Risklere Dayanıklı Kurumun Oluşturulması: Kurumsal Risk Yönetimi Eğitimi

23 Haziran 2022

pwc

Eğitim Programı

OAİB
ORTA ANADOLU
İHRACATÇI BİRLİKLERİ

14:00 – 15:10

Risk ve Kurumsal Risk Yönetimine Yönelik Temel Kavram ve Tanımlar

Kurumsal Risk Yönetimine Yönelik Uluslararası Çerçeveler

Kurumsal Risk Yönetimi Metodolojisi (Risklerin Belirlenmesi, Değerlendirilmesi, Önceliklendirilmesi, Risk Kararlarının Verilmesi, Risklerin İzlenmesi ve Raporlanması)

15:10 – 15:20

Eğitim Arası

15:20 – 16:20

Mevzuat Çerçevesinde Kurumsal Risk Yönetimi

Kurumsal Risk Yönetiminde Sorumluluklar

Kurumsal Risk Yönetiminde Kritik Başarı Faktörleri

16:20 – 16:30

Soru Cevap

Risk?

Risk…

"risk ≠ sorun"

Risk…

Kurumun **stratejisini ve amaçlarını** gerçekleştirmesini etkileyecek olayların **gerçekleşme olasılığı**dır.

COSO

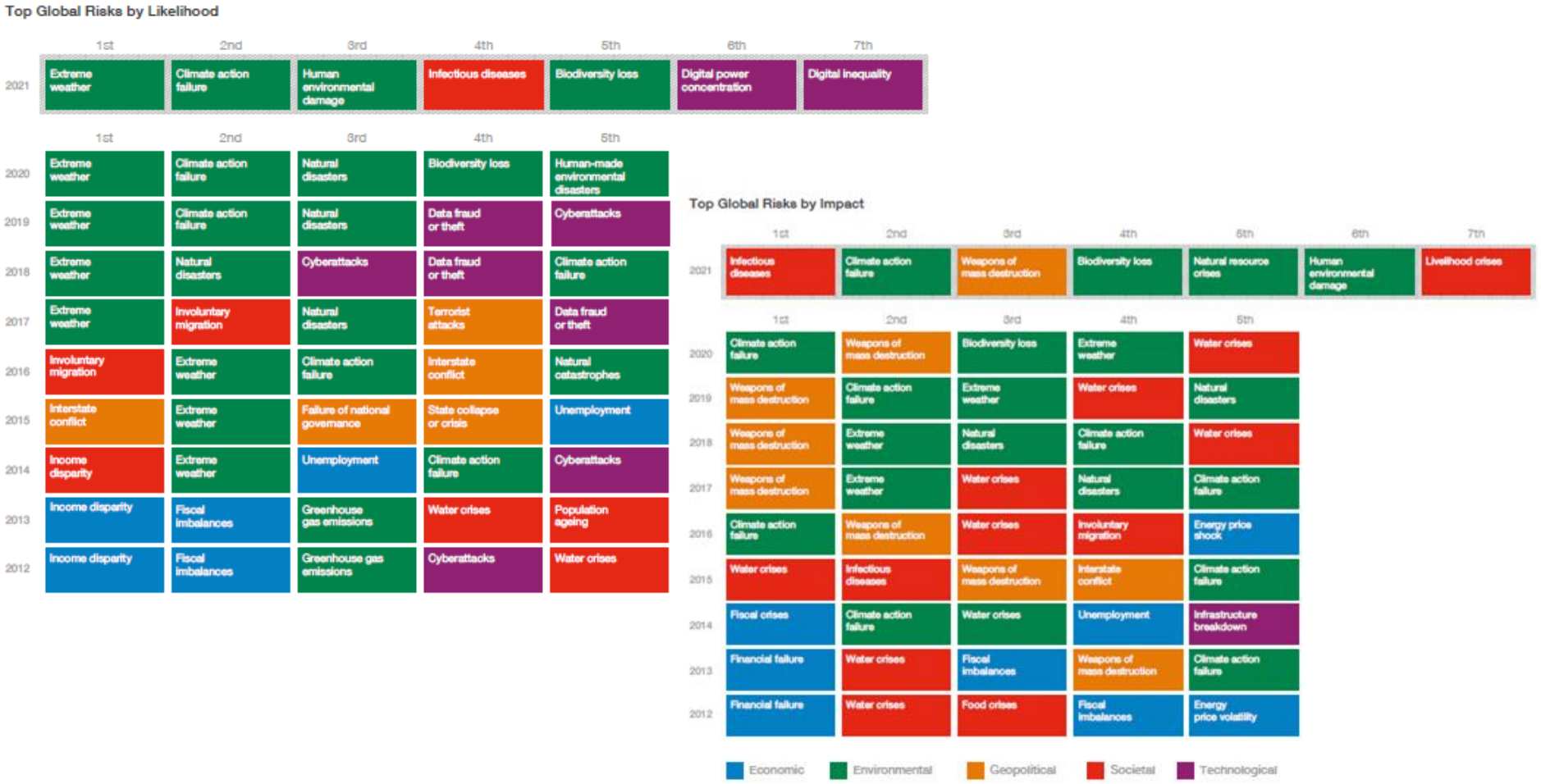
Belirsizliğin hedefler üzerine olan **etkisidir**.

ISO 31000 Risk Yönetimi Standartı

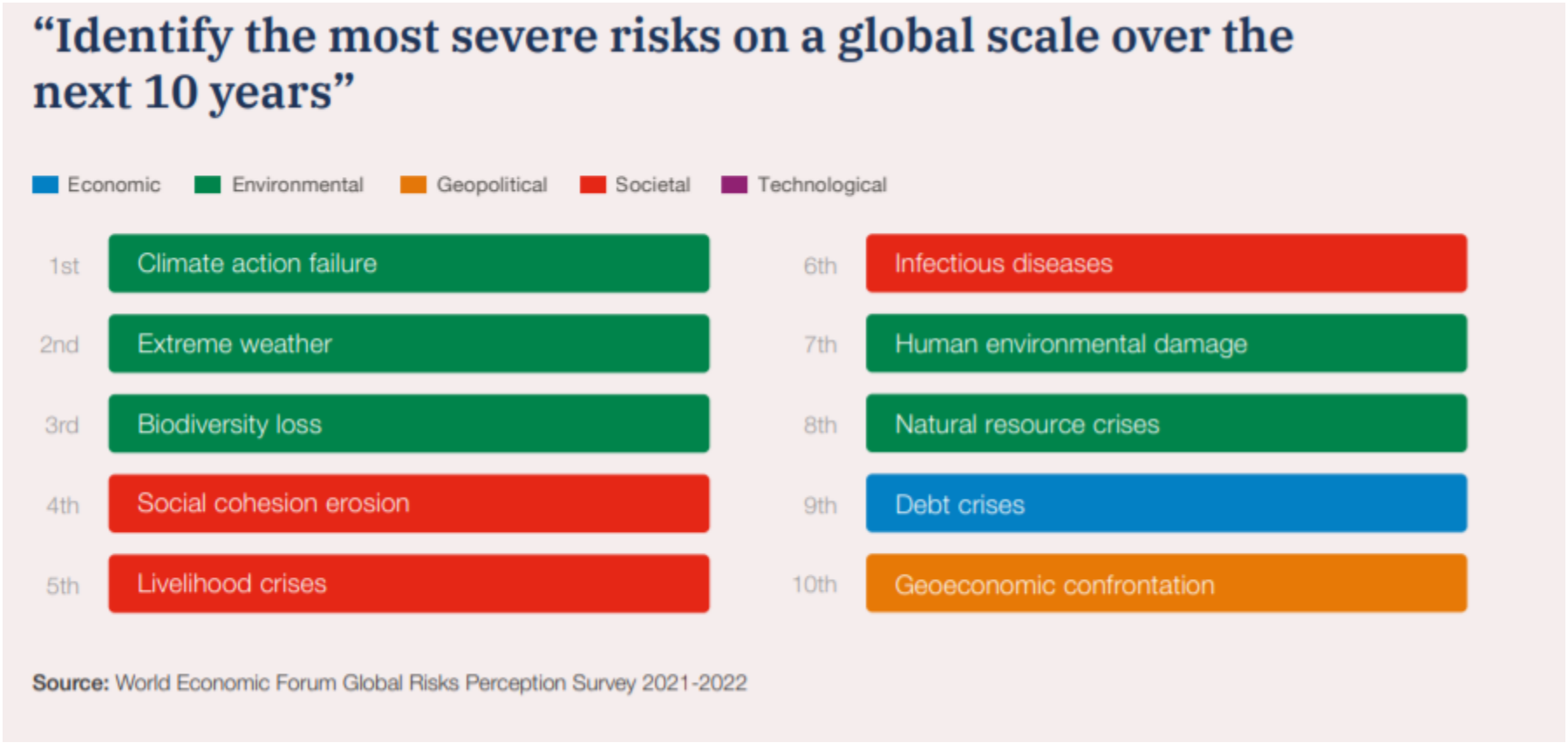
Birlikte düşünelim…

Bugüne kadar aldığınız en **büyük** risk?

