıdır. Stratejik, taktiksel ve işlevsel düzeyde farklı bakış açılarından kurum kültürüyle bütünleşecek şekilde olmalıdır (IRM, 2011: 7-8). Bir diğer ifadeyle yönetim katmanında risk iştahı düzeyine üç şekilde veya bunların karması olacak şekilde karar verilebilir. İlki, yönetim tarafından her bir riskin ayrı ayrı risk iştah düzeyi belirlenebilir. İkincisi, kurumun stratejik hedeflerinin önemine göre her bir amaç için risk iştahı belirlenebilir. Üçüncüsü, kurum genelini kapsayacak şekilde bir risk iştah düzeyi belirlenebilir. Kurum ve kuruluşlar risk iştahı belirlerken karşılaşacağı riskler için harcayacağı zaman, istihdam edilecek personel ve harcanacak bütçe ihtiyaçlarını da göz önünde bulundurmalıdır (Derici, 2015: 44).

Alınan risklerin bir anlam ifade edebilmesi için, tek ve sabit bir kavram olmayan risk iştahının ölçülebilir olması gerekir (INTOSAI, 2007: 18). Genel risk yönetim stratejisi oluşturmada önemli bir aşama olan risk iştahının tanımlanması kişiden kişiye göre değişebilir bunun nedeni kurum ve kuruluşların riskin önemini nasıl algıladığına göre değişir (INTOSAI, 2004: 25). Nicel veya nitel olarak değerlendirilmekle birlikte genellikle yüksek, orta ve düşük şeklinde nitel olarak ifade edilmektedir (COSO, 2009b: 9). Risk iştahının belirlenmesi kurumun üst yönetiminin görüşü dahilinde risk değerlemesine başlamadan önce yapılması gerekmektedir.

Risk iştahı belirlemenin kuruma sağladığı yararlara örnek vermek gerekirse; (IRM, 2011: 9).

- Kurumun güvende aralığında kalmasını sağlar
- Yönetimin daha iyi kararlar alabilmesine olanak sağlar
- Beklenmeyen sürprizlerle karşılaşma oranını düşürür

- Sorun teşkil edecek olayların ilk aşamada belirlenmesini sağlar
- Yapılandırılmış düşünce modeli geliştirir
- Uzun vadeli hedeflere ulaşmada başarı sağlar
- Risk yönetim sürecine açıklık getirir

4.2.1.3.**Risk Toleransı**

Risk toleransı, kurum ve kuruluşların belirledikleri hedeflerine ulaşabilmesiyle ilgili ölçülebilir kabul edilebilir değişim oranı olarak tanımlanmaktadır (COSO, 2009b: 8). Kurumun temel misyon, değer ve hedefleriyle ilgili riskin önemine göre risk toleransı değişkenlik göstermektedir. Bu sebeple kuruma göre önemli görülen her bir risk için risk toleransı belirlenmelidir. Kurum ve kuruluşlarda risk toleransının uygulanması, kurumun faaliyetlerinde risk iştahı kapsamında hareket etmesine ve dolayısıyla da kurumun hedeflerine başarıyla ulaşabileceğine yönelik yönetime kabul edilebilir bir güvence sağlar (Rittenberg ve Martens, 2012: 11).

Bir diğer ifadeyle risk toleransı kurumun amaçlarının gerçekleştirilmesiyle ilgili olarak makul fark düzeyidir. Bunun yanında risk toleransı, amaçların ilişkili olduğu aynı birimle ölçülebilen performans hedeflerinin yardımıyla ölçülebilir. Sonuç olarak kurum faaliyetlerini risk toleransı çerçevesinde yaptığı takdirde yönetime iki konuda kabul edilebilir bir güvence sağlayabilir; birincisi kurumun risk iştahı içerisinde kalmasını ve ikincisi de kurumun amaçlarını gerçekleştirebilmesidir58.

4.2.1.4.**Yönetim Kurulunun Tutumu**

Yönetim kurulu kurum ve kuruluşlarda risklerin yönlendirilmesi ve denetlenmesi konularında etkilidirler. İç çevrenin önemli bir ögesi olmasının yanı sıra iç ortamın diğer ögelerinde de etki sahibidirler (Moeller, 2011: 57). Bir diğer tanıma göre yönetim kurulları; kurumun tecrübe, bağımsızlık ve kurumsallık kazanabilmesinde önemli bir rolü olan yönetim kademesini temsil etmektedir. Yönetim kurulu iç ortamın önemli bir parçasıdır ve diğer unsurları da doğrudan etkilemektedir (COSO, 2004a: 29).

Etkin bir risk yönetimi sağlanabilmesi yönetim kurulunun etkili olmasına bağlıdır. Etkili bir yönetim kurulunun oluşturulması için üyelerinin deneyimli olmalarının önemi büyüktür. Bir diğer ifadeyle yönetim kurulunun kurumun faaliyetlerinde karşılaşılacak riskleri öngörebilme ve gerekli tedbirleri önceden alabilmek için üstlendiği yönetim ve gözetim sorumluluklarını yerine getirebilmelidir. Bunun için de teknik ve diğer konularda bilgi ve

tecrübe sahibi olmalıdır. Etkin bir kurumsal risk yönetimi ortamının oluşturulmasında bu durum büyük önem arz etmektedir. Yönetim kurulunun başarılı bir yönetim ve gözetim faaliyetinde bulunabilmesinin bir diğer kritik unsuru da yönetimde gerekli kontrol ve denge unsuru olabilmesi için bağımsız üye de bulundurulmalıdır. Yönetim kurulunda bağımsız üyenin oluşu yönetim kuruluna danışmanlık, doğru yön verme, kontrol ve dengeleyici bir unsur olarak katkı sağlayabilir (COSO, 2004a: 29).

4.2.1.5.Dürüstlük ve Etik Değerler

Kurum ve kuruluşların davranış standartları ve stilini yansıtan bu değerler kurumsal risk yönetiminin başarısı için kritik bir unsurdur (COSO, 2004a: 29). İç ortamın bu ögesi kurumda yazılı davranış kurallarının çok daha ötesindedir. Kurumda çalışan tüm personel için bütüncül etik kuralları ve davranış standartları zincirini içermektedir. Buna ek olarak kurumun güçlü bir kültürüne sahip olması kurumun her seviyesinde alınan kararların risk temelli olmasına yardımcı olacaktır (Moeller, 2011: 57).

Kurum kültürünün oluşumunda yönetimin dürüstlük ve etik davranış kuralları çerçevesinde bu olguların kurum faaliyetleri üzerinde ne şekilde uygulandığı veya ne derece esnetildiği önem arz etmektedir. Bunun yanında kurum kültürünün oluşumunda üst yönetimin önemli rolü bulunmaktadır. Ancak genellikle yönetim kurulu başkanının etik tavrı bu kültürün oluşmasında etkili olmaktadır. Ayrıca yönetim katmanının dürüstlüğü ve etik değerlere bağlılığı zamanla kurum içerisinde davranış standartlarına dönüşmesinde etkili olacaktır.

Başarılı yönetilen bir kurumun yöneticileri etik kurallar çerçevesinde yapılan davranışların uzun vadede kuruma faydasının yanı sıra kazanç sağladığı görüşünü kabul etmektedirler (COSO, 2004a: 29). Kurumun etik değerleri başlangıçta iç ortamda kendini göstermekteyken ileri düzeylerde kurumun stratejileri ve belirlenecek hedeflerin geliştirilmesi ve belgelendirilmesinde de önemli ölçüde kendini hissettirecektir (Marchetti, 2012: 33).

4.2.1.6.Yetenek Yükümlülüğü

Yetenek kavramı verilmiş bir görevi yapabilmek için gerekli olan bilgi ve becerileri ifade etmektedir. Yetenek yükümlülüğü genel tanımıyla, herhangi bir göreve atanmak için gerekli olan bilgi ve yetenekle ilgili hususlardır (COSO, 2004a: 31). Yönetim katmanı kurum genelinde verilecek görevlerin başarıyla yerine getirilebilmesi ve buna yönelik stratejilerin oluşturulabilmesi amacıyla kişileri atama yoluyla karar vermektedir (Moeller, 2011: 58).

Kurum genelinde yerine getirilecek faaliyetler için yönetim gerekli olan yetenek seviyesini belirler ve bu faaliyetlerin gerçekleştirilebilmesi için kişilerin seçiminde bir takım unsurlar dikkate alınır bunlar;

- Bireylerin zekâ düzeyleri
- Geçmiş tecrübeleri
- Aldıkları eğitimleri
- Konuyla ilgili bilgi düzeyleri

Yönetim bu hususlar çerçevesinde, yerine getirilmesi istenilen görevin doğası ve görevin gerektirdiği kararların derecesi dikkate alarak ilgili kişilerin atamasını yapar (COSO, 2004a: 31). Kurumlarda ki yetenek standartlarına güçlü bağlılık kurumun her kademesindeki personel için hedeflere ulaşma yolunda gereken adımların atılmasını sağlayabilecektir (Moeller, 2011: 58).

4.2.1.7.**Kurumsal Yapı**

Kurumsal yapı iç ortamın bir diğer ögesidir ve kurum ve kuruluşların genelini kapsayacak şekilde plan, yürütme, kontrol ve izleme faaliyetlerine bir çerçeve olarak ifade edilmektedir. Bunun yanında her kurum ihtiyaçlarına uygun olarak kendine bir kurumsal yapı oluşturmaktadır. Oluşturulan bu yapının uygunluğu kısmen büyüklüğüne ve gerçekleştirilen faaliyetlerin niteliğine bağlıdır (COSO, 2004a: 31).

Çeşitli kurumsal yapı örnekleri bulunmakla birlikte bu yapıların temel amacı kurum içindeki iletişimin kolaylaştırılması yönünde olmalıdır. Bunun yanında kurum genelindeki roller ve sorumlulukları da net bir şekilde ortaya koyabilmelidir. Bu sayede yönetimin kurum içerisindeki farklı birimlerin performans planlamasının yapılması, kontrol edilebilmesi ve başarılarının ölçülebilmesine olanak sağlanabilecektir. Bir diğer ifadeyle kurumsal yapılar, kurumda yetki ve sorumlulukların atanması ve kurum içi rollerin belirlenmesinde önemli bir araçtır (Cendrowski ve Mair, 2009: 92).

Kurum ve kuruluşlar gelişen ve değişen şartlar doğrultusunda büyümeye veya küçülmeye gidebilir bu sebeple bu tarz değişimlere uygun olarak kurumsal yapının da şekillendirilmesi gerekmektedir. Sonuç olarak ne çeşit bir kurumsal yapı tercih edilirse edilsin, kurumsal risk yönetiminin etkin bir şekilde uygulanabilecek ve kurum hedeflerine başarılı bir şekilde ulaşılabilecek şekilde kurumsal yapı organize edilmelidir (COSO, 2004a: 31).

4.2.1.8.**Yetki ve Sorumluluk Belirleme**

Kurum ve kuruluşlarda yetki ve sorumlulukların belirlenmesi genel bir ifadeyle, kurum içerisindeki sorunların çözümü için bireysel olarak veya takım halinde kimlerin yetkilendirilmesi ve desteklenmesi gerektiğinin belirlenmesidir (COSO, 2004a: 32). Buna ek olarak bu ögenin içinde hesap verebilirlik, sorumluluk ve sahiplik kavramları bulunmaktadır. Kurumsal risk yönetimi açısından bakıldığında personellerin kurum içerisindeki rollerinin kurum hedeflerine başarılı bir şekilde ulaşabilmesi için ne şekilde katkıda bulunacağının yönetim katında anlaşılabilmesidir. Bu yönde bütün personelin üstleneceği sorumluluklar ve yetki sınırları net bir şekilde belirlenmelidir (Marchetti, 2012: 33-34).

Yetki ve sorumlulukların belirlenmesinde kurumların daha yatay bir düzeyde faaliyetlerini yerine getirilebilmesi için yetki ve sorumlulukların alt kademeye devri önem arz etmektedir. Müşterilerle doğrudan iletişim kuran ilk kademe çalışanlara üst kademeden yetki ve sorumluluk devriyle personele inisiyatif alma ve onaylama yetkisi verilmesiyle orta düzeydeki yöneticileri kaldırıp kuruma yatay bir işlerlik kazandırılması sağlanmaktadır (Moeller, 2011: 59). Kurum genelinde üst yönetim tarafından alınan kararların yetki ve sorumluluk devri çerçevesinde alt kademelere verilmesi sayesinde inisiyatif alabilen personel sorunlar ortaya çıktığı anda büyümeden önlem alabileceğinden çalışanların uzun vadede kurumdaki etkinlik ve verimliliğinin artması sağlanabilecektir (Aytürk, 2000: 81).

Yetki ve sorumlulukların devrinde personellerin karşılaşılan sorunları çözmeye yönelik alacakları kararlarda ve bu konuda ne kadar yetkili olduklarının bilincinde olmaları gerekmektedir. Bu noktada kurumların karşılaşabileceği en büyük sınırlılık faaliyetin gerektirdiği veya ulaşılmak istenen hedefin gerçekleşmesi amacıyla yapılacak yetki devrinin gereken ölçüsünü doğru belirleyebilmektir. Bir diğer sınırlılık ise, çalışanların tamamı tarafından kurum hedeflerinin net bir şekilde anlaşılması ve bu doğrultuda gerçekleştirilen faaliyetlerde gereken özveriyi göstermeleri olacaktır. Sonuç olarak personeller inisiyatif kullandıklarında bu durumun kurum hedefleriyle çelişip çelişmediği veya katkı sağlayıp sağlayamadığının bilincinde olmaları gerekmektedir çünkü iç ortam personellerin bu bilinç düzeyinden doğrudan etkilenmektedir (COSO, 2004a: 32-33).

4.2.1.9.**İnsan Kaynakları Standartları**

Kurum ve kuruluşlarda personellerin işe alım, uyum sağlama, eğitim, değerlendirme ve terfi gibi süreçleri kapsamaktadır (COSO, 2004a: 33). Buna ek olarak uygulanan insan

kaynakları uygulamaları, kurumun etik davranış ve çalışma yeterlilik düzeylerine ilişkin gerekli bilgilendirmelerin personele yapılmasını sağlamaktır (Moeller, 2011: 59).

Kurum genelinde ihtiyaç duyulan personelin seçilmesinde personelde aranan özelliklerin kurum kültürüne uygunluğunun belirlenmesi, gelişen ve değişen şartlar doğrultusunda personellere gereken eğitim vb. desteklemelerin yapılması gerekmektedir. İhtiyaç duyulan personelin en kalifiyeli, dürüstlük ve etik davranışlara uygun, gerekli tecrübeye sahip, eğitimli ve yetenekli olması gibi konular dikkate alınmalıdır (COSO, 2004a: 33).

4.2.2. **Hedeflerin Belirlenmesi**

Hedef belirleme, kurumsal risk yönetiminde karşılaşılması muhtemel risklerin doğru yönetilebilmesi amacıyla kurum ve kuruluşların yönetimi tarafından misyon ve risk iştahına uyumlu olarak hedeflerini belirleme sürecidir (Mattie ve Cassidy, 2008: 4). Bir diğer deyişle, kurumun stratejik ve operasyonel hedefleri, risk iştahı ve risk toleransının kurum tarafından belirlenmiş misyon ve vizyonla arasındaki ilişkilerdir. Kurumun hedeflerini belirleme sürecinde bu ilişkileri göz önünde bulundurması gerekmektedir (Schanfield ve Miller, 2005: 1).

Kurum ve kuruluşlar tarafından hedefler belirlenirken dikkat edilmesi gereken hususlar bulunmaktadır (Burnaby ve Hass, 2009: 545). Hedeflerde aşağıdaki özelliklerin bulunmasına dikkat edilmelidir;

- Belirgin
- Anlaşılır
- Ölçülebilir
- Ulaşılabilir
- Sonuç odaklı
- Güncel olması

Ayrıca hedef belirleme; olay tanımlama, risk değerleme ve risk tutumunun belirlenmesinden önce yerine getirilmesi gereken bir önkoşuldur (Reding, vd., 2009: 4-7). Diğer bir deyişle hedeflerin belirlenmesi, kurumların karşılaştıkları iç ve dış kaynaklı çeşitli risklerin etkili bir şekilde yönetilebilmesi amacıyla yapılan olay tanımlama, risk değerleme ve risk tutumu aşamalarının doğru işletilebilmesi için gereklidir.

Kurum ve kuruluşların sahip oldukları farklı kültür ve yönetim tarzı hedeflerin belirlenmesinde çeşitlilik olmasına sebep olmakla birlikte bazı hedefler bütün kurumlar için

ortak olma özelliği göstermektedir. Bu ortak hedefler stratejik, faaliyet, raporlama ve uygunluk olarak dört ana kategoride sınıflandırılmıştır (COSO, 2004a: 21). Dört kategoride sınıflandırılmış bu hedefler kurumlarda genel olarak kurumsal risk yönetimi hedefine odaklanılmasını sağlamaktadır (Frigo ve Anderson, 2011: 21).

Özetle kurumsal risk yönetimi kapsamında her kurum öncelikle hedeflerini belirlemelidir. Çünkü potansiyel risk ve fırsatların değerlendirilebilmesi için kurumun misyon ve vizyonuyla çelişmeyen, risk iştahına uygun hedefler belirlendiği takdirde kurumsal risk yönetimi hedeflere ulaşmada yardımcı olan bir süreç olacaktır.

4.2.2.1. **Stratejik Hedefler**

Stratejik hedefler genel olarak, kurum ve kuruluşların misyon ve vizyonu ile uyumlu ve bunları destekleyen üst düzey amaçlardır buna ek olarak kurum yönetiminin paydaşlara değer katabilmek amacıyla yaptığı seçimler olarak ifade edilmektedir (COSO, 2004a: 35).

Misyon, kurumun amacı veya stratejik hedefi olmasından öte daha geniş bir anlamı bulunmaktadır. Bir kurumun varlık nedenini tanımlamakla birlikte belirlenen hedefler doğrultusunda izlenecek yolu belirten bir rehberdir (Bryson, 2018: 6). Bir kurumda misyon ve stratejik hedefler genelde birbiriyle dengeli ve sabittir. Ancak stratejisi ve buna bağlı diğer hedefler gelişen ve değişen iç ve dış koşullara uyum sağlamak adına daha dinamik yapıdadır. Özetle stratejik hedefler, kurum yönetimi tarafından belirlenecek hedeflere ulaşmak amacıyla alınacak kritik kararlardır (Messier, Glover ve Prawitt, 2012: 104).

4.2.2.2. **Faaliyet Hedefleri**

Kurumun faaliyetlerindeki etkinlik ve verimliliği etkileyen, performans, karlılık hedefleri ve kaynakların olası kayıplara karşı korunmasını da içeren hedeflerdir. Yönetimin yapı ve performansla ilgili seçimlerine göre değişiklik gösterebilir (INTOSAI, 2007: 10). Bir diğer ifadeyle kurum kaynaklarını etkin ve verimli bir şekilde kullanılabilmesini sağlayan tüm faaliyetleri içeren hedeflerdir. Bu hedefler belirlenirken kurum ve kuruluşların faaliyette bulundukları pazarın gerekliliklerini yansıtmasına dikkat edilmelidir.

Bu hedef türü tanımlanırken göz önünde bulundurulması gereken kritik nokta, kurumun kaynaklarının yönlendirilmesi bu hedefin odak noktasını oluşturmaktadır bu sebeple kurum hedeflerinin iyi tasarlanamaması veya netleştirilememesi sonucu kaynaklar yanlış yönlendirilip fazla veya eksik kullanım gibi sıkıntılar ortaya çıkabilmektedir (COSO, 2004a: 37). Sonuç olarak hedefler anlamlı ve performansı ölçülebilir bir şekilde tanımlanmalıdır.

4.2.2.3. **Raporlama Hedefleri**

Raporlama hedeflerindeki temel amaç kurumda oluşturulan finansal veya finansal olmayan raporların güvenilir olmasını sağlamaktır. Bu sayede hazırlanan raporlar yönetim katında kurumun hedeflerine ulaşma yolunda doğru kararlar alınabilmesini ve gerçekleşmiş kurum faaliyetlerinin yanında performansının da izlenebilmesi sağlanabilir (COSO, 2004a: 36-37).

Bu raporlara aşağıdaki raporlar örnek olarak verilebilir (Marchetti, 2012: 37);

- Pazarlama faaliyetlerinin sonuçları
- Günlük satış raporları
- Müşteri veya personel memnuniyeti anket sonuçları
- Üretim raporları
- Mali durum raporları
- Yönetimin görüş ve analizleri

4.2.2.4. **Uygunluk Hedefleri**

Uygunluk hedefleri genel bir tanımlamayla; kurum ve kuruluşların faaliyetlerini kanunlara uygun yürütülmesi olarak ifade edilebilir (INTOSAI, 2007: 23). Bir diğer ifadeyle kurumlar faaliyette bulundukları ülke, endüstri veya sektörle ilgili kanun ve yönetmelikler çerçevesinde faaliyetlerini yürütmelidirler (Marchetti, 2012: 37). Kanunlar ve yönetmelikler çerçevesinde faaliyetlerin yapılması, kurumun faaliyetlerini uygunluk hedeflerine dâhil ettiği başlangıç düzeyi olarak belirlenmelidir örneğin; pazar şartları, iş sağlığı ve güvenliği, fiyatlandırma politikaları, personellerin hak ve çalışma şartları, vergilendirme, çevrenin korunması gibi olgular güncel düzenlemelere uygun olmalıdır (COSO, 2004a: 37-38). Bu hedefin belirlenip buna uygun hareket edilmesi kurumun itibarı ve finansal durumu üzerinde önemli bir etkiye sahiptir (Marchetti, 2012:38).

4.2.3. **Olayların Tanımlanması**

Bu kısımda öncelikle olayın tanımını yapmak gerekirse; kurum ve kuruluşlarda stratejilerin uygulanmasını ya da belirlenmiş hedeflere ulaşılmasını etkileyen iç veya dış kaynaklı bir hadisedir (Hopkin, 2012: 63). Bu noktada olay olarak tanımlanan aslında karşılaşılabilecek riskleri belirtmektedir. Olayların tanımlanması ise bir araştırmada şu şekilde ifade edilmiştir; kurumların hedeflerine ulaşma yolunda karşılaşılabilecek iç ve dış kaynaklı olayların tanımlanıp sınıflandırılma sürecidir (Mattie ve Cassidy, 2008: 4).

Olay tanımlama aşamasında olaylar yönetim tarafından kurumun hedeflerine ulaşmasına engel mi olacak yoksa fırsat mı sağlayacağı değerlendirilir. Kurumsal risk yönetiminin bir parçası olarak yönetim kademesinde olaylar tanımlanırken iç ve dış kaynaklı birçok faktör göz önünde bulundurularak risk veya fırsat olarak değerlendirileceğine karar verir (COSO, 2004a: 41). Kurumsal risk yönetimi kurumu olumsuz yönde etkileyebilecek olayların etkisini minimize edebilmek ve olumlu etkisi olabilecek olayların etkisini de maksimize edebilecek şekilde kurumları desteklemektedir (Marchetti, 2012: 38). Kurumsal risk yönetimi çerçevesinde yönetim katmanında içsel ve dışsal faktörleri ve bunlardan kaynaklanabilecek olayların türlerini de anlaşılması gerekmektedir. Olayları tanımlarken kurumun göz önünde bulundurması gereken içsel ve dışsal faktörler tablo 4.1.'de gösterilmiştir (COSO, 2004a: 46-47).

Tablo 4.1: Olayları Etkileyen Dışsal ve İçsel Faktörler

OLAYLARI ETKİLEYEN DIŞSAL VE İÇSEL FAKTÖRLER	
DIŞSAL FAKTÖRLER	**İÇSEL FAKTÖRLER**
EKONOMİK • Sermaye Kullanılabilirliği • Kredi Alma ya da Ödeyememe • Yoğunlaşturma • Likidite • Finansal Piyasalar • İşsizlik • Rekabet • İşletme Birleşimleri/Devralma DOĞAL ÇEVRE • Zehirli Gaz ve Atıklar • Enerji • Doğal Afetler • Sürdürülebilir Kalkınma POLİTİK • Hükümet Değişikliği • Mevzuat • Devlet Politikaları • Yönetmelikler, Yasal Düzenlemeler SOSYAL • Demografik Özellikler • Tüketici Davranışları • Kurumsal Vatandaşlık • Gizlilik Hakkı • Terör TEKNOLOJİK • Kesintiler • Elektronik Ticaret • Dış Veriler • Gelişen Teknolojiler	ALTYAPI • Varlıkların Kullanılabilirliği • Varlıkların Kapasitesi • Sermaye Olanakları • Karmaşıklık ÇALIŞAN (PERSONEL) • Çalışanların Yeteneği • Hileli Faaliyetler • Çalışan Sağlığı ve Güvenliği SÜREÇ • Kapasite • Tasarım • Uygulama • Tedarikçiler/Bağlılıklar TEKNOLOJİ • Veri Bütünlüğü • Veri ve Sistem Kullanılabilirliği • Sistem Seçimi • Geliştirme • Kurulum • Bakım

Kaynak: COSO, 2004a: 46-47

4.2.3.1.Olay Tanımlama Teknikleri

Kurum ve kuruluşların geçmiş olaylardan ders çıkarabilmesi ve gelecekte karşılaşılabilecek olayları doğru değerlendirebilmesi amacıyla olayların tanımlanması önem arz etmektedir. Bu yönde olay tanımlama teknikleri hem geçmişi hem de geleceği dikkate alarak çeşitli teknikler yardımıyla olayların değerlendirilmesine yarar. Olay tanımlama tekniklerinin geçmiş ve gelecekteki olaylara odaklandığı noktalara örneklemek gerekirse. Geçmişte yaşanmış olaylar; kurumlarda yapılmış ödeme hataları, bütçe tahminlerinde yanlışlık, emtia fiyatlarındaki beklenmeyen değişimlerin neden olduğu kayıplar veya kazalar şeklinde örneklenebilir. Gelecekte yaşanabilecek olaylar ise; pazardaki yeni gelişimler, rakiplerdeki gelişim ve değişimler, müşteri veya paydaşların isteklerinde oluşabilecek değişiklikler ve demografik yapıdaki değişimler olarak örneklendirilebilir. Olay tanımlama teknikleri kurum ve kuruluşlarda kullanıldığı yere göre farklılık gösterebilir. Bazıları detaylı veri analizlerine odaklanarak aşağıdan yukarıya doğru bir olay görünümü oluştururken diğerleri de yukarıdan aşağıya doğru bir görünüm oluşturabilir (INTOSAI, 2007: 25; COSO, 2004b: 22-23).

