

ferma



AVRUPA RISK
YÖNETİMİ
DERNEKLERİ
FEDERASYONU

RISK YÖNETİM STANDARTI





Giriş

Risk Yönetim Standardı İngiltere'deki önde gelen risk yönetim organizasyonlarından - The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) ve The National Forum for Risk Management in the Public Sector (ALARM) - oluşan bir ekibin ürünüdür.

Buna ek olarak, kapsamlı bir geliştirme dönemi içerisinde, risk yönetimi ile ilgili diğer profesyonel organizasyonların da görüş ve fikirlerini almıştır.

Risk yönetimi hızla gelişen bir disiplindir ve risk yönetiminin gelişimi, nasıl yapılacağı ve ne için gerekli olduğu konularında birçok ve değişik görüş ve tanım vardır. Aşağıda listelenen konularda fikir birliğinin oluşması için bir standarda ihtiyaç bulunmaktadır:

- *kullanılan kelimelerle ilgili terminoloji*
- *risk yönetiminin yürütülebileceği bir süreç*
- *risk yönetimi için organizasyonel yapı*
- *risk yönetiminin amacı*

Önemli bir husus ise, Standart, riskin hem olumlu hem de olumsuz yönde olduğunu kabul eder.

Risk yönetimi sadece şirketler ve kamu kurumları için olmaktan öte aynı zamanda kısa ya da uzun vadeli herhangi bir faaliyet için de kullanılabilir. Faydalar ve fırsatlar sadece faaliyetin kendi çerçevesinde değil, faaliyetten etkilenebilecek birden fazla ve değişik menfaat sahipleri açısından da incelenmelidir.

Risk yönetimi amaçlarının gerçekleştirilmesi için birçok yol vardır ve bunların hepsini bir belgeye sığdırmaya çalışmak imkansız olacaktır. Bu nedenle, kutuları işaretlemekten ibaret uygulamalara yol açacak sıkı kurallar koyan bir standart geliştirmek ya da sertifikalanabilecek süreçler oluşturmak hiçbir zaman amaçlanılmamıştır. Bu standardın farklı bileşen parçalarının gerçekleştirilmesi ile, her ne kadar farklı yollarla olursa olsun, şirketler uyumu sağladıklarını rapor edebilecek düzeye gelecektir. Standart, şirketlerin kendilerini karşılaştırabilecekleri en iyi uygulamayı göstermektedir.

Standart içerisinde, mümkün olan her yerde The International Organization for Standardization (ISO) tarafından ISO/IEC Guide 73 Risk Management - Vocabulary - Guidelines belgesi ile belirlenmiş terminoloji kullanılmıştır.

Bu alandaki hızlı gelişmeler dikkate alındığında, yazarlar, standardı uygulamaya koyan şirketlerden geri bildirim almaktan memnun olacaktırlar (adresler bu kılavuzun arka kapağında verilmiştir). En iyi uygulamaların ışığında standartta düzenli değişiklikler yapılması öngörülmüştür.



1. Risk

Risk bir olayın olma olasılıđı ile etkilerinin bir birleşimi olarak tanımlanabilir (ISO/IEC Guide 73).

Her türlü girişimde, fayda fırsatlarını (olumlu yönde) ya da başarıyı engelleyecek tehditleri (olumsuz yönde) ortaya çıkartacak olaylar ve sonuçları için potansiyel bulunmaktadır.

Risk Yönetimi, giderek daha sık görülen bir şekilde, riskin hem olumlu hem de olumsuz yanlarıyla ilgilenmektedir. Bu nedenle, bu standart riski her iki açıdan da ele almaktadır.

Güvenlik alanında, etkiler genel olarak sadece olumsuz olarak değerlendirilir ve bu yüzden güvenlik riskinin yönetimi zararın engellenmesi ve hafifletilmesi üzerine odaklanmıştır.

2. Risk Yönetimi

Risk yönetimi herhangi bir organizasyonunun stratejik yönetiminin merkezi bir parçasıdır. Risk yönetimi, şirketlerin, her faaliyetinde ve faaliyetler portföyleri kapsamında sürdürülebilir karı sağlamak amacıyla, faaliyetleri ile ilgili risklerini metodik olarak değerlendirdikleri yönettikleri süreçtir.

İyi risk yönetiminin odađı bu risklerin belirlenmesi ve risk yönetim aksiyonlarının alınmasıdır. Amacı, şirketin bütün faaliyetlerine maksimum sürdürülebilir değeri katmaktır. Risk yönetimi, organizasyonu etkileyebilecek bütün faktörlerin olumlu ve olumsuz potansiyel

eğilimlerinin anlaşılmasını sağlar. Başarı olasılıđını artırır, başarısızlık olasılıđını ve organizasyonun amaçlarına ulaşmasındaki belirsizliđi azaltır. Risk yönetimi, organizasyonun stratejisi çerçevesinde ve bu stratejinin uygulamasında yürütülen sürekli ve gelişen bir süreç olmalıdır. Organizasyonun geçmiş, mevcut ve özellikle gelecek faaliyetlerindeki bütün riskleri metodik olarak ele almalıdır.

Risk yönetimi, en üst yönetim tarafından ortaya konmuş bir politika ve yürütülen bir program dâhilinde organizasyonun kültürü ile bütünleştirilmelidir. Stratejinin, taktiksel ve operasyonel hedeflere dönüştürülmesini, organizasyon içerisindeki tüm yöneticilerin ve çalışanların risk konularında sorumlulukların iş tanımlarının bir parçası haline getirilmesini sağlamalıdır. Risk yönetimi hesap verebilirlik, performans yönetimi ve ödüllendirmeyi destekleyerek her seviyedeki operasyonel etkinliđi artırır.