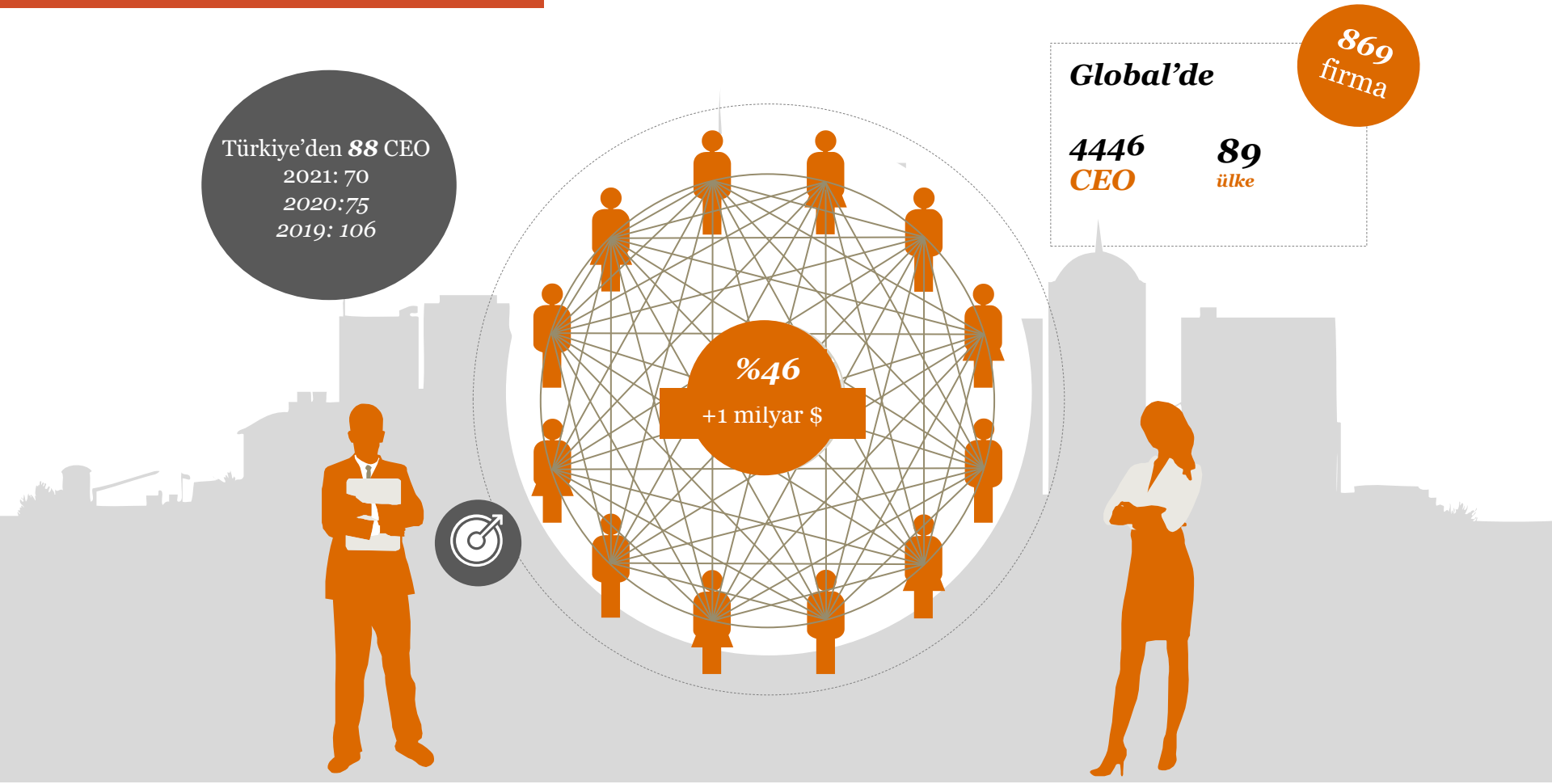
Global Riskler - Risk Dağılımları 2012 - 2021



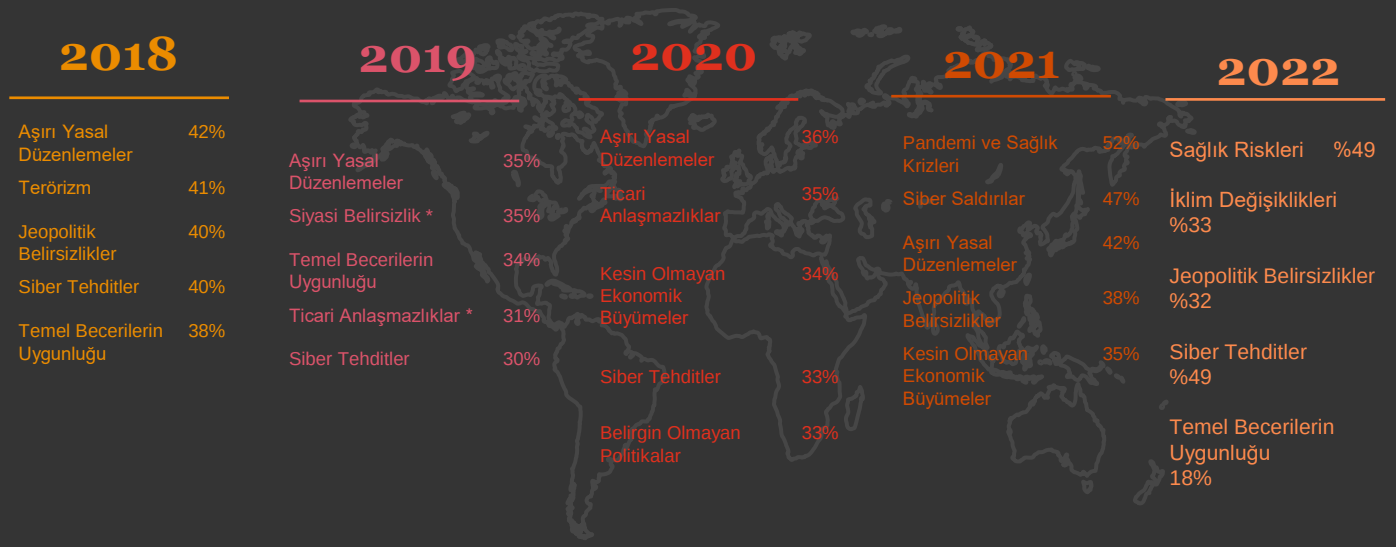
Risk Dağılımları 2021



25. Küresel CEO Araştırması



CEO’ların gözüyle büyümeyi tehdit eden faktörler (Global)



2018

Aşırı Yasal Düzenlemeler	42%
Terörizm	41%
Jeopolitik Belirsizlikler	40%
Siber Tehditler	40%
Temel Becerilerin Uygunluğu	38%

2019

Aşırı Yasal Düzenlemeler	35%
Siyasi Belirsizlik *	35%
Temel Becerilerin Uygunluğu	34%
Ticari Anlaşmazlıklar *	31%
Siber Tehditler	30%

2020

Aşırı Yasal Düzenlemeler	36%
Ticari Anlaşmazlıklar	35%
Kesin Olmayan Ekonomik Büyümeler	34%
Siber Tehditler	33%
Belirgin Olmayan Politikalar	33%

2021

Pandemi ve Sağlık Krizleri	52%
Siber Saldırılar	47%
Aşırı Yasal Düzenlemeler	42%
Jeopolitik Belirsizlikler	38%
Kesin Olmayan Ekonomik Büyümeler	35%

2022

- Sağlık Riskleri %49
- İklim Değişiklikleri %33
- Jeopolitik Belirsizlikler %32
- Siber Tehditler %49
- Temel Becerilerin Uygunluğu 18%

Kaynak: PwC, 25th Annual Global CEO Survey

CEO’ların gözüyle büyümeyi tehdit eden faktörler (Türkiye-2022)

Kaynak: PwC, 25th Annual Global CEO Survey

88 CEO

Birlikte düşünelim…

Şirketinizin aldığı büyük risk?

Risk…

Şirketinizde aşağıdaki fonksiyonlarda / rollerde risk nasıl tanımlanırdı?

- Satın Alma
- Bilgi Teknolojileri
- İnsan Kaynakları
- Genel Müdür
- Finans / Muhasebe
- Yönetim Kurulu

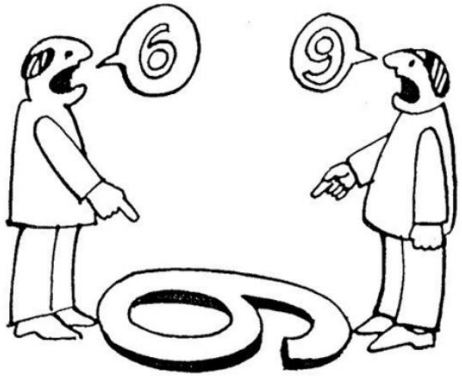
Biraz nostalji…

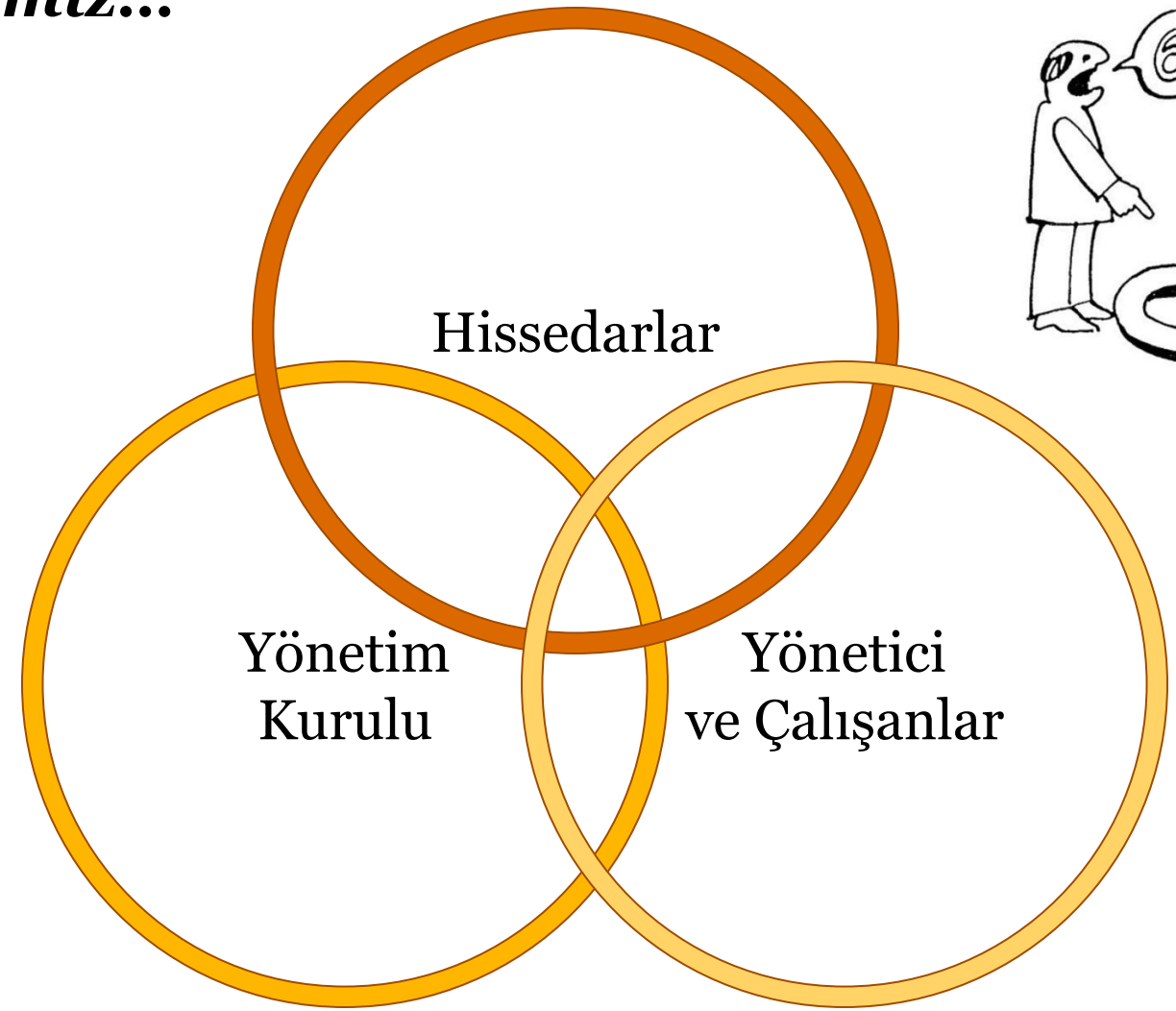
Hepimizin risk alma isteği aynı mı?