Olay tanımlama teknikleri aşağıdaki şekilde ifade edilmektedir (COSO, 2004a: 44-45).

- Olay Envanteri Oluşturma
- İç Analiz Yapma
- Yükseliş ya da Başlangıç (Threshold) Tetikleyicileri
- Atölye Çalışmaları ve Görüşmeler
- Süreç Akış Analizi
- Önemli Olay Göstergeleri
- Kayıp Olay Veri Yöntemi

4.2.3.1.1. Olay Envanteri Oluşturma

Karşılaşılması muhtemel olayların detaylı bir şekilde listelenmesidir. Bir diğer deyişle kurum ve kuruluşların faaliyette bulundukları sektörde veya sektörler arası ortak olarak kabul edilen potansiyel olaylara ait detaylı listelerdir. Bu listeler genel olarak kullanımda olan yazılımlar vasıtasıyla kolaylıkla oluşturulup olay tanımlamada başlangıç noktası olarak kabul edilmektedir. Bu listelere bir örnek vermek gerekirse yazılım geliştiren bir işletme yazılım geliştirme aşamasında karşılaşılması muhtemel tüm olayların detaylı bir listesini sektörde ortak olarak tanımlanmış olayları baz alarak tanımlayabilir ve kullanabilir.

4.2.3.1.2. İç Analiz Yapma

Kurum ve kuruluşların rutin işlerinin planlanması sürecinde kullanılan bu teknikte kurumun kendi geçmiş deneyimlerinin yanı sıra dışarıdan müşterilerden, paydaşlardan veya konunun uzmanı olan kişilerden bilgi alınır. Yeni bir ürün veya mevcut ürünü yenilikçi bir fikirle geliştirilmesi istendiğinde bu teknik sayesinde pazardaki benzer örnekler kıyaslanarak bu isteğin başarı durumu hakkında yönetime farklı bir bakış açısı kazandırılabilir.

4.2.3.1.3. Yükseliş ya da Başlangıç (Threshold) Tetikleyicileri

Kurumun hâlihazırda yürüttüğü faaliyetlerinde karşılaştığı olayları önceden tanımlı ölçütlerle kıyaslama yapılarak yönetime oluşması muhtemel problemler hakkında bilgilendirme amaçlanmaktadır. Bu sayede gerektiğinde oluşan duruma karşı acil bir tepki belirlenmesi için öngörü sağlanabilir. Örnek olarak kaynakların etkin yönetilebilmesi amacıyla pazardaki satış eğilimine bakılarak reklam veya pazarlama araçları yeniden değerlendirilebilir.

4.2.3.1.4. Atölye Çalışmaları ve Görüşmeler

Bu tekniği kurum içi çalıştay düzenleme olarak değerlendirilebilir. Şöyle ki herhangi bir konuda olay tanımlaması yapılacağında yönetim, personel ve paydaşların tecrübe ve bilgi birikimlerinden faydalanılmasıdır. Örnek olarak satış biriminde uygulanacak yeni satış tekniğinde beyin fırtınası yapılarak yöneticilerin veya personellerin fikirleri alınarak olası olayların tanımlaması yapılabilir.

4.2.3.1.5. Süreç Akış Analizi

Bu teknikte kurum içerisinde yürütülen faaliyetlerin başlangıç ve bitişi arasındaki süreçte görev, sorumluluk ve sonuçların birleşimi olarak değerlendirilmesidir. Örneğin kurumda satın alma sürecinde görevlendirilmiş personelin, alımı kabul eden yöneticinin ve ödemesini yapan muhasebe görevlisinin de dahil olduğu satın alma süreci planlanırken karşılaşılabilecek muhtemel olaylar tanımlanır.

4.2.3.1.6. Önemli Olay Göstergeleri

Kurum ve kuruluşlar herhangi bir olayın oluşmasını tetikleyecek veya bu olayla ilişkili diğer olayları göz önünde bulundurarak bu olayın oluşma sebeplerini veya şartlarını tespit edebilir. Örneğin yazılım geliştiriciler test aşamasının yazılımın canlı ortama çıkmadan önce oluşması muhtemel olayları önceden tespit ettikleri için canlı ortamda karşılaşılabilecek

olayları bu aşamada en aza indirebilmektedirler.

4.2.3.1.7. Kayıp Olay Veri Yöntemi

Kurum ve kuruluşların karşılaşılması muhtemel olaylar hakkında daha önceden var olan kayıp olay veri havuzundan yararlanarak bu olayların oluşmasındaki ana sebepler ve oluşuma giden yolun yönetim tarafından görülebilmesini sağlamaktadır. Bu sayede yönetim herhangi bir olayın temel sebebi ve eğilimleri daha rahat tespit edebilecektir.

Olayların tanımlanmasında kullanılan tekniklerde baz alınan derinlik, genişlik, zaman ve disiplin kurumlar arasında farklılık göstermektedir. Yukarıda açıklanan teknikler yardımıyla olayların bir risk mi yoksa fırsat mı olduğu belirlenebilir. Yönetim katında olay tanımlamada risk yönetim felsefesine uygun bir teknik seçilmelidir ve bu yönde olayları tanımlamak için gereken becerinin yanında bunu destekleyici araçların geliştirilmesi gerekmektedir. Ancak buradaki kritik unsur, yönetimin bu tekniklerden hangisinin ya da hangilerinin birlikte kullanılacağını doğru tespit edebilmesidir (Erdem ve Gündem, 2014: 43). Buna ek olarak olay tanımlama sürecine kurum içerisinde veya dışında farklı bakış açısına ve tecrübeye sahip kişilerin dâhil edilerek hangi risklerle karşılaşılacağına kolaylıkla odaklanılabilir (Arslan, 2008: 33). Olayların tanımlanması risk tanımlama ve risk tutumu belirlenmesine temel oluşturduğu için en doğru şekilde yapılmalıdır.

4.2.4. Risk Değerlendirme

Kurumsal risk yönetim sisteminin temel unsuru olan risk değerlendirme, risklerin gizli bir tehlike veya fırsat içerdiğini tanımlamak için kullanılmaktadır (PWC, 2008: 3). Bir diğer tanıma göre risk değerlendirme, işletmelerde risklerin yönetim tarzını belirleyebilmek ve buna göre risk tutumu geliştirmek için karşılaşılan risklerin olasılıklarını ve sonuçlarını odak noktasına alıp analiz edilmesi şeklinde ifade edilmiştir (Kalyoncu, 2013: 118).

Kurumsal risk yönetimi sisteminde yukarıda belirtilen ilk üç bileşen olan iç ortam, hedeflerin belirlenmesi ve olay tanımlama riskler için genel anlamda bilgi toplama ve bir çerçeve oluşturulması amaçlanmaktadır. Bunun yanında diğer beş bileşen risk değerlendirme, risk tutumu, kontrol faaliyetleri, bilgi ve iletişim ve son olarak izleme ise risklere karşı yürütülecek faaliyetleri kapsamaktadır. Bu aşamada risk değerlendirme sürecinden elde edilecek veriler diğer bileşenlerde risklere karşı yürütülecek faaliyetlere yön verecektir(Pehlivanlı, 2010: 78).

Risk değerlendirme süreci kurum ve kuruluşların belirledikleri hedeflerine ulaşması yolunda ortaya çıkabilecek risklerin tanımlanması, analiz edilmesi ve bu yönde gerekli tutumun belirlenmesidir ve aşağıda belirtilen dört aşamayı kapsamaktadır (INTOSAI, 2004: 22):

- Risk tanımlama: Kurumun hedefleriyle alakalı iç ve dış faktörlere bağlı risklerin detaylı bir şekilde tanımlanmasıdır.
- Risk değerlendirme: Oluşabilecek riskin önem ve etki derecesini tahmin etme ve oluşma olasılığını değerlendirmedir.
- Kurum risk iştahını değerlendirme.
- Risk tutumu belirleme: Karşılaşılan risklere karşı alınacak aksiyonları ifade eder. Bunlar kaçınma, azaltma, paylaşma ve kabul etmedir. Son aşamada da önleyici, düzeltici, yönlendirici ve denetleyici kontrol yöntemleri uygulanır.

Risk değerlendirme sürecinden en iyi şekilde yararlanabilmek için gelişen ve değişen ortama göre hedefler, riskler, risk tutumları ve kontrollerin düzenli olarak yeniden değerlendirilerek güncellenmesi gerekmektedir. Bir diğer ifadeyle risk değerlendirme kurumlarda tek seferlik yapılan bir faaliyet olmamakla birlikte kurum genelinde süreklilik gösteren ve yinelenen bir faaliyettir. Bu yüzden risk değerlendirme kurumsal risk yönetim sisteminin etkin bir şekilde uygulanabilmesinin temel sürecini belirtmektedir (PriceWaterHouseCoopers, 2008: 3,6). Özetle kurum geneline hitap etmeyen ve kurumun yapısal özellikleri göz önünde bulundurulmayan bir risk değerlendirme süreci sonunda ortaya çıkacak değerlendirmelerden kurumun başarı elde etmesi oldukça düşük bir ihtimaldir (Koç, 2012: 130).

Aşağıda belirtilen üç ilke risk değerlendirme sürecinde önemli bir yere sahiptir. Bunlar (Treasury, 2004; The Orange Book, 2004: 19):

- Risk değerlendirme süreci, risklerin önceliklerini tanımlama ve izlenmesini kolaylaştıracak bir şekilde olmalıdır.
- Doğal ve kalıntı risk arasındaki farkın açıkça bilinmesi gerekir.
- Kurumda her bir risk için olasılık ve etkisinin dikkate alınarak değerlendirildiği bir süreç olmalıdır.

Kurum ve kuruluşlar etkin bir kurumsal risk yönetim programı oluşturabilmek ve elde edilebilecek fırsatları daha iyi değerlendirebilmek amacıyla risk değerlendirme sonuçlarını kullanırlar (PriceWaterHouseCoopers, 2008: 3). Risk değerlendirme sürecinin belgelenmesi kurumda risk profili oluşmasını sağlar.

Kurumlarda risk profili oluşmasının birtakım faydaları bulunmaktadır bunlardan bazıları aşağıdaki gibidir (The Orange Book, 2004: 20):

- Öncelikli risklerin belirlenebilmesi,
- Risk değerlendirme sürecini kolaylaştırması,
- Risklere karşı alınmış kararların sebeplerinin açıkça görülebilmesi,
- Risk yönetimine yönelik oluşabilecek kaygıların giderilmesi,
- Risklerin ve risk profilindeki süreçlerin gözden geçirilebilmesi ve izlenebilmesini kolaylaştırır.

Geniş bir spektrumda yapılan risk değerlendirme kurum ve kuruluşların başarısını etkileyen önemli bir faktördür. Ancak bu sürecin istikrarlı bir şekilde ilerlemesini engelleme konusunda çeşitli sorunlar bulunmaktadır. Bu sorunlardan ilki tehdit ve risklerin ölçülmesinin zorluğudur. Mevcut tehditler henüz gerçekleşmemiş birer olasılıktır dolayısıyla zaman içerisinde herhangi bir noktada değerlendirilmesi ve bu yönde raporlamaların yapılmasının beklenen sonuçları tam kapsayamaması gibi sorunlar ortaya çıkabilir. İkinci bir sorun ise, gelişen ve değişen şartlar nedeniyle riskler hızla değişebilir bu durumda muhtemel değişiklikler riskler ölçülmeden önce tanımlanması gerekmektedir. Risklerin ölçülmesi, kurumun mevcut durumunu analiz etmesinden daha zordur bununla birlikte iş süreçlerini detaylı analizlerini kolaylaştırabildiği için kurum yöneticileri ve ilintili paydaşlar tarafından takip edilmektedir (Kinney, 2003: 133). Üçüncü bir sorun da, belirlenmiş beklenen tehditler faaliyetler yapılırken gerçekleşmeyebilir bu sebeple tam olarak değerlendirilemez. Ancak yapılacak kontrol faaliyetleriyle bu sorunların etkileri azaltılabilir veya önlenebilir.

Risk değerlendirme sürecinin etkili ve verimli olabilmesi için öncelikle sürecin nasıl yönetileceği açıkça belirtilmeli ve kurumun hedefleri sürecin her aşamasında dikkate alınmalıdır. Yönetim katında karar alma sürecini desteklemek amacıyla riskler birer portföy olarak ele alınmalı ve önemli görülen göstergeleri muhtemel risklerin aslını anlamaya yönelik kullanılmalıdır (PriceWaterHouseCoopers, 2008: 15-19).

4.2.4.1. **Risk Tanımlama**

Risk değerlendirme sürecinin ilk adımı risk tanımlamadır. Risk tanımlamadaki amaç bir kurumun karşılaştığı belirsizlikleri tanımlamak içindir. Risk tanımlamada başarılı sonuçlar elde edebilmek için kurumla ilgili göz önünde bulundurulması gerekenler şu şekilde

sıralanabilir; Yasal, sosyal, politik ve siyasi yapısı, faaliyet gösterdiği alan ve bu alanın özellikleri, stratejik durumu, faaliyetlerinin çerçevesi, uygunluk ve raporlama hedefleriyle birlikte kurumun hedeflerine ulaşmasını engelleyen veya kolaylaştıran tehdit ve fırsatlardır. Kurum içerisinde yapılan tüm önemli faaliyetler ve bu faaliyetlere yönelik risklerin tespiti risk tanımlama sürecinde metodolojik bir şekilde ele alınmaktadır *(AIRMIC, ALARM, IRM, 2002: 5).*

Risk tanımlama sürecinde kurumun hedeflerine başarıyla ulaşabilmesi amacıyla kritik öneme sahip risklerin tanımlanması başarı olasılığını artırmada önemli bir unsurdur. Risklerin tanımlanırken kuruma ait hedeflerin farklı kategorilerinde etki gösterebilir. Bu nedenle risk tanımlamanın doğru bir şekilde yapılabilmesi kurumun risklere karşı alacağı tutumların en iyi şekilde olabilmesini ve karşılaşılan durumdan fırsatların elde edilebilme olasılığını artırmada büyük önem arz etmektedir (Harris, Kinkela ve Hayes, 2011: 13-14).

Risk değerlendirme sürecinde yönetim katında riskler iki noktada gruplandırılabilir; bunlar içsel (doğal-inherent) ve kalıntı (artık-residual) risklerdir (Moeller, 2011: 71). Bir başka tanıma göre doğal risk "brüt risk", artık risk ise "net risk"tir (Reding, vd., 2009: 4-7). Kurum genelinde öncelikle doğal risk yani riskin saf hali belirlenir (Griffiths, 2005: 66). Doğal risklere karşı yönetim tarafından risk tutumu belirlendikten sonra artık riskler değerlendirilir (Reding, vd., 2009: 4-7). Bu iki risk türünü biraz daha detaylı açıklamasını aşağıdaki şekilde yapabiliriz.

İçsel (doğal-inherent) risk, risklerin olma olasılığına veya etkilerine karşı yönetim katında herhangi bir faaliyette bulunulmaması tercih edilen risklerdir (COSO, 2004a: 49). Bir diğer deyişle içsel riskler, riskleri yönetebilmek adına herhangi bir faaliyet gösterilmediğinde ortaya çıkan risklerdir (The Orange Book, 2004: 49). Satış ve pazarlama biriminde çalışan personelin kullandığı araçların gerekli bakımlarının yapılmaması veya personelin araç kullanmada tecrübeli olup olmadığı göz önünde bulundurulmadığı durumlarda ortaya çıkabilecek risklerdir. Ancak belirtilen bu risklere karşı araçların zamanında bakımları yapılır ve personelin araç kullanma becerilerini geliştirmek için gerekli tedbirler alınırsa ortaya çıkabilecek riskler en az düzeye indirilebilir. Dolayısıyla kurum ve kuruluşlarda öncelikle içsel risklerin belirlenmesi gerekir ve sonrasında bu risklerin kontrolleri sonucunda risklerin etkilerinin kabul edilebilir bir seviyeye gelip gelmediğinin analizi yapılmalıdır (Ernst & Young, 2005).

Kalıntı (artık-residual) risk ise, risklerin olma olasılığını veya etkilerini azaltmaya yönelik

aldığı tedbirlerden sonra artakalan riskleri ifade eder (Maliye Bakanlığı, 2013). Bir diğer deyişle kalıntı risk, riski yönetmek adına gerekli faaliyetlerin yapılmasından sonra kalan risklerdir (The Orange Book, 2004: 49). Risklere karşı yönetim tarafından verilen tepkiler ve alınan önlemler ne olursa olsun kurumlarda her zaman bir miktar artık risk kalacaktır (Moeller, 2011: 71).

Risk tanımlama süreci kayıt altına alınmalı ve tutulan kayıtlarda aşağıdaki bilgilere yer verilmelidir (Vose, 2008: 13-14):

- Riski tanımlayan bir isim verilmelidir.
- Riskten sorumlu ve yönetecek kişilerin isimleri.
- Riskin tanımlaması veya ne olduğu açıklanmalı.
- Riski meydana getiren sebep veya sebepler.
- Riske ait sürekli güncellenen bilgiler.
- Riskin oluşma olasılığını etkileyen faktörler.
- Riskin etkisinin boyutuna yönelik tahminler.
- Riskleri azaltmaya yönelik stratejilerin detayı.
- Risk yönetim stratejisine bağlı olarak, riskin etkisinin ve olasılığının azaltma yöntemlerinin uygulanıp uygulanmadığı veya hangilerinin uygulandığı bilgisi.
- Etkisinin veya olasılığının azaltıldığı risklerin sıralaması.
- Risk azaltma stratejilerinin sonucunda ortaya çıkabilecek artık riskleri belirlenmesi ve tanımlanması.

4.2.4.1.1. Risk Tanımlamada Kullanılan Teknikler

Kurumsal risk yönetim sistemi, kurumlarda önemli risklerin doğru ve bütüncül bir yaklaşımla yukarıdan aşağıya doğru sıralanabilmesini sağlar (COSO, 2009a: 3). Kurum tarafından bu sıralamanın doğru bir şekilde yapılabilmesi amacıyla kuruma uygun bir yaklaşım veya tekniğin belirlenmesi gerekir. Risk tanımlamada kullanılan en genel iki yaklaşım aşağıdaki gibidir (The Orange Book, 2004: 16);

- Risk Değerlendirme Görevlendirmesi
- Risk Öz Değerlendirme

Risk değerlendirme görevlendirmesinde, hedeflerle ilgili faaliyetleri değerlendirmek ve bu faaliyetlerle ilgili riskleri tespit edebilmek amacıyla kurum tarafından bir ekip oluşturulur. Kurum genelinde işleyişin bir parçası olarak her birimde kritik pozisyondaki personeller ile

iletişim içerisinde bütün faaliyetleri kapsayan bir risk profili oluşturulur. Bu noktada yönetimin yetki ve sorumluluklarına karşı bir aksiyon alınmaması önem arz etmektedir.

Risk öz değerlendirmesinde ise, kurum genelinde her seviye ve birimdeki kişilerin katılımı sağlanarak gösterilen faaliyetleri değerlendirme ve karşılaşma ihtimali bulunan riskleri değerlendirme yoluna gidilen bir yaklaşımdır. Bu yaklaşım birinci elden riski üstlenen kişiler tarafından tanımlanması, alınacak kararları sahiplenmede önemli bir avantaj sağlamaktadır.

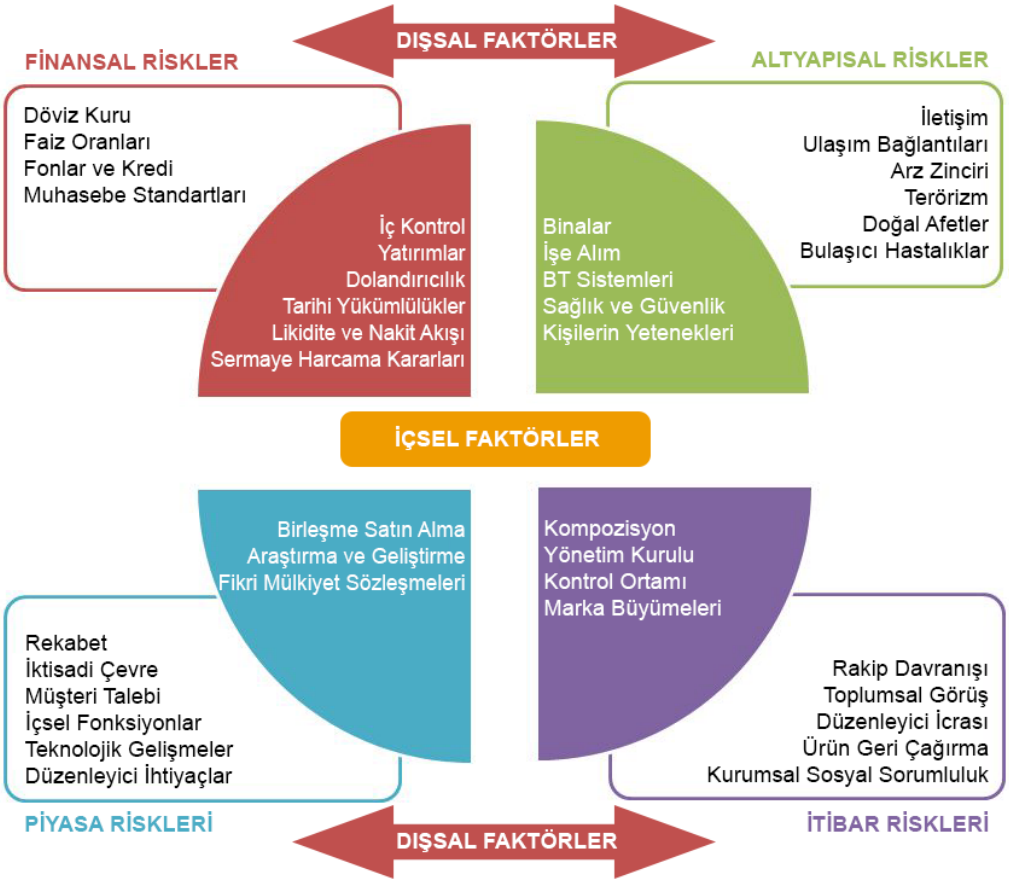
Bu iki yaklaşım dışında başka teknikler de risk tanımlamak için kullanılmaktadır. Bunlar şu şekilde listelenebilir (Shenkir ve Walker, 2007: 4).

- Beyin fırtınası
- Olay sonuç envanteri çıkartma
- Zarar kayıp belirleme
- Görüşmeler ve öz değerlendirme
- Çalıştaylar
- GZFT analizi
- Risk anketleri
- Senaryo analizleri
- Teknoloji kullanımı

Beyin Fırtınası: Katılımcıların bir takım çalışması halinde riskleri tanımlamak amacıyla herkesin fikrini açıkça belirtebileceği bir çalıştay olarak nitelendirilebilir. Bu oturumlarda kurumun olay envanterini çıkartmak, kurumla ilgili bütün riskleri belirlemek ve ortaya konulacak fikirlerle tüm katılımcılara farkındalık kazandırılması amaçlanmaktadır. Beyin fırtınası oturumlarının başarıya ulaşabilmesinde kritik nokta, katılımcılar fikirlerinden dolayı küçük düşürülmeyeceklerinden veya görevlerinde bir alt seviyeye düşürülmeyeceklerinden emin olmalıdır. Aksi takdirde olası riskleri belirtme noktasında çekince gösterebilirler (Shenkir ve Walker, 2007: 4-5).

Olay Sonuç Envanteri Çıkarma: Kurumlar olay veya karşılaşabilecekleri risklerin envanterini oluştururlar. Risklerin tanımlanmasının ardından risklerin sınıflandırılması yönetilmesi için yararlı olacaktır. Envanter oluşturulurken çok sayıda risk belirlenmesi neticesinde bunların yönetilmesinde zorlanılıyorsa bu riskler sınıflandırılabilir (Shenkir ve Walker, 2007: 12). Risklerin sınıflandırılmasında, stratejik, faaliyet, finansal ve dış riskler olarak sınıflandırılabilmektedir (Griffiths, 2005: 22-23). Şekil 4.4.'de riskler içsel ve dışsal

olmak üzere finansal, altyapısal, piyasa ve itibar riskleri olarak sınıflandırılmıştır.

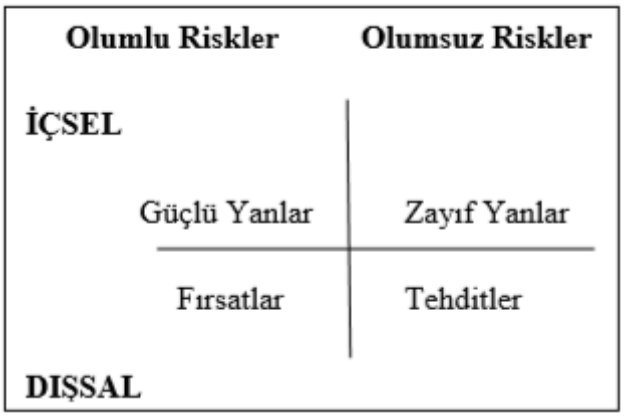


Şekil 4.4: İç ve Dış Kaynaklı Önemli Risk Faktörleri
Kaynak: AIRMIC, ALARM, IRM, 2002:3; AIRMIC, ALARM, IRM, 2010b

Görüşmeler ve Öz Değerlendirme: Bu teknikte asıl amaç, çalışanlar bazında kurumun hedeflerine ulaşmasını engelleyici risklerin belirlenebileceği bir şablon çerçevesinde birimlerin kendi risk yönetim kapasitesini değerlendirmesidir. Çalışanlara verilen şablonda kurumun strateji ve hedeflerine yönelik risklere ilişkin bilgiler yer almaktadır. Birimler kendi risk yönetim kapasitesini belirledikten sonra bu bilgiler risk yönetim personeli veya koordinatörüne verilir. Sonuçlar değerlendirilerek her birimin riskleri belirlenip tanımlanır. Bu yöntem kolaylaştırılmış çalıştaylar ile kombine bir şekilde kullanılabilir (Shenkir ve Walker, 2007: 6-7).

Çalıştaylar: Riskler belirlenip tanımlandıktan sonra kurum içerisinde çalışanlardan oluşan bir yönetim takımı oluşturularak derlenen bilgiler bu ekip tarafından tartışılır. Ekip içerisindeki kişilerin isimleri yazılmadan riskler oylanıp numaralandırılması sayesinde bireylerin düşüncelerini rahatça ifade edilmesi sağlanır. Ekip içerisinde yönetici olarak bulunan çalışanlar bu şekilde yönetime muhalefet olma kaygısı gütmeden görüşlerini rahat bir şekilde ifade edebilir (Shenkir ve Walker, 2007: 7).