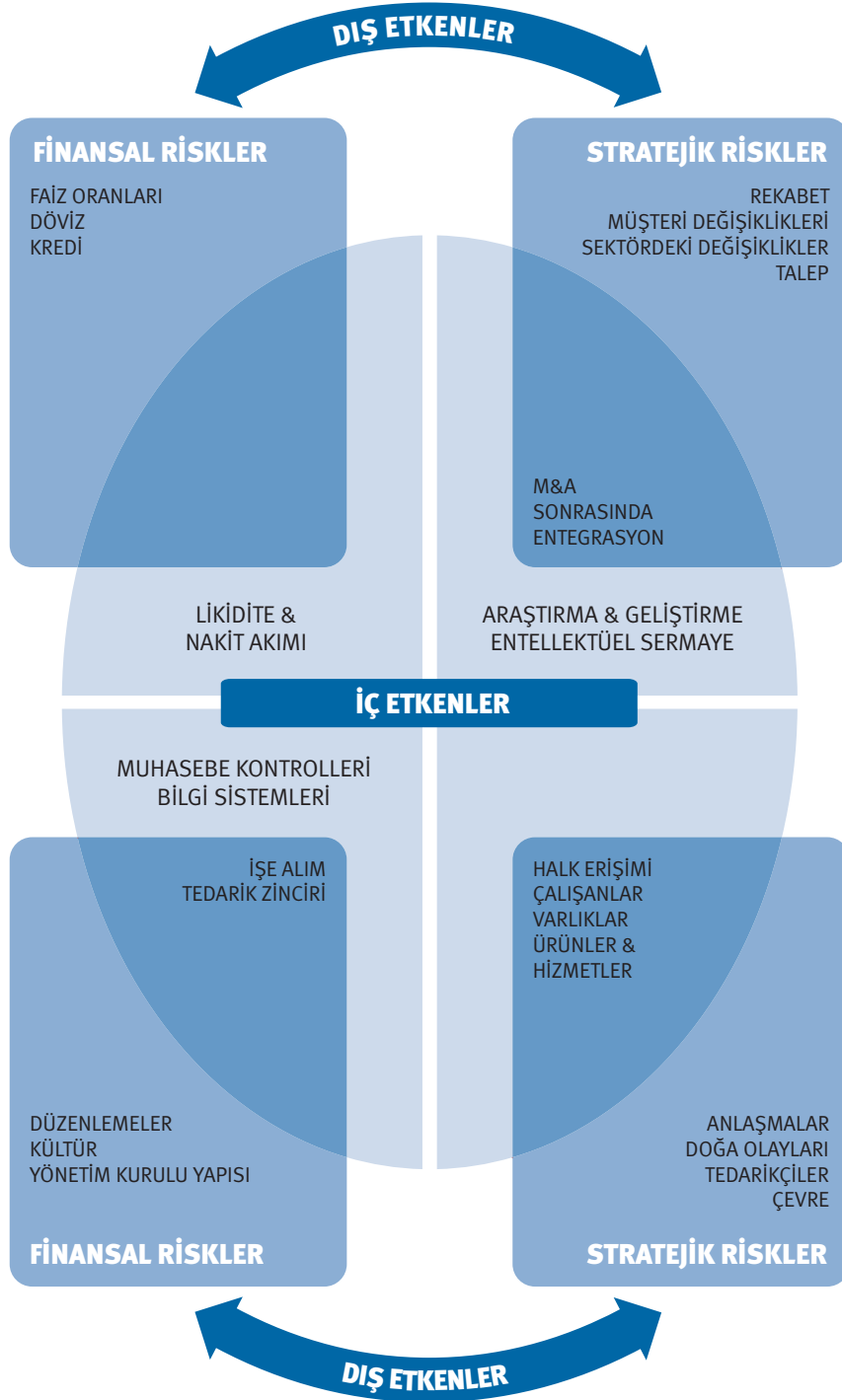
2.1 İç ve Dış Faktörler

Bir organizasyonun ve faaliyetlerinin karşı karşıya kaldıđı riskler hem iç hem de dış faktörlerden kaynaklanabilir.

Diđer sayfadaki diyagram bu alanlardaki ana riskleri özetlemektedir. Bazı riskler hem iç hem de dış nedenlerden oluşmakta ve bu yüzden her iki alanda da gösterilmektedir. Bu riskler stratejik, finansal, operasyonel, zarar v.b. gibi alt kategorilere de ayrılabilirler.



Figure 2.1: Önemli Risklerin Sebeplerine Örnekler





2.2 Risk Yönetimi Süreci



Risk yönetimi aşağıdakilerin sağlanmasıyla organizasyonun hedeflerini destekleyerek, organizasyonun ve menfaat sahiplerinin değerlerini korur ve artırır:

- organizasyona gelecekteki faaliyetlerinin tutarlı ve kontrollü bir şekilde yürütülmesini sağlayan bir çerçeve sunarak
- iş faaliyetlerinin, volatilitenin ve proje fırsatları/tehditlerinin etrafı ve yapısal bir anlayışın oturtulmasıyla karar alma, planlama ve önceliklendirme aşamalarını geliştirerek
- organizasyon içerisinde daha etkin sermaye paylaşımı ve kullanımına katkıda bulunarak
- işin aslı olmayan alanlarındaki volatilitiyi düşürerek
- varlıkları ve şirket imajını koruyarak ve bunları geliştirerek
- organizasyonun bilgi bazını ve çalışanları geliştirip destekleyerek
- operasyonel etkinliği en uygun seviyeye getirerek