*Sırada **önde** mi olurdunuz, **arkada** mı?*

En kritik risklerimiz ve yönetme şeklimiz…

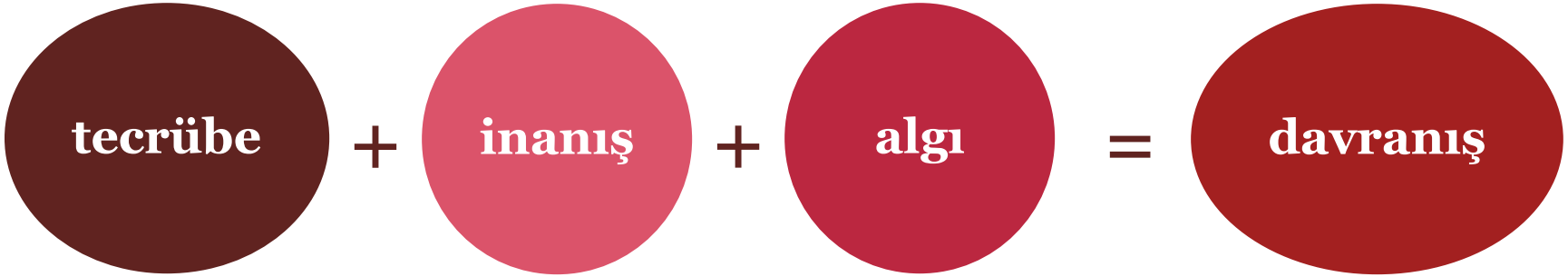
Hepimiz aynı algıda mıyız?





En kritik risklerimiz ve yönetme şeklimiz…

Davranışsal risk yönetimi



Politikalar
Prosedürler
Süreçler & Yapılar
Metodolojiler
Sistem

Değerler
Hedefler
Davranışlar
Bağlılık
İletişim

Risk Kültürü

En önemli hedef…

Risk farkındalığını arttırmak

Ortak risk algısı oluşturmak

Risklere yönelik ortak refleks geliştirmek

Risk yönetimi?

Kurumsal risk yönetimi…

kültür

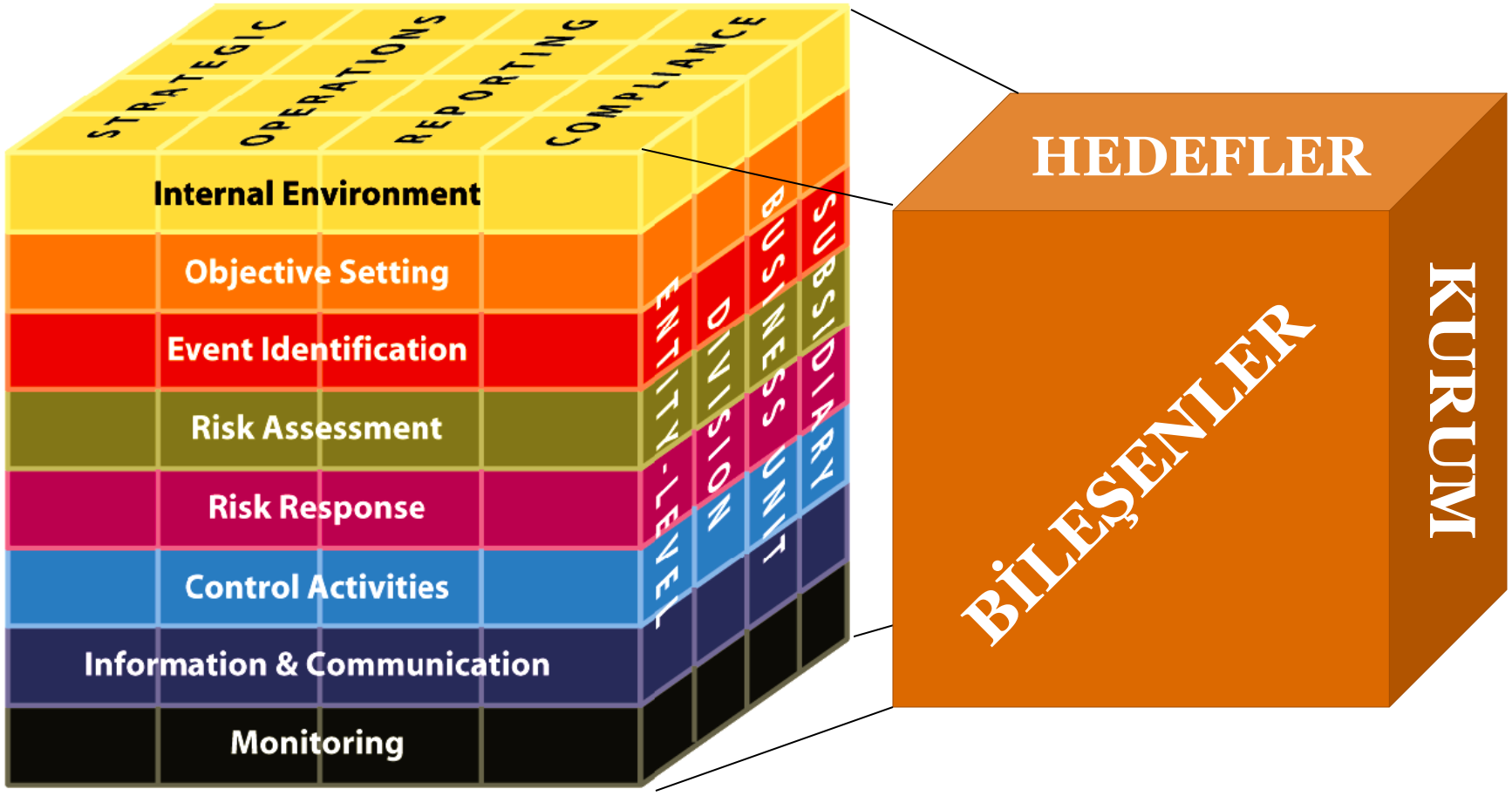
değer yaratma

uygulamalar

> Kurumların **değer yaratma** ve söz konusu **değeri koruma** amacıyla, **strateji belirleme ve performans yönetimi süreçlerine entegre ettikleri risk kültürü** ve **risk yönetimi uygulamalarıdır.**
>
> **COSO KRY Çerçevesi**

strateji performans risk entegrasyonu

COSO kurumsal risk yönetimi çerçevesi (2004)



COSO kurumsal risk yönetimi çerçevesi (2017)

Yönetişim & Kültür	Strateji & Hedef Belirleme	Performans	Gözden Geçirme & Düzeltme	Bilgi, İletişim & Raporlama
1. Yönetim kurulu risk gözetimini yerine getirir.	6. İş ortamını analiz eder.	10. Riskleri belirler.	15. Önemli değişimleri değerlendirir.	18. Bilgi ve teknoloji avantajlarından yararlanır.
2. Operasyonel yapıyı oluşturur.	7. Risk iştahını tanımlar.	11. Riskleri segmente eder.	16. Riskleri ve performansı gözden geçirir.	19. Risk bilgisinin iletişimini yapar.
3. Arzu edilen kültürü tanımlar.	8. Alternatif stratejileri değerlendirir.	12. Riskleri önceliklendirir.	17. Kurumsal risk yönetiminde iyileştirmeleri takip eder.	20. Risk, kültür ve performans hakkında raporlama yapar.
4. Temel değerlere bağlılık gösterir.	9. İş hedeflerini oluşturur.	13.Risk cevaplarını uygular.		
5. Yetenekli personeli çeker, geliştirir ve elde tutar.		14. Portföy bakış açısı geliştirir.		

COSO kurumsal risk yönetimi çerçevesi (2017)