GZFT Analizi: Kurumun stratejisini belirlemeye yönelik kullanılan bu teknikte, içsel ve dışsal riskler değerlendirilir. Kurumun güçlü ve zayıf olduğu alanlar içsel, fırsatlar ve tehditler ise dışsal olarak görülmektedir. İçsel risklere örnek olarak, kurumun yapısı, finans ve insan kaynakları verilebilir. Politik, çevresel ve toplumsal faktörler de dışsal risklere örnek olarak verilebilir.



Şekil 4.5: GZFT Analizi
Kaynak: Nazir:4.

Kurumlarda genellikle kurumun güçlü ve fırsatların olduğu alana daha fazla, zayıflık ve tehditlerin bulunduğu alana daha az zaman harcama eğilimi bulunmaktadır. Ancak bu analizin başarılı olabilmesi için kurumun zayıf ve tehdit oluşturan yönlerinin değerlendirilmesi amaçlı gereken zaman ve çabanın harcanması gerekir. Bu analiz çerçevesinde fikir birliğine varılarak bir risk haritası oluşturulmalı ve bu harita dikkate alınarak elde edilmek istenen kazanımlarla birlikte mevcut iş durumu analiz edilmelidir (Shenkir ve Walker, 2007:7-8).

Risk Soru Formu ve Risk Anketleri: İçsel ve dışsal kurumu etkileyen tüm olaylara ilişkin soruların sorulduğu risk soru formları, basit risklere yönelik sorulan sorularla kurumun kendi risk değerlendirmesini yapmaya olanak tanır. Ancak kurumun stratejileriyle doğrudan bağlantılı olmayan bu formlar yerine daha geniş spektrumda risklerin değerlendirilebileceği risk anketinin uygulanması kuruma daha faydalı olabilmektedir. Bu anketler alt seviyedeki yöneticilerden birimlerin hedeflerine, üst düzey yöneticilerden de kurumun hedeflerine ulaşmayı engelleyici risklerin tanımlanması istenir. Elde edilen cevaplara birden ona kadar etki değerleri verilerek öncelik tanımlanır. Anketler ve risk soru formları çalıştaylar da kullanılabilir (Shenkir ve Walker, 2007: 8).

Senaryo Analizleri: Genellikle kurumun stratejik hedeflerine ulaşmasını engelleyici risklerin tanımlanmasına yönelik kullanılan bu yöntemde, gerçekleşme olasılığı düşük ancak

yüksek oranda etkiye sahip olan risklerin tanımlanması için etkili bir yöntemdir. Diğer bir ifadeyle, kurumun itibarı, müşteri kaybı veya taleplere cevap verememe gibi durumlarda oluşabilecek kayıpların uzun vadede sonuçlarının anlaşılmasını sağlamaktadır (Shenkir ve Walker, 2007: 8).

Teknoloji Kullanımı: Kurum ve kuruluşlar risk tanımlamaya yönelik teknolojik imkânlardan faydalanabilmektedir. Buna yönelik kurumsal risk yönetim yazılımı kullanılarak, kurumun maruz kalabileceği risklerin tanımlanması sağlanabilmektedir. Kurumsal risk yönetiminden sorumlu grup, bu yazılımı birimlerin kullanmasını sağlayarak kurum genelinde bütün personele ulaşması sağlanabilir (Shenkir ve Walker, 2007: 9). Teknoloji kullanımı risklerin tanımlanmasında dinamik bir yapı oluşturacağı için kurumların riskleri yönetmede üstünlük sağlayacaktır.

Kurum ve kuruluşların risk tanımlamadan bir sonraki aşamaya geçebilmesi ve orada başarılı olabilmesi için risklerin doğru bir şekilde tanımlanması gerekir. Riskler tanımlanırken yanlış listelenmesi veya tanımlanmayan riskler kalırsa kurumun bu aşamada başarısını olumsuz etkileyecektir. Bu yüzden kurum tarafından risklerin doğru bir şekilde tanımlandığından emin olunmalıdır.

4.2.4.2.**Risk Değerlendirmede Kurumun Risk İştahı**

Kurumsal risk yönetim sistemi çerçevesinde risk değerlendirme ve sonrasında risk tutumunda da büyük öneme sahip olan risk iştahının belirlenmesidir. Her kurum da risk iştahı seviyesi farklıdır. Kimi kurumlarda yüksek risk unsuru olarak görülüp göze alınması düşünülmeyen bir durum kimi kurumlarda da büyük öneme sahip olmayabilir. Kurum yöneticilerinin risk iştahı yüksek olup fazlaca riske katlanabilirler. Ancak bu noktada kurumun risk toleransı daha fazla kritik rol oynamaktadır. Çünkü risk toleransı kurum tarafından belirlenen hedeflerdeki kabul edilebilecek değişkenliği ifade etmekle birlikte kurumun maruz kalacağı risklerin tolere edilebilme seviyesi başarı için kritik bir unsurdur. İstatistikte bu değişkenlik varyans olarak adlandırılmaktadır. Sonuç olarak yönetim tarafından hedeflere ulaşmak amacıyla belirlenmiş risk iştahı sınırında hareket edilmesi kuruma kabul edilebilir bir güvence sağlar (COSO, 2004a).

4.2.4.3.**Olasılık ve Etki Tahmini**

Risk değerlendirme süreci, kurumda yürütülen faaliyetlerde mevcut bulunan potansiyel risklerin kurum hedeflerine ulaşmasını etkileme derecesini belirlemeye yarar. Riskler

değerlendirilirken iki nokta göz önünde bulundurulur bunlar, gerçekleşme ihtimali (olasılık) ve potansiyel etkisi (etki) olarak ifade edilmektedir (Moeller, 2011: 71). Bir diğer ifadeyle risk değerlendirme sürecinde, belirlenen potansiyel risklerin oluşma ihtimalleri ve oluştuğu takdirde muhtemel etkilerinin tahmin edilmesinin yanı sıra bu sonuçlara göre bir sınıflandırma yaparak öncelik verilmesi yer almaktadır (Derici, 2015: 19).

Kurumsal risk yönetiminin esas unsurlarından olan risk değerlendirme sürecinde, karşılaşılması muhtemel risklerden hangilerinin fırsat veya gizli bir tehlike içerdiğini belirlenmesi esastır38. Bu aşamada oluşması muhtemel risklerin, gerçekleşme olasılığı ve kurum üzerinde olası etkisi göz önünde bulundurularak değerlendirilip bir öncelik belirlenir. Riskler değerlendirilmeden önce kuruma uygun bir risk modeli oluşturulmalıdır. Bu risk modelinde, risk değerlendirilmesinde kullanılacak etki kriterleri, riske açıklık kriterleri ve derecelendirme yapmak için bir skala bulunur. Risklerin etkilerini değerlendirirken, finansal etki, itibar etkisi, operasyonlar üzerindeki etki ve yasal etki gibi kriterler kullanılabilmektedir. Matematiksel ifadeler içerdiği için finansal etkinin değerlendirilmesi diğerlerine göre daha objektif olurken, diğer etkilerin değerlendirilmesinde sübjektif değerlendirmeler ağır basabilmektedir. Bu sebeple risk modelinde belirlenen skalanın detaylı bir şekilde açıklanması gerekmektedir. Risklerin oluşma olasılıkları yani riske açıklık değerlendirilirken, mevcut kontrollerin etkinliği, insan kaynağının yeterlilik ve yetkinliği ile süreçte kullanılan otomasyonun başarı derecesi gibi kriterler kullanılabilmektedir39.

Risklerin değerlendirilmesinde, risklerin çeşitleri dolayısıyla hangi risklere ne kadar öncelik verileceği konusunda yönetim tarafından alınacak kararlar zorlayıcı olabilmektedir. Öyle ki oluşma olasılığı düşük ve muhtemel etkisi az olan riskler için ayrılacak kaynak ve harcanacak zamanın yönetim tarafından daha az öncelikli kabul edilmesinin yanı sıra bu durumun tam tersi olan gerçekleşme olasılığı yüksek ve önemli derecede muhtemel etkisi bulunan riskler daha çok dikkatle değerlendirilmektedir. Ancak her iki durumda da ihtimal söz konusu olduğundan önemsiz görülen risklerin gerçekleşip önemli görülen riskler gerçekleşmediğinde ne gibi bir durumla karşılaşılacağı konusu yönetim katında endişe oluşturmaktadır. Bu nedenle risk değerlendirme sürecinde mantıklı ve dikkatli davranılması büyük önem arz etmektedir (COSO, 2004a: 50). Bu konuda yönetime risklerin değerlendirilip analiz edilmesi konusunda kabul görmüş çeşitli teknikler bulunmaktadır.

4.2.4.4.**Risklerin Analiz Edilmesi ve Ölçülmesi**

Risklerin önem derecelerine göre sıralanmasına risklerin analizi denir. Herhangi bir olayın önemi yalnızca gerçekleştiğinde etkisi değil oluşma olasılığını da kapsar. Bir olayın oluşma olasılığı, olayın gerçekleşme ihtimalini, etkisi ise kurumun ne derece etkileneceğini belirtir. Risklerin analiz edilmesi esnasında etki ve olasılıklarının makul ve ölçülü bir şekilde değerlendirilmesi gerekir (COSO, 2004a: 50).

Bugün önemsiz olarak görülen risklerin göz ardı edilmesi zaman içerisinde bu risklerin yönetilmemesi neticesinde kurumu ciddi derecede etkileyen riskler olarak ortaya çıkabilir. Tam tersi önemli olarak görülen riskler de zaman içerisinde değişen koşullar nedeniyle önemini yitirip kurumun fazladan kaynak vb. götürülere sebep olabilir. Bu nedenle riskler arasındaki korelasyonun dikkate alınarak yönetilmesi risklerin verimli bir şekilde yönetilmesini sağlayabilir (Shenkir ve Walker, 2007: 15).

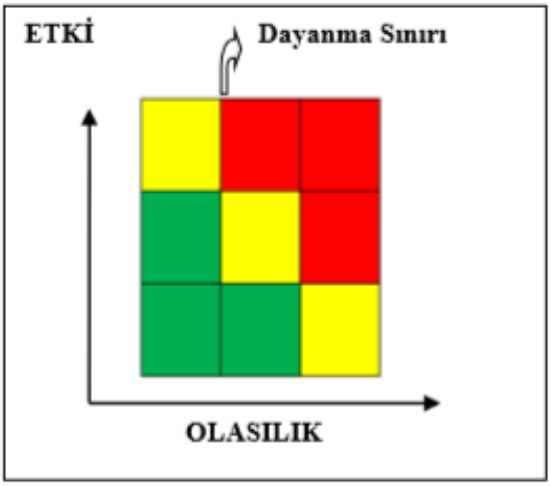
Kurumsal risk yönetimi kapsamında riskler analiz edilirken sektör bazlı veya risk tipine bağlı olarak çok çeşitli teknikler kullanılmaktadır. Örneğin bazı kurumlar risklerin etki ve olasılıklarına yönelik bir risk haritası oluşturmaktadır. Bu haritalandırma basit gibi görünmekle beraber risk tutumunun belirlenmesinde etkin rol oynamaktadır. Bu haritada risklerin olasılıklarını ve etkilerini değerlendirmek üzere çeşitli ölçüm düzeyleri geliştirilmiştir. Olasılıklar için örneğin olarak: düşük, orta, yüksek veya olanaksız, olası, yüksek olasılıklı gibi şiddet ölçüm seviyeleri bulunmaktadır. Benzer şekilde etki değerlendirme için: düşük, orta, yüksek veya az, orta kritik, hayatta kalma şeklinde ifade edilmektedir (Shenkir ve Walker, 2007: 14). Aşağıdaki tablo bu haritalandırmaya örnek olarak verilebilir.

Tablo 4.2: Risk Analizi ve Yönetim Modeli

		Önemsiz	**Zararlı**	**Yıkıcı**
Meydana Gelme Olasılığı	**Muhtemel**	Riskler en iyi şekilde yönetilmeli	Riskler izlenmeli ve yönetilmeli	İleri düzey risk yönetimi uygulanmalı
	Olası	Riskler takip edilmeli ve makul seviyeye indirecek tedbirler alınmalı	Yönetim süreçlerin takipçisi olmalı	Yönetimin çaba göstermesi gerekir
	Olasılık Dışı	Riskler kabul edilir	Riskler kabul edilebilir, ancak takip edilmeli	Riskler yönetilmeli ve izlenmeli
			Kuruma Etkisi	

Kaynak: Burnaby, ve Hass, 2009:545.

Risklerin sınıflandırılırken dikkate alınan bu tabloda etki ve olasılık seviyesi yüksek olanlara öncelik verilir. Bu sonuçlar çerçevesinde kurumlar belirlenen risk iştahına bağlı olarak bu riskleri azaltma veya kabul edilebilir bir seviyeye getirmek üzere risk tutumlarını belirler (Burnaby ve Hass, 2009: 544). Kurumların risk tutumları çeşitlilik gösterebilir, ancak bazı kurumlar genellikle düşük, orta ve yüksek şeklinde niteleyen 3*3 matrisi kullanmaktadır (The Orange Book, 2004: 19).



Şekil 4.6: 3*3 Risk Matrisi
Kaynak: The Orange Book, 2004:s.19

Sonuç olarak risklerin analiz edilmesinde kurumların çeşitli teknikler kullandığı bilinmektedir bu tekniklerin bir kısmı aşağıda detaylı olarak incelenecektir.

4.2.4.5.**Değerlendirme Teknikleri**

Risklerin değerlendirilmesi aşamasında kullanılan teknikler, değerlendirmenin kapsamı ve risk faktörlerine göre farklılık gösterebilir (Kumaş ve Birgören, 2010: 32). Kurumun risk değerlendirme yöntemleri, hem nicel hem nitel hem de ikisinin birleşiminden oluşan karma bir bileşimi içerebilmektedir. Ancak bütün riskler matematiksel olarak ifade edilemediğinden hem nitel hem de nicel değerlendirme yöntemlerini birlikte karma olarak kullanılmasının daha faydalı olacağı ifade edilmektedir (INTOSAI, 2004).

Nitel değerlendirme teknikleri yönetim tarafından genellikle niceliksel değerlendirme amacıyla yeterli ve güvenilir verilerin olmadığı veya bu verilerin elde edilme maliyetinin fazla olduğu durumlarda tercih edilmektedir (COSO, 2004a: 52). Yönetim tarafından daha çok sübjektif kararlar alınmasını sağlayan bu teknikte, eğer kurumun risk iştahı yüksek ise ve bu risklerden çekinmeyip bunları fırsata dönüştürme isteği oluşacaktır (Hillson ve Murray, 2006: 26). Ayrıca kurum tarafından detaylı analiz gerektiren risklerin

tanımlanabilmesi amacıyla yapılan hazırlık çalışmalarında bazı risklerin yapısal özellikleri nedeniyle nitel tekniklerden de yararlanılabilir. Nitel tekniklerde, risk derecelerinin kolayca sıralanabilmesi ve acil aksiyon alınması gereken durumların tanımlanabilmesi birer avantaj olarak görülmektedir (Kumaş ve Birgören, 2010: 32).

Nicel değerlendirme teknikleri sayesinde kurum genelinde elde edilen sayısal veriler kullanılarak belirli matematiksel modellerle risklerin olasılık dağılımları ve etkileri belirlenebilmektedir. Diğer bir ifadeyle nicel değerlendirme, etki ve olasılık tahminlerinin rakamsal değerlerle ifade edilmesidir. (Shenkir ve Walker, 2007: 14). Bu tekniklerin kritik başarı unsuru olarak, verilerin doğruluğu ve kullanılan modelin geçerliliği önem arz etmektedir. Bilgisayar temelli otomasyon sistemleri kullanılarak uygulanan bu tekniklerde kuruma ait geçmiş sayısal veriler kullanılmaktadır. Nicel değerlendirme teknikleri sayesinde daha hassas sonuçlar elde edilmektedir. Çünkü bu tekniklerde genelde matematiksel modeller kullanılmakla birlikte yüksek derecede çaba ve titizlikle sonuçlar elde edilmektedir (COSO, 2004a: 52). Nicel teknikler bilgisayar temelli ve matematiksel modeller sayesinde nitel tekniklere göre daha objektif sonuçlar üretse de kurumsal risk yönetim sisteminin kurulum aşamasında nitel tekniklerden yararlanılması önerilmektedir (Merna ve Al-Thani, 2008: 68).

Çalışmada nitel, nicel ve karma olmak üzere çeşitli sektörlerde ihtiyaca göre kullanılan risk analiz metotlarının bir kısmı incelenecektir. Günümüzde en yaygın kullanılan metotlar şu şekilde listelenebilir (Özçelik, 2013):

- Risk Haritası
- Ön Tehlike Analizi (PHA)
- İş Güvenlik Analizi (JSA)
- Olursa Ne Olur? Analizi (What if?)
- Kontrol Listesi Kullanarak Birincil Risk Analizi (Checklists CLA)
- Birincil Risk Analizi (PRA)
- Risk Analizi Karar Matrisi
    - L Tipi Matris
    - Çok Değişkenli X Tipi Matris
- Tehlike ve İşletilebilme Çalışması (HAZOP)
- Hata Ağacı Analizi (FTA)
- Olası Hata Türleri ve Etki Analizi (FMEA)

- Güvenlik Fonksiyon Analizi (SFA)
- Olay Ağacı Analizi (ETA)
- Neden Sonuç Analizi (CCA)
- Fine-Kinney Risk Analizi

4.2.4.5.1. Risk Haritası

Kurum ve kuruluşlardaki birimlerin tümünde aynı derecede tehlike bulunmadığından tehlikeli görülen birimler, derecelerine göre birbirinden ayrılması bu yöntemde kritik rol oynamaktadır. Bu sayede yüksek riskli alanlar odak noktasına alınabilir ve tedbirlerin isabetli olması sağlanabilir. Tehlikeleri makro ve mikro ayrıştırma yapılarak ön görülen tehlikelerin daha net bir şekilde tespit edilebilmesi sağlanır. Mikro ayrıştırma sayesinde kurum içerisindeki tehlike ve riskler ortaya konulurken, makro ayrıştırmayla dış faktörlerden kaynaklanan tehlike ve riskler ortaya konulabilir (Özkılıç, 2005:70-75).

4.2.4.5.2. Ön Tehlike Analizi (PHA)

Bu yöntem herhangi bir projenin, sistemin başlangıç risk araştırması veya mevcut sistemde yapılacak ayrıntılı bir risk analizinin ilk adımı olarak kullanılabilmektedir. Ayrıca basit bir sistem de risk analizi olarak da kullanılabilmektedir (Rausand, 2005:4). Bu yöntemle hızlı bir şekilde risk değerlendirmesi hazırlanıp ortaya çıkan sonuçlardan hangi tür tehlikelerin ne sıklıkla ortaya çıktığı ve hangi analiz metotlarının uygulanması gerektiği belirlenebilir.

Tablo 4.3: Ön Tehlike Analizi Risk Değerlendirme Seçim Matrisi

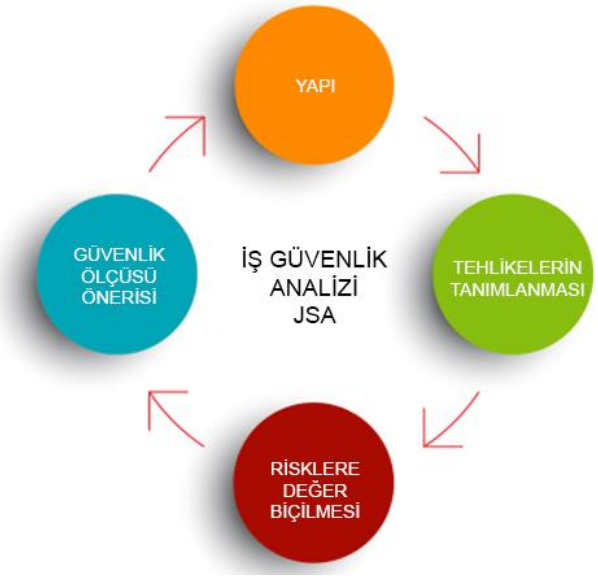
	ŞİDDET			
FREKANS	**(1) Katostrofik (Felakete yol açan)**	**(2) Tehlikeli**	**(3) Marjinal (Pek Az)**	**(4) Önemsiz**
(A) Sık Sık Tekrarlanan	**1A**	**2A**	**3A**	**4A**
(B) Muhtemel	**1B**	**2B**	**3B**	**4B**
(C)Ara Sıra Olan	**1C**	**2C**	**3C**	**4C**
(D) Pek Az	**1D**	**2D**	**3D**	**4D**
(E) İhtimal Dışı (Olanaksız)	**1E**	**2E**	**3E**	**4E**
Risk Kategorisi	**Yüksek**	**Ciddi**	**Orta**	**Düşük**

Kaynak: Özkılıç, 2005: s.104

Ön tehlike analizi sonucuna göre risklere yönelik alınacak tedbirler risk değerlendirme formu yardımıyla yapılabilmektedir.

4.2.4.5.3. İş Güvenlik Analizi (JSA)

Kurum genelinde yapılacak olan iş ve yerine getirilecek görevlerin iyi tanımlanması bu yöntemin kullanımı için kritik unsurdur. Çünkü bu analiz türü grup veya bireysel olarak çalışanların faaliyetleri üzerine yoğunlaşmıştır. Yapılacak olan bu analizde herhangi bir faaliyette yerine getirilecek görevden kaynaklanan tehlikelerin doğası doğrudan incelenmektedir (Safety management services, 2002). Bu yöntemin uygulanmasındaki asıl amaç tehlikelere karşı proaktif bir yaklaşım oluşturabilmektir. İş güvenlik analizi dört aşamadan oluşmaktadır. Bunlar (Özkılıç, 2005: 106);



Şekil 4.7: İş Güvenliği Analizi Aşamaları

- Yapı, herhangi bir faaliyette yer alan çalışanların üstlendikleri görevleri ve bu görevlerin gerçekleştirilmesinde gereken alt görevleri belirleme ve belirlenen bu görevleri engelleyecek durumların tespitinin yapılmasıdır.
- Tehlikelerin tanımlanması, ilk aşamada tanımlanan görevlerin yerine getirilmesini engelleyici tehlikelerin tanımlanmasıdır. Bu tanımlama esnasında aşağıdaki sorular tanımlamayı kolaylaştıracaktır;
    - Hangi türde bir zarar meydana gelebilir?
    - Görevin başarıya ulaşabilmesi için alternatif bir yol var mı?
    - Görev yapılırken özel nedenlerden kaynaklanan problemler oluşabilir mi?
    - Görevin zorluk derecesi nedir?
    - Görevde kullanılan bir makine, materyal vb. tehlikeli mi?

- Risklere Değer Biçilmesi: Tanımlanan tehlikelerin gerçekleşmesine bağlı olarak ortaya çıkacak olan etkisinin şiddeti, etkilenecek çalışan sayısı ve gerçekleşme olasılığına göre risklere bir değer verilmesidir.
- Güvenlik Ölçüsü Önerisi: Bu aşamada asıl amaç, kolayca oluşturulabilecek kontrol ölçümleri yardımıyla riskin azaltılmasına yönelik tavsiyelerde bulunmaktır.

Tehlikelerin gerçekleşme olasılıkları aşağıdaki tablo 4.5. yardımıyla belirlenebilmektedir.

Tablo 4.4: JSA Tehlikenin Gerçekleşme Olasılığı

OLASILIK	**DERECELENDİRME**
SIK SIK	10 saat veya fazla
ARA SIRA	6-9 saat
SEYREK	3-5 saat
ÇOK SEYREK	Olası olmayan

Kaynak: Özkılıç, 2005: s.106

Tehlikelerin gerçekleştikleri takdirde ortaya çıkabilecek etkilerinin değerlendirilmesi için aşağıdaki tablo yardımıyla belirlenebilmektedir.

Tablo 4.5: JSA Tehlikenin Şiddeti

RİSK POTANSİYELİ	**DERECELENDİRME**
HAFİF	Geçici sakatlığa, hastalığa veya yaralanmaya yol açacak durumlar
ORTA	Ciddi yaralanma veya hastalığa, iş günü kaybına, ekipman ve malzeme kaybına neden olan durumlar
CİDDİ	İnsan yaşamını tehlikeye düşürecek, kalıcı sakatlığa yol açacak veya iş gücü, ekipman veya malzeme kaybına neden olan durumlar

Kaynak: Özkılıç, 2005: s.107

Riskler değerlendirilirken ortaya çıkan tablo aşağıdaki gibidir.

Tablo 4.6: JSA Risk Değerlendirme Seçim Matrisi

	OLASILIK			
POTANSİYEL	SIK SIK	ARA SIRA	SEYREK	ÇOK SEYREK
HAFİF	4	3	2	1
ORTA	8	6	4	2
CİDDİ	12	9	6	3

Kaynak: Özkılıç, 2005: s.107

4.2.4.5.4. Olursa Ne Olur? Analizi (What if?)

Kurum genelinde yerine getirilen faaliyetler esnasında karşılaşılabilecek olası tehlikelerin herhangi bir zamanda değerlendirme yapan analistlerin tecrübelerine bağlı olarak önceden öngörülmesi ve gereken tedbirlerin alınması amaçlı yapılmaktadır (Özkılıç, 2005:106). Analistlerin değerlendirmeleri esnasında yalnızca bir noktaya odaklanılması ve tecrübe yetersizliğinden dolayı eksik tehlike tanımı yapılabilmektedir (Kuo, 1998). Analiz değerlendirme yapan analistlerin bilgi ve tecrübelerine dayandığı için resmi olmayan bir metottur. Aşağıdaki tabloda örnek bir analiz görülebilir.