3. Risk Değerlendirmesi

Risk Değerlendirmesi, ISO/ IEC Guide 73 belgesinde risk analizi ve risk değerlemenin genel süreci olarak tanımlanmıştır. (Bkz: Ek)

4. Risk Analizi

4.1 Riskin Belirlenmesi

Riskin belirlenmesi, bir organizasyonun belirsizliğe olan maruziyetini tanımlamayı amaçlar. Bu amaç, organizasyonu, faaliyette bulunduğu pazarı, bulunduğu yasal, sosyal, politik ve kültürel ortamı yakından tanımayı gerektirir. Bununla birlikte, organizasyonun stratejik ve operasyonel amaçları, başarısını etkileyen kritik faktörler ve bu amaçlara ulaşmakta etkili olacak tehdit ve fırsatlar iyi bir şekilde anlaşılmalıdır.

Riskin belirlenmesi, organizasyon içerisindeki bütün önemli faaliyetlerin ve bu faaliyetlerden ortaya çıkan risklerin belirlendiğinden emin olunması için metodik bir yaklaşım ile yürütülmelidir.

Bu faaliyetlerle ilişkili tüm volatilite belirlenmeli ve sınıflandırılmalıdır.

İş faaliyetleri ve kararları birçok şekilde sınıflandırılabilir. Örneğin :

- *Stratejik – Bu grup organizasyonun uzun vadeli stratejik amaçları ile ilgilidir. Sermaye yeterliliği, politik risk, yasa ve düzenleme değişiklikleri, itibar ve fiziksel çevredeki değişiklikler bu gruptaki iş faaliyetlerini etkileyebilir.*
- *Operasyonel – Bu grup organizasyonun stratejik amaçlarını gerçekleştirmeye çalışırken karşısına çıkan günlük konuları içermektedir.*
- *Finansal – Bu grup organizasyonun mali durumunun etkin bir şekilde yönetimi ve kontrol edilmesi, kredi, döviz kurları, faiz oranlarının hareketi gibi dış faktörlerin etkileri ile ilgilidir.*

- *Bilgi yönetimi – Bu grup bilgi kaynaklarının etkin yönetimi ve kontrolü, bilginin üretimi, korunması ve iletişimi ile ilgilidir. Fikri mülkiyetin izinsiz kullanımı ya da suistimali, güç kaybı ve rekabetçi teknoloji dış faktörler arasında sayılabilir. Sistemdeki aksaklıklar ya da kilit personelin işten ayrılması iç faktörler arasında sayılabilir.*
- *Uyum – Bu grup sağlık ve güvenlik, çevre, ticaret tanımları, müşterinin korunması, verilerin korunması, iş tutumu ve düzenleme konuları gibi sorunlarla ilgilidir.*

Riskin belirlenmesi dış danışmanlar tarafından da yapılabileceği gibi, tutarlı ve iyi düzenlenmiş süreçler ve araçlar (Bkz: Ek) kullanılarak organizasyon içerisinde yürütülmesi yaklaşımının daha etkili olması daha olasıdır. Risk yönetim sürecinin organizasyon içerisinde “sahiplenilmesi” gereklidir.

4.2 Risk Tanımlanması

Risk tanımlanmasının amacı, belirlenmiş risklerin yapısal bir formatta, örneğin bir tablo yardımıyla, gösterilmesidir. Bir sonraki sayfadaki risk tanımlama tablosu risklerin tanımlanması ve değerlendirilmesine yardımcı olmak için kullanılabilir. Kapsamlı bir risk belirleme, tanımlama ve değerlendirme süreci için iyi tasarlanmış bir yapı gereklidir. Tabloda listelenen her bir riskin olasılık ve etkisi göz önünde bulundurularak daha detaylı bir şekilde incelenmesi gereken ana riskler önceliklendirilebilir. İş faaliyetleri ve karar alma ile ilgili risklerin belirlenmesi, stratejik, proje/taktik ve operasyonel gibi sınıflara ayrılabilir. Projenin kavram aşaması süresince ve de özel bir projenin bütün aşamalarında risk yönetiminin sürece dâhil edilmesi önemlidir.



4.2.1 Tablo - Risk Tanımı

1. Riskin İsmi	
2. Riskin Kapsamı	Olayların niteliksel tanımı, boyutları, tipi, sayısı ve olaylara bağımlı durumlar
3. Riskin Niteliği	Örnek: Stratejik, operasyonel, finansal, bilgi veya uyum
4. Menfaat Sahipleri	Menfaat sahipleri ve beklentileri
5. Riskin Ölçülmesi	Önem derecesi ve Olasılık
6. Risk Toleransı /Risk Alma İsteği Seviyesi	Kayıp potansiyeli ve riskin finansal etkisi Riske maruz değer (Value at Risk) Potansiyel kayıp/kazançların olasılık ve boyutları Riskin kontrolü için amaç(lar) ve istenilen performans seviyesi
7. Risk Yönetim Aksiyonu ve Kontrol Mekanizması	Riskin mevcut durumda yönetildiği ana yöntemler Mevcut kontrole duyulan güven seviyesi İzleme ve gözden geçirme için protokollerin belirlenmesi
8. Gelişim için Potansiyel Aksiyon	Riskin azaltılması için öneriler
9. Strateji ve Politika Geliştirme	Strateji ve politika geliştirmeden sorumlu fonksiyonun belirlenmesi

4.3 Risk Tahmini

Risk tahmini, olma olasılığı ve olası etkiler açısından kantitatif, yarı kantitatif ya da kalitatif olabilir.