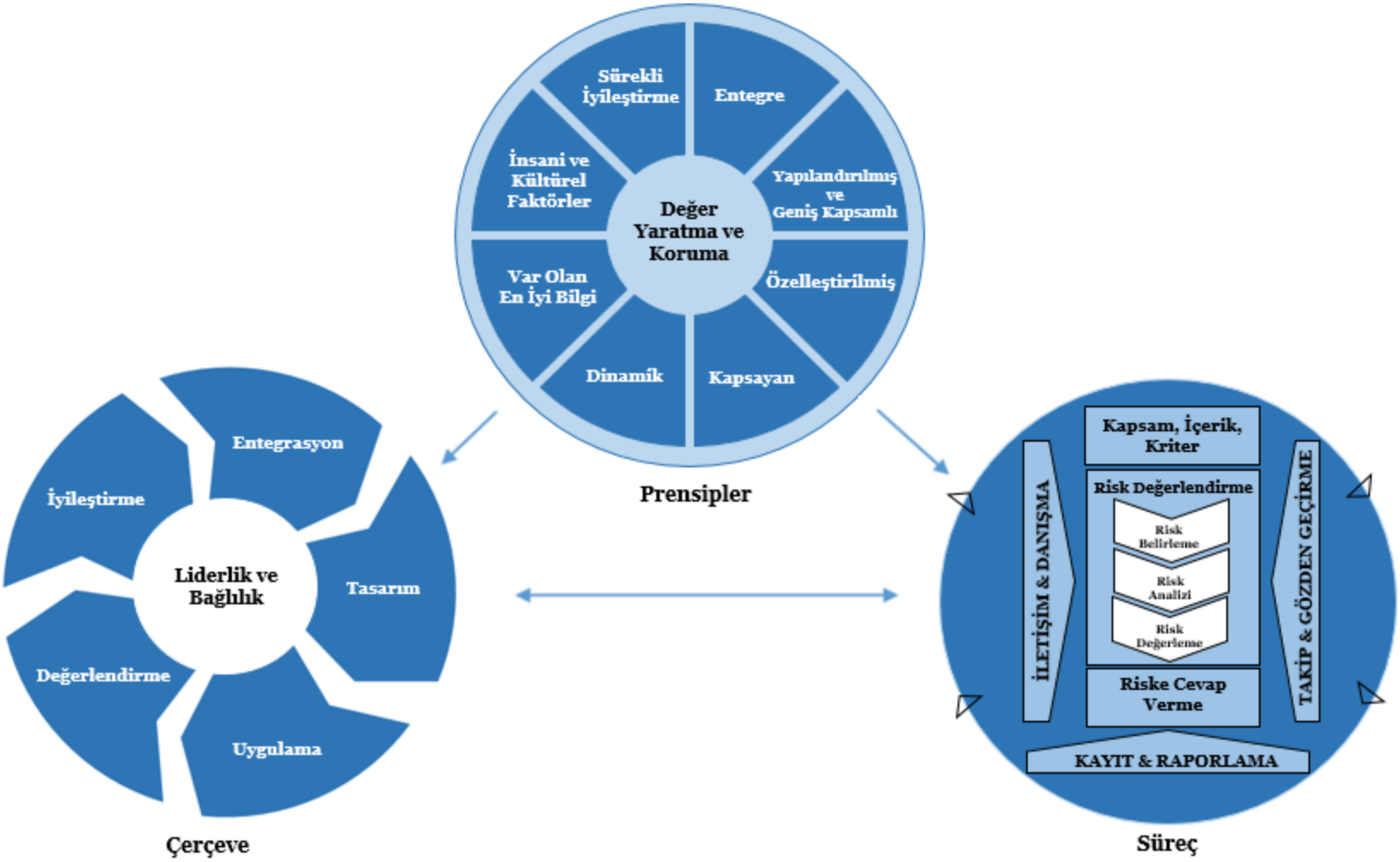
Stratejik planlamayı desteklemesi

Performansa odaklanması

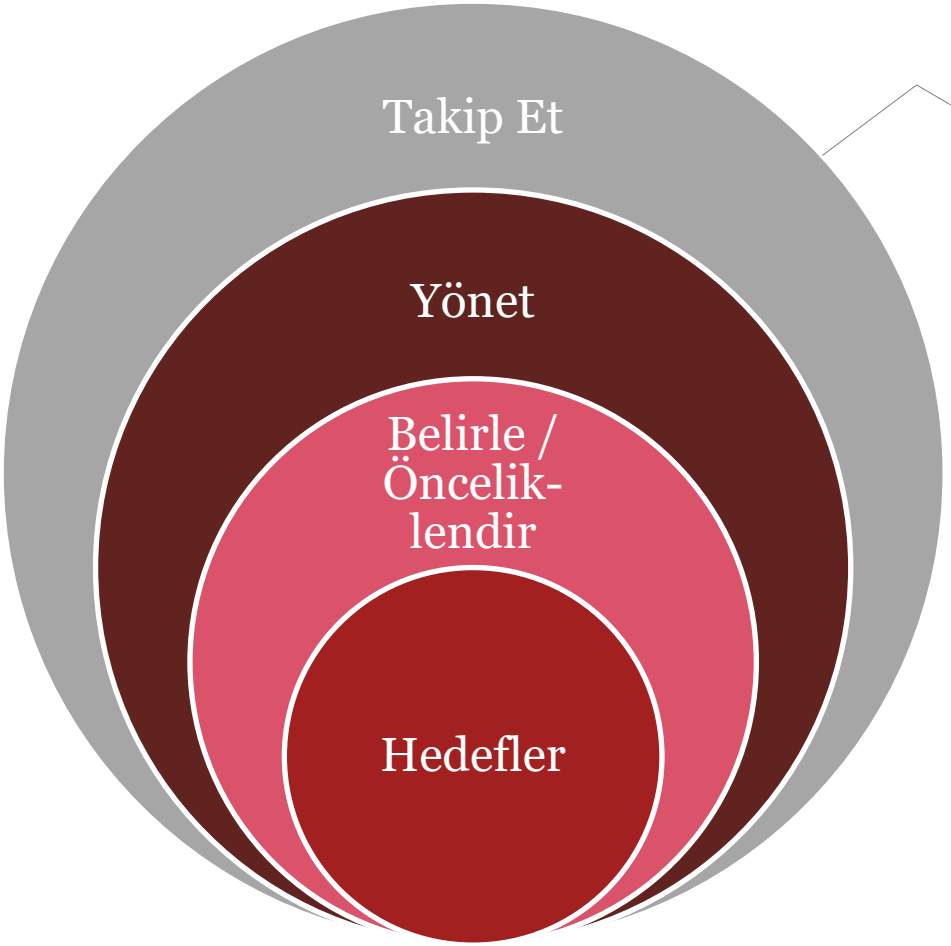
Karar alma süreçlerine entegre edilmesi (Kültür)

İç kontrolü desteklemesi

ISO 31000 standardı (2009 - 2018)



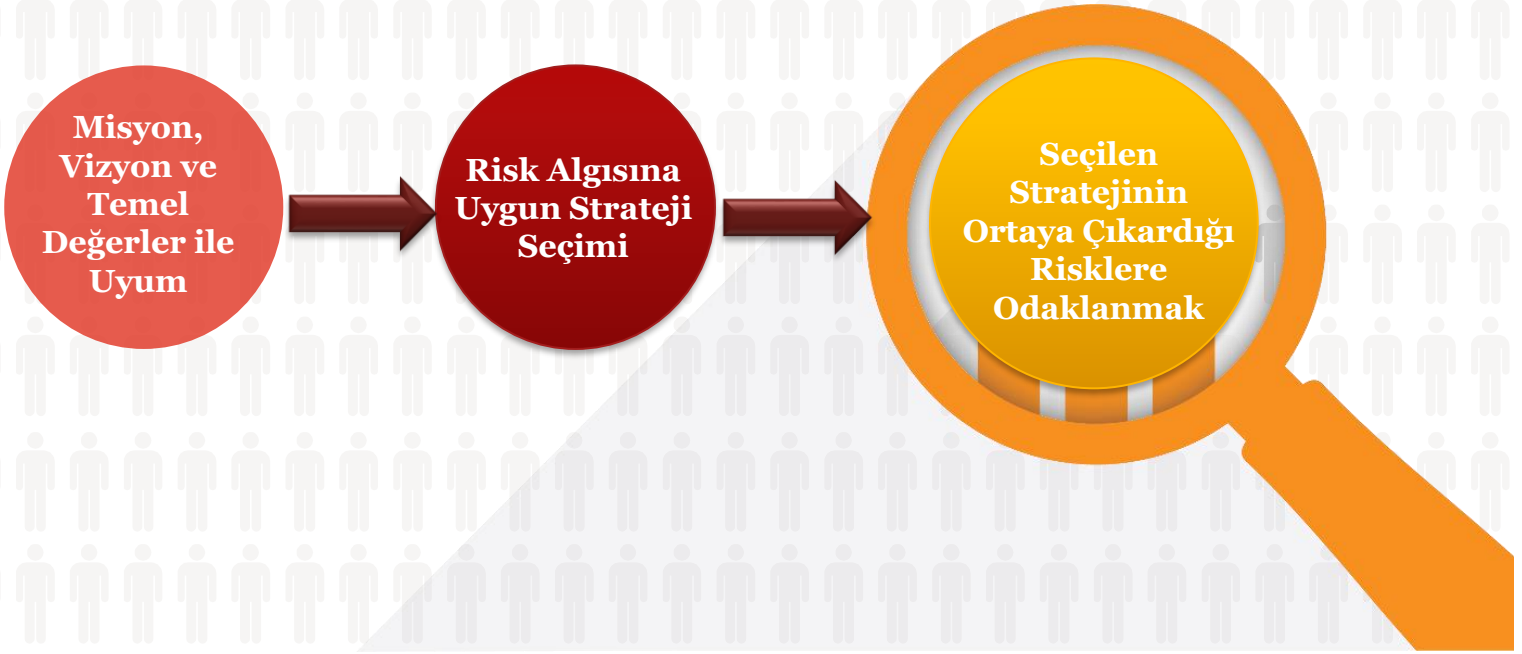
Yaklaşımlardaki ortak nokta



Tüm kurumsal risk yönetimi çerçevelerinin özündeki mantık …

Kurumsal risk yönetimi ve kurumun stratejisi…
Amaç, Hedef ve Risk

Risk yönetiminin stratejik planlama ve hedeflerle ilişkisi, amaç ve hedeflerin **'belirlenmeden önce'**, **'belirleme aşamasında'** ve **'belirlendikten sonraki'** tüm aşamalarını kapsayacak şekilde aşağıda detayları belirtilen 3 ana yaklaşım üzerinde kurgulanır.



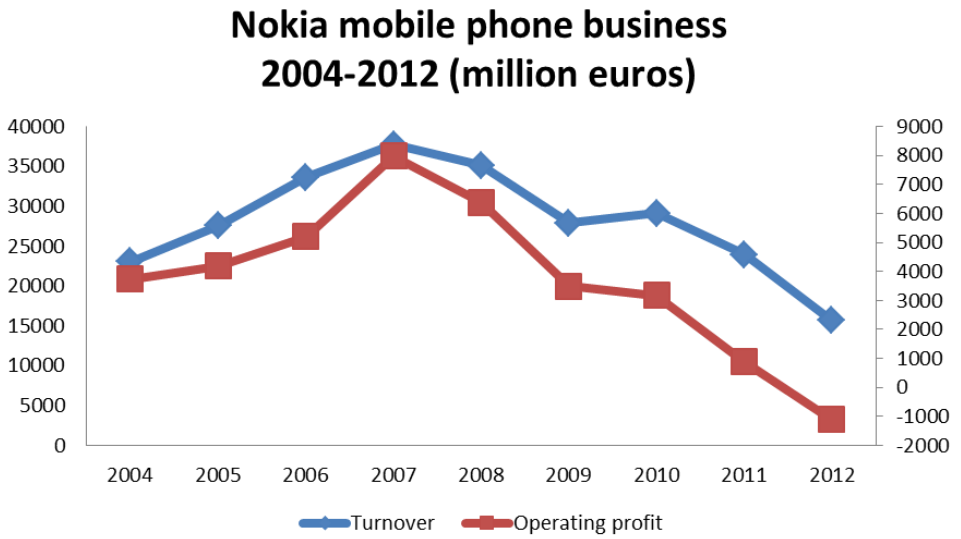
Kurumsal risk yönetiminin önemi – bir örnek

1 *Global değişim trendlerini izleyememek*

2 *Riskleri doğru tanımlayamamak (fırsat & tehdit)*

3 *Piyasa ve rakip analizlerini etkin yürütmemek*

4 *Önleyici kontrol mekanizması algısından uzaklaşmak*



Kurumsal risk yönetimi adımları

Risklerin belirlenmesi:

Kurumun hedeflerine ulaşmasını engelleyebilecek durumlar nelerdir?

Risklerin analiz edilmesi:

Risklerin etkisi ve gerçekleşme olasılığı nedir?

Risklere yönelik olarak uygulanan kontrollerin etkinlik durumu nedir?

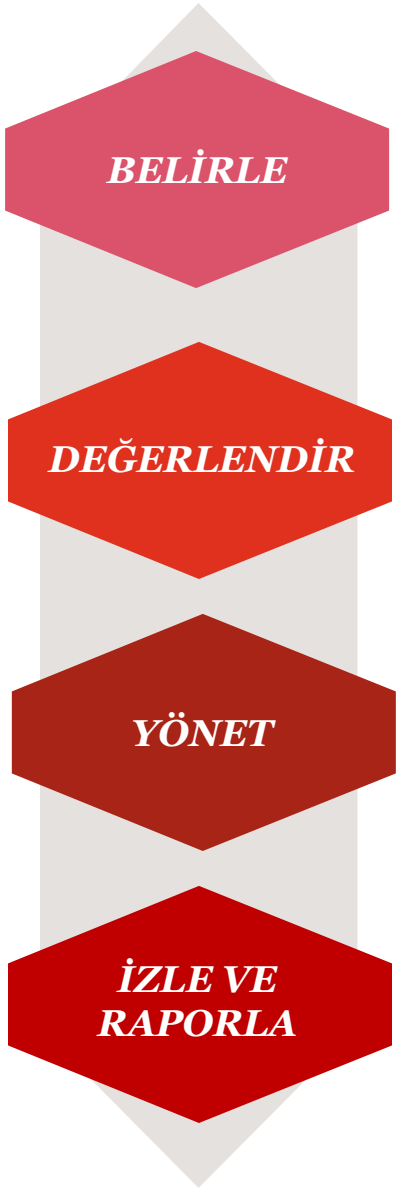
Öncelikli riskler hangileridir?