Tablo 4.7: Olursa Ne Olur? Analizi Form Örneği

OLURSA…	NE OLUR?	OLASILIK	SONUÇLAR	GÖRÜŞLER
Testere çatlak	Kırılır	Yüksek	Ciddi	Hemen Değiştirilir
Testere çatlak	Kırılır	Yüksek	Ciddi - Önemli	Çalışmadan önce kontrol edilir
Testere gevşek	Eli kapar	Olası	Önemli	Çalışmadan önce kontrol edilir

Kaynak: Esin, 2006

4.2.4.5.5. Kontrol Listesi Kullanarak Birincil Risk Analizi (Checklists CLA)

Yürütülen faaliyetlerde kurumun potansiyel tehlikeli alanları veya kullanılan ekipmanlarda karşılaşılacak tehlikeleri belirleyip bunlara bir değer vererek gerçekleşecek olayların olasılıklarını ortaya koymak amacıyla uygulanan bu yöntem sayesinde risklerin azaltılmasına yönelik öneriler verilebilmektedir (Özkılıç, 2005). Oluşturulan bu kontrol listeleri, bir faaliyete yeni başlanacağında ve faaliyet sürecinde karşılaşılacak risklere yönelik tespitleri içerdiği için çevresel bir değerlendirme olarak değerlendirilebilir. Tecrübeli analistlerin bu değerlendirmeleri yapmaları başarılı sonuçlar elde edilmesini sağlayacaktır. Bu yöntem sayesinde kuruma sağladığı yararlar aşağıdaki gibi sıralanabilir (Özkılıç, 2005):

- Kurumda kullanılan ekipman ve tesisatlar da herhangi bir sorun olup olmadığını ortaya koyar
- Kontrol edilecek noktaların gözden kaçmaması sağlanır
- Tespit edilen eksiklik veya sorunlar için gerekli önlemler alınması sağlanır.

Bu yöntemde kullanılabilecek bir kontrol listesi örneği aşağıdaki tabloda görülebilir.

Tablo 4.8: CLA Birincil Risk Değerlendirme Kontrol Listesi

PRA KONTROL LİSTESİ			
Proses Sistem:		Tarih	
Alt Sistem:		Rezivyon No:	
Formu Dolduran:		Sayfa No:	
Birimi:			
Görevi:			
Doküman No:			
TEHLİKELER	**EVET**	**HAYIR**	**AÇIKLAMA**
A01.			
A02.			
A03.			
B01.			
B02.			
C01.			
C02			
C03.			
C04.			

Kaynak: Özkılıç, 2005: s.109

Kontrol listesiyle tespit edilen tehlikelerin değerlendirildiği risk değerlendirme formu aşağıdaki tabloda görülebilir.

Tablo 4.9: CLA Kontrol Listesi Kullanılarak Birincil Risk Analizi Temelli Risk Değerlendirme Formu

1	FİRMA:	TARİH:
2	SUNULACAK ÜST BİRİM:	REVİZYON NO:
3	RİSK DEĞERLENDİRMESİNİ YAPAN İSİM/GÖREV:	
4	BİRİMİ:	
5	DEĞERLENDİRMENİN YAPILDIĞI PROSES/SİSTEM:	
6	ALT SİSTEMLER VEYA FONKSİYONLAR:	
7	TEHLİKE KODU (KONTROL LİSTESİNDE TESPİT EDİLEN)	
8	POTANSİYEL KAZA	
9	POTANSİYEL KAZAYI GÖSTEREN OLAY:	
a)	Tehlikeli Parça:	
b)	Tehlikeli Durumu Gösteren Olay:	
c)	Tehlikeli Durum:	
10	CİDDİYET:	
11	SONUÇ:	
12	ÖNLEYİCİ ÖLÇÜMLER:	
13	ÖNLEMLERİN YERİNE GETİRİLME ÖLÇÜMÜ:	
	İMZA	

Kaynak: Özkılıç, 2005: s.110

4.2.4.5.6. Birincil Risk Analizi (PRA)

Bu yöntemde yürütülen faaliyetler esnasında gerçekleşme ihtimali olan olayların analiz edilerek oluşması muhtemel olayların önlenmesi veya sebeplerinin yok edilmesi amaçlanmaktadır. Analiz sonucunda riskler tanımlanıp, azaltmaya yönelik tavsiyelerde bulunulur (Özkılıç, 2005: 111).

Olası tehlikelerin gerçekleşmesine sebep olan faktörlerin belirlenebilmesine yönelik şu şekilde bir soru sorulabilir: "Faaliyet yürütülürken, bu tehlikenin oluşmasına sebep olan en önemli etken nedir? Cevap olarak gözden geçirilmesi gerekenler ise şu şekilde sıralanabilir:

- Makinenin arızalanması
- Sistemde donanımsal bir hata
- Yönetimden kaynaklanan bir hata
- İnsandan kaynaklanan bir hata, vb.

Öngörülen tehlikenin gerçekleşmesi durumunda olası etkilerin azaltılmasına yönelik soru ise şu şekilde olabilir: "Faaliyet yürütülürken hangi alanda düzeltme yapıldığı takdirde olayın etki şiddeti azaltılabilir? Cevap olarak aşağıdaki önlemler göz önünde bulundurulabilir:

- Yönetim tarafından alınan kararlarda düzenlemeler
- Faaliyet planlamalarında iyileştirme
- Makine teçhizat yenileme veya bakım onarımı
- Çalışanlara eğitim ve bilgilendirme yapılması, vb.

Aşağıdaki şekil ve tablo kullanılarak olaylara bir frekans değeri verilir ve olayın gerçekleşmesi sonucunda şiddeti belirlenir. Her bir frekans hesaplanırken, etkisi olan olayların toplam frekansına dayandırılmalıdır. Böylece elde edilen veriler aşağıdaki tabloda verilen risk değerlendirme formuna aktarılır. Ortalama risk indeks numarasını hesaplamaya yönelik aşağıdaki denklem kullanılır:

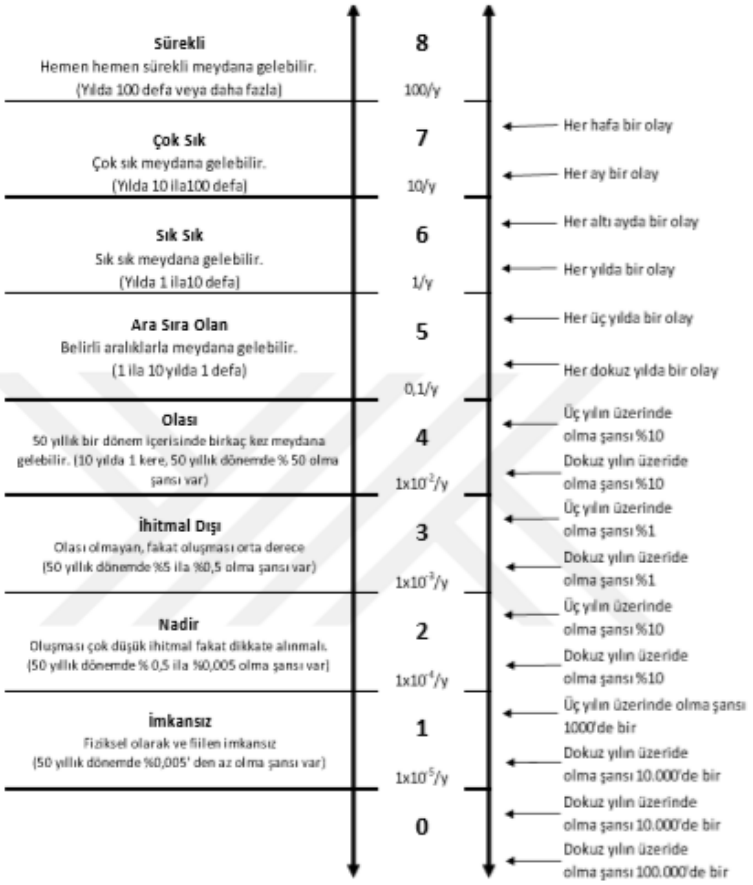
Risk İndeks Numarası = [(FxC)Olay kategorisi;1 + (FxC)Olay kategorisi;2 + (FxC)Olay kategorisi;3 + ...]/10.000

C: Olayın ortalama frekansı; (Yıl başına olay sayısı), F: Olayın ortalama sonucu; (Yıl başına maliyeti). Bu değerlerin hesaplanmasında, geçmiş yıllarda gerçekleşmiş olayların bilgileri kullanılarak tanımlanabilir veya her bir olayın şiddet aralığının orta noktası alınarak da tanımlanabilir (Özkılıç, 2005: 111).

Tablo 4.10: PRA Riskin Şiddetiyle Etkisi Arasındaki İlişki

ŞİDDET	GÜVENLİK ETKİSİ	ÇEVRESEL ETKİ	EKONOMİK ETKİ	KAYIP ETKİSİ
(1) MAJOR	Bir veya daha fazla ölüm veya sürekli sakat kalma	Ekosistemin uzun süreli kesintiye uğramasına neden olan veya uzun süreli kronik sağlık riskli açığa çıkması	>500.000$	>500.000$
(2) ORTA	Hastanede yatmayı gerektirecek yaralanma ve iş günü kaybı	Ekosistemi kısa süreli kesintiye uğratan etki	10.000-500.000$	10.000-500.000$
(3) MİNÖR	İlk yardım gerektiren yaralanmalar	Küçük akut çevresel kirlilik veya halk sağlığına etki	1-10.000$	1-10.000$

Kaynak: Özkılıç, 2005: s.111



Şekil 4.8: Birincil Risk Analizi Frekans Çizelgesi
Kaynak: Özkılıç, 2007: s.324

4.2.4.5.7. Risk Analizi Karar Matrisi

Bu yöntemde, oluşturulan matris diyagramları iki veya daha fazla değişken arasındaki ilişkiyi analiz etmeye yönelik kullanılan bir değerlendirme aracıdır. Çok sıklıkla kullanımı tercih edilen bu yaklaşım ABD askeri standardı olarak "MIL_STD_882-D" olarak bilinmektedir. L tipi matris diyagramı ve çok değişkenli X tipi matris diyagramı olmak üzere iki çeşidi vardır.

L Tipi Matris

Sebep-sonuç ilişkilerinin değerlendirilmesine yönelik kullanılan bu yöntem, basit bir metot olmasından dolayı tek başına analiz yapmak isteyen analistler için daha uygundur. Ancak farklı süreçler içeren veya birbirinden farklı akış şemasına sahip faaliyetlerin hepsi için yeterli değildir ve yöntemin başarısı analistin bilgi ve tecrübesine bağlı olarak değişkenlik gösterebilir (Özkılıç, 2005: 113). Kurumlarda yürütülen faaliyetlerde ivedilikle önlem alınması gereken risklerin tespitine yönelik, bir olayın gerçekleşmesi durumunda etkilerinin derecelendirilip ölçümlenmesi amaçlanmaktadır. Risklerin derecelendirilebilmesi amaçlı aşağıdaki formül kullanılmaktadır:

Risk Skoru = İhtimal x Zarar Derecesi

Tablo 4.11: L Tipi Matris Olasılık Tablosu

OLASILIK	**DERECELENDİRME**
ÇOK KÜÇÜK	Hemen hemen hiç
KÜÇÜK	Çok az (yılda bir kez), sadece normal olmayan durumlarda
ORTA	Az (yılda birkaç kez)
YÜKSEK	Sıklıkla (ayda bir)
ÇOK YÜKSEK	Çok sıklıkla (haftada bir, her gün), normal çalışma şartlarında

Kaynak: ÇAKMAK, 2014

Tablo 4.12: L Tipi Matris Şiddet Tablosu

SONUÇ	**DERECELENDİRME**
ÇOK HAFİF	İş saati kaybı yok, ilkyardım gerektirmeyen
HAFİF	İş günü kaybı yok, kalıcı etkisi olmayan ayakta tedavi, ilkyardım gerektiren
ORTA	Hafif yaralanma, yatarak tedavi gerekir
CİDDİ	Ciddi yaralanma, uzun süreli tedavi, meslek hastalığı
ÇOK CİDDİ	Ölüm, sürekli iş göremezlik

Kaynak: ÇAKMAK, 2014

Tablo 4.13: L Tipi Matris Risk Skor Tablosu

	ŞİDDET				
OLASILIK	1 (Çok Hafif)	2 (Hafif)	3 (Orta)	4 (Ciddi)	5 (Çok Ciddi)
1 (Çok Küçük)	Anlamsız 1	Düşük 2	Düşük 3	Düşük 4	Düşük 5
2 (Küçük)	Düşük 2	Düşük 4	Düşük 6	Orta 8	Orta 10
3 (Orta)	Düşük 3	Düşük 6	Orta 9	Orta 12	Yüksek 15
4 (Yüksek)	Düşük 4	Orta 8	Orta 12	Yüksek 16	Yüksek 20
5 (Çok Yüksek)	Düşük 5	Orta 10	Yüksek 15	Yüksek 20	Tolere Edilemez 25

Kaynak: ÇAKMAK, 2014

Tablo 4.14: L Tipi Matris Risk Sonucu Değerlendirme Tablosu

SONUÇ	**EYLEM**
Katlanılamaz Riskler (25)	Belirlenen risk kabul edilebilir bir seviyede düşürülünceye kadar iş başlatılmamalı eğer devam eden bir faaliyet varsa derhal durdurulmalıdır. Gerçekleştirilen faaliyetlere rağmen riski düşürmek mümkün olmuyorsa, faaliyet engellenmelidir.
Önemli Riskler (15, 16, 20)	Belirlenen risk azaltılıncaya kadar iş başlatılmamalı, eğer devam eden bir faaliyet varsa derhal durdurulmalıdır. Risk işin devam etmesi ile ilgiliyse acil önlem alınmalı ve bu önlemler sonucunda faaliyetin devamına karar verilmelidir.
Orta Düzey Riskler (8, 9, 10, 12)	Belirlenen riskleri düşürmek için faaliyetler başlatılmalıdır. Risk azaltma önlemleri zaman alabilir.
Katlanılabilir Riskler (2, 3, 4, 5, 6)	Belirlenen riskleri ortadan kaldırmak için ilave kontrol proseslerine ihtiyaç olmayabilir. Ancak, mevcut kontroller sürdürülmeli ve bu kontrollerin sürdürüldüğü denetlenmelidir.
Önemsiz Riskler (1)	Belirlenen riskleri ortadan kaldırmak için kontrol prosesleri planlamaya ve gerçekleştirilecek faaliyetlerin kayıtlarını saklamaya gerek olmayabilir.

Kaynak: Özkılıç, 2005: s.114

Tablo 9, Tablo 10 ve Tablo 11'den elde edilen değerler matris metodolojisi temelli risk değerlendirme tablosuna kaydedilir ve Tablo 12' de belirtilen eylemlere göre en büyük değerden başlayarak riskler için gerekli tedbirler alınmalıdır. Gerekli önlemler alındıktan sonra tespit edilen risk için yeni bir risk skoru belirlenmeli ve Tablo 13' deki form yeniden doldurulmalıdır

Çok Değişkenli X Tipi Matris

Bu yöntemde kullanılan matris, kurumun olaylara geniş bir spektrumda bakmasını sağlayarak olayların gerçekleşmeden öngörülmesini sağlamaktadır. Bu metot kullanılan form vasıtasıyla olaya sebep olan faktörler ve bunların aralarındaki ilişkinin tanımlanması yapılıp grafiksel olarak ilişkilerin gösterilmesi sağlanabilmektedir. Karmaşık olan faaliyet veya süreçlerin başarıyla analiz edilebilmesi için, bilgili ve tecrübeli bir ekibin disiplinli bir şekilde çalışması ve en az beş yıllık geçmiş verilere ihtiyaç duyulmaktadır. Geçmişte gerçekleşmiş olayların veya bu olaylardan kaynaklanan diğer olayların yeniden oluşma olasılığı da incelenmelidir (Özkılıç, 2005:115). Değerlendirme sonucunda riskin giderilmesine yönelik alınacak tedbirlerin maliyet analizi yapılmalı, riskin transfer edilme imkanı varsa bunun maliyetiyle karşılaştırma yapılmalıdır.

Tablo 4.15: X Tipi Matris Olasılık Tablosu

OLASILIK	**DERECELENDİRME**
ÇOK KÜÇÜK	Sadece olağanüstü durumlarda gerçekleşir
KÜÇÜK	Çoklu ekipman, valf, insan, botu hattı hatası veya tanklarındaki proses hattındaki veya borulamalarında hata
ORTA	İnsan hatası ile ekipman hatasının kombinasyonu veya proses hattındaki veya borulamalarda hata
YÜKSEK	İkili ekipman hatası, ekipmandan sızıntı veya hortum yırtılması, borulamada kırılma, insan hatası
ÇOK YÜKSEK	Basit ekipman hatası veya valf hatası, hortumdan sızıntı veya günlük aktivitelerde gerçekleşebilecek insan hatası

Kaynak: Özkılıç, 2005: s.114

Tablo 4.16: X Tipi Matris Kontrol Değerlendirme Tablosu

SONUÇ	**KONTROL DERECESİ**
VAR	Kontrol var, sistemin çalışması ekipmanla takip ediliyor
ORTA	Kontrol var, ancak amir gözetimiyle yapılıyor
ZAYIF	Belli aralıklarla çalışanların uyarılması sağlanıyor
YOK	Tamamen çalışanın inisiyatifinde

Kaynak: Özkılıç, 2005: s.116

Tablo 4.17: X Tipi Matris Şiddet Tablosu

SONUÇ	DERECELENDİRME
ÇOK HAFİF	Personel: Hafif sıyrıklar, 3 günden az iş günü kayıplı kazalar
	Toplum: Doğrudan etkisi yok
	Çevre: Tamamen kontrol altında tutulabilecek çevresel etki
	Ekipman: Fabrika hasarı/kayıp değeri 1-1.000$ arası
HAFİF	Personel: ilkyardım gerektiren yaralanmalar
	Toplum: Korku veya gürültü sonucu rahatsızlık doğrudan etki yok
	Çevre: Kontrol altına alınabilecek çevresel etki
	Ekipman: Fabrika hasarı/ kayıp değeri 1.000-10.000 arası
ORTA	Personel: Doktor müdahalesi gerektiren yaralanmalar
	Toplum: Doktor müdahalesi gerektiren yaralanmalar
	Çevre: kontrol altına alınamayan küçük düzeyde çevresel etki
	Ekipman: Fabrika hasarı/ kayıp değeri 10.000-100.000 arası
CİDDİ	Personel: Hayatı tehdit edici yaralanmalar
	Toplum: Hayatı tehdit edici yaralanma, ölüm
	Çevre: kontrol altına alınamayan orta düzeyde çevresel etki
	Ekipman: Fabrika hasarı/ kayıp değeri 100.000$-1.000.000$ arası
ÇOK CİDDİ	Personel: Birçok çalışanın hayatını kaybedecek şekilde yaralanması
	Toplum: Hayatı tehdit edici yaralanma, birden çok ölüm
	Çevre: Kontrol altına alınamayan büyük düzeyde çevresel etki
	Ekipman: Fabrika hasarı/ kayıp değeri 1.000.000$ üzeri

Kaynak: Özkılıç, 2005: s.117

Tablo 4.18: X Tipi Matris Önceki Kazaların Sonucu

SONUÇ	ÖNCEKİ KAZALAR
Ö	Ölümlü kaza
UK	Uzuv kayıplı hayati tehlike yaratabilecek kaza, hayati tehlike yaratacak meslek hastalığı
İGK	İş günü kaybı, uzun süreli tedavi gerektiren iş kazası veya meslek hastalığı
HY	Hafif yaralanma
KRK	Kazaya ramak kalma, tehlikeli durum

Kaynak: Özkılıç, 2005: s.117

Risk skorunun belirlenebilmesi için RDS = A + B + C + D formülünde gereken değerler Tablo 4.19, Tablo 4.20, Tablo 4.21 ve Tablo 4.22. den elde edilerek hesaplanır.



Şekil 4.9: X Tipi Matris Risk Değerlendirme Değişkenler Matrisi
Kaynak: Özkılıç, 2005: s.116

Ortaya çıkan değerler matris diyagramında kendisine karşı gelen sonucun şiddetinin dercesine göre en büyük şiddet değerinden başlayıp gereken önlemler sıralanır. Saptanan veriler ve alınacak önlemler X tipi matris formunda yazılıp uygulanır (Özkılıç, 2005:115).

Tablo 4.19: X Tipi Derecelendirme Matrisi

Ö	5	10	15	20	25	ÖNCEKİ BENZER KAZALAR	5	10	15	20	25
UK	4	8	12	16	20		4	8	12	16	20
İGK	3	6	9	12	15		3	6	9	12	15
HY	2	4	6	8	10		2	4	6	8	10
KRK	1	2	3	4	5		1	2	3	4	5
	OLASILIK						PERSONEL SAYISI				
ÇOK CİDDİ	5	10	15	20	25	ŞİDDET	5	10	15	20	25
CİDDİ	4	8	12	16	20		4	8	12	16	20
ORTA	3	6	9	12	15		3	6	9	12	15
HAFİF	2	4	6	8	10		2	4	6	8	10
ÇOK HAFİF	1	2	3	4	5		1	2	3	4	5
	ÇOK KÜÇÜK	KÜÇÜK	ORTA	YÜKSEK	ÇOK YÜKSEK		1 KİŞİ	1-3 KİŞİ	5 KİŞİ	10 KİŞİ	10'DAN FAZLA
ETKİ YOK		ORTA DERECE ETKİ				YÜKSEK DERECE ETKİ				KABUL EDİLEMEZ BÖLGE	

Kaynak: Özkılıç, 2005: s.119

4.2.4.5.8. Tehlike ve İşletilebilme Çalışması (HAZOP)

Organize ve metodik bir süreç olan HAZOP, bir sistemin operasyonel yönleri ve risklerini tanımlamak amaçlı kullanılmaktadır. Diğer bir ifadeyle bir bütün olarak herhangi bir tesiste teknik özelliklerden veya dolayı yönden meydana gelebilecek potansiyel tehlikelerin değerlendirilmesidir. Aşağıdaki Tablo da verilen anahtar kelimeler kullanılarak yapılan bir beyin fırtınası çalışmasıdır. "Tehlike ve İşletilebilme Çalışmaları" olarak adlandırılan bu metot, kimya endüstrisinde tehlikelerin tanımlanmasına yardımcı olmak amacıyla süreçlerin tasarlanması ve bu süreçlerin işletilmesine yönelik yaygın olarak kullanılmaktadır. Analiz disiplinli bir takım tarafından gerçekleştirilip bir takım lideri tarafından yönetilmelidir.

Tablo 4.20: HAZOP Metodolojisi Uygulamasında Kullanılan Anahtar Kelimeler

ANAHTAR KELİMELER	**ANLAMI**
Fazla (more)	Kantitatif Çoğalma
Az (less)	Kantitatif Azalma
Hiç (none)	Mevcut Değil
Ters (reverse)	Öngörülen Yönün Aksine
Parçası (part of)	Sistemin Bir Bölümü Olması Gerekenden Farklı
… Kadar iyi (as well as)	Aynı Derecede
… dan Başka (other than)	Tamamen Farklı

Kaynak: Özkılıç, 2005: s.119

HAZOP Takımı, öncelikle süreç veya operasyon adımının bir değişkenini seçer, Tablo 4.25'te verilen anahtar kelimeleri kullanarak anlamlı tehlikeli sapmayı belirler. Tanımlanan sapma için neden araştırması ve paralel olarak sonuç araştırması yapılır. Uygulama esnasında dikkat edilmesi gereken noktalar aşağıdaki şekilde listelenebilir (Özkılıç, 2005:124):

- Risk değerlendirmesinde HAZOP takımının belirlediği sürelerde,
- Çalışma koşullarında önemli bir değişiklik olduğunda,
- Ortam ölçümleri ve sağlık gözetimlerinin sonuçlarına göre gerektiğinde,
- Süreç veya operasyonda kimyasal maddeler nedeni ile herhangi bir kaza olduğunda,
- En az beş yılda bir defa,
- Tamir ve bakım işlerine başlamadan önce,
- Süreç veya operasyona bir eklenti veya tehlikeli kimyasal maddeler içeren yeni bir faaliyette yenilenmelidir.

Tablo 4.21: HAZOP Tehlike ve İşletilebilme Çalışma Formu

PROSES / SİSTEM:	REVİZYON TARİHİ:
EYLEM NO:	TOPLANTI GÜNÜ:
İSTEKTE BULUNAN:	DOKÜMAN REFERANS:
BAŞLIK:	
NEDEN:	
SONUÇ:	
KORUNMA AÇIKLAMA:	
ETKİ:	
CEVAP VEREN: YANIT: TARİH: İMZA:	

Kaynak: Özkılıç, 2005: s.116

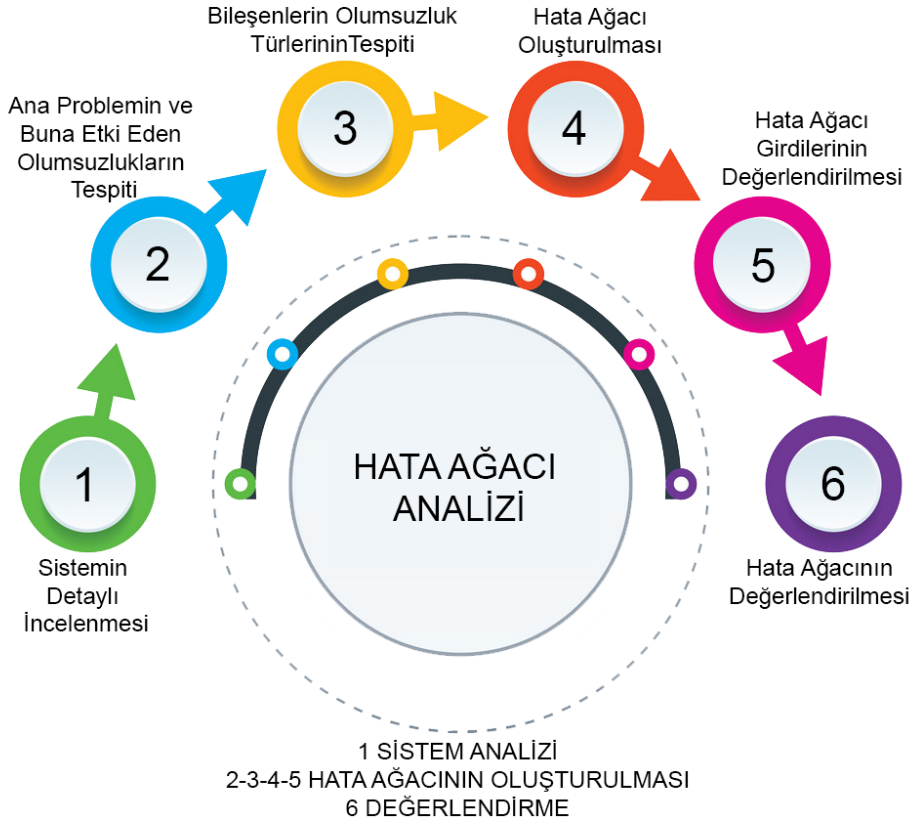
4.2.4.5.9. Hata Ağacı Analizi (FTA)

Bu teknikte temel amaç, gerçekleşmesi istenmeyen "Tepe Olay" olarak adlandırılan bir durumun analizinin yapılmasıdır. Tekniğin uygulanmasında ele alınan tepe olaydan geriye doğru gidilerek, gerçekleşmesi istenmeyen bu sonucu ortaya çıkarabilecek olayları bir sıra içinde ayrıntılı bir şekilde incelemektir. Teknik 1961-1962 yıllarında Bell Telephone Laboratories tarafından yürütülen bir havacılık projesi kapsamında geliştirilmiştir (Fussell vd., 1974: 51-55).