Örneğin, tehditler (olumsuz eğilimli riskler) ve fırsatlar (olumlu yönde riskler) açısından etkiler yüksek, orta ya da düşük olabilir (Bkz 4.3.1). Olasılık, yüksek, orta ya da düşük olabilir ancak tehditler ve fırsatlar açısından değişik tanımlar gerektirmektedir (Bkz Tablo 4.3.2 ve 4.3.3).

Bir sonraki tabloda örnekler listelenmiştir. Farklı organizasyonlar, ihtiyaçlarına en iyi cevabın farklı etki ve olasılık ölçüleri tarafından verildiğini görecektir.

Örneğin, birçok organizasyon etki ve olasılığın yüksek, orta ve düşük şeklinde değerlendirilmesini ve bunların 3'e 3 bir matrisle gösterilmesini kendi ihtiyaçları için oldukça yeterli bulmaktadır.

Diğer organizasyonlar etki ve olasılığın 5'e 5 bir matrisle gösterilmesiyle daha iyi bir değerlendirme çalışması yapıldığını düşünmektedir.

**4.3.1 Tablo: Etki – Tehdit ve Fırsatlar**

Yüksek	Organizasyondaki finansal etki £x miktarını geçme eğiliminde Organizasyonun stratejisi ve operasyonel faaliyetleri üzerine önemli etki Menfaat sahiplerinin kayda değer endişesi
Orta	Organizasyondaki finansal etki £x ve £y miktarlarının arasında olma eğiliminde Organizasyonun stratejisi ve operasyonel faaliyetleri üzerine orta seviyede etki Menfaat sahiplerinin makul seviyede endişesi
Düşük	Organizasyondaki finansal etki £y miktarından az olma eğiliminde Organizasyonun stratejisi ve operasyonel faaliyetleri üzerine orta seviyede etki Menfaat sahiplerinin düşük seviyede endişesi

4.3.2 Tablo: Olma Olasılığı – Tehditler

Tahmin	Tanım	Gösterge
Yüksek (Olası)	Her yıl olabilir ya da olma olasılığı %25'ten yüksek.	Zaman dilimi içerisinde (örneğin 10 yıl) birçok defa olma potansiyeli var. Son zamanlarda meydana geldi.
Orta (Olası)	10 yıllık bir zaman diliminde olabilir ya da olma olasılığı %25'ten düşük.	Zaman dilimi içerisinde (örneğin 10 yıl) bir defadan fazla meydana gelebilir. Bazı dış olaylar nedeniyle kontrol etmek zor olabilir. Olay kaydı var mı?
Düşük (Düşük olasılık)	10 yıllık bir zaman diliminde olma olasılığı yok ya da olma olasılığı %2'den düşük.	Henüz oluşmadı. Olması muhtemel değil.



4.3.3 Tablo: Olma Olasılığı – Fırsatlar

Tahmin	Tanım	Gösterge
Yüksek (Olası)	Olumlu sonuç bir yıl içerisinde olabilir ya da olma olasılığı %75'ten yüksek.	Mevcut yönetim süreçleri dâhilinde kısa vadede gerçekleşeceğine makul bir kesinlikle güvenilen açık fırsatlar.
Orta (Olası)	Olumlu sonucun bir yıl içerisinde gerçekleşme ihtimali %25 ile %75 arasında.	Ulaşılabilecek ancak dikkatli yönetim gerektiren fırsatlar. Planın dışında ortaya çıkabilecek fırsatlar.
Düşük (Düşük olasılık)	Olumlu sonuç orta vadede elde edilebilir ya da olma olasılığı yok ya da olma olasılığı %25'ten düşük.	Yönetim tarafından etraflıca araştırılması gereken olası fırsat. Mevcut durumda kullanılan yönetim kaynakları itibarıyla başarılı olma olasılığı düşük olan fırsat.

4.4 Risk Analizi Yöntem ve Teknikleri

Riskleri incelemek için birçok teknik kullanılabilir. Bu teknikler sadece olumlu ya da sadece olumsuz eğilimleri incelemek için olabileceği gibi her iki türde riski incelemek için de kullanılabilir. (Bkz. Ek).

4.5 Risk Profili

Risk analizi sürecinden elde edilen sonuç, her riske önemlilik derecesi atamak ve risk yönetim aksiyonu çalışmalarını önceliklendirmek için bir araç sağlayan bir risk profili yaratmak üzere kullanılabilir. Bu çalışma, göreceli önem

seviyeleri hakkında bir fikir vermek için belirlenen her riski sıralamak için kullanılacaktır.

Bu süreç, riskin etkilenen iş alanı ile ilişkilendirilmesini, uygulamada olan öncelikli kontrol prosedürlerinin tanımlanmasını ve de risk kontrol yatırımlarının artırılması, düşürülmesi ya da yeniden yapılandırılması gereken alanların belirlenmesini sağlar.

Hesap verilebilirlik riskin sahiplenilmesine ve uygun kaynakların sağlanmasına yardımcı olur.



5. Risk Değerlemesi

Risk analizi süreci tamamlandıktan sonra, tahmin edilen risklerin organizasyonun belirlediği risk kriterleri kullanılarak karşılaştırılması gereklidir. Risk kriterleri ilgili fayda ve maliyetleri, yasal gereksinimleri, sosyo-ekonomik ve çevresel faktörleri, menfaat sahiplerinin endişelerini kapsayabilir. Bu nedenle, risk değerlendirme, risklerin organizasyon için önem derecesi ve her bir riskin kabul edilmesi ya da uygun aksiyonun alınması konularında karar vermek üzere kullanılır.