Risk yönetimi kararlarının verilmesi:

Kaynaklarımla riskleri nasıl yönetirim?

Risklerin izlenmesi ve raporlanması:

Şirkete, Üst Yönetime ve paydaşlara değer katacak risk bilgisi nedir?



Riskler ne kadar öngörülebilir?

Bildiğimizi
bildiğimiz...

Bilmediğimizi
bildiğimiz...

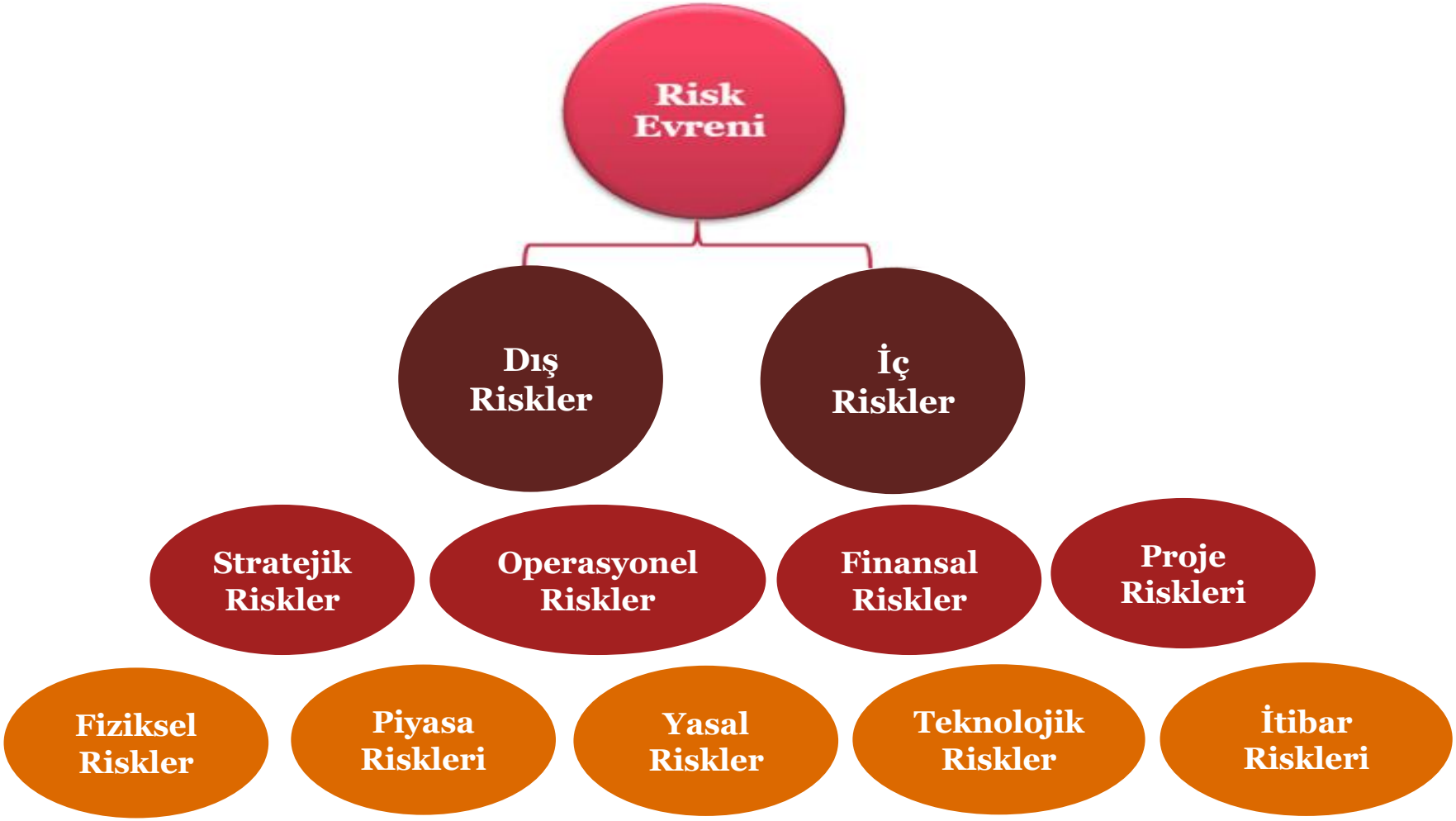
Bilmediğimizi
bilmediğimiz...

Dayanıklılık

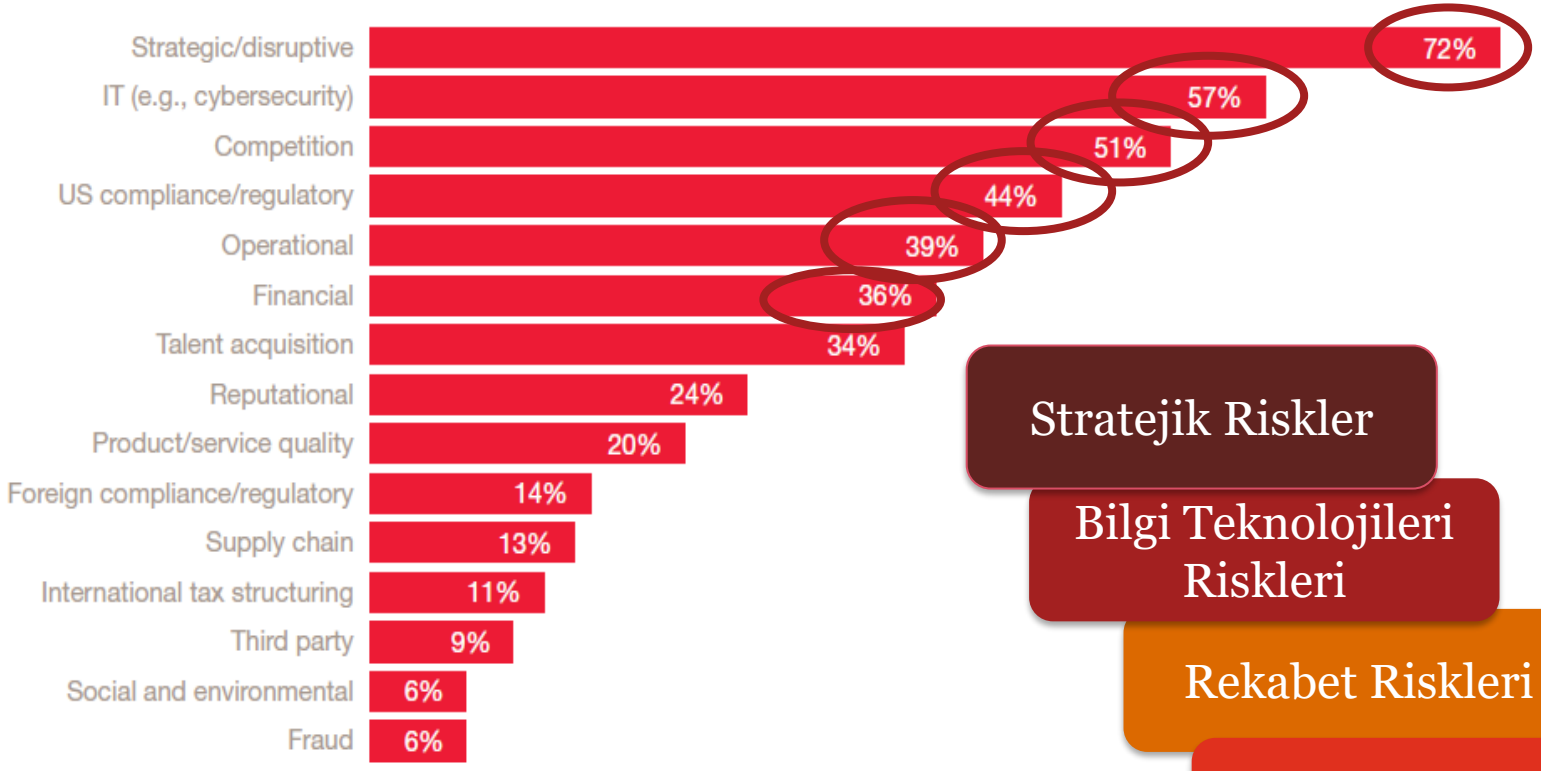
1

Riskleri Belirle

Riskleri nerede arayalım?



Yönetim Kurulu'nun gözetiminde en çok zorlandığı riskler…



Stratejik Riskler

Bilgi Teknolojileri Riskleri

Rekabet Riskleri

Uyum Riskleri

Kaynak: PwC Annual Corporate Directors Survey

Risk nasıl tanımlanır?

Veri Güvenliği

RİSK TANIMI	ALT KÖK NEDENLER	ETKİ/SONUÇ
Veri güvenliğinin sağlanamaması sonucu verilerin amacı dışında kullanılması	• Bilgi ve belgelerin korunması ile ilgili kurum politika ve prosedürlerinin bulunmaması • Kurum içerisinde kritik bilgilerin yönetilmesinden, işlenmesinden ve imhasından sorumlu kişilerin atanmamış olması • Kritik bilgilerin sınıflandırılmaması ve ilgili bilgilere erişim yetkilerinin belirlenmemesi • Kritik verileri içeren medyaların (usb, cd vb.) şifreli olmaması, bilgi paylaşım araçlarının güvenliğinin yeterince sağlanmaması	Varlıkların gizliliğine, bütünlüğüne ve kullanılabilirliğine ilişkin güvenlik açıklarının ortaya çıkması Kritik verilerin istenmeyen kişilerce ele geçirilmesi Kurum itibarının zedelenmesi

Risk tanımlama örnekleri

Stratejik Hedef

Hızla gelişen teknolojinin sürekli takibi ve dijital dönüşüm süreçlerinin kurum çapında projelerle desteklenmesi

Hatalı/Eksik Risk Tanımlaması

Dijital dönüşüme ayak uydurulamaması

Doğru Risk Tanımlaması

Yaşanan dijital dönüşüm sürecine etkin şekilde entegre olunamaması sebebiyle müşteriler, tüketiciler, reklamcılar, yatırımcılar ve hükümet yetkilileri dahil olmak üzere, kurumun çeşitli kesimlerinden algılanan imaj ve itibarın olumsuz etkilenmesi

Risk iştahı
Nereye Kadar Risk Almalıyız?