Hata Ağacı Analizinde aşağıdaki adımlar uygulanır (Özkılıç, 2005: 127):

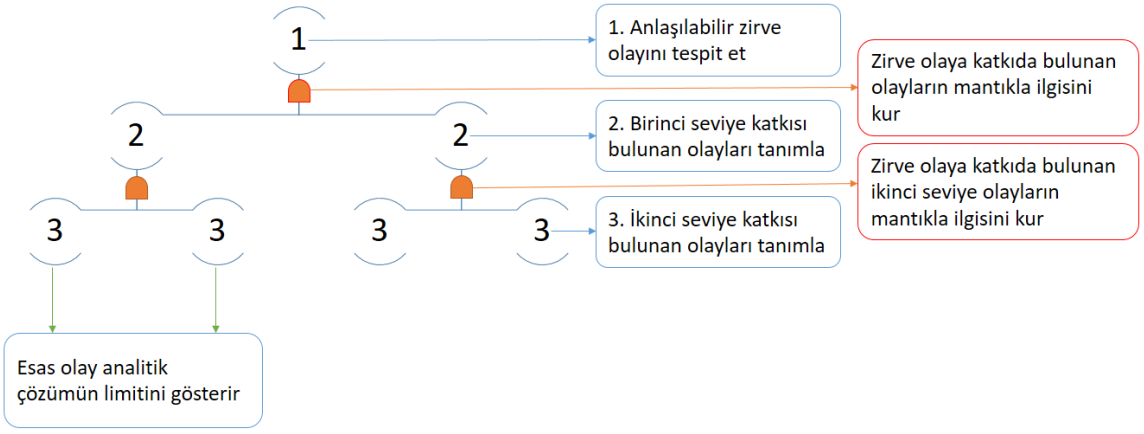
- Sistem analizi.
- Hata ağacının oluşturulması.
- Hata ağacının değerlendirilmesi.

Hata Ağacı Analizi uygulanmasında bulunan temel adımlar ve aşamalar Şekil 4.10.'da sunulmuştur.



Şekil 4.10: Hata Ağacı Analizi'nin 3 Temel Adımı ve Aşamaları
Kaynak: Özkılıç, 2005: 127

Hata ağacı yönteminin, kullanım alanının geniş olması, karmaşık yapılı sistemlerin analiz edilebilmesini sağlaması, teknik veya insan kaynaklı hataların tespit ve analiz edilebilmesini sağlaması ve sunumunun mantıksal bir düzende olması avantaj olarak sayılabilir. Ancak, büyük ve karmaşık sistemler de yapılan analizlerin zaman alması, tüm olayların bağımsız ele alınması gerekmesi ve hata ağacının yanlışsız oluşturulmasında analistler için zorluklar bulunması da dezavantaj olarak göz önünde bulundurulmalıdır (Yılmaz, 2000).



Şekil 4.11: Hata Ağacı Oluşturma Aşamaları
Kaynak: Özkılıç, 2005: 114

4.2.4.5.10. Olası Hata Türleri ve Etki Analizi (FMEA)

Bu analiz yöntemi otomasyon kullanan kimya endüstrisi ve otomobil sanayiinde yaygın olarak kullanılan bir metottur. Kolay kullanımı ve kullanımda teorik bilgiye çok ihtiyaç duyulmadan fazla tecrübeli olmayan orta düzey analistler tarafından kullanılabiliyor olması yayın kullanılmasının temel nedenidir (Özkılıç, 2005). Bu teknikte ana amaç hataların oluşmadan önce tespit edilerek nedenlerin gözden geçirilerek gerekli önlemlerin alınmasını sağlamaktır (Şardan, 2004: 27). Kazandırdığı öngörü sayesinde faaliyetlerin yürütülmesi esnasında yapılması gereken denetim ve oluşabilecek hataların maliyetlerinden kurtulmayı sağlamaktadır.

Bu tekniğin uygulanmasında ilk adımı, Tablo 23'de gösterilen olası hata türleri belirlenir. İkinci adımı, Tablo 24'te gösterilen tehlikelerin gerçekleşmesi durumunda doğuracağı etkinin şiddeti belirlenir. Üçüncü adımı, Tablo 25'te gösterilen saptanabilme durumu ve olasılığının belirlenmesi gerekir. Dördüncü ve son adım olarak, Tablo 26'da gösterilen Risk Öncelik Değerinin hesaplanmasıdır (Yılmaz 2000).

Tablo 4.22: FMEA Hatanın Gerçekleşme Olasılığı

HATA OLASILIĞI	HATANIN İHTİMALİ	DERECE
Çok Yüksek: Kaçınılmaz Hata	1/2'den fazla	10
	1/3	9
Yüksek: Tekrar Tekrar Hata	1/8	8
	1/20	7
Orta: Ara Sıra Olan Hata	1/80	6
	1/400	5
	1/2.000	4
Düşük: Nispeten Az Olan Hata	1/15.000	3
	1/150.000	2
Pez Az Olası: Olmayan Hata	1/1.500.000'den düşük	1

Kaynak: Yılmaz, 2000

Tablo 4.23: FMEA Şiddet Etki Sınıflaması

ETKİ	ŞİDDETİN ETKİSİ	DERECE
Uyarısız Gelen Tehlike	Felakete yol açabilecek etkiye sahip olan hata	10
	Yüksek hasara ve toplu ölüme yol açabilecek etkiye sahip hata	9
Çok Yüksek	Sistemin tamamen hasar görmesini sağlayan yıkıcı etkiye sahip, ağır yaralanmalara, 3. Derece yanık vb. etkiye sahip hata	8
Yüksek	Ekipmanın tamamen hasar görmesine sebep olan ve ölüm, zehirlenme, 3. Derece yanık vb. etkiye sahip hata	7
Orta	Sistemin performansını etkileyen, uzuv ve organ kaybı, ağır yaralanma, kanser vb. etkilere yol açan hata	6
Düşük	Kırık, kalıcı küçük kesik, iş görememezlik, 2. Derece yanık; beyin sarsıntısı vb. etkiye sahip hata	5
Çok Düşük	İncinme, küçük kesik ve sıyrıklar, ezilmeler vb. hafif yaralanmalar ile kısa süreli rahatsızlıklara neden olan hata	4
Küçük	Sistemin çalışmasını yavaşlatan hata	3
Çok Küçük	Sistemin çalışmasında kargaşaya yol açan hata	2
Yok	Etki Yok	1

Kaynak: Yılmaz, 2000

Tablo 4.24: FMEA Saptanabilme Olasılığı ve Derecelendirilmesi

SAPTANABİLME	SAPTANABİLME OLASILIĞI	DERECE
Tespit Edilemez	Potansiyel hatanın nedeni ve takip eden hatanın keşfedilebilmesi mümkün değil	10
Çok Az	Potansiyel hatanın nedeni ve takip eden hatanın keşfedilebilmesi çok uzak	9
Az	Potansiyel hatanın nedeni ve takip eden hatanın keşfedilebilmesi uzak	8
Çok Düşük	Potansiyel hatanın nedeni ve takip eden hatanın keşfedilebilmesi çok düşük	7
Düşük	Potansiyel hatanın nedeni ve takip eden hatanın keşfedilebilmesi düşük	6
Orta	Potansiyel hatanın nedeni ve takip eden hatanın keşfedilebilmesi orta	5
Yüksek Ortalama	Potansiyel hatanın nedeni ve takip eden hatanın keşfedilebilmesi yüksek ortalama	4
Yüksek	Potansiyel hatanın nedeni ve takip eden hatanın keşfedilebilmesi yüksek	3
Çok Yüksek	Potansiyel hatanın nedeni ve takip eden hatanın keşfedilebilmesi çok yüksek	2
Hemen Hemen Kesin	Potansiyel hatanın nedeni ve takip eden hatanın keşfedilebilmesi hemen hemen kesin	1

Kaynak: Yılmaz, 2000

Tablo 4.25: FMEA Risk Öncelik Değerleri ve Karar

SIRA	RİSK ÖNCELİK DEĞERİ (RÖD)	KARAR
1	01 – 50 arası	Düşük Riskli
2	50 – 100 arası	Orta Riskli
3	100 – 200 arası	Yüksek Riskli
4	200 – 1000 arası	Çok Yüksek Riskli

Kaynak: Yılmaz, 2000

Risk öncelik değerinin hesaplanmasında aşağıdaki değerler dikkate alınır:

Olasılık (P): Her hatanın meydana gelme olasılığının değeri (1 – 10 arası).

Şiddet (S): Hatanın oluşması halinde zararlarının düzeyini belirten değer (1 – 10 arası).

Fark edilebilirlik (Saptanabilirlik) (D): Hatanın istenilmeyen sonuçları oluşturmadan önce fark edilebilme seviyesini belirten değer (1 – 10 arası).

RÖD: Risk öncelik değeri (1 – 1000 arası değer alabilir).

Risk Öncelik Değeri (RÖD) = P x S x D

Bu değerler dikkate alınarak analiz gerçekleştirilir. Önem arz eden değerler saptandıktan sonra ortaya çıkmalarını önlemek amacıyla tedbirler alınır. RÖD katsayısının en büyük değeri en büyük zararı ifade ettiğinden önlemlerin alınmasına RÖD katsayısının en büyük değerinden başlanır.

4.2.4.5.11. Güvenlik Fonksiyon Analizi (SFA)

Bu analiz faaliyetlerin yerinde incelenmesi ve kontrol listelerinin oluşturulması şeklinde iki metodun birleşiminden oluşmaktadır. Bu yöntemin Birincil Risk Analizinden temel farkı, tehlikeli alanların tanımlanıp sınıflandırılmış olmasıdır (Özkılıç, 2005: 144). Diğer bir ifadeyle risk haritasının oluşturulmuş olması gerekir. Ayrıca kolay uygulanabilir olmasından dolayı fazla tecrübesi olmayan analistler tarafından da yapılabilir.

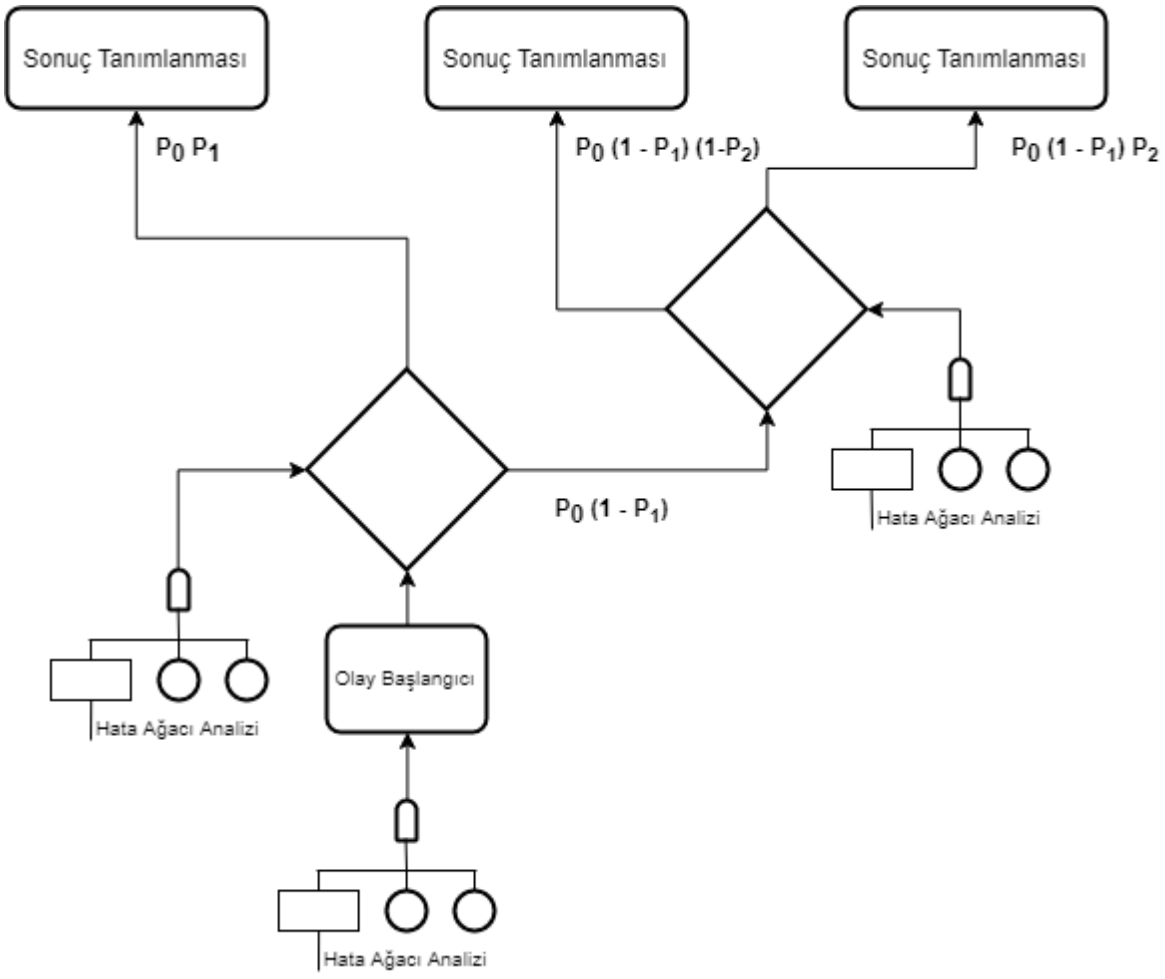
4.2.4.5.12. Olay Ağacı Analizi (ETA)

Herhangi bir tehlikenin gerçekleşmesi durumunda ortaya çıkarabilecek olayların analiz edildiği bir yöntemdir. Bu yöntem tümevarım mantığını kullandığı için, hata ağacı analizi metodunun tam tersi bir yapıya sahiptir. Tehlikenin gerçekleşmeden önce ve gerçekleştikten sonra ortaya çıkabilecek durumları ortaya koyduğu için sonuç odaklı analizlerin başında

gelmektedir. Bu analizde tehlikenin gerçekleşme sıklığı ve ihtimali sayısal olarak belirlenebilmektedir (Özkılıç, 2005). İlk olarak nükleer sanayiinde enerji santrallerinin işletilmesine yönelik analizlerde uygulanmış ve başarılı sonuçlar elde edilmesiyle diğer sektörlerde de yaygınlaşmıştır. Hem nicel hem de nitel olarak uygulanabilmesi diğer analiz yöntemlerinden ayrışmasını sağlamaktadır.

4.2.4.5.13. Neden Sonuç Analizi (CCA)

Hata ağacı analizi ve olay ağacı analizlerinin birleşimi olan bu analiz yönteminde hem tümdengelim hem de tümevarım tekniği kullanılmaktadır. Bu yöntemdeki ana amaç, olaylar arasındaki zincir tanımlanırken istenmeyen sonuçların sebeplerinin belirlenmesidir. Şekil 11'de gösterildiği üzere, neden - sonuç diyagramında olayların gerçekleşme olasılığıyla, ortaya çıkan sonuçların olasılıklarının hesaplanması yapılabilir. Böylece sistemde var olan risklerin dereceleri saptanmış olur (Özkılıç, 2005).



Şekil 4.12: Genel Bir Neden-Sonuç Temelli Risk Metodu Akış Diyagramı
Kaynak: Özkılıç, 2005: s.114

Metodun avantajları (Özkılıç, 2005);

- " En kötü durum" kalıbıyla sınırlandırılmamıştır.
- En son gerçekleşecek olayı tahmin etmeye gereksinim duyulmaz
- Birçok hatayı veya yanlışı barındıran sistemleri değerlendirmede elverişlidir.
- Olayların gerçekleşme sırası dikkatli bir şekilde incelenir.
- Oluşacak kayıpların düzeyleri belirlenebilir ve bundan dolayı elde edilen başarıların veya kayba göre hataların düzeyleri saptanabilir.

4.2.4.5.14. Fine-Kinney Risk Analizi

Bu risk analiz yönteminde, tehlikelerin gerçekleşmesini engelleme ve oluşma ihtimalini kontrol edebilmek adına matematiksel olarak riskin değerlendirilmesi söz konusudur. Sonuçta risk, tehlikeli olayların olasılıklarına, etkisine ve gerçekleşme sıklığına bağlı olarak değişkenlik göstermektedir. Bu yöntem G. F. Kinney ve A. D. Wiruth tarafından 1976 yılında ortaya çıkarılmıştır.

Bu metotta risk değeri hesaplanırken şu formül kullanılmaktadır (Özkılıç, 2005):

Risk Değeri = İ x F x D

Şans(İ): Olayın gerçekleşme olasılığı (Tablo 10).

Frekans(F): Zaman içerisinde olayın gerçekleşme sıklığı (Tablo 11).

Şiddet(D): Gerçekleşmesi halinde etkisi (Tablo 12).

Formülün sonucuna göre elde edilen değer, Tablo 13'te belirtilen şekilde tedbir alınmalıdır (Özkılıç, 2005).

Tablo 4.26: Fine-Kinney Zararın Gerçekleşme Olasılığı

DEĞER	KATEGORİ
0.2	Pratik Olarak Gerçekleşmesi Beklenmez
0.5	Zayıf İhtimal
1	Düşük İhtimal
3	Nadir Fakat Olasılığı Var
6	Yüksek İhtimal
10	Çok Kuvvetli İhtimal / Kesin

Kaynak: Özkılıç, 2005

Tablo 4.27: Fine-Kinney Tehlikenin Gerçekleşme Frekansı

DEĞER	AÇIKLAMA	KATEGORİ
0.5	Çok Nadir	Yılda bir ya da daha az
1	Oldukça Nadir.	Yılda bir ya da birkaç kez
2	Nadir	Ayda bir ya da birkaç kez
3	Ara Sıra	Haftada bir ya da birkaç kez
6	Sıklıkla	Günde bir ya da birkaç kez
10	Sürekli	Sürekli ya da saatte birden fazla

Kaynak: Özkılıç, 2005

Tablo 4.28: Etki/Zarar-Sonuç Tablosu

DEĞER	AÇIKLAMA	KATEGORİ
1	Dikkate Alınmalı	Hafif – zararsız veya önemsiz
3	Önemli	Minör – düşük iş kaybı, küçük hasar, ilkyardım
7	Ciddi	Majör – önemli zarar, dış tedavi, işgünü kaybı
15	Çok Ciddi	Sakatlık, uzuv kaybı, çevresel etki
40	Çok Kötü	Ölüm, tam maluliyet, ağır çevresel etki
100	Felaket	Birden çok ölüm, önemli çevre felaketi

Kaynak: Özkılıç, 2005

Tablo 4.29: Fine-Kinney Risk Düzeyine Göre Karar ve Eylem

SIRA	RİSK DEĞERİ	KARAR	EYLEM
1	R<20	Kabul Edilebilir Risk	Acil tedbir gerekmeyebilir
2	20<R<70	Kesin Risk	Eylem planına alınmalı
3	70<R<200	Önemli Risk	Dikkatle izlenmeli ve yıllık eylem planına alınarak giderilmeli
4	200<R<400	Yüksek Risk	Kısa vadeli eylem planına alınarak giderilmeli (Birkaç ay)
5	R>400	Çok Yüksek Risk	Çalışmaya ara verilerek derhal önlem alınmalı

Kaynak: Özkılıç, 2005

Şengöz ve Merdan (2017) ve Özkan ve Uluata (2017) yaptıkları karşılaştırmalı araştırmalarda, risk değerlendirmede yöntem seçiminin riskin doğru belirlenmesinde etkili olduğu belirtilmektedir. Tehlike ve risklere bağlı olarak her testin duyarlılığı ve verdiği sonuçlar değişkenlik gösterebilmektedir. Fine-Kinney risk analiz yönteminin diğer yöntemlere göre daha hassas sonuçlar ortaya koyduğu düşünülmektedir.

4.2.5. **Risk Tutumu**

Riske tutumu veya diğer bir deyişle risk yanıtlama aşamasında riskler belirlenip değerlendirildikten sonra yönetim tarafından bu risklere nasıl cevap verileceği ya da risklerin nasıl yönetileceğinin belirlenmesi sürecidir (Hopkin, 2012: 63). Diğer bir ifadeyle, risk değerlendirme sürecinin devamında risk yönetimi kapsamında risk tepkileri veya riske verilecek cevaplardan oluşan faaliyetler olarak ifade edilmektedir (Ekici, 2015: 107). Risk tutumu belirlenirken yönetim, nicel, nitel veya her ikisinin birleşimiyle hazırlanan risk analizlerinin ışığında risklerin etki ve olasılık ile maliyet fayda değerlendirmesini yapar. Değerlendirme sonucunda ise mümkünse seçeneklerin geliştirilmesini ve tehdit unsurlarının azaltılmasını hedefler (Olson ve Wu, 2010: 47). Ayrıca yönetim tarafından yapılan değerlendirmeler sonucunda elde edilen verilerin kurumun risk iştahı sınırlarını aşan risklere karşı acil önlem alınması gerekenleri tespit eder ve buna göre risklere karşı tutum belirlenir (Pehlivanlı, 2010: 84). Kurumun risk iştahı belirlenecek risk tutumları üzerinde doğrudan bir etkisi bulunmaktadır. Dolayısıyla risklere karşı, riskten etkilenen değeri kazanca dönüştürmek üzere bir yöntem tercih edilmelidir (Griffiths, 2006: 10).

Kurumlar tarafından bazı risklere karşı verilecek yanıtlar belirlidir, ancak bazıları araştırılmalı ve analizler yapılmalıdır. Yönetim tarafından risk tutumu belirlenirken aşağıdaki noktalara dikkat edilmelidir (COSO, 2004a: 56):

- Risk tutumunun kurum tarafından belirlenen risk toleransına uyumluluğuna,
- Risk tutumunun, risklerin etki ve olasılıklarına ne derece etki ettiğine,
- Risk tutumunun fayda-maliyet analizine,
- Risk tutumlarında yalnızca riskleri azaltmaya odaklanmak yerine elde edilebilecek fırsatların da varlığını dikkate almak gerekmektedir.

Risklere karşı kurumun tercih edebileceği dört ana risk tutumu bulunmaktadır bunlar şu şekilde ifade edilmektedir: Azaltma, paylaşma, kabullenme ve kaçınma şeklindedir.

4.2.5.1. **Riski Azaltma**

Riskin gerçekleşme olasılığı, olumsuz etkileri veya her ikisini de azaltmaya yönelik gerçekleştirilen faaliyetlerdir (INTOSAI, 2007: 30). Tedavi etme süreci olarak da adlandırılan bu yöntemde riskler, kurumun belirlediği risk iştahının altına itilmesine yönelik uygulanan bir iç kontrol sistemi olarak da ifade edilmektedir (Griffiths, 2006: 10). Bu yöntem genellikle risk olasılığının yüksek ve etkisinin düşük olduğu durumlarda kullanılır (Vose, 2008: 18). Sonuç olarak riskleri kontrol etmeye yönelik yapılan faaliyetlerdir.

4.2.5.2. **Riski Paylaşma**

Riskin etki veya olasılığının transfer edilmesi veya bir kısmının paylaşılarak riskin azaltılması sürecidir. Diğer bir deyişle, riski bir varlıktan diğerine transfer etmek olarak ifade edilmektedir (Marchetti, 2012: 29). Riski paylaşma, riskin oluşma olasılığının düşük ancak etkisinin yüksek olduğu durumlarda tercih edilmektedir (Vose, 2008: 18). Kurum ve kuruluşlar risklerden korunmak ve etkilerini paylaşmak amaçlı sigortalama yoluna gitmektedir. Bu tutumda sigorta yaptırmanın yanında bazı farklı teknikler de bulunmaktadır (Moeller, 2011: 75). Riskin oluşma olasılığını paylaşmaya yönelik bu teknikler içinde ortaklıklar kurma veya çeşitli anlaşmalar yapılması örnek olarak gösterilebilir. Bu tutumda dikkat edilmesi gereken kritik unsur, riskin paylaşılmasında sigortalama yaptırırken bir maliyet ortaya çıkmasıdır. Yönetim fayda-maliyet analizini dikkatli bir şekilde yaparak yeni bir risk ortaya çıkmamasına dikkat etmelidir.

4.2.5.3. **Riski Kabul Etme**

Riskin mevcut seviyesinde kabul edilmesidir. Diğer bir ifadeyle, riskin oluşma olasılığıyla etkilerini önlemek için herhangi bir faaliyette bulunulmamasıdır (COSO, 2004a: 55). Kurum ve kuruluşlar faaliyetlerinde bazı kaçınılmaz riskleri kabul etmek durumunda kalabilir. Bu durumda yönetim tarafından, riski azaltmaya yönelik ortaya çıkan maliyet ile kabul edildiğinde ortaya çıkan maliyet arasında fayda maliyet analizi yapılarak riskler kabul edilme yoluna gidilebilir (Marchetti, 2012: 29). Bu tutum riskin oluşmasının ve etkisinin düşük olduğu durumlarda tercih edilmektedir. Bu tutumun tercih edilmesi durumunda her ihtimale karşı riske yönelik acil durum planı yapılarak değerlendirmeye tabi tutulmalıdır (Vose, 2008: 7, 18).

4.2.5.4.**Riskten Kaçınma**

Bazı riskleri azaltmak veya paylaşmak mümkün olmayabilir bu gibi durumlarda riski oluşturan veya risk artışına neden olan faaliyetlerden vazgeçilmesidir (Emhan, 2009: 217). Diğer bir ifadeyle, riske neden olan iş birimini satmak, endişe veren bir coğrafi bölgeden çıkmak veya bir ürün grubunu bırakmak şeklinde yapılan faaliyetlerle riskten uzaklaşılması sürecidir (Reding, vd., 2009: 4-7). Riskten kaçınma, riskin oluşma ve etkisinin de olasılığı yüksek olduğu durumda tercih edilir (Vose, 2008: 18). Sonuç olarak yönetim tarafından riskin olasılığı ve etkisi kabul edilebilir bir seviyeye indirgenemediği durumda risk tutumu olarak riskten kaçınma tercih edilmelidir (Marchetti, 2012: 42).