6. Risk Yönetim Aksiyonu

Risk yönetim aksiyonu riskin değiştirilmesi için ölçülerin seçilmesi ve uygulanması sürecidir. Risk yönetim aksiyonunun ana ögesi risk kontrolü/azaltmasıdır. Ancak, bununla birlikte, riskin görmezden gelinmesi, risk transferi ve riskin finansmanı gibi unsurları da içerir.

NOT: Bu standartta risk finansmanı, riskin finansal etkilerinin finanse edilmesi için gerekli mekanizmaları (ör: sigorta programları) temsil etmektedir. Risk finansmanı, genel olarak, risk yönetim aksiyonunu (ISO/IEC Guide 73'te tanımlandığı şekilde) uygulamak için ayrılan masraf karşılığını olarak düşünülmemektedir.

Herhangi bir risk yönetim aksiyonu en az şunları içermelidir:

- organizasyonun etkin ve verimli operasyonu
- etkin iç kontroller
- yasalar ve düzenlemelere uyum

Risk analizi süreci, yönetimin dikkatini gerektiren riskleri belirleyerek organizasyonun etkin ve verimli operasyonuna katkıda bulunur. Risk kontrol aksiyonlarının organizasyona olan potansiyel yararı göz önünde bulundurularak önceliklendirilmesi gereklidir.

İç kontrol etkinliği, riskin önerilen kontrol ölçüleri ile azaltılması ya da tamamen ortadan kaldırılmasının derecesini belirler.

İç kontrollerin maliyet etkinliği, kontrolün uygulama maliyetinin riskin azaltılmasından beklenen yararlarla karşılaştırılması ile belirlenir.

Önerilen kontroller, hiçbir aksiyonun alınmadığı durumdaki potansiyel ekonomik yarar ile önerilen aksiyonun maliyeti karşılaştırılarak ölçülmelidir. Genel olarak, bu ölçümün yapılması için mevcut bilgi ve varsayımlardan daha detaylı bilgilere ihtiyaç duyulur.

İlk olarak, uygulamanın maliyeti belirlenmelidir. Bu maliyet ilerde maliyet verimliliği hesapları için taban değer olarak kullanılacağından hesaplamalarda kesinlik faktörüne önem verilmelidir. Hiçbir aksiyon alınmadığı durumlarda ortaya çıkacak olan maliyet de hesaplanmalıdır. Bu sonuçları karşılaştırarak yönetim kontrol ölçülerinin uygulanıp uygulanmaması yönünde karar alabilir.

Yasa ve düzenlemelerle uyum bir seçim değildir. Bir organizasyon uygulanabilir kanunları anlamalı ve uyumu sağlamak için bir kontroller sistemi uygulamalıdır. Sadece bazı durumlarda riskin azaltılmasının maliyetinin risk ile tamamen oransız olması, bazı esnekliklere sebep olabilir.

Risklerin etkilerine karşı finansal açıdan korunmanın bir yolu da sigortayı da kapsayan risk finansmanı yöntemidir. Ancak, bazı kayıpların ya da bir kaybın bazı kısımlarının sigorta yapılmaya uygun olmayabileceği unutulmamalıdır. Örneğin, organizasyonun itibarını ve çalışanların moralini etkileyebilecek işle ilgili sağlık, güvenlik ve çevre ile ilgili kazaların maliyetleri sigortalanmaya uygun değildir.



7. Risk Raporlama ve İletişim

7.1 İç Raporlama

Bir organizasyon içerisindeki değişik seviyeler, risk yönetimi süreci içinde farklı bilgilere ihtiyaç duyarlar.

Yönetim Kurulu,

- organizasyonun karşılaştığı en önemli riskleri bilmeli,
- beklenen performans değerlerindeki değişimin hissedar değeri üzerindeki olası etkilerini bilmeli,
- organizasyon içerisinde uygun bir bilinirlik düzeyi sağlamalı,
- organizasyonun bir krizi nasıl yöneteceğini bilmeli,
- menfaat sahiplerinin organizasyona olan güvenlerinin önemini kavramalı,
- yatırım camiası ile iletişimin nasıl yönlendirileceğini bilmeli,
- risk yönetimi sürecinin etkin bir şekilde yürütüldüğünden emin olmalı,
- risk yönetimi felsefesi ve sorumluluklarını kapsayan açık bir risk yönetim politikası yayımlamalıdır.

İş Birimleri,

- kendi sorumluluk alanlarına giren risklerden, bu risklerin diğer alanlardaki olası etkilerinden ve diğer alanların kendi alanlarına etkilerinden haberdar olmalı,
- kritik iş süreçleri ve finansal faaliyetleri izlemek, amaçlara yaklaşmak ve müdahale gerektiren gelişmeleri (örneğin tahmin ve bütçeler) belirlemek için performans göstergelerini belirlemeli,

- aksiyon alınmasını sağlayan sıklıkta bütçe ve tahminlerdeki değişiklikleri iletişime geçiren bir sistemleri olmalı,
- yeni farkına varılan riskleri ya da mevcut kontrol ölçülerinin herhangi bir hatasını anında ve sistematik bir şekilde üst yönetime bildirmelidirler.