Süreçler → Risk Alma İstekliliği

Konu Başlığı	Risk İştah Sınıfı	Risk İştah Sınıfı Açıklaması	Risk İştahı Seviyesi
Bilgi Teknolojileri Yönetimi	Veri Güvenliği Yönetimi	Kurum sahipliğinde bulunan tüm verilerin tamlığını, bütünlüğünü, gizliliğini ve güvenliğini etkileyebilecek riskler	**Riskten Kaçınan**
Genel	Uluslararası Operasyonlar	Kurum'un yurt dışında yürütmekte olduğu operasyonlarını etkileyebilecek riskler	**Riske Toleranslı**
Genel	Yönetim Raporlamaları	Kurum yönetimi tarafından doğru stratejik kararlar verilmesini ve performansın etkin şekilde izlenmesini destekleyen yönetim raporlamalarının tamlığını, doğruluğunu ve bütünlüğünü etkileyebilecek riskler	**Ilımlı Şekilde Riskten Kaçınan**

Risk Kapasitesi

Risk kapasitesi, şirketin faaliyetlerine son vermeden alabileceği en yüksek risk seviyesidir. Bir şirketin risk kapasitesi, risklere en fazla ne kadar dayanabileceğini bilmesi açısından önemlidir.

HEDEF	**Güncel teknolojilerden faydalanarak iş yapış biçimlerini, iş akışlarını ve iş ortamlarını dijital olarak dönüştürme**
RİSK İŞTAHI	Yüksek – Teknolojik gelişmelere ayak uydurarak öncü adımlar atan bir şirket olarak dijital dönüşüm projelerine tam destek verilecektir.
RİSK KAPASİTESİ	BT alt yapısının ilgili dijital dönüşümü destekleyecek yapıda olmaması, temel operasyonel faaliyetlerin yürütülemeyecek duruma gelmesi (Dönüşüm süreçlerinde bankacılık hizmetlerinin 5 gün süreli olarak kesilmesi)

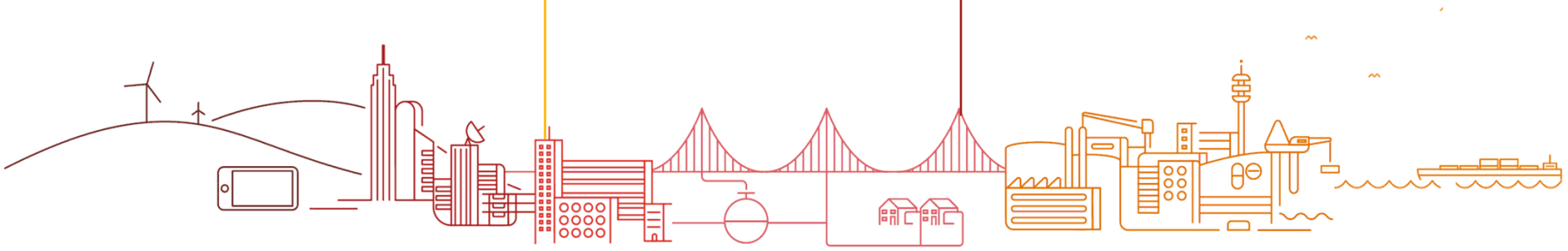
Risklerin Değerlendirilmesi
Doğru risklerle başlamak…

2

Riskleri değerlendir

‘Stratejilerimizin hayata geçmesini etkileyecek en kritik riskler hangileri?’

‘Kaynaklarımızı öncelikli olarak hangi risklere yönlendirelim?’



Risklerin değerlendirilmesi

Risk seviyelerinin belirlenmesi aşamasında, **mevcut kontrol faaliyetleri** göz önünde bulundurularak risklerin **etki ve olasılık seviyeleri** ölçülür.

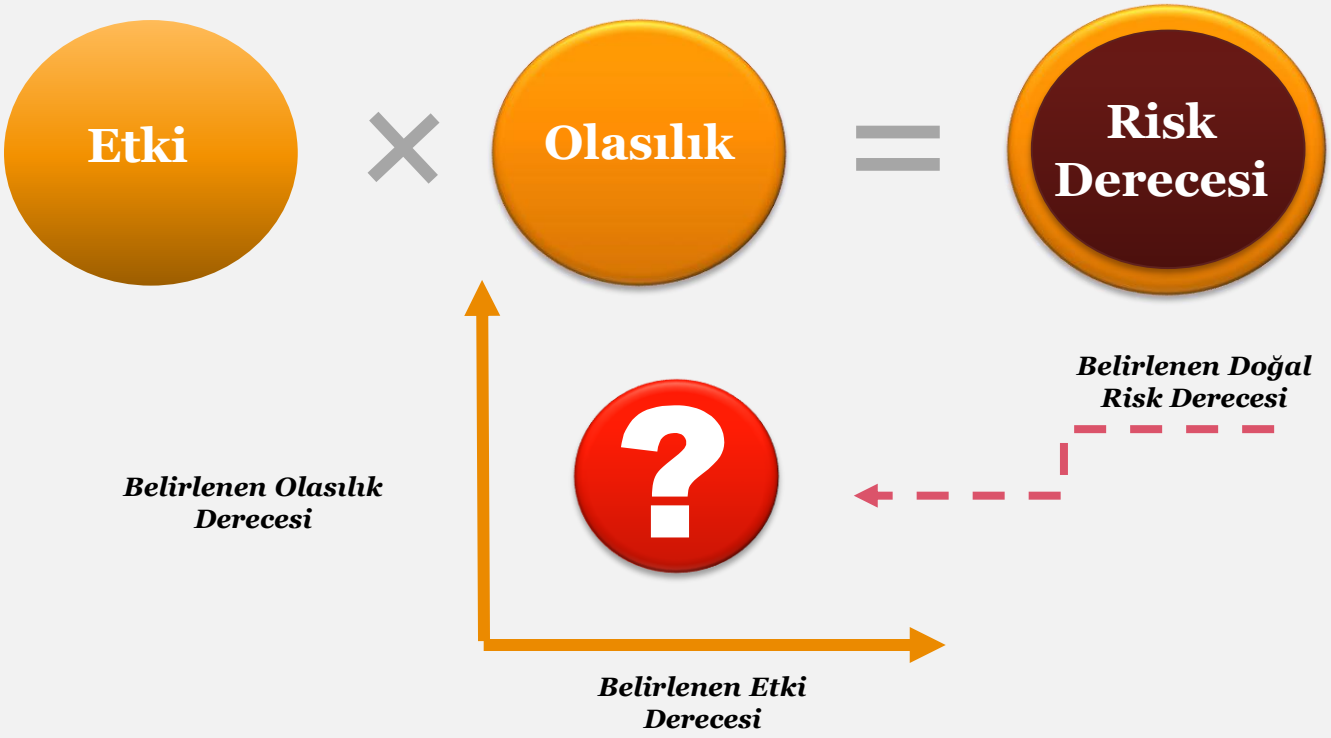
Mevcut Kontrol Faaliyetlerinin Değerlendirilmesi

Risklerin Etki ve Olasılık Seviyelerinin Belirlenmesi

Risklerin etki ve olasılık seviyelerinin belirlenmesi

02

Riskin belirlenen etki ve olasılık seviyeleri kullanılarak “risk derecesi” hesaplanır.



Olasılık seviyeleri

OLASILIK PUANI	OLASILIK SEVİYESİ	AÇIKLAMA
5	Neredeyse Kesin	Amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı kesin olan olay veya durumlar
4	Yüksek Olasılık	Amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı yüksek olan muhtemel olay veya durumlar
3	Olası	Amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı mümkün olay veya durumlar
2	Zayıf Olasılık	Amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı düşük olmakla birlikte imkansız olmayan olay veya durumlar
1	Çok Zayıf Olasılık	Amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı pek muhtemel olmayan olay veya durumlar

Etki seviyeleri

ETKİ PUANI	ETKİ SEVİYESİ	AÇIKLAMA
5	Çok Yüksek	Kurumun amaç ve hedeflerine ulaşamamasına, stratejik amaç ve hedeflerinden **ciddi derecede sapmasına** veya kurum tarafından sunulan hizmetlerin **uzun süre duraklamasına** neden olabilecek olay veya durumlar
4	Yüksek	Kurumun amaç ve hedeflerinden **önemli derecede sapmasına** veya kurum tarafından sunulan hizmetlerin **önemli bir süre duraklamasına** neden olabilecek olay veya durumlar
3	Orta	Kurumun amaç ve hedeflerinden **kabul edilebilir derecede sapmasına** veya kurum tarafından sunulan hizmetlerin **belirli bir süre duraklamasına** neden olabilecek olay veya durumlar
2	Düşük	Kurumun amaç ve hedeflerine ulaşmasında **düşük seviyede etkisi** olabilecek olay veya durumlar
1	Çok Düşük	Kurumun amaç ve hedeflerine ulaşmasında **çok düşük, kolaylıkla gözlemlenemeyecek** seviyede etkisi olabilecek olay veya durumlar

Etki kriterleri

Belirlenen riskin birden fazla etki kriterinin olması durumunda, en yüksek etki seviyesi göz önünde bulundurulmalıdır.

ETKİ PUANI	FİNANSAL ETKİ	OPERASYONEL ETKİ	İTİBAR ETKİSİ	UYUM ETKİSİ	STRATEJİK ETKİ
5	Çok önemli seviyede maddi kayba neden olabilecek olay veya durumlar (Örneğin; + 10 Milyon USD Maddi Kayıp)	Ciddi operasyonel kesintilere sebep olan olayların yaşanması hizmet sağlanmasında ciddi gecikmelerin yaşanması (Örneğin; 1 haftadan fazla)	Anahtar paydaşların uzun süreli ve tamamen güven kaybı	Ağır yaptırımlar Kritik önem derecesine sahip hakların kaybedilmesi	Kurumun hedeflerine ulaşamaması
4	Önemli seviyede maddi kayba neden olabilecek olay veya durumlar (Örneğin; + 1 Milyon USD Maddi Kayıp)	Önemli operasyonel kesintilere sebep olan olayların yaşanması, hizmet sağlanmasında gecikmelerin yaşanması (Örneğin; 2-3 gün)	Uzun süreli ve geniş çaplı güven kaybı	Önemli yaptırımlar Önemli hakların kaybedilmesi	Kurumun hedeflerine ulaşmasında ciddi başarısızlıklar yaşaması
3	Orta düzeyde maddi kayba neden olabilecek olay veya durumlar (Örneğin; + 250.000 USD Maddi Kayıp)	Bazı operasyonel kesintilere sebep olan olayların yaşanması, hizmet sağlanmasında önemsiz gecikmelerin yaşanması (Örneğin; 6 saat)	Önemli ancak kısa süreli güven kaybı	Orta derece yaptırımlar Bazı hakların kaybedilmesi	Kurumun hedeflerine ulaşmasında bazı başarısızlıklar yaşaması
2	Düşük düzeyde maddi kayba neden olabilecek olay veya durumlar (50.000 USD Maddi Kayıp)	Önemsiz operasyonel kesintilere sebep olan olayların yaşanması, hizmet devamlılığının küçük aksaklıklarla devam etmesi (Örneğin; 2 saatten az)	Kısa süreli ve bazı paydaşlar ile sınırlı güven kaybı	Kınama Düşük derece yaptırım	Kurumun hedeflerine ulaşmasına engel olmaması ama olumsuz etkilemesi
1	Çok düşük düzeyde maddi kayba neden olabilecek olay veya durumlar (10.000 USD ve altı Maddi Kayıp)	Kurum faaliyetlerinin sürekliliğini kesintiye uğratmayacak olayların yaşanması (Örneğin; 1-2 dakika)	Kamuoyuna yansımayan sadece kurum içinde fark edilebilecek düzeyde kısa süreli yaşanan güven kaybı	Uyarı Herhangi bir kayba sebebiyet vermeyecek seviyede çok düşük derece yaptırım	Kurumun hedeflerine ulaşmasına engel olmaması ve Kurumu fark edilemeyecek düzeyde olumsuz etkilemesi