Şekil 4.13: Risk Tutum Matrisi
Kaynak: Florea ve Florea, 2009:42

4.2.6. **Kontrol Faaliyetleri**

Kontrol faaliyetleri, uygun risk tutumlarının gerçekleştirilmesini sağlamaya yardımcı olan politika ve prosedürlerdir. Kurumda risk tutumu belirlendikten sonra yönetim tarafından bu risk tutumlarını zamanında ve etkili bir şekilde gerçekleştirilebilmesi için gerekli kontrol faaliyetleri yürütülmelidir (Moeller, 2011: 78). Bu kontrol faaliyetlerinin risk tutumları ile bütünleşmiş olmasına dikkat edilmelidir (Mattie ve Cassidy, 2008: 5). Ayrıca kontrol faaliyetleri, kurum genelinde birimlerin tüm sevilerinde yer alacak şekilde yürütülmelidir (Cendrowski ve Mair, 2009: 95).

Kontrol faaliyetleri genellikle risklerin azaltılmasına odaklanırken, belirli kontrol faaliyetleri de diğer risk tutum yöntemleri uygulanırken gerekli olabilmektedir (Reding, vd., 2009: 49). Kontrol faaliyetleri oluşturulurken öncelikle alınacak aksiyon net bir şekilde tanımlanmalı ve sorumlusu atanarak bir tamamlanma tarihi belirlenmelidir. Kontrol faaliyetleri risk tutumlarının etkinliğini ölçmek için kullanılsa da bazen kontrol faaliyetlerinin kendisi birer risk tutumu görevi üstlenmektedir. Bu nedenle kontrol faaliyetleri kurum genelinde hedeflere ulaşabilme yolunda kritik bir görev üstlenmektedir (COSO, 2004a: 61-62).

Kurumsal risk yönetimi çerçevesinde kontrol faaliyetleri dört ana yöntemle uygulanmaktadır bunlar (The Orange Book, 2004: 28):

- Önleyici
- Yönlendirici
- Düzeltici
- Denetleyici

4.2.6.1. **Önleyici kontrol**

Gerçekleşmeye yaklaşmış bir riskin olasılığını sınırlandırmak ve istenmeyen muhtemel sonuçlarını azaltmaya yönelik faaliyetlerdir.

4.2.6.2. **Yönlendirici kontrol**

İstenmeyen olaylarla karşılaşılmasını önlemeye yönelik belirli bir sonuç elde edebilmek amacıyla yürütülen faaliyetlerdir.

4.2.6.3. **Düzeltici kontrol**

Gerçekleşmiş istenmeyen sonuçları düzeltmeye yönelik kayıp ve zarara karşı geri kazanım amacıyla yürütülen faaliyetlerdir.

4.2.6.4. **Denetleyici kontrol**

İstenmeyen olayın gerçekleşmesinin ardından sonuçlarının ortaya çıkma olasılığını azaltmaya yönelik faaliyetlerdir.

Yukarıdaki dört ana kontrol faaliyetlerinin yanında yayın olarak kullanılan kontrol faaliyetleri şu şekilde listelenebilir (Reding, vd., 2009: 4-9):

- Bilgi işlem süreci
- Üst düzey incelemeler

- Doğrudan yönetim veya faaliyet yönetimi
- Fiziksel kontrol
- Performans ölçümü
- Görevler ayrılığı

Kurumların yapılarına bağlı olarak kontrol faaliyetleri çeşitlilik gösterebilir. Genelde kurumlar tarafından birkaç kontrol faaliyetinin birleşimi kullanılması tercih edilmektedir (COSO, 2004a: 62-63). Son olarak kontrol faaliyetleri belirlenirken dikkat edilmesi gereken kritik bir unsur da, kurumda en uygun kontrol seviyesini belirleyebilmektir. Şayet kurumun rutin işleyişini engellemeyecek şekilde esnek ve hedeflere ulaşabilme yolunda yönetimi destekleyici sertlikte bir kontrol tutumu sergilenirse kurumda etkin bir kontrol faaliyeti tesis edilebilir.

4.2.7. **Bilgi ve İletişim**

Bilgi ve iletişim, kurumsal risk yönetim sisteminde bulunan bütün aşamalarda, bileşenlerde ve değerlendirmelerde kritik bir öneme sahiptir (Cendrowski ve Mair, 2009: 95). Çünkü kurum genelinde riskleri tanımlama, değerlendirme, tutum belirleme ve sonuç olarak hedeflere ulaşabilmek için bilgi gereklidir. Bu nedenle bilgi sistemleri, hem kurum içinde hem de dışında gerçekleşen olaylardan bilgileri toplamak ve bu bilgiler yardımıyla risklerin etkin bir şekilde yönetilebilmesinin yanı sıra kurumun hedeflerine ulaşabilmesi yolunda bilinçli kararlar alabilmek için kullanılmaktadır (COSO, 2004a: 67).

Kurumsal risk yönetim sisteminin etkin bir şekilde kullanılabilmesi amacıyla kurum ve kuruluşlar hem geçmiş hem de güncel verileri kullanmaktadır. Kurumun gerçekleşen performansı, hedefleri, planları ve beklentileri geçmiş veriler sayesinde görülebilir. Bunun yanında kurumun alacağı dersler de bu sayede anlaşılabilir. Şimdiki veriler ise kurumun pozisyonunun belirlenmiş risk toleransı içerisinde olup olmadığını görülmesini sağlar. Aynı zamanda mevcut durumda yürütülen faaliyetler ve işletilen süreçlerde gerçekleşen değişimlerden kaynaklanan risklerin tespit edilebilmesini sağlar. Dolayısıyla bilgi sistemleri, kurumlara performanslarını ölçme ve izleme becerilerini artırmanın yanı sıra kurumsal düzeyde analitik bilgi edinilmesini sağlamaktadır (COSO, 2004a: 69).

Kurum ve kuruluşlarda otomatik karar verme ve süreçlerin hızlandırılmasına katkısından dolayı bilgi sistemlerinin kullanımı giderek artmaktadır. Ancak bu sistemlerde verilerin güvenilirliği sisteme olan güven açısından son derece önemlidir. Çünkü alınan yanlış veriler

sebebiyle risk tanımlama veya değerlendirme aşamalarında yönetimin yanlış yönlendirilmesi söz konusu olabilir. Bilgi, kurumun her seviyesinde riskleri tanımlamak, değerlendirmek ve tutum belirlemek için gereklidir. Bu nedenle elde edilen bilgilerin kaliteli ve doğru olması gerekmektedir. Aşağıdaki sorularla bilginin kalitesi doğrulanabilir (COSO, 2004a: 70):

- Bilgi doğru mu?
- Bilgi geçerli mi?
- Bilgi güncel mi?
- Doğru detaylandırılmış mı?
- Ulaşılabilir mi?

Kurumsal risk yönetiminin etkin olabilmesi için, doğru bilgiyi ihtiyaç duyulduğu zaman ve doğru kaynaktan alabilmek önemlidir (COSO, 2004a: 71). Bu nedenle bilgi uygun ve doğru seviyede detaylandırılmalı, doğru, güvenilir, kesin, güncel ve ulaşılabilir olmalıdır (Reding, vd., 2009: 4-9,10).

Bilgi sisteminin olmazsa olmazı iletişimdir. Uygun personelin kurumun stratejik, faaliyet, raporlama ve uygunluk hedeflerini doğru bir şekilde alabildiği ve gerekli sorumluluğunu yürütebilmesi için iletişim zorunludur (COSO, 2004a: 71). Kurum içerisinde bilginin aşağı, yukarı ve yatay yönde ulaşması iletişim sayesinde sağlanabilir. İletişimin aşağı yönde olması, yönetim tarafından belirlenen planların personele aktarılabilmesidir. Yukarı yönde bir iletişim ise, personellerin üst yönetime bilgi aktarabilmesidir. Yatay yönde iletişim ise aynı seviyedeki birimlerin arasında olan iletişim olarak ifade edilmektedir (Pehlivanlı, 2010: 87).

Etkili iletişim aşağıdaki unsurları içermelidir (COSO, 2004a: 71):

- Etkili kurumsal risk yönetimin önem ve anlamını,
- Kurum hedeflerini,
- Kurum risk iştah ve toleransını,
- Genel risk dilini,
- Kurumsal risk yönetim unsurlarını etkilemek ve desteklemek için personelin rol ve sorumluluklarını.

İletişim yöntemlerine e-posta, internet tabanlı uygulamalar, sesli ve görüntülü mesajların yanı sıra ilan tahtaları örnek olarak gösterilebilir. Kurumlar bu yönde gerekli olan açık

iletişim kanallarını oluşturmalı ve sürdürülebilir olmasını sağlamalıdır. Yönetim tarafından iletişim tarzı, süreci ve etkililiğini destekleyici teknolojik gelişmeler takip edilmelidir (Marchetti, 2012: 46). İletişimin etkili olması yalnızca kurum içi değil ortaklar, hissedarlar, tedarikçiler ve müşteriler açısından da önem arz etmektedir (Aksoy, 2005: 193-194; Reding, vd., 2009: 4-10). İletişimin geniş bir spektrumda ele alınması kuruma risk yönetiminde etkili bir bakış açısı kazandırabilir. Bunun yanında iletişimin, anlamlı, geçerli, zamanında ve yasal şartlara uygun olmasına dikkat edilmesi gerekmektedir (COSO, 2004a: 73).

Sonuç olarak kurumsal risk yönetim sisteminin etkin bir şekilde işletilebilmesi için bürokrasinin azalması ve hızlı sonuç alma mekanizmalarının geliştirilmesi önemlidir. Kurum tarafından personellerin yetki alanları belirlendikten sonra buna uygun şekilde iletişim kanalları tesis edilip yönetilmelidir. Etkin bir iletişim sistemi için doğru ve kaliteli bilginin yatay, dikey ve çapraz iletişim kanalları kullanılarak kurum genelinde dinamik bir yapı kurulabilir.

4.2.8. **İzleme**

Kurum ve kuruluşlar sürekli gelişen ve değişen bir ortamda faaliyet göstermektedirler. Bu sebeple kurumsal risk yönetim sisteminde bu aşamada kurumlar hem iç hem de dış değişiklikleri yönetim tarafından değerlendirmelidir (AIRMIC, ALARM, IRM, 2002: 11). Bir başka ifadeye göre izleme süreci, kurumlarda sistemin işlerliğini kontrol eden, tanımlanan prosedürlerin anlaşılıp doğru uygulandığını ve bunların takip edildiğine yönelik kuruma bir güvence sağlamalıdır (Griffiths, 2005: 25).

Kurumsal risk yönetim sisteminin düzenli ve etkin bir şekilde izlenmesi çalışanlar üzerinde sorumluluk duygularının canlılığına katkı sağlayacaktır. Bu sebeple izleme sürecinde değerlendirmenin doğru yapılabilmesi için aşağıda belirtilen noktalara dikkat edilmelidir (Ferma, 2003: 15):

- Uygulanan prosedürler ile toplanan bilgilerin uyumlu olup olmadığı,
- Süreç içerisinde elde edilen bilgilerin daha iyi kararlar alınmasına katkısı olup olmadığı ve İlerleyen zaman içerisinde alınacak kararlara etkisinin olup olmadığı,
- Risk yönetimi çerçevesinde kurum olarak alınacak derslerin açıkça belirtilmesidir.

Kurum ve kuruluşlarda kurumsal risk yönetim sistemi zaman içerisinde değişime uğrayabilir. Başlangıçta çok önemli olarak tanımlanan bir risk zaman içerisinde önem derecesi değişebilir ve bu riske karşı tutum da değişime uğrayacaktır. Bununla birlikte

yalnızca riskler değil kontrol faaliyetlerinde de değişim söz konusu olabilir. Bu değişiklikler kurumun yapısal veya yönetim değişiklikleri, yeni personel istihdamı, faaliyetlerde değişiklikler olması veya yeni bir sürecin başlamasından kaynaklanabilir. Bu nedenle karşılaşılan değişiklikler ve kurumsal risk yönetiminin yapı ve işleyişinin zamanında değerlendirip etkinliğini koruyabilmek için izleme yapılmaktadır (Ferma, 2003: 15). Ayrıca yeni oluşan risklerin yönetimi için gereken önlemlerin alınması veya daha önceden tanımlanmış risklerde meydana gelen değişimlerin değerlendirilmesi gerekmektedir (The Orange Book, 2004: 31).

Bu noktada kurumsal risk yönetim sisteminde izleme ve raporlama yapmaktaki asıl amaç olarak şu şekilde ifade edilebilir;

- Risk profilinde değişiklik olup olmadığının değerlendirilmesi,
- Risk yönetim sürecinin etkili olduğuna yönelik bir güvence oluşturmak,
- Değişiklik durumunda yeni bir eylemin gerekli olup olmadığı.

Kurumsal risk yönetim sisteminde izleme ve değerlendirme yapmanın çerçevesi ve ne sıklıkla yapılacağı, riskler, risk tutumları ve kontrollerin risk yönetimindeki önem derecesine göre değişebilir. Önemli görülen veya yüksek riskli faaliyetler ve buna karşı tutumlar daha sık değerlendirilebilir. Bu değerlendirmelerin kapsamı stratejik, faaliyet, raporlama ve uygunluk alanlarından hangisinin değerlendirileceğine göre değişmektedir (COSO, 2004a: 77).

İzleme süreci, sürekli izleme ve ayrı değerlendirmeler şeklinde iki yolla gerçekleştirilebilir. Sürekli izleme hâlihazırda yürütülen faaliyetler için kurum içine yerleşmiş bir şekilde, gerçekleşen durumlara karşı dinamik olarak tepki verebilecek şekilde yapılmaktadır. Kurumsal risk yönetim sistemi kendi kendini izlemeye yönelik tasarlanmıştır ve bu durum ayrı değerlendirmelerden daha etkilidir. Çünkü ayrı değerlendirmeler gerçekleşen olaylardan sonra uygulanırken, sürekli izleme de problemler hızlı bir şekilde belirlenebilmektedir. Buna rağmen bu iki yöntemin yalnız birinin kullanılması başarı elde edilmesini etkilemektedir. Bu nedenle birçok kurum bu iki yöntemin bir kombinasyonunu kullanmayı tercih etmektedir (COSO, 2004a: 75).

Sonuç olarak bu süreçten elde edilecek bilgilerle hem risk yöneticileri hem de iç denetçiler sistemin etkinliğine yönelik üst yönetime sunmak üzere bir rapor hazırlamaktadırlar. Bu raporda aşağıdaki hususlara dikkat edilmelidir (Karabeyli, 1999: 47):

- Sade ve anlaşılır bir üslup kullanılmalıdır.
- Sonuç ve bulgular yeterli denetim kanıtlarıyla desteklenmelidir.
- Sayısal ve grafiksel verilerle desteklenebilir.
- Süreklilik sağlayacak hususlar, başarılı uygulama örnekleriyle belirtilmelidir.
- Sistemin işleyişinde tespit edilen hatalar belirtilip, bu hatalara yönelik çözüm önerileri geliştirilmelidir.

5. BÖLÜM

ARAŞTIRMANIN YÖNTEMİ

Bu çalışmada, kurumların risk süreçlerini her yerden yönetebileceği web tabanlı bir uygulama geliştirilmesine odaklanılmıştır. Geliştirilen uygulama ile kurumsal risk yönetim sisteminde, kurum yöneticilerinin oluşabilecek riskler için anlık kararlar verebilecekleri bir karar destek sistemi oluşturulmaya çalışılmıştır. Çalışmanın yöntemi nitel araştırma desenlerinden durum (örnek olay) çalışması ve eylem araştırması olarak belirlenmiştir.

Çalışma Konya ilinde faaliyet gösteren bir anonim şirkette yapılan araştırmalar sonucunda uygulamanın işleyiş yapısını ve hangi aşamalarda ne gibi verilerin işleneceğine karar verilmiştir. Kurumsal risk yönetimi süreçlerinin adım adım hangi aşamalarda neler yapıldığına dair firmanın 2010 yılından bu yana risk yönetim faaliyetlerine yönelik gerçekleştirilen uygulamalar, hazırlanan belge ve raporlar incelenmiştir. Yapılan incelemeler sonucunda kurumsal risk yönetim sisteminin bir uygulama üzerinden çalıştırılıp yönetilebilmesi için geliştirilen öneriler ışığında bir süreç tasarlanıp algoritma oluşturulmuştur.

Durum çalışmalarında veri toplama yöntemi olarak doküman incelemesi, yerinde gözlem ve görüşme yöntemlerine başvurulmuştur. Dokümanların incelenmesinde kurumsal risk yönetim süreçlerinin literatürde belirtilen uygulama örneklerine göre benzerlikleri dikkate alınmıştır. Yerinde gözlem tekniğiyle risk yönetimine yönelik hangi uygulamaların ne şekilde yapıldığı gözlemlenmiştir. Görüşme yöntemiyle de risk yönetim faaliyetinde yer alan personeller ile süreçler ve uygulamalar üzerine incelemeler yapılmıştır. İncelemeler sonucunda geliştirilecek uygulamada yararlanılabilecek öneriler geliştirilmiş ve iyileştirme çalışmaları yapılmıştır. Ayrıca inceleme sonucunda elde edilen veriler ışığında oluşturulan algoritmanın uygulamaya dönüştürülmesinde şirketin stratejik, finansal, faaliyet ve dış çevre risklerinin objektif olarak değerlendirilebilmesine yönelik literatür taraması yapılmış ve risk değerlendirme metotlarından Fine-Kinney risk analiz yöntemi örnek değerlendirme için tercih edilmiştir.

Araştırma ve incelemeler sonucunda elde edilen veriler ışığında risk değerlendirme platformunda olması gereken özellikler belirlenmiştir. Belirlenen bu özelliklere göre uygulama geliştirme öncesinde aşağıda belirtilen noktalarda, personeller ile yapılan görüşmeler sonucunda kritik kararlar verilip uygulama geliştirilmiştir;

- Sunucu özellikleri
- Platformun belirlenmesi
- Uygulama geliştirme dili
- Veri tabanının özellikleri
- Uygulamada olması gereken modüller.

5.1. **Sunucu Özellikleri**

Uygulama web tabanlı olduğu için internet üzerinde yayın yapan bir bilgisayar üzerinde barındırılıp çalıştırılmasına sunucu yayını denir. Uygulamanın teknolojik bütün aygıtlar tarafından kullanılacağı, aynı anda en az 50 personelin kullanacağı, tehlike ve risk tanımlamalarının yapılırken görsel ögeler yükleneceği ve aynı anda birden fazla riskin hesaplanacağı ön görüldüğü için sunucunun bu iş ve işlemleri yapabilecek şekilde seçilmesi gerekmiştir. Bu nedenle aşağıda belirtilen özelliklerde bir sunucu kullanımı tercih edilmiş olup uygulamanın çalışması için gereken hız ve depolama alanı sağlanmıştır.

İşlemci: 2 Core CPU

Ram: 4 GB RAM

Hdd: 60 GB

5.2. **Platformun Belirlenmesi**

Uygulamanın kurum genelinde çalışan bütün personel tarafından kurum içinde veya dışında bilgisayar, tablet veya cep telefonları üzerinden kullanılabilmesi amaçlanmıştır. Bu nedenle bilgisayarlar üzerinde Windows veya Linux, tablet ve cep telefonlarında Android veya IOS işletim sistemlerinin tamamında çalışabilecek şekilde olması için uygulamanın web tabanlı olması ve internet tarayıcısı bulunan bütün cihazlardan erişilebilmesi amaçlanmıştır.

5.3. **Uygulama Geliştirme Dili**

Web tabanlı uygulama geliştirmek için bir programlama diline ihtiyaç duyulmaktadır. Hâlihazırda bu programlama dillerine örnek olarak; PHP, ASP.NET, PHYTON vb. diller verilebilir.

PHP, "PHP: Hypertext Preprocessor" kelimelerinin baş harflerini temsil eden, HTML içine gömülebilir(inline), açık kaynak kodlu, genel amaçlı, özellikle web siteleri geliştirmeye uygun bir betik dilidir. PHP dili, yapısının önemli bir kısmını C, Java ve Perl gibi dillerden almış, kendisine has özelliklerle bu yapıyı pekiştirmiş, kolay öğrenilen bir dildir. Dilin ana amacı, site geliştiricilerinin dinamik sayfalar oluşturmasını çabuklaştırmaksa da PHP ile çok daha fazlası yapılabilmektedir (Php Kılavuzu).

5.4. Veri Tabanı Özellikleri

Uygulamalar verilerini veri tabanları üzerinde depolayarak herhangi bir zamanda talep edildiğinde istenilen veriyi hızlı ve anlaşılır bir şekilde kullanıcıya getirir. Verilerin bu şekilde depolanıp istenildiğinde erişilebilmesini sağlayan veri tabanıdır. Uygulamanın geliştirilmesinde Php dili ile tam uyumlu olarak çalışan Mysql veri tabanı tercih edilmiştir.

MySQL, uygulama geliştiriciler tarafından küçük, orta ve büyük ölçekli uygulamalarda yaklaşık olarak altı milyondan fazla sistemde yüklü bulunan çoklu iş parçacıklı, çok kullanıcılı, hızlı ve sağlam bir veri tabanı yönetim sistemidir. UNIX, OS/2 ve Windows platformları için ücretsiz dağıtılmakla birlikte ticari lisans kullanmak isteyenler için de ücretli bir lisans seçeneği de mevcuttur (Mysql Kılavuzu).

5.5. Uygulamada Olması Gereken Modüller

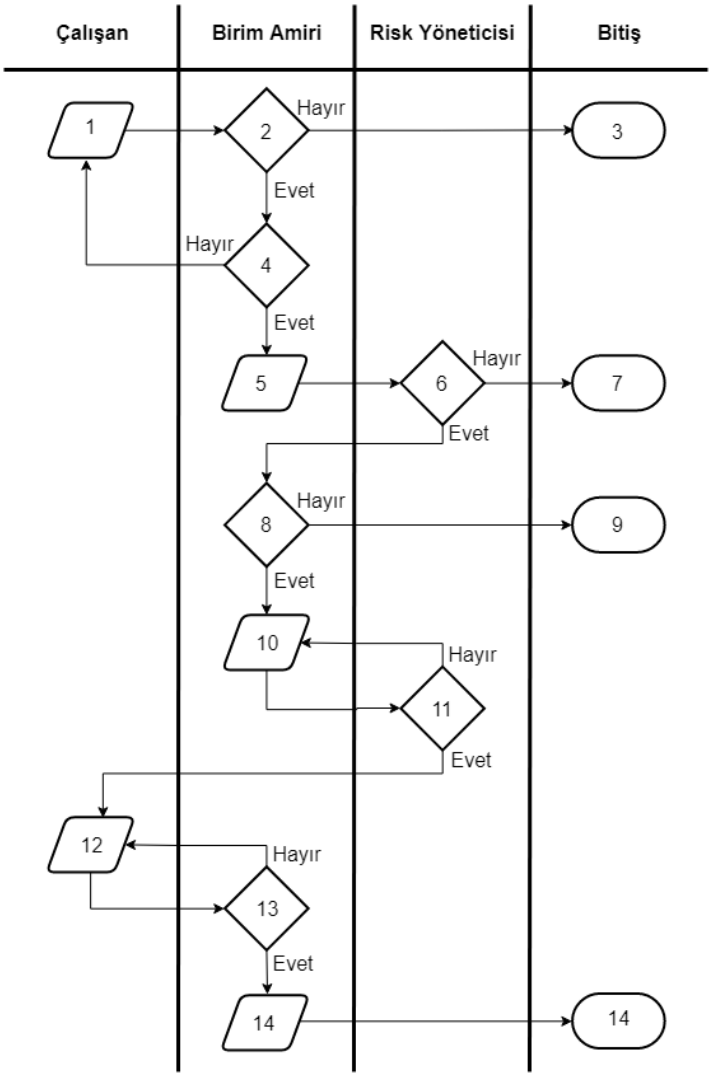
Uygulama tasarlanırken önce algoritma yani akış şeması oluşturulmuş ve buna uygun olarak da uygulamada kullanılacak modüller tasarlanmıştır. Modüllerin anlatımı Bölüm 6'da detaylı olarak yapılmıştır.

6. BÖLÜM

KURUMSAL RİSK YÖNETİM UYGULAMASI

Kurumsal risk yönetimi kapsamında bir kurumda risklerin yönetilmesine yönelik web tabanlı bir uygulama geliştirilmiştir. Bu bölümde uygulama iki aşamada incelenecektir. İlki uygulamanın, algoritması, işleyiş aşamalarının tanıtıldığı bölüm, diğeri ise uygulamanın çalışmasında kullanılan modüllerin tanıtımıdır.

6.1. Uygulamanın Algoritması



Şekil 6.1: Uygulama Algoritması

6.1.1. Tehlikenin Tanımlanması

Kurum çalışanı karşılaştığı herhangi bir tehlike veya tehlike içeren faaliyeti sisteme tanımlaması aşamasıdır. Bu aşamada çalışan aşağıdaki alanlara gerekli bilgileri girer:

- Faaliyet-Tehlikenin Tanımı, tehlikeyi tanımlayıcı bilgiler girer.
- Faaliyet-Tehlikeyle İlgili Alınmış Önlemler, varsa alınan önlemleri yazar.
- Faaliyet-Tehlikenin Görüldüğü Tesis, tehlikenin bulunduğu ana tesisi yazar.
- Faaliyet-Tehlikenin Tespit Edildiği Birim, tehlikenin tesis içerisinde bulunduğu birimi yazar.
- Tesisten Sorumlu Risk Değerlendirme Ekip Lideri, tesisten sorumlu kişiler otomatik olarak listeye gelir. İstediği sorumluyu seçer.
- Faaliyet-Tehlikeyi Tespit Etme Tarihi, tarih otomatik olarak formun açıldığı tarih gelir. Ancak istenirse manuel değiştirilebilir.
- Faaliyet-Tehlikeye Ait Fotoğraf ve Video, tehlikeye ait varsa fotoğraf veya video yüklenir.

6.1.2. Tehlikenin Değerlendirilmesi

Tehlikenin tanımlanması esnasında kurum çalışanı tarafından seçilen tesisteki birim amirinin tehlikeyi değerlendirmesi aşamasıdır.

6.1.3. Tehlikenin Kapatılması

Birim amiri değerlendirdiği tehlikenin gereksiz görürse veya herhangi bir işlem yapılmasına gerek görmezse tehlikeyi kapatıp süreci sonlandırabilir. Birim amiri kapatmak istediği tehlikeye ait kapatma sebebini Tehlike Kapatma Formuna yazması gerekir.

6.1.4. Tehlikenin Gerekli Görülmesi

Birim amiri tehlikenin değerlendirmeye alınmasına karar verirse, iki işlem yapabilir. İlki tehlikenin tanımlanmasında herhangi bir eksiklik veya düzeltme gereği görürse tehlikenin yeniden tanımlanması veya düzenlenmesi için süreci 1. adıma tekrar geri döndürebilir. İkinci durumda ise, 5. adıma geçer.