Bireyler,

- bireysel riskler için hesap verebilmeli,
- risk yönetiminin sürekli gelişimini nasıl sağlayabileceklerini anlamalı,
- risk yönetimi ve riskleri tanımanın bir organizasyonun kültürü için ne kadar önemli olduğunu anlamalı,
- yeni farkına varılan riskleri ya da mevcut kontrol ölçülerinin herhangi bir hatasını anında ve sistematik bir şekilde üst yönetime bildirmelidirler.

7.2 Dış Raporlama

Bir şirket, risk yönetimi politikaları ve amaçlarına ulaşmadaki verimliliği hakkında menfaat sahiplerini düzenli bir şekilde bilgilendirmelidir.

Menfaat sahipleri, bir organizasyonda, kamu işleri, insan hakları, işçi hakları, sağlık ve güvenlik ve çevre konuları gibi finansal olmayan konuların etkin yönetiminin sağlanıp sağlanmadığına artan bir şekilde önem vermektedir.

İyi bir kurumsal yönetim, şirketlerin risk yönetimine metodik bir yaklaşımın benimsenmesini gerektirir. Risk yönetimi :

- menfaat sahiplerinin çıkarlarını korur



- *yönetim kurulu'nun organizasyonun performansını izleme, değer sağlama ve strateji belirleme görevlerini yerine getirdiğini doğrular*
- *yönetim kontrollerinin uygun bir şekilde uygulanmasını sağlar*

Risk yönetiminin resmi olarak raporlamasına yönelik düzenlemeler açık bir şekilde belirlenmeli ve menfaat sahiplerinin erişimine açık olmalıdır.

Resmi raporlama aşağıdakileri içermelidir:

- *kontrol metodları – özellikle yönetimin risk yönetimi sorumlulukları*
- *riskleri belirlemede kullanılan süreçler ve bunların risk yönetimi sistemleri tarafından nasıl ele alınacağı*
- *önemli riskleri yönetmekte kullanılan başlıca kontrol sistemleri*
- *uygulamadaki izleme ve gözden geçirme sistemi*

Sistemin içermediği her türlü önemli aksaklık ve bu aksaklıkları gidermek için atılan adımlar birlikte rapor edilmelidir.

8. Risk Yönetiminin İdaresi ve Yapısı

8.1 Risk Yönetimi Politikası

Bir organizasyonun risk yönetimi politikası riske yaklaşımını, risk alma isteğini ve risk yönetimine yaklaşımını içermelidir. Politika, organizasyon çapında risk yönetimi için sorumlulukları da belirtmelidir.

Ayrıca, örneğin sağlık ve güvenlik v.b. politika bildirimleri için olan yasal gereksinimleri de kapsamalıdır.

Risk yönetimi süreçlerini uygulamak, iş süreçlerinin farklı evrelerinde kullanılacak araç ve tekniklerinin kullanılmasıdır.

Bir risk yönetimi sürecinin etkin çalışması için aşağıdakilere ihtiyacı vardır:

- *organizasyonun idari yönetiminin ve CEO'sunun desteğini*
- *organizasyon içerisinde sorumlulukların belirlenmesini*
- *bütün menfaat sahiplerinin riskler konusundaki farkındalıklarının geliştirilmesi ve bu konuda eğitim verilmesi için gerekli kaynağın ayrılmasını.*

8.2 Yönetim Kurulunun Rolü

Kurul, organizasyonun stratejik yönelimini belirlemeden ve etkin operasyon için risk yönetimi yapılarının ve ortamının kurulmasından sorumludur.

Bu görev idari bir grup, idari olmayan bir komite, bir denetim komitesi veya risk yönetimini 'sponsor' edebilecek ve organizasyonun faaliyetlerine uyan diğer bir fonksiyon aracılığıyla yürütülebilir.

Kurul, iç kontrol sistemini değerlendirirken en azından şu hususları göz önünde bulundurmalıdır:

- *Şirketin kendi iş alanında kabul edilebilir olan olumsuz risklerin yapısı ve boyutu*
- *Bu tip risklerin gerçekleşme olasılığı*
- *Kabul edilemeyen risklerin nasıl yönetilmesi gerektiği*
- *Şirketin iş üzerindeki etki ve olasılığı indirmedeki başarısı*
- *Kontrol faaliyeti ve riskin maliyet ve yararı*
- *Risk yönetimi sürecinin etkinliği*
- *Kurul kararlarının risk yaptırımları.*



8.3 İş Birimlerinin Rolü

Bu rol aşağıdakileri içerir:

- günlük risklerin yönetiminden iş birimleri sorumludur
- iş birimi yönetimi faaliyet alanlarında risk bilinirliğini artırmaktan sorumludur: iş alanlarına risk yönetimi amaçlarını adapte etmelidirler
- risk yönetimi, maruz kalınan risklerin gözden geçirilmesi ve etkin risk yönetimi analizi aracılığı ile işlerin tekrar önceliklendirilmesi için olağan bir toplantı konusu olmalıdır
- iş birimi yönetimi risk yönetiminin projelerin tasarım aşamasıyla beraber bütün süreç boyunca uygulanmasını sağlamalıdır

8.4 Risk Yönetiminin Rolü

Fonksiyon:

Organizasyonun boyutuna bağlı olarak, risk yönetimi fonksiyonu tek bir çalışan, yarı-zamanlı bir risk yöneticisi ya da bir risk yönetimi bölümünün sorumluluğunda yürütülebilir.