Risklerin etki ve olasılık seviyelerinin belirlenmesi

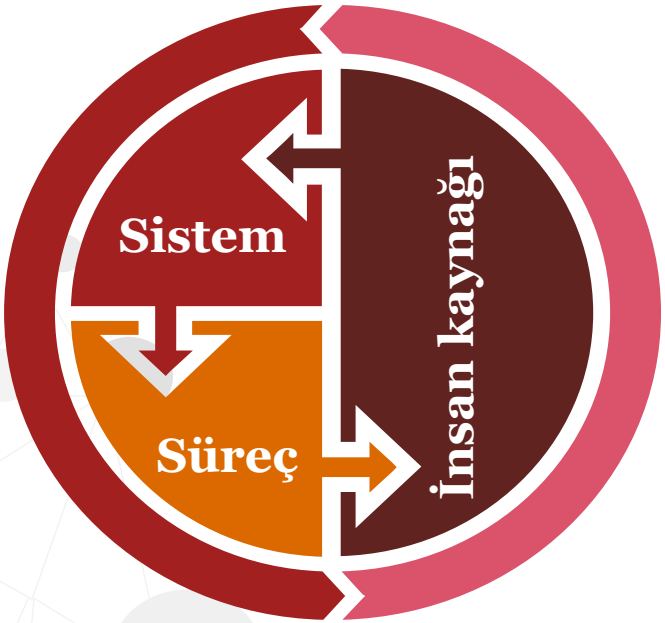
ETKİ PUANI	ETKİ SEVİYESİ
5	Çok Yüksek
4	Yüksek
3	Orta
2	Düşük
1	Çok Düşük

OLASILIK PUANI	OLASILIK SEVİYESİ
5	Neredeyse Kesin
4	Yüksek Olasılık
3	Olası
2	Zayıf Olasılık
1	Çok Zayıf Olasılık

RİSK PUANI	RİSK SEVİYESİ
20, 25	ÇOK YÜKSEK
12, 15, 16	YÜKSEK
6, 8, 9, 10	ORTA
3, 4, 5	DÜŞÜK
1, 2	ÇOK DÜŞÜK

Mevcut kontrol faaliyetlerinin değerlendirilmesi

01



- *Mevcut kontroller, riski Şirket için kabul edilebilir düzeye indiriyor mu?*
- *Kontroller, olası önemli kayıpları önlüyor mu?*
- *Kontrollerin yürütülmesi için Şirket yeterli teknolojik altyapıya sahip mi?*
- *Şirket kaynakları kontrol faaliyetlerinde etkin kullanılıyor mu?*

Mevcut kontrol faaliyetlerinin değerlendirilmesi - Örnek

Sistem	Süreç	İnsan Kaynağı
Süreçler otomatik olup manüel müdahale limitlidir. Otomasyonun güvenilirliği düzenli testlerle ölçülmektedir.	Etkin olarak tasarlanmış kontroller mevcuttur. Operasyon ve tasarım etkinliği için periyodik testler yapılmaktadır. Düzenli olarak raporlar hazırlanmaktadır. Raporlarda önemli bir hataya rastlanmamaktadır.	Tüm görevler zamanında ve planlanan şekilde tamamlanmaktadır. Tüm çalışanlar için yazılı ve güncel iş tanımları bulunmaktadır. Çalışanlar yetkin ve sayıca yeterlidir. Görevlerin ayrılığı prensibi tam olarak uygulanmaktadır.

Risklerin etki ve olasılık seviyelerinin belirlenmesi

Mevcut Kontrollerin Etkinliğinin Değerlendirmesiyle:

ETKİ PUANI	ETKİ SEVİYESİ
5	Çok Yüksek
4	Yüksek
3	Orta
2	Düşük
1	Çok Düşük

OLASILIK PUANI	OLASILIK SEVİYESİ
5	Neredeyse Kesin
4	Yüksek Olasılık
3	Olası
2	Zayıf Olasılık
1	Çok Zayıf Olasılık

RİSK PUANI	RİSK SEVİYESİ
20, 25	ÇOK YÜKSEK
12, 15, 16	YÜKSEK
6, 8, 9, 10	ORTA
3, 4, 5	DÜŞÜK
1, 2	ÇOK DÜŞÜK

Risk seviyelerinin belirlenmesi – örnek 1

Risk Tanımı	Etki	Olasılık	Doğal Risk Seviyesi	Etki	Olasılık	Artık Risk Seviyesi
Sistem veri güvenliğinin sağlanamaması sonucu verilerin amacı dışında kullanılması	**ÇOK YÜKSEK**	**YÜKSEK**	**ÇOK YÜKSEK**	**YÜKSEK**	**ORTA**	**YÜKSEK**

Veri güvenliğinin sağlanamaması sonucu hem **Kişisel Verilerin Korunması Kanunu'na uyumsuzluk** söz konusu olmakta hem de **verilerin istenmeyen kişilerin eline geçmesi** sonucu kurum **itibar kaybına uğrayabilmektedir.**

Siber saldırıların arttığı ve Kurum içinde **sistem değişikliklerinin** olduğu bir dönemdir.

- Bilgi ve belgelerin korunması ile **ilgili kurum politika ve prosedürleri** oluşturulmuş, **gerekli eğitimler** verilmiştir.
- Kurum içerisinde **kritik bilgilerin yönetilmesinden, işlenmesinden ve imhasından sorumlu kişiler** atanmıştır.
- **Kritik bilgiler sınıflandırılmış** ve sistem üzerinde **erişim yetkileri** belirlenmiştir.

Risk seviyelerinin belirlenmesi – örnek 2

Risk Tanımı	Etki	Olasılık	Doğal Risk Seviyesi	Etki	Olasılık	Artık Risk Seviyesi
Sistem veri güvenliğinin sağlanamaması sonucu verilerin amacı dışında kullanılması	**ÇOK YÜKSEK**	**YÜKSEK**	**ÇOK YÜKSEK**	**ORTA**	**ÇOK ZAYIF OLASILIK**	**DÜŞÜK**

Veri güvenliğinin sağlanamaması sonucu hem **Kişisel Verilerin Korunması Kanunu'na uyumsuzluk** söz konusu olmakta hem de **verilerin istenmeyen kişilerin eline geçmesi** sonucu kurum **itibar kaybına uğrayabilmektedir.**

Siber saldırıların arttığı ve Kurum içinde **sistem değişikliklerinin** olduğu bir dönemdir.

Bir önceki slaytta yer alanlara ek olarak;

- **USB portları** kapatılmış ve bilgisayarlardan dışarı aktarılan tüm verilerin **loglanması** sağlanmıştır.
- **Veri transferi** için standart paylaşım platformları belirlenmiştir.
- Düzenli olarak **sızma testleri yapılmakta** ve **güvenlik açıkları** kapatılmaktadır.

Risklere yönelik kararların verilmesi…

3

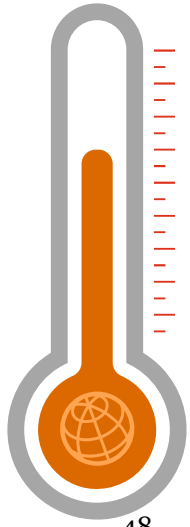
Riskleri yönet

Operasyonel kararlar

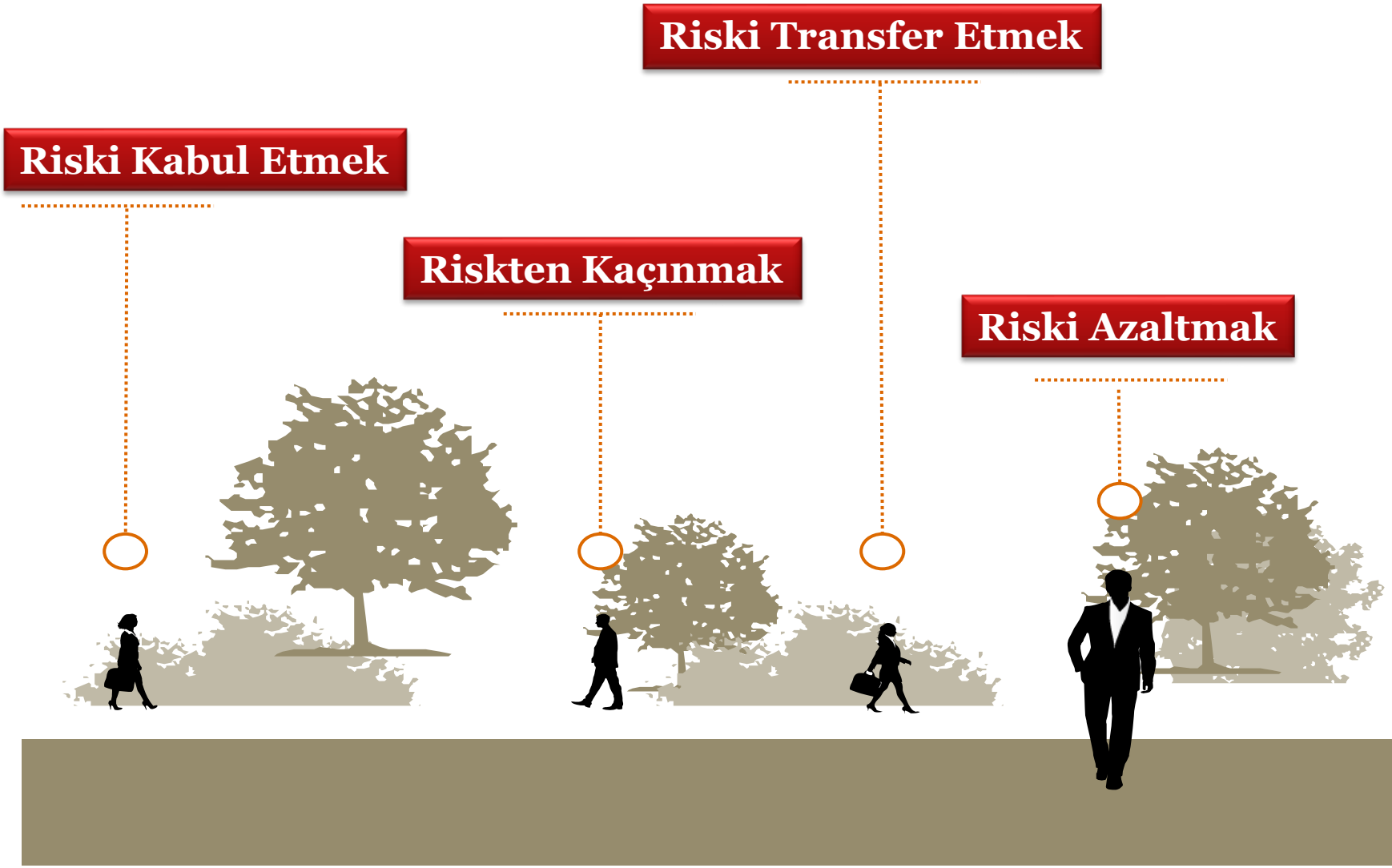
Stratejik kararlar

‘Bu riskleri daha iyi yönetmek için ne yapabiliriz?’