6.1.5. Risklerin Tanımlanıp Hesaplanması

Birim amiri tehlikenin gerçekleşmesi durumunda oluşması muhtemel bütün riskleri teker teker tanımlar. Riskleri tanımlama formunda aşağıdaki bilgiler girilir:

- Risk Türü: Oluşması muhtemel görülen risk şablonlarda tanımlanmış risk türü listesinden hangi kategoriye giriyorsa seçilir.
- Riskin Adı: Olası riske bir ad verilir.
- Riskin Çevresel Etkisi: Riskin gerçekleşmesi durumunda çevreye vereceği zararın tanımlanması yapılır.
- Olasılık: Riskin gerçekleşme olasılığı şablonlarda tanımlanmış risk olasılıkları listesinden seçilir.
- Şiddet: Riskin gerçekleşmesi durumunda ne kadar etkisinin olacağı, daha önce şablonlarda tanımlanan risk şiddeti listesinden seçilir.
- Frekans: Riskin gerçekleşme sıklığı, şablonlarda risk frekans listesinden seçilir.
- Değerlendirme Tarihi: Tarih otomatik olarak gelmektedir. Ancak istendiği takdirde manuel olarak değiştirilebilmektedir.

6.1.6. **Olası Risklerin Değerlendirilmesi**

Birim amiri tarafından tanımlanan olası risklerin risk yöneticisi tarafından değerlendirilme aşamasıdır.

6.1.7. **Risklerin Kapatılması**

Risk yöneticisi, birim amiri tarafından olası risklerin gereksiz görürse veya herhangi bir işlem yapılmasına gerek görmezse riski kapatıp süreci sonlandırabilir. Risk yöneticisi kapatmak istediği riske ait kapatma sebebini Risk Onay Formuna yazması gerekir.

6.1.8. **Risk Azaltıcı Faaliyet Değerlendirmesi**

Birim amiri risk yöneticisinin riski onaylama esnasında yazdığı yönlendirmeler ışığında riskin azaltılmasına yönelik herhangi bir faaliyet yapılması gerekip gerekmediğine karar verir.

6.1.9. **Risk Azaltma Faaliyeti Yapılmadan Kapatılması**

Birim amiri, risk yöneticisi tarafından değerlendirmek üzere kendisine gönderilen riski, azaltmaya yönelik herhangi bir faaliyete gerek olmadığına karar verirse riski kapatıp süreci sonlandırabilir.

6.1.10. **Riski Azaltma Faaliyeti Tanımı**

Birim amiri, riskin azaltılmasına yönelik faaliyetleri tanımlayıp, önce onaylanmak üzere risk yöneticisine sonra da faaliyetleri yapmak üzere belirlediği sorumluya bu tanımlamayı

gönderebilir. Risk azaltma faaliyeti tanımlama formunda aşağıdaki bilgiler girilir:

- Riski azaltacak faaliyetler: Birim amirinin yapılmasını ön gördüğü faaliyetler yazılır.
- Sorumlusu: Yapılacak faaliyetlerin kim tarafından yapılması gerektiği seçilir.
- Başlama Tarihi: Faaliyetlerin başlama tarihi seçilir.
- Bitiş Tarihi: Faaliyetlerin bitirilmesi gereken en son tarih seçilir.
- Kaynaklar: Faaliyetler esnasında kuruma ait veya dışarıdan kullanılması gereken kaynaklar yazılır.

6.1.11. **Risk Azaltma Faaliyetinin Değerlendirilmesi**

Birim amiri tarafından tanımlanan risk azaltma faaliyetleri risk yöneticisi tarafından değerlendirilir. Risk yöneticisi, faaliyetin düzeltilmesi veya yeniden tanımlanması amacıyla 10. adıma, faaliyeti birim amirine geri gönderebilir. Eğer faaliyetin tanımlanan sorumlu tarafından yapılmasını uygun görürse 12. adıma süreci ilerletir.

6.1.12. **Risk Azaltma Faaliyetlerinin Yapılması**

Birim amiri tarafından faaliyetleri yerine getirmek üzere atanan kurum çalışanı, belirtilen kaynakları kullanarak faaliyetleri yapar ve faaliyet formunu doldurarak onaylanmak üzere birim amirine gönderebilir. Kurum çalışanı tarafından doldurulan faaliyet formunda aşağıdaki bilgiler girilir:

- Yapılan Faaliyetler: Kurum çalışanı riskin azaltılmasına yönelik yapılması gereken faaliyet hakkında yaptıklarını yazar.
- Başlama Tarihi: Faaliyetlere başlama tarihi seçilir.
- Bitiş Tarihi: Faaliyetlerin tamamlandığı tarih seçilir.
- Riskin Son Durumu: Yapılan faaliyetler sonrasında riskin son durumu hakkında bilgi yazılır.
- Faaliyete Ait Fotoğraf ve Video: Yapılan faaliyetler esnasında kaydedilen fotoğraf veya videolar yüklenir.

6.1.13. **Yapılan Faaliyetlerin Değerlendirilmesi**

Kurum çalışanı tarafından riskleri azaltmaya yönelik yapılan faaliyetlerin birim amiri tarafından değerlendirilmesi aşamasıdır. Birim amiri yapılan faaliyetlerde eksiklik veya yanlışlık olduğuna karar verirse, kurum çalışanı tarafından düzeltilmesi amaçlı 12. Adıma geri gönderir. Birim amiri, eğer yapılan faaliyet yeterli görülürse riskin son durumu hakkında bilgi girişi için süreci 14. adıma ilerletir.

6.1.14. **Riskin Son Durumunu Tanımlama**

Birim amiri riskin azaltılmaya yönelik yerine getirilen faaliyet sonrasında, riskin son durumu hakkında Risk Son Durumu Değerlendirme Formunu doldurur. Riskin azaltılma faaliyeti sonrasında form doldurulurken aşağıdaki bilgiler girilir:

- Olasılık: Riskin yeniden gerçekleşme olasılığı seçilir.
- Şiddet: Riskin yeniden gerçekleşmesi durumunda yapacağı etki seçilir.
- Frekans: Riskin yeniden gerçekleşme sıklığı seçilir.
- Değerlendirme Tarihi: Son durumun değerlendirildiği tarih seçilir.

6.1.15. **Sürecin Sonlandırılması**

Birim amiri tarafından riskin son durumu hakkında bilgiler girildikten sonra otomatik olarak süreç sonlanır. Bundan sonra yönetici istediği herhangi bir zamanda tehlike, risk, azaltma faaliyetleri ve riskin son durumu hakkında detaylı rapor alarak sürecin tamamında ne gibi iş ve işlemlerin kimler tarafından yapıldığını görebilir.

6.2. **Uygulamanın Modülleri**

Uygulama içerisinde toplam sekiz modül bulunmaktadır. Bunlar:

- Risk Yönetimi
- Şablonlar
- Kullanıcılar
- Raporlar
- Mesajlar
- Ajanda
- İstek / Hata / Geliştirme

6.2.1. **Risk Yönetimi**

Uygulama üzerinde kullanıcılar yetkilerine göre risklerin yönetilmesine yönelik aşağıdaki işlemleri yapabilmektedir:

- Tehlike Tanımı: Kullanıcıların tamamı herhangi bir yerde gördükleri tehlikeleri uygulama üzerinde tanımlayıp giderilmesine yönelik süreci başlatabilirler.
- Risk Tanımı: Kullanıcılar yetkilerine göre, tanımlanan tehlikelerden dolayı olası riskleri tanımlayabilirler.

- Risk Hesaplama: Kullanıcılar yetkilerine göre, tanımlanan olası risklerin; olasılık, şiddet ve frekanslarına göre riskin hesaplamasını yapabilirler.
- Risk Azaltma Faaliyet Tanımı: Kullanıcılar yetkilerine göre, olası risklerin giderilmesine veya azaltılmasına yönelik faaliyetleri tanımlayabilirler.

6.2.2. **Şablonlar**

Sistemin genelinde kullanılacak olan bilgilerin dinamik bir şekilde kaydedilip güncellenebilmesini sağlanmak amacıyla tasarlanan modüldür. Burada kaydedilecek verilerde herhangi bir sınır bulunmamaktadır. Tanımlamaların tamamında güncelleme ve silme işlemleri yapılabilmektedir. Bu bölümde aşağıdaki iş ve işlemler yapılabilir.

6.2.2.1.**Kurum Bilgileri**

Sistemin kullanıcısı durumundaki kurumun unvan, adres ve logo tanımı yapılabilir ve bilgiler güncellenebilir.

6.2.2.2.**Tesis Listesi**

Yeni tesis tanımı yapılabilir ve tanımlanmış tesislerin listesi görülebilir. Bu tesisler güncellenebilir ve silinebilir. Tehlike – faaliyet tanımı, risk tanımları ve risk yönetim faaliyetlerinin tanımlanıp yönetilmesi aşamalarında tanımlanacak olan bu tesisler seçilecektir. Aksaray Üniversitesi bünyesinde bulunan fakülte, enstitü, meslek yüksekokulu vb. yerler tesislere örnek olarak verilebilir.

6.2.2.3.**Birim Listesi**

Tanımlanmış tesislere ait birimlerin tanımları yapılabilir ve tanımlanmış birimlerin listesi görülebilir. Bu birimler güncellenebilir ve silinebilir. Tehlike – faaliyet tanımı, risk tanımları ve risk yönetim faaliyetlerinin tanımlanıp yönetilmesi aşamalarında tanımlanacak olan bu birimler seçilecektir. Mercedes-Benz Türk Aksaray Kamyon Fabrikasında bulunan üretim, kalite, satış, muhasebe vb. bulunan bütün birimler örnek olarak verilebilir.

6.2.2.4.**Sorumlu Ekip Lideri Listesi**

Tanımlanmış tesislerin birimlerinden sorumlu ekip liderlerinin tanımı yapılabilir ve tanımlanmış ekip liderleri listesi görülebilir. Bu ekip liderleri güncellenebilir ve silinebilir. Tehlike – faaliyet tanımı, risk tanımları ve risk yönetim faaliyetlerinin tanımlanıp yönetilmesi aşamalarında tanımlanacak olan bu ekip liderleri Şekil 4.1. de belirtilen Birim Amiri olarak seçilecektir.

6.2.2.5.**Risk Türleri**

Sistem üzerinde kullanılacak risklerin türleri tanımlanabilir ve tanımlanmış risk türleri görülebilir. Tanımlanan tehlike veya faaliyetlerin ortaya çıkarabilecekleri riskler seçilirken bu risk türleri seçilecektir. Çalışmanın bölüm 1.2.'de belirtilen risk türleri örnek olarak değerlendirilebilir.

6.2.2.6.**Risk Olasılıkları**

Bir riskin gerçekleşme olasılığının ve riskin hesaplanmasında kullanılacak bu olasılığa ait puanın tanımı yapılabilir ve tanımlanmış risk olasılıkları listesi görülebilir. Çalışmanın bölüm 4.2.4.5.14'te belirtilen Fine-Kinney Risk Analizi yönteminde açıklanan tablo 4.33. "Zararın ortaya çıkma olasılığı tablosu" verileri örnek olarak uygulamaya girilmiştir.

6.2.2.7.**Risk Şiddetleri**

Bir riskin gerçekleşmesi durumunda ortaya çıkabilecek etkinin ve riskin hesaplanmasında kullanılacak bu etkiye ait puanın tanımı yapılabilir ve bu etkilerin listesi görülebilir. Çalışmanın bölüm 4.2.4.5.14'te belirtilen Fine-Kinney Risk Analizi yönteminde açıklanan tablo 4.35. "Etki/Zarar-Sonuç Tablosu" verileri örnek olarak uygulamaya girilmiştir.

6.2.2.8.**Risk Frekansları**

Bir riskin gerçekleşme sıklığı ve riskin hesaplanmasında bu sıklığın puan tanımı yapılabilir ve risk frekansları listesi görülebilir. Çalışmanın bölüm 4.2.4.5.14'te belirtilen Fine-Kinney Risk Analizi yönteminde açıklanan tablo 4.34. "Tehlikeye Maruz Kalma Frekansı Tablosu" verileri örnek olarak uygulamaya girilmiştir.

6.2.2.9.**Risk Dereceleri**

Riskin hesaplanmasının ardından elde edilecek toplam risk puanının derecelendirilmesine yönelik kullanılacak olan risk derecelerinin tanımı yapılabilir ve bu derecelerin listesi görülebilir. Çalışmanın bölüm 4.2.4.5.14'te belirtilen Fine-Kinney Risk Analizi yönteminde açıklanan tablo 4.36. "Fine-Kinney Risk Düzeyine Göre Karar ve Eylem" verileri örnek olarak uygulamaya girilmiştir.

6.2.3. **Kullanıcılar**

Sistem üzerinde tanımlanabilecek kullanıcılar ve yetkileri aşağıdaki şekilde tanımlanmıştır.

6.2.3.1. **Sistem Yöneticisi**

Web tabanlı çalışan uygulamada bütün haklara sahiptir. Sistemin ana yöneticisidir. Yapabildiği işlemler;

- Ana Sayfa: Faaliyet – tehlike, riskler ve risk yönetim süreçlerine ait bilgilendirmeleri görebilir.
- Kullanıcı Tanımı: Yeni kullanıcı tanımlayabilir, güncelleyebilir ve silebilir.
- Şablon Tanımları: Sistemin genelinde kullanılan şablonları tanımlayabilir, güncelleyebilir ve silebilir.
- Faaliyet veya Tehlike: Faaliyet veya tehlikelere yönelik aşağıdaki iş ve işlemleri yapabilir veya görebilir.
    - Yeni Faaliyet veya tehlike tanımlayabilir,
    - Tanımlanan yeni faaliyet veya tehlike listesi,
    - Revize edilecek faaliyet veya tehlike listesi,
    - İşlem gören faaliyet veya tehlike listesi,
    - Kapatılan faaliyet veya tehlike listesi.
- Risk Değerlendirme: Tanımlanan tehlike veya faaliyetlerin oluşturacağı risklerin değerlendirilmesi aşaması. Bu aşamada aşağıdaki iş ve işlemleri yapabilir veya görebilir.
    - İşlem bekleyen yeni tanımlanmış risklerin listesi,
    - Revize bekleyen risklerin listesi,
    - Kapatılan risklerin listesi,
    - Onaylanacak risk listesi.
- Risk Yönetimi: Risklerin yönetilmesine yönelik aşağıdaki iş ve işlemleri yapabilir veya görebilir.
    - Programa alınmış faaliyetler,
    - Revize edilecek faaliyetler,
    - Risk yönetimi faaliyeti hazırlanacak riskler,
    - Revize edilecek risk yönetim faaliyetleri,
    - Onaylanacak risk yönetim faaliyetleri,
    - Risk yönetim faaliyeti hazırlanmamış riskler,

- Onaylanacak risk yönetimi.

- Raporlar: Tanımlanmış bütün faaliyet veya tehlikeler ve bunlardan dolayı ortaya çıkabilecek risklere ilişkin detaylı rapor alabilir.
- Mesajlar: Sistemi kullanan bütün kullanıcılarla mesajlaşabilir.
- Ajandam: Kendine ait veya bir başka kullanıcıyla ilgili yapacağı görevler veya hatırlatmalar ekleyebilir.
- İstek / Hata / Geliştirme: Sistemin kullanımında karşılaşılan bir sorun veya yeni bir istek için yazılımcıya mesaj gönderebilir.

6.2.3.2. **Risk Yöneticisi**

Uygulamada tanımlanmış bir tesisin yöneticisidir. Tanımlı olduğu yerle ilgili bütün haklara sahiptir. Yapabildiği işlemler;

- Ana Sayfa: Faaliyet – tehlike, riskler ve risk yönetim süreçlerine ait tanımlı olduğu tesisle ilgili bilgilendirmeleri görebilir.
- Faaliyet veya Tehlike: Faaliyet veya tehlikelere yönelik tanımlı olduğu tesisle ilgili aşağıdaki iş ve işlemleri yapabilir veya görebilir.
    - Yeni Faaliyet veya tehlike tanımlayabilir,
    - Tanımlanan yeni faaliyet veya tehlike listesi,
    - Revize edilecek faaliyet veya tehlike listesi,
    - Kapatılan faaliyet veya tehlike listesi.
- Risk Değerlendirme: Tanımlanan tehlike veya faaliyetlerin oluşturacağı risklerin değerlendirilmesi aşaması. Bu aşamada tanımlı olduğu tesisle ilgili aşağıdaki iş ve işlemleri yapabilir veya görebilir.
    - Onaylanacak risk listesi.
- Risk Yönetimi: Risklerin yönetilmesine yönelik tanımlı olduğu tesisle ilgili aşağıdaki iş ve işlemleri yapabilir veya görebilir.
    - Risk yönetim faaliyeti hazırlanmamış riskler,
    - Onaylanacak risk yönetimi.
- Raporlar: Tanımlanmış bütün faaliyet veya tehlikeler ve bunlardan dolayı ortaya çıkabilecek risklere ilişkin tanımlı olduğu tesisle ilgili detaylı rapor alabilir.
- Mesajlar: Sistemi kullanan bütün kullanıcılarla mesajlaşabilir.
- Ajandam: Kendine ait veya bir başka kullanıcıyla ilgili yapacağı görevler veya hatırlatmalar ekleyebilir.

- İstek / Hata / Geliştirme: Sistemin kullanımında karşılaşılan bir sorun veya yeni bir istek için yazılımcıya mesaj gönderebilir.

6.2.3.3. **Birim Amiri**

Uygulamada tanımlanmış bir tesisin veya alt birimin sorumlusudur. Tanımlı olduğu yerle ilgili bütün haklara sahiptir. Yapabildiği işlemler;

- Ana Sayfa: Faaliyet – tehlike, riskler ve risk yönetim süreçlerine ait tanımlı olduğu tesisle ilgili bilgilendirmeleri görebilir.
- Faaliyet veya Tehlike: Faaliyet veya tehlikelere yönelik tanımlı olduğu tesisle ilgili aşağıdaki iş ve işlemleri yapabilir veya görebilir.
    - Yeni Faaliyet veya tehlike tanımlayabilir,
    - Tanımlanan yeni faaliyet veya tehlike listesi,
    - Revize edilecek faaliyet veya tehlike listesi,
    - İşlem gören faaliyet veya tehlike listesi.
- Risk Değerlendirme: Tanımlanan tehlike veya faaliyetlerin oluşturacağı risklerin değerlendirilmesi aşaması. Bu aşamada tanımlı olduğu tesisle ilgili aşağıdaki iş ve işlemleri yapabilir veya görebilir.
    - Onay bekleyen risk listesi.
    - Revize bekleyen risklerin listesi,
    - Kapatılan risklerin listesi.
- Risk Yönetimi: Risklerin yönetilmesine yönelik tanımlı olduğu tesisle ilgili aşağıdaki iş ve işlemleri yapabilir veya görebilir.
    - Risk yönetimi faaliyeti hazırlanacak riskler,
    - Revize edilecek risk yönetim faaliyetleri,
    - Onaylanacak risk yönetim faaliyetleri.
- Mesajlar: Sistemi kullanan bütün kullanıcılarla mesajlaşabilir.
- Ajandam: Kendine ait veya bir başka kullanıcıyla ilgili yapacağı görevler veya hatırlatmalar ekleyebilir.
- İstek / Hata / Geliştirme: Sistemin kullanımında karşılaşılan bir sorun veya yeni bir istek için yazılımcıya mesaj gönderebilir.

6.2.3.4. **Kurum Çalışanı**

Uygulamada tanımlanmış bir tesisin veya alt birimin veri giriş elemanıdır. Tanımlı olduğu yerle ilgili bütün haklara sahiptir. Yapabildiği işlemler;

- Ana Sayfa: Faaliyet – tehlike ve risk yönetim süreçlerine ait tanımlı olduğu tesisle ilgili bilgilendirmeleri görebilir.
- Faaliyet veya Tehlike: Faaliyet veya tehlikelere yönelik tanımlı olduğu tesisle ilgili aşağıdaki iş ve işlemleri yapabilir veya görebilir.
    - Yeni Faaliyet veya tehlike tanımlayabilir,
    - Tanımlanan yeni faaliyet veya tehlike listesi,
    - Revize edilecek faaliyet veya tehlike listesi.
- Risk Yönetimi: Risklerin yönetilmesine yönelik tanımlı olduğu tesisle ilgili aşağıdaki iş ve işlemleri yapabilir veya görebilir.
    - Risk yönetimi faaliyeti hazırlanacak riskler,
    - Revize edilecek risk yönetim faaliyetleri.
- Mesajlar: Sistemi kullanan bütün kullanıcılarla mesajlaşabilir.
- Ajandam: Kendine ait veya bir başka kullanıcıyla ilgili yapacağı görevler veya hatırlatmalar ekleyebilir.
- İstek / Hata / Geliştirme: Sistemin kullanımında karşılaşılan bir sorun veya yeni bir istek için yazılımcıya mesaj gönderebilir.

6.2.4. **Raporlar**

Risk yönetici yetkisine sahip kullanıcılar tarafından uygulama üzerinde herhangi bir zamanda tanımlanan tehlikeler, riskler ve riskleri azaltıcı faaliyetlere yönelik yapılmış bütün işlemleri detaylı bir şekilde görebildikleri modüldür. Rapor oluşturma esnasında kullanıcıya esnek rapor oluşturma yetkisi verilmiştir. Kullanıcı tesis bazlı, birim bazlı, istediği tarih aralığında veya bunların karması olacak şekillerde raporlar oluşturabilmektedir.

6.2.5. **Mesajlar**

Uygulama üzerinde tanımlı bütün kullanıcılar birbirleriyle bu modül aracılığıyla mesajlaşabilmektedir. Bu modül sayesinde kullanıcılar bir başka iletişim aracına ihtiyaç duymadan hızlı ve kolay bir yolla iletişim sağlayabilmektedir. Modül üzerinde gönderilip alınan mesajlar bir e-posta istemcisi gibi çalışmakta okunmuş ve henüz okunmamış mesajlar tarih sırasına göre sıralanmaktadır. Bu sayede kullanıcılar, kendilerine gönderilen mesajları

gözden kaçırmamaktadır.

6.2.6. **Ajanda**

Uygulama üzerinde tanımlı bütün kullanıcıların kullanabileceği bu modülde, kullanıcılar risk yönetimiyle ilgili üzerlerine verilmiş görevleri veya bireysel olarak ihtiyaç duydukları hatırlatmaları kaydedebilmektedir. Aylık takvim görünümünde olan bu modülde ayrıca kullanıcılar önemli gördükleri hatırlatmaları diğer bir uygulama kullanıcısının ajandasına da hatırlatma olarak ekleyebilmektedir.

6.2.7. **İstek / Hata / Geliştirme**

Bu modül uygulamanın kullanımı esnasında bütün kullanıcıların karşılaşabilecekleri hatalar, ihtiyaç duyacakları yeni bir özellik veya düzeltmelerin yazılımcıya iletmelerini sağlamaktadır.

SONUÇ

Yaşamımızın her alanında karşı karşıya bulunduğumuz tehlikeler birer olumsuz risk örneği oluşturmaktadır. Ancak bu risklerin doğru yönetilmesiyle fırsatlar elde edilebilir. Bu nedenle gerek bireysel gerekse kurumsal anlamda yürütülen faaliyetlerde karşılaşılabilecek risklerin etkin bir şekilde yönetilmesi gerekmektedir. Kurum ve kuruluşlar piyasa şartlarına uygun şekilde bir dinamizm sergileyebilmeleri, belirledikleri hedeflere ulaşmada büyük önem arz etmektedir. Bunu sağlayabilmelerinin temel şartı olarak riskten kaçınmak yerine yönetmeye odaklanmalarıdır. Bu yönde çağımızın gerekliliklerine göre benimsenmiş modern risk yönetim tekniklerini odak noktasına almalıyız. Buna yönelik çalışmada, riskin tanımlanması aşamasından yönetilmesi ve sonuçlarının izlenmesine kadar gereken bütün adımlar COSO kurumsal risk yönetimi çerçevesinde ele alınmıştır.

Kurumsal risk yönetimi açısından genel kabul görmüş en iyi risk yönetim anlayışı olan COSO, riskin etkin bir şekilde yönetilmesi için risk değerlendirmesini üç boyutlu olarak ele almaktadır. Kurumun geneline hitap edecek şekilde riskler değerlendirilip, gereken önlemlerin alınması yönünde bir yol çizmektedir. Kurumsal risk yönetiminin etkin bir şekilde uygulanabilmesini sağlamak amacıyla teknolojinin sağladığı kolaylıkların kullanılması, kurumların dinamizmini artırmaya yönelik büyük katkıları olduğu değerlendirilmektedir. Bu nedenle teknolojik aygıtların erişebildiği bir uygulama üzerinden risk yönetimine yönelik bir sistem tasarımı yapılmıştır. Uygulamanın mobil cihazlar ve bilgisayardan erişilebilir olması platform bağımsızlığını sağlamakta ve böylelikle kullanıcıların sabit yerde veya hareket halinde oldukları halde sisteme kolaylıkla erişebilmelerini sağlamaktadır. Uygulamada risk hesaplama için yapılan araştırma ve testler sonrasında kararlı ve yüksek doğruluk oranına sahip olan Fine-Kinney metodu örnek olarak tercih edilmiştir. Uygulamanın en önemli özelliği olan risk hesaplama parametrelerinin dinamik olarak yetkili kullanıcılar tarafından değiştirilip bir başka hesaplama metodu uygulanabilmektedir. Bu sayede kurum ve kuruluşların yapılarına veya sektörlerine uygun geliştirilmiş risk hesaplama metotlarını uygulamaya dinamik olarak tanımlayıp kullanabilmeleri mümkün olabilmektedir. Risk analizinde karşılaşılan en kritik unsurlardan

biri olan yetki karmaşasıdır. Uygulamada kullanıcı tanımları ana yetkili kullanıcı tarafından tanımlanabilmekte ve yetkileri tanımlama esnasında atanabilmektedir. Bu sayede yetki karmaşası da ortadan kaldırılmaktadır. Ayrıca risklerin tanımlanıp gereken önlemlerin alınması bir sürece bağlandığı için yetkisiz kimseler tarafından risklerin görmezden gelinmesi veya gözden kaçması gibi durumlar da engellenmiştir.