Risk Yönetimi fonksiyonu şunları içermektedir:

- risk yönetimi için politika ve strateji belirlemek
- stratejik ve operasyonel seviyede risk yönetiminin öncelikli savunucusu olmak
- organizasyon içerisinde bir risk kültürü oturtmak ve uygun eğitimi sağlamak
- iş birimleri için dahili risk politika ve yapılarını belirlemek

- risk yönetimi süreçlerini tasarlamak ve gözden geçirmek
- organizasyon içerisindeki risk yönetimi konularında etkisi olan çeşitli fonksiyonel faaliyetlerin koordinasyonunu sağlamak
- acil durum ve iş devamlılığı planlarını da içeren süreçleri geliştirmek
- kurul ve menfaat sahipleri için risk raporları hazırlamak.

8.5 İç Denetimin Rolü

İç denetimin rolü organizasyondan organizasyona değişiklik gösterebilir.

Uygulamada, iç denetimin görevleri arasında aşağıdakilerden bazıları veya hepsi bulunur:

- yönetim tarafından belirlenen önemli risklere odaklanmak ve organizasyon çapında risk yönetim sürecini denetlemek
- risk yönetiminin yapıldığını doğrulamak
- risk yönetim sürecine aktif olarak katılmak ve bu süreci desteklemek
- risk tanımlama/değerlendirme süreçlerini kolaylaştırmak ve personeli risk yönetimi ve iç kontrol konularında eğitmek
- kurul ve denetim komitesine verilen risk raporlarını koordine etmek

İç denetim, bir organizasyon için en uygun rolü belirlerken, tarafsızlık ve bağımsızlık ilkelerinin profesyonel gereklerinin uygulandığından emin olmalıdır.



8.6 Kaynaklar ve Uygulama

Organizasyonun risk yönetim politikasını uygulamak için gerekli kaynaklar risk yönetiminin her seviyesinde ve her iş biriminde açık bir şekilde belirlenmelidir.

Risk yönetimi sürecine katılan birimlerin, diğer operasyonel fonksiyonlarının yanında, risk yönetimi politikası/stratejisi koordinasyonu görevleri açıkça tanımlanmalıdır. Aynı şekilde, denetim ve iç kontrollerin gözden geçirilmesi ile risk yönetim sürecinin kolaylaştırılması görevleri de açık bir şekilde tanımlanmalıdır.

Risk yönetimi strateji ve bütçe süreçleri yoluyla organizasyon içerisine eklenmelidir. Uygulamaya alma ve diğer tüm eğitim ve gelişimlerde ve ayı zamanda operasyonel süreçler içerisinde, örneğin ürün/servis geliştirme projeleri, vurgulanmalıdır.

9. Risk Yönetimi Sürecinin İzlenmesi ve Gözden Geçirilmesi

Etkin risk yönetimi, risklerin etkin bir şekilde tanımlanması ve ele alınması ve uygun kontrol ve cevapların uygulamada olması için bir raporlama ve gözden geçirme yapısına ihtiyaç duyar. İlerleme fırsatlarının belirlenmesi için politika ve standartların düzenli denetimi

yapılmalı ve standartların performansları gözden geçirilmelidir. Organizasyonların dinamik olduğu ve dinamik ortamlarda faaliyet gösterdikleri unutulmamalıdır. Organizasyondaki değişiklikler ve faaliyette bulunulan ortam belirlenmeli ve sistemde uygun değişiklikler yapılmalıdır.

İzleme süreci, organizasyonun faaliyetlerine uygun kontrollerin kullanılmasını ve prosedürlerin anlaşılması ve takip ediliyor olmasını sağlamalıdır. Organizasyondaki değişiklikler ve faaliyette bulunulan ortam belirlenmeli ve sistemde uygun değişiklikler yapılmalıdır.

İzleme ve gözden geçirme süreçleri aynı zamanda şu konulara açıklık getirir:

- *uygulanan ölçülerin istenilen sonuçlara ulaşım sağlayacağı*
- *değerlendirmeyi yapabilmek için uygulanan prosedürlerin ve toplanan bilginin uygun olup olmadığı*
- *geliştirilmiş bilginin daha iyi kararlar almaya yardımcı olup olmayacağı ve gelecekteki değerlendirmeler ve risk yönetimi çalışmalarını için hangi derslerin çıkarılacağı*



10. Ekler

Risk Tanımlama Teknikleri – Örnekler

- *Beyin fırtınası*
- *Soru formu*
- *Her iş sürecini dikkate alan bu süreçleri etkileyebilecek iç ve dış faktörleri tanımlayan iş araştırmaları*
- *Sektör kıyaslama*
- *Senaryo analizi*
- *Risk değerlendirme çalışmaları*
- *Olay incelemeleri*
- *Denetleme ve inceleme*
- *HAZOP (Hazard & Operability Studies)*

Risk Analizi Metotları ve Teknikleri – Örnekler

Olumlu Risk

- *Pazar araştırması*
- *Beklentiler*
- *Deneme pazarlama*
- *Araştırma ve geliştirme*
- *İş etkisi analizi*

Olumlu ve Olumsuz Risk

- *Bağımlılık modellemesi*
- *SWOT analizi (Güçlü noktalar, Zayıf noktalar, Fırsatlar, Tehditler)*
- *Olay ağacı analizi*
- *İş devamlılık planı*
- *BPEST (İş, Politik, Ekonomik, Sosyal, Teknolojik) analizi*
- *Reel opsiyon analizi*
- *Risk ve belirsizlik ortamında karar alma*
- *İstatistiksel analizler*
- *Merkezi eğilim ve dağılım ölçüleri*
- *PESTLE (Politik Ekonomik Sosyal Teknik Yasal Çevre)*