Tasarlanan risk yönetim uygulamasında hedeflenenler şu şekilde sıralanabilir:

- Tehlikelerin doğru değerlendirilmesi,
- Risklerin doğru tanımlanması,
- Tanımlanan risklerin doğru değerlendirilmesi,
- Risklerin yönetilmesine yönelik gereken tedbirlerin hızlı bir şekilde alınabilmesi,
- Tedbirlerde kullanılacak kaynakların doğru yönlendirilmesi,
- Risklerin son durumlarının değerlendirilerek gerekli olanlarının sürekli izlemeye alınması şeklinde özetlenebilir.

Uygulama tezin yayımlanmasından sonra bir yıl süreyle http://www.btmarge.com/rasy adresinden erişilebilir olacaktır. Ana kullanıcı adı: sistem şifresi: sistem.123 olarak tanımlanmıştır.

Uygulama, gelecek araştırmalarda risklerin daha etkin yönetilebilmesi için, karar verme aşamalarında makine öğrenmesi kullanılarak yapay zekâ destekli önerilerle risk yöneticilerinin karar alma süreçlerini kolaylaştırması sağlanabilir. Ayrıca uygulamada risklerin hesaplanması aşamasında, kullanıcıların risk hesaplama yöntemlerinden istediğini seçebileceği ve ihtiyaç duyulan yeni bir risk hesaplama yöntemini sisteme İstek / Hata / Geliştirme modülü üzerinden dinamik olarak yükleyip kullanabileceği şekilde bu modülün dinamik bir şekle dönüştürülmesi sağlanabilir.

KAYNAKÇA

Ababneh, W. A. (2000). *An integrated approach of construction risk management and evaluation.* Yayınlanmamış Doktora tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Airmic, Alarm, Irm. (2002). A Risk Management Standard. 23.04.2019 tarihinde http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf sayfasından erişilmiştir.

Airmic, Alarm, Irm. (2010a). Kurumsal Risk Yönetimine Yapısal Bakış Açısı ve ISO 31000 Yükümlülükleri. 23.04.2019 tarihinde http://www.theirm.org/documents/SARM_ERM_000.pdf sayfasından erişilmiştir.

Airmic, Alarm, Irm. (2010b). A Structured Approach to Enterprise Risk Management and the Requirements of ISO 31000. 23.04.2019 tarihinde http://www.theirm.org/documents/SARM_FINAL.pdf sayfasından erişilmiştir.

Akgüç, Ö. (1994). *Finansal Yönetim.* İstanbul: Avcıol Basım-Yayın.

Aksoy, T. (2005). Bağımsız Denetim Şirketleri İçin Ulusal ve Uluslararası Düzenlemelerle Uyumlu Çok Yönlü Bir İç Kontrol Anket Formu Önerisi. *Mali Çözüm İSMMM Yayın Organı,* (73), 168-202.

Aktaş, R. (2008). *Kurumsal Risk Yönetimi*. TOBB Üniversitesi Ders Notları. 25.04.2019 tarihinde https://slideplayer.biz.tr/slide/1978190/ sayfasından erişilmiştir.

Altay, E. (2004). *Sermaye Piyasası'nda varlık fiyatlama teorileri: sermaye piyasası teorisi-arbitraj fiyatlama teorisi*. İstanbul: Derin.

Argüden, Y. (2006). *An overview of the Turkish economy: outlook and current perspectives*. http://www.arge.com/wp-content/uploads/2013/02/turkisheconomy.pdf sayfasından erişilmiştir.

Arslan, I. (2008). *Kurumsal Risk Yönetimi.* Yayınlanmamış Uzmanlık Tezi, Maliye Bakanlığı Strateji Geliştirme Başkanlığı, Ankara.

Aybars, A. (1998). 24.04.2019 tarihinde Dünya Gazetesi 24.02.1998 www.dünya.com/Arsiv /yazar/aa. soz.htm sayfasından erişilmiştir.

Aytürk, N. (2000). Yönetimde Yetki Devri ve İmza Yetkileri. *Amme İdaresi Dergisi*, 33(1), 79-110.

Babuşcu, Ş. (2005). *Basel II Düzenlemeleri Çerçevesinde Bankalarda Risk Yönetimi*. Ankara: Akademi.

Bahtiyar, H. (2008). *Ticari bankalarda operasyonel risk yönetimi: örnek bir uygulama*. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya.

Barrett, P. (2003). *Strategic insights into enterprise risk management (ERM).* In Conference Audience: Address to the ACT Chapter of the Australian.

Barton, T. L., Shenkir, W. G. & Walker, P. L. (2002). *Making enterprise risk management pay off*. USA: FT Press.

Bolak, M. (2004). *Risk Yönetimi*. İstanbul: Birsen.

Bryson, J. M. (2018). *Strategic planning for public and nonprofit organizations: A guide to strengthening and sustaining organizational achievement*. New Jersey: John Wiley & Sons.

Burnaby, P. A., Hass, S., Paape, L. & Abdolmohammadi, M. (2009). A global summary of the common body of knowledge. *Internal Auditing*, 24(1), 3-26.

Campbell, D. (1992). *Writing Security United States Foreign Policy and the Politics of Identitiy*. Minneapolis: University of Minnesota.

CAS, Casualty Actuarial Society, (2003). *Overview of Enterprise Risk Management*. 27.04.2019 tarihinde https://www.casact.org/area/erm/overview.pdf sayfasından erişilmiştir.

Cendrowski, H. & Mair, W. C. (2009). *Enterprise risk management and COSO: A guide for directors, executives and practitioners*. New Jersey: John Wiley & Sons.

Chapman, R. J. (2006). *Simple Tools and Techniques for Enterprise Risk Management.* West Sussex: John Wiley & Sons.

Chapman, C. (2003). Bringing ERM into focus: A new COSO study provides some much-needed clarity and structure to the fluid topic of enterprise risk management. *Internal auditor,* 60(3), 30-36.

Chorafas, D. N. (1997). *Market Risk Amendment.* New York: McGraw-Hill.

Cohrssen, J. J. & Covello V. T. (1989), *Risk Analysis: A Guide of Principles and Methods for Analyzing Health and Environmental Risk.* Minneapolis: University of Minnesota.

Colquitt, L. L., Hoyt, R.E. & Lee, R. B. (1999). Integrated Risk Management and The Role of the Risk Manager. *Risk Management and Insurance Review*, 2(3), 43-61.

COSO. (2004a). *Enterprise Risk Management-Integrated Frmaework Executive Summary Framework*. 13.04.2019 tarihinde https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf sayfasından erişilmiştir.

COSO. (2004b). *Enterprise Risk Management-Integrated Framework Application Techniques.* September. 13.04.2019 tarihinde http://www.coso.org/documents/ COSOBoardsERM4pagerFINALRELEASEVERSION82409_001.pdf sayfasından erişilmiştir.

COSO. (2009a). *Effective Enterprise Risk Oversight - The Role of the Board of Directors.* 13.04.2019 tarihinde http://www.coso.org/documents/COSOBoardsERM4pager FINALRELEASEVERSION82409_001.pdf sayfasından erişilmiştir.

COSO. (2009b). *Strengthening Enterprise Risk Management For Strategic Advantage.* 13.04.2019 tarihinde http://www.coso.org/documents/COSO_09_board_position_ final102309PRIN TandWEBFINAL_000.pdf sayfasından erişilmiştir.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *COSO Enterprise Risk Management: Integrating with Strategy and Performancement*. 17.04.2019 tarihinde https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf sayfasından erişilmiştir.

Çağırgan, M. (1997). *Risk Yönetimi.* Yayınlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Çakmak, E. (2014). *Atölye Tipi Üretim Yapan Sanayi İşletmelerinde İş Sağlığı ve Güvenliği.* Yayınlanmamış Uzmanlık Tezi, TC Çalışma ve Sosyal Güvenlik Bakanlığı, Çalışma ve Sosyal Güvenlik Eğitim ve Araştırma Merkezi, Ankara.

D'Arcy, S. P. & Brogan, J. C. (2001). Enterprise risk management. *Journal of Risk Management of Korea, 12*(1), 207-228.

Damodaran, A. (2008). *Strategic Risk Taking: A Framework For Risk Management*. New Jersey: Whartoon School.

Delikanlı, İ. U. (2000). *Bankalarda Uluslararası Standartlara Uygun Risk Yönetimi ve Kontrolü.* İktisadi Araştırmalar Vakfı Semineri, İstanbul.

Demirtaş, Ö. & Güngör, Z. (2004). *P*ortföy Yönetimi Ve Portföy Seçimine Yönelik Uygulama. *Havacılık ve Uzay Teknolojileri Dergisi*, 1(4), 103-109.

Kalyoncu, D. (2013). *Risksiz Risk Yönetiminin Alternatif Yolları*. Yayınlanmamış Yüksek Lisans Tezi, Okan Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Derici, O. (2015). *İç Kontrol ve Risk Yönetimi*. Antalya: Bekad.

Derici, O., Tüysüz, Z. & Sarı, A. (2007). Kurumsal Risk Yönetimi ve Sayıştay Uygulaması. *Sayıştay Dergisi,* 65(Özel Sayı), 151-172.

Dickinson, G. (2001). Enterprise Risk Management: Its Origins and Conceptual Foundation. *The Geneva Papers on Risk and Insurance,* 26 (23), 360-366.

Ekici, H. (2015). *Kurumsal Risk Yönetimi*. Konya: Çizgi.

Emhan, A. (2009). Risk Yönetim Süreci Ve Risk Yönetmekte Kullanılan Teknikler. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi,* 23(3), 209-220.

Eranti, E. (2008). *Sustainable Development or The Will to Power?, The European Union And Finland Pursuing Environmental Policy.* Helsinki: Helsinki University of Technology Water Resources.

Erdem, A. & Gündem, T. İ. (2014). M-FDBSCAN: A multicore density-based uncertain data clustering algorithm. *Turkish Journal of Electrical Engineering & Computer Sciences,* 22(1), 143-154.

Ernst&Young. (2005). *Risk Management and Accounting Audit in accordance with Corporate Governance Principles*. 18.04.2019 tarihinde https://www.ey.com/tr/tr/ issues/managing-risk sayfasından erişilmiştir.

Ferma. (2003). *Risk Management Standard*. 13.04.2019 tarihinde http://www.ferma.eu/ wp-content/uploads/2011/11/a-risk-management-standard-turkish-version.pdf sayfasından erişilmiştir.

Florea R. & Florea, R. (2009). Internal Audit-in Risk Management Approach. *Economy Transdisciplinarity Cognition,* 2(1), 38-44.

Frigo, M. L. & Anderson, R. J. (2011). Strategic risk management: A foundation for improving enterprise risk management and governance. *The Journal of Corporate Accounting & Finance,* 22(3), 81-88.

Funston, R. (2003). Creating a risk-intelligent organization: using enterprise risk management, organizations can systematically identify potential exposures, take corrective action early, and learn from those actions to better achieve objectives. *Internal Auditor, 60*(2), 59-64.

Fussell, J. B., Powers, G. J. & Bennetts, R. G. (1974). Fault Trees A State of the Art Discussion. *IEEE Transactions on Reliability,* 23(1), 51-55.

Gacar, A. (2017). İşletmelerde Kurumsal Risk Yönetimi Kapsamında Riskin Erken Saptanması ve Yönetimi Komiteleri: Borsa İstanbul'da Nitel Bir Araştırma. *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi,* 52, 123-133.

Göğüş, H. (2015). *Risk Odaklı İç Denetimde Risklerin Saptanması ve Değerlendirilmesi*. İstanbul: Türkmen.

Güneş, Ş. (2009). *Kurumsal Risk Yönetimi ve Türkiye'de Farkındalığına İlişkin Bir Uygulama.* Yayınlanmamış Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Griffiths, D. (2006). *Risk Based Internal Auditing.* 23.04.2019 tarihinde www.internalaudit.biz sayfasından erişilmiştir.

Griffiths, P. (2005). *Risk Based Auditing. Gower Publishing Limited.* Burlington: Gower.

Gupta, P. P. (2009). COSO 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices. *Published as a Research Monograph by the Institute of Management Accountants.* 19.04.2019 tarihinde https://ssrn.com/abstract=1417604 sayfasından erişilmiştir.

Haksöz, Ç. (2013). Risk Zekâsı: Düşer isen Tez Doğrul. *Denetişim Dergisi,* 12, 84-85.

Harris, P., Kinkela, K. & Hayes, N. T. (2011). Internal auditing developments: COSO studies key risk assessment as a component of enterprise risk management. *Internal Auditing-Boston,* 26(5), 11-15.

Hillson, D. A. & Murray-Webster, R. (2006). Understanding risk attitude. *Association for Project Management (APM) Yearbook,* 2006/2007, 25-27.

Hopkin, P. (2012). Understanding the causes of corporate failure. *Financial Management,* 14719185, 50-53.

Hoyt, R. E. & Liebenberg, A. P. (2011). The Value of Enterprise Risk Management. *The Journal of Risk and Insurance,* 78(4), 795-822.

INTOSAI Auditing Standards Committee. (2004). *Implementation guidelines for performance auditing.* International Congress of Supreme Audit Institutions, Vienna.

INTOSAI. (2007). *Guidelines for Internal Control Standards for the Public SectorFurther Information on Entity Risk Management.* 20.04.2019 tarihinde http://www.issai.org/ data/files/76/F3/84/55/EACD65107FA83C65BA5818A8/intosai_gov_9130_e.pdf sayfasından erişilmiştir.

IRM. (2011). *Risk Appetite and Risk Tolerance A Consultation Paper from the Institute of Risk Manegement.* 23.04.2019 tarihinde http://www.theirm.org/publications/ documents/IRM_Risk_Appetite_Consultati on_Paper_Final_Web.pdf sayfasından erişilmiştir.

İnal, H. & Günay, S. (1993). *Olasılık ve Matematiksel İstatistik*. Ankara: Hacettepe Üniversitesi Fen Bilimleri Fakültesi.

Karabeyli, L. (1999). Risk Denetimi Temel Kavramlar ve Yaklaşımlar. *Sayıştay Hizmet İçi Yayınları,* 4, 1-54.

Kaya, S. (2015). *Üretim işletmelerinde iç kontrol ve iç denetim.* Yayınlanmamış Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Kidder, (2013). *KRY Tanımı ve Temel Unsurları*. İstanbul: KİDDER.

Kinney, G. F. & Wiruth, A. D. (1976). *Practical risk analysis for safety management.* California: Naval Weapons Center China Lake.

Kızıldağ, D. (2011). *Yönetsel Açıdan Risk Yönetimine Bir Bakış: ISO 31000 Risk Yönetimi*. Ankara: Seçkin.

Klinke, A. & Renn, O. (2002). A new approach to risk evaluation and management: risk-based, precaution-based, and discourse-based strategies. *Risk analysis: an official publication of the Society for Risk Analysis,* 22(6), 1071-1094.

Koç, S. (2012). *Basel II Kapsamında Kurumsal Risk Yönetimi: Türkiye'de Bankacılık Sektöründe Bir Uygulama.* Yayınlanmamış Doktora Tezi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri.

Kumaş, E. & Birgören, B. (2010). E-Devlet Kapısı Projesi Bilgi Güvenliği ve Risk Yönetimi: Türkiye Uygulaması. *Bilişim Teknolojileri Dergisi*, 3(2), Mayıs, 29-36.

Kuo, F. E., Bacaicoa, M. & Sullivan, W. C. (1998). Transforming inner-city landscapes: Trees, sense of safety, and preference. *Environment and Behavior*, 30(1), 28-59.

Kuyucu, E. (2008), *İnşaat Projelerinde Risk Analizi, Yöntemleri: Bir Petrokimya Fabrikasında Uygulanması*. Yayınlanmamış Yüksek Lisans Tezi, T.C Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir.

Küçükşahin, A. (2006). Güvenlik Bağlamında, Risk ve Tehdit Kavramları Arasındaki Farklar Nelerdir ve Nasıl Belirlenmelidir? *Güvenlik Stratejileri Dergisi,* 4, 7-40.

Lam, J. (2003). *Enterprise Risk Management From Incentives to Controls*. New Jersey: John Wiley & Sons.

Maliye Bakanlığı. (2013). *Kurumsal Risk Yönetimi*, Defterdarlıklar İç Kontrol Eğitim Sunumu, Ankara.

Manab, N. A., Hussin, M. R. & Kassim, I. (2010). Enterprise-Wide Risk Management (EWRM) Practices: Between Corporate Governance Compliance and Value Creation. *International Review of Business Research Papers*, 6(2), 239-252.

Mandacı, P. E. (2003). Türk Bankacılık Sektörünün Taşıdığı Riskler ve Finansal Krizi Aşmada Kullanılan Risk Ölçüm Teknikleri. *Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi,* 5(1), 67-84.

Marchetti, A. M. (2012). *Enterprise Risk Management: From Assessment to Compliance*. New Jersey: John Wiley & Sons.

Mattie, J. A. & Cassidy, D. L. (2008). *Achieving goals, protecting reputation: Enterprise Risk Management for Educational Institutions.* 24.06.2019 tarihinde https://regents.universityofcalifornia.edu/regmeet/july08/a7a.pdf sayfasından erişilmiştir.

Merna, T. & Al-Thani, F. (2008). *Corporate Risk Management.* West Sussex: John Wiley & Sons.

Messier, W. F., Glover, S. M. & Prawitt, D. F. (2008). *Auditing & assurance services: A systematic approach*. New York: McGraw-Hill.

Moeller, R. R. (2011). *COSO enterprise risk management: establishing effective governance, risk, and compliance processes*. New Jersey: John Wiley & Sons.

Mysql Kılavuzu. *Mysql Nedir*. 22.04.2019 tarihinde https://www.mysql.com/why-mysql/ sayfasından erişilmiştir.

Nazir, M. M. & CISA, C. (2011). *Implementation of ERM under COSO Framework*. 20.04.2019 tarihinde http://www.mubashirnazir.org/RM/R0001-ERM-COSO-Framework.pdf sayfasından erişilmiştir.

Olson, D. L. & Wu, D. D. (2010). A review of enterprise risk management in supply chain. *Kybernetes,* 39(5), 694-706.

Ökdemir, Y. & Çelenk, H. (2010). Bankalarda Operasyonel Risk Denetimi Ve Türkiye'de Faaliyet Gösteren Bankalar Üzerine Bir Araştırma. *Maliye ve Finans Yazıları*, 87, 77-111.

Özkan, N. F. & Ulutaş, B. H. (2017). A Novel to Approach to Quantify the Risk Probabilities for a Risk Analysis Methodology. *Advances in Social & Occupational Ergonomics*, 487, 341-347.

Özbilgin, İ. G. (2012). Risk ve Risk Çeşitleri. *Bilişim Dergisi,* 145, 86-93.

Özçelik, A. (2013). *İş sağlığı ve güvenliğinde Fine-Kinney yöntemiyle risk yönetimi: mermer işletmesi örneği*. Yayınlanmamış Yüksek Lisans Tezi, Eskişehir Osmangazi Üniversitesi Fen Bilimleri Enstitüsü. Eskişehir.

Özkılıç, Ö. (2005). *İş Sağlığı ve Güvenliği, Yönetim Sistemleri ve Risk Değerlendirme Metodolojileri.* Ankara: Tisk.

Özsoy, M. T. (2012). Yeni Türk Ticaret Kanunu ve Şirketlerde Kurumsal Risk Yönetimi. *Mali Çözüm Dergisi,* 3, 165-186.

Pehlivanlı, D. (2010). *Modern iç denetim: güncel iç denetim uygulamaları*. İstanbul: Beta.

Pehlivanlı, D. (2008). *Kurumsal Risk Yönetimi Temelli İç Denetim ve Türkiye Uygulamaları*. Yayınlanmamış Doktora Tezi, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli.

Php Kılavuzu. *Php Nedir.* 22.04.2019 tarihinde https://www.php.net/manual/tr/preface.php sayfasından erişilmiştir.

PriceWaterHouseCoopers, (2008). *A Practical Guide to Risk Assessment.* 15.04.2019 tarihinde http://www.pwc.com/en_US/us/issues/enterprise-risk-management/assets/risk_assessment_guide.pdf sayfasından erişilmiştir.

Protiviti Inc. (2006). Enterprise Risk Management: Practical Implementation Advice. *The Bulletin,* 2(6).

PWC. (2006). *Her Yönüyle Kurumsal Risk Yönetimi.* İstanbul: Infomag.

Rausand, M. (2005). Preliminary Hazard Analysis. *Wiley,* 2, 1-36.

Reding, F. K., Sobel, P. J., Anderson, L. U., Head, M. J., Ramamoorti, S., Salamasick, M. & Riddle, C. (2009). *Internal Auditing: Assurance&Consulting Services.* Lake Mary: The IIA Research Foundation.

Risk Management and Control Guidance For Securities Firms and Their Supervisors. (1998). 15.04.2019 tarihinde https://www.iosco.org/library/pubdocs/pdf/IOSCOPD78.pdf sayfasından erişilmiştir.

Rittenberg, L. & Martens, F. (2012). *Understanding and communicating risk appetite. Enterprise risk management.* 18.04.2019 tarihinde https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf sayfasından erişilmiştir.

Safety Management Services inc. (2002). *Proses Hazard Analiysis, Risk Management.* 25.04.2019 tarihinde https://www.smsenergetics.com/risk-management/ sayfasından erişilmiştir.

Saka, T. (2002). Operasyonel Risk Ölçüm Tekniklerine Genel Bir Bakış. *Active Bankacılık ve Finans Dergisi*, 25, 4.

Saka, T. (2008). *Kurumsal Risk Yönetimi ve 2008 Yılı Risk Öngörüleri.* 20.04.2019 tarihinde https://tusiad.org/tr/tum/item/download/2468_47d48b480878ef141e0ded0518703d78 sayfasından erişilmiştir.

Schanfield, A. Miller, M. (2005). A sustainable approach to ERM: as best practices begin to emerge, one company uses a phased plan to create a fully functioning, integrated enterprise risk management system. *Internal Auditor*, 62(2), 79-83.

Seuamsothabandith, S. (2004). An Examination on Enterprise Risk Management. USA: Western Illinois University.

Shenkir, W. G. & Walker, P. L. (2007). Enterprise risk management: Tools and techniques for effective implementation. *Institute of Management Accountants*, 1-31.

Staciokas, R. & Rupsys, R. (2005). Internal audit and its role in organizational government. *Organizaciju Vadyba*, 33, 169-180.

Şardan, H. S. (2004). *İş Sağlığı ve Güvenliğinde Yeni Oluşumlar; Risk Değerlendirmesi ve OHSAS 18001*, Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Şengöz, M. C. & Merdan, M. (2017). Fine-Kinney Risk Analizi Metoduyla, İş Yerlerinde Elektrik Nedenli Yangınların Önlenmesinde Yeni Bir Yöntem. *Gazi Mühendislik Bilimleri Dergisi*, 3 (3), 74-82.

Şimşek, K. Ç. (2007). *Bankacılıkta risk ve risk ölçüm yöntemleri*. Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Tekgül, E. (2007). *Kurumsal Risk Yönetimi ve Risk Zekâsı.* 21.04.2019 tarihinde http://www.denetimnet.net/UserFiles/Documents/Makaleler/%C4%B0%C3%A7%20Denetim/Kurumsal%20Risk%20Yonetimi_Emrah%20Tekgul_ERS.pdf sayfasından erişilmiştir.

The IIA. (2009). *IAA Pozisyon Raporu: İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol*. 21.04.2019 tarihinde https://na.theiia.org/translations/PublicDocuments/PP-The-Role-of-Internal-Auditing-in-Enterprise-wide-Risk-Management-Turkish.pdf sayfasından erişilmiştir.

The Orange Book. (2004). *Management of Risk Priciples and Concepts*. London: HM Treasury.

Thomas, E. M. (2007). The Seven-Step Process to Risk-Based Auditing. *FSA Times*, 1-6.

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

Tüzün, Y. (2002*).* Risk Nedir?. *İç Denetim Dergisi*, 4(Yaz Dönemi), 26-32.

Usul, H. & Mizrahi R. (2016). *Risk Odaklı Denetim*. Ankara: Detay.

Uzun, A. K. (2011). Kurumsal Risk Yönetimi ve İç Denetim. *Önce Kalite Dergisi,* 151(3), 1-4.

Üzer, H. E. (2002). *Risk Yönetiminde Kullanılan Stres Testi Yöntemi*, Sermaye Piyasası Kurulu Yeterlilik Etüdü. Ankara

Vaughan, E. J. & Vaughan, T. (2007). *Fundamentals of Risk and Insurance.* Hoboken: John Wiley & Sons.

Vose, D. (2008). *Risk analysis: a quantitative guide*. West Wessex: John Wiley & Sons.

Wiener, Z. (1999). Introduction to VaR (value-at-risk) Risk management and Regulation in Banking. *Business School, The Hebrew University of Jerusalem*, 12(1), 47-63.

Yalçınkaya, T. (2004). *Risk ve Belirsizlik Algılamasının İktisadi Davranışlara Yansımaları*. Muğla Üniversitesi İktisadi ve İdari Bilimler Fakültesi Tartışma Tebliğleri, No: 2004/05. Muğla.

Yılmaz, A. K. (2007). *Havaalanlarında Kurumsal Risk Yönetimi Atatürk Havalimanı Terminalleri İşletmesi için Kurumsal Risk Yönetimi Model Önerisi*. Yayınlanmamış Doktora Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir.

Yılmaz, B. S. (2000). Hata Türleri ve Etkileri Analizi, *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 2(4), 133-150.

Yüzbaşıoğlu, A. N. (2003). *Risk Yönetimi ve Bankaların Denetimi.* 25.04.2019 tarihinde https://www.tbb.org.tr/Dosyalar/Konferans_Sunumlari/riskmanagementNY.pdf sayfasından erişilmiştir.

ÖZGEÇMİŞ

Kişisel Bilgiler	
Soyadı, Adı	ÖZDEMİR Muhammed
Uyruğu	T.C.
Doğum tarihi ve yeri	25.08.1983 Konya
Medeni hali	Evli
Telefon	0538 245 61 58
e-Posta	muhammedozdemir@windowslive.com

Eğitim Derecesi	Okul / Program	Mezuniyet Yılı
Lise	Konya / Selçuklu İmam Hatip Lisesi	2001
Üniversite	KKTC / Girne Amerikan Üniversitesi Bilgisayar Mühendisliği	2008
Yüksek Lisans	Aksaray Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Bilişim Sistemleri	2019

İş Deneyimi, Yıl	Çalıştığı Yer	Görev
6 Yıl	Konya Valiliği Bilgi İşlem Şb. Md.	Programcı
3 Yıl	İçişleri Bakanlığı Bilgi İşlem Daire Başkanlığı	Programcı
7 Yıl	Özel Sektörde Çeşitli Firmalar	Yazılımcı

Yabancı Dil	İngilizce (İyi Düzeyde)