Olumsuz Risk

- *Tehdit analizi*
- *Hata ağacı analizi – FTA (Fault tree analysis)*
- *Hata Biçim ve Etki Analizi - FMEA (Failure Mode & Effect Analysis)*



AGERS - Asociación Española de Gerencia de Riesgos y Seguros
Príncipe de Vergara, 86 - 1ª Esc., 2º Izda.- 28006 Madrid - SPAIN
Tel: + 34 91 562 84 25 – Fax: + 34 91 590 07 80 – Email: gerencia@agers.es – www.agers.es



AIRMIC - The association of Insurance and Risk Managers
Lloyd's Avenue, 6 – London EC3N3AX - UK
Tel: + 44 207 480 76 10 – Fax: + 44 207 702 37 52 – Email: enquiries@airmic.co.uk – www.airmic.com



AMRAE - Association pour le Management des Risques et des Assurances de l'Entreprise
Avenue Franklin Roosevelt, 9-11 – 75008 Paris - FRANCE
Tel: + 33 1 42 89 33 16 – Fax: + 33 1 42 89 33 14 – Email: amrae@amrae.fr – www.amrae.fr



ANRA - Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali
Via del Gonfalone 3, I-20123 Milano - ITALY
Tel: + 39 02 58 10 33 00 – Fax: + 39 02 58 10 32 33 – Email: anra@betam.it – www.anra.it



APOGERIS - Associação Portuguesa de Gestão de Riscos e Seguros
Avenida da Boavista, 1245, 3a Esq. – 4100-130 Porto – PORTUGAL
Tel: + 351 22 608 24 62 – Fax: + 351 22 608 24 73 – E-mail: anfernandes@sonae.pt – www.apogeris.pt



ASPAR CR - Association of Insurance and Risk Management of the Czech Republic o.s.
Nad Ohradou 7 – 13000 Praha 3 – Tel: + 420 602 384 256 – Email: asparcr@volny.cz



BELRIM - Belgian Risk Management Association
Rue Gatti de Gamond, 254 – 1180 Bruxelles - BELGIUM
Tel: + 32 2 389 23 95 – Fax: + 32 2 389 22 72 – Email: info@belrim.com – www.belrim.com



bfv - Bundesverband firmenverbundener Versicherungsvermittler und -Gesellschaften e.V.
c/o Mr Hans-Otto GEIGER – Postfach 1916 – D-67209 Frankenthal – GERMANY
Tel: + 49 6233 86 2507 - Fax: + 49 6233 86 2507 - Email: hans-otto.geiger@ksb.com – www.bfv-fvv.de



BRIMA - Bulgarian Risk Management Association
101, Tzarigradsko chaussee, floor 4 – Sofia 1113 – BULGARIA
Tel: + 359 878 100292 – Fax: + 359 2 971 0702 – Email: office@brima.biz – www.brima.biz



DARIM - DI's Risk Management Forening
DK-1787 Copenhagen – DENMARK
Tel: + 45 33 77 33 77 – Fax: + 45 33 77 33 00 – Email: darim@di.dk – www.di.dk



DVS - Deutscher Versicherungs-Schutzverband e.V.
Breite Strasse 98 - D 53111 Bonn - GERMANY
Tel: + 49 228 98 22 30 - Fax: + 49 228 63 16 51- Email: dvs@dvs-schutzverband.de – www.dvs-schutzverband.de



FINNRIMA - Finnish Risk Management Association
Talvikkitie 40 A 33, 01300 Vantaa – FINLAND
Tel: + 358 9 5607 5361 – Fax: + 358 9 5607 5365 – Email: srhy@hennax.fi – www.srhy.fi



NARIM - Nederlandse Associatie van Risk en Insurance Managers
P.O. Box 65707 - 2506 EA Den Haag – THE NETHERLANDS
Tel: + 31 70 345 7426 – Fax: + 31 70 427 3263 – Email: ielsdewild@imfo.nl – www.narim.com



POLRISK - Polish Risk Management Association
ul. Rzymowskiego 30 lok. 424 - 02-697 Warszawa - POLAND
Tel: + 48 22 331 8121 – Fax: + 48 22 331 81 22 – Email: info@polrisk.pl – www.polrisk.pl



RUSRISK - Russian Risk Management Society
Address Expert Institute, Staraya Ploshchad 10/4, Moscow, 103070 – RUSSIA
Tel: + 7 495 231 53 56 - Fax: + 7 495 231 53 56 - Email: info@rrms.ru – www.rrms.ru



SIRM - Swiss Association of Insurance and Risk Managers
Gutenbergstrasse 1, Postfach 5464, CH-3001 Bern - SWITZERLAND
Tel: + 41 31 388 87 89 – Fax: + 41 31 388 87 88 – Email: info@sirm.ch – www.sirm.ch

SWERMA - Swedish Risk Management Association
Gränsvägen 15 - SE-135 47 Tyresö - SWEDEN
Tel: + 468 742 13 07 - Fax: + 468 798 83 11- E-mail: info@swerma.se – www.swerma.se

ALARM - The National Forum for Risk Management in the Public Sector
Queens Drive, Exmouth - Devon, EX8 2AY
Tel: + 44 1395 223399 - Fax: + 44 1395 223304 - Email: admin@alarm.uk.com - www.alarm-uk.com



IRM - The Institute of Risk Management
6 Lloyd's Avenue - London EC3N 3AX
Tel: + 44 20 7709 9808 - Facsimile + 44 20 7709 0716 - Email: enquiries@theirm.org - www.theirm.org