Dayanıklılığımızı arttırmak



Riske yönelik kararların belirlenmesi



Riske yönelik kararların belirlenmesi

Riskten Kaçınmak

Kurum çalışanlarının, bordro bilgilerine sistem üzerinden erişebilmelerini sağlayacak yeni bir teknolojik uygulamanın, kurum için bilgi güvenliği riski doğuracağı ve kurumun bu **riski azaltmaya yönelik gerekli risk yönetimi faaliyetlerini**, **kaynak yetersizliği sebebiyle gerçekleştiremeyeceği** sonucuna varılması ile **bu teknolojik uygulamadan vazgeçilerek** ilgili riskten kaçınma yolunun tercih edilmesi

Riski Transfer Etmek

- Güvenlik, ulaşım, bakım onarım vb. faaliyetlerin, konusunda **uzman kuruluşlara taşere edilmesi,**
- Büyük çaplı projelerde yüklenici olarak yer almak yerine, **yap işlet devret ve benzeri modeller** ile bu projelere ait **finansal ve operasyonel risklerin projeyi gerçekleştiren şirketlere devredilmesi**

Riski Kabul Etmek

Kurumda kritik çalışanlara yönelik **yedek personel** uygulaması yapılması planlanabilir ancak **ek maliyetlerin oluşması** sebebiyle kurum, yedek personel uygulamasını başlatmak yerine **herhangi bir kontrol faaliyeti gerçekleştirmemeyi ve riskleri kabul etmeyi** seçebilir.

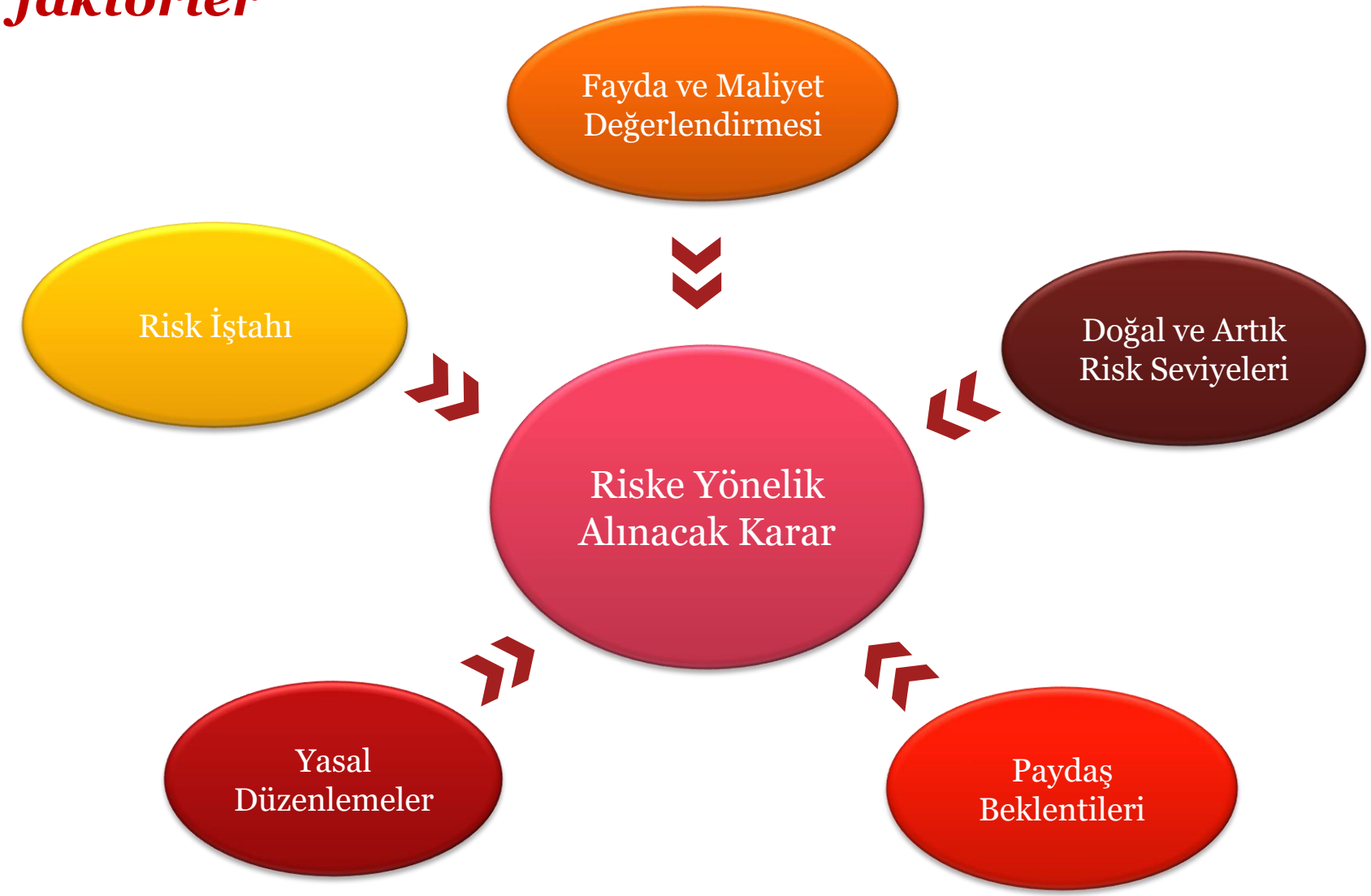
Riske yönelik kararların belirlenmesi

RİSK	KÖK NEDEN	AKSİYON/KONTROL
Kurumda personel tarafından görev ve sorumluluklar net olarak algılanmayabilir, yürütülen süreçlerde standart bir yaklaşımdan ziyade görevi yürütenlere bağlı bir anlayış oluşabilir.	Unvan bazında görev tanımlarının oluşturulmamış olması İşe başlayan personele görev tanımlarının verilmemesi ve sorumluluk sınırları konusunda yeterli bilgilendirme yapılmaması	Kurum içerisinde yer alan her bir unvan için rol ve sorumlulukların belirlenmesi ve bu rol ve sorumlulukların görev tanımları içerisinde dokümante edilmesi İşe yeni başlayan her personele görev tanımlarının verilmesi ve imzalatılarak özlük dosyalarına kaldırılması Değişen rol ve sorumlulukların zamanında görev tanımlarına yansıtılması

RİSK	KÖK NEDEN	AKSİYON/KONTROL
Kurum performans yönetimi sisteminin kurulmaması sonucu genel ve kişisel performans takibi etkin yapılamayabilir.	Kurum içerisinde entegre bir performans yönetimi sisteminin bulunmaması Kurum ve personel seviyesinde KPI'ların belirlenmemiş olması Performans göstergeleri aracılığı ile Şirket hedeflerinin çalışan seviyesine indirilmemesi (Kurum KPI ile personel KPI'larının ilişkilendirilmemesi)	Performans yönetim sisteminin kurulmasına yönelik olarak; Kurum stratejik amaç ve hedefleri ile ilişkili indikatörlerin belirlenmesi Her bir departman ve personel için süreç seviyesinde performans indikatörlerinin belirlenmesi Stratejik hedefler seviyesinde belirlenen indikatörler ile süreç ve personel seviyesinde belirlenen indikatörlerin birbiri ile ilişkilendirilmesi

Riskleri azaltmak için tanımlanan kontroller…

Riske yönelik alınacak kararları etkileyen faktörler



Öncü/Anahtar risk göstergeleri

- **Riskin gerçekleşmesini tetikleyici nedenleri göstergeler ile tespit edebilirsek risk gerçekleştiğinde kuruma etkisi indirgenebilir ve riske yanıt zamanı uzar.**

- Öncü risk göstergelerinin **etkin takibi** stratejilerin planlandığı şekilde uygulanabilmesi olasılığını arttırır, stratejilerdeki olası değişiklikler için gereken zamanı optimize eder, **hedeflere ulaşabilme konusundaki güvence artar.**

Öncü risk göstergeleri - Örnek

RİSK	*ÖNCÜ RİSK GÖSTERGESİ*	*HEDEF*	*AKSİYON*
Kritik personelin kurumda tutundurulamaması	Kritik personelin kurumda çalışma süreleri Çalışan memnuniyet anket sonuçları	En az 8 sene %80 Memnuniyet oranı	Çalışan haklarının iyileştirilmesi Mentörlük prosedürlerinin güçlendirilmesi Liderlik eğitimlerinin organize edilmesi vs.
HEDEF	*ÖNCÜ RİSK GÖSTERGESİ*	*HEDEF*	*AKSİYON*
Sürdürülebilirlik vizyonu ile hareket eden bir marka olmak	Yıl içerisinde gerçekleşen sürdürülebilirlik proje sayısı/planlanan proje sayısı (%)	Oranın %50'nin altında kalması	Strateji seçimlerinin gözden geçirilmesi Sürdürülebilirlik Komitesi oluşturulması ve tüm projelerin bu komiteye raporlanarak takip edilmesi

Öncü Risk Göstergesi, Risk İştahı ve Risk Toleransı İlişkisi

Proje

Proje Hedefleri

Ürün kalitesini 4.0 sigma'da tutmak

Risk İştahı

Ürün kalitesinde azalma kabul edilemez

Düşük

Öncü Risk Göstergesi	Gösterge Hedefi	Risk Toleransı
Ölçüm	**Hedef**	**Tolerans– Makul Aralık**
1-Ürün kalite endeksi	4.0 sigma	4.0 – 4.5 sigma

Süreç

Birim Hedefleri

Kaliteli tedarikçiler ile çalışmak

Risk İştahı

Tedarikçi değerlendirme puanı 65'in üzerinde tedarikçiler kabul edilebilir

Orta

Öncü Risk Göstergesi	Gösterge Hedefi	Risk Toleransı
Ölçüm	**Hedef**	**Tolerans– Makul Aralık**
1-Denetim Sayısı/Tedarikçi Sayısı	**1- %85**	1- %80 – %100
2-Tedarikçi değerlendirme puanı	**2- 90 puan**	**2- 65 puan - 100 puan**

Risklerin gündemde ve takipte olması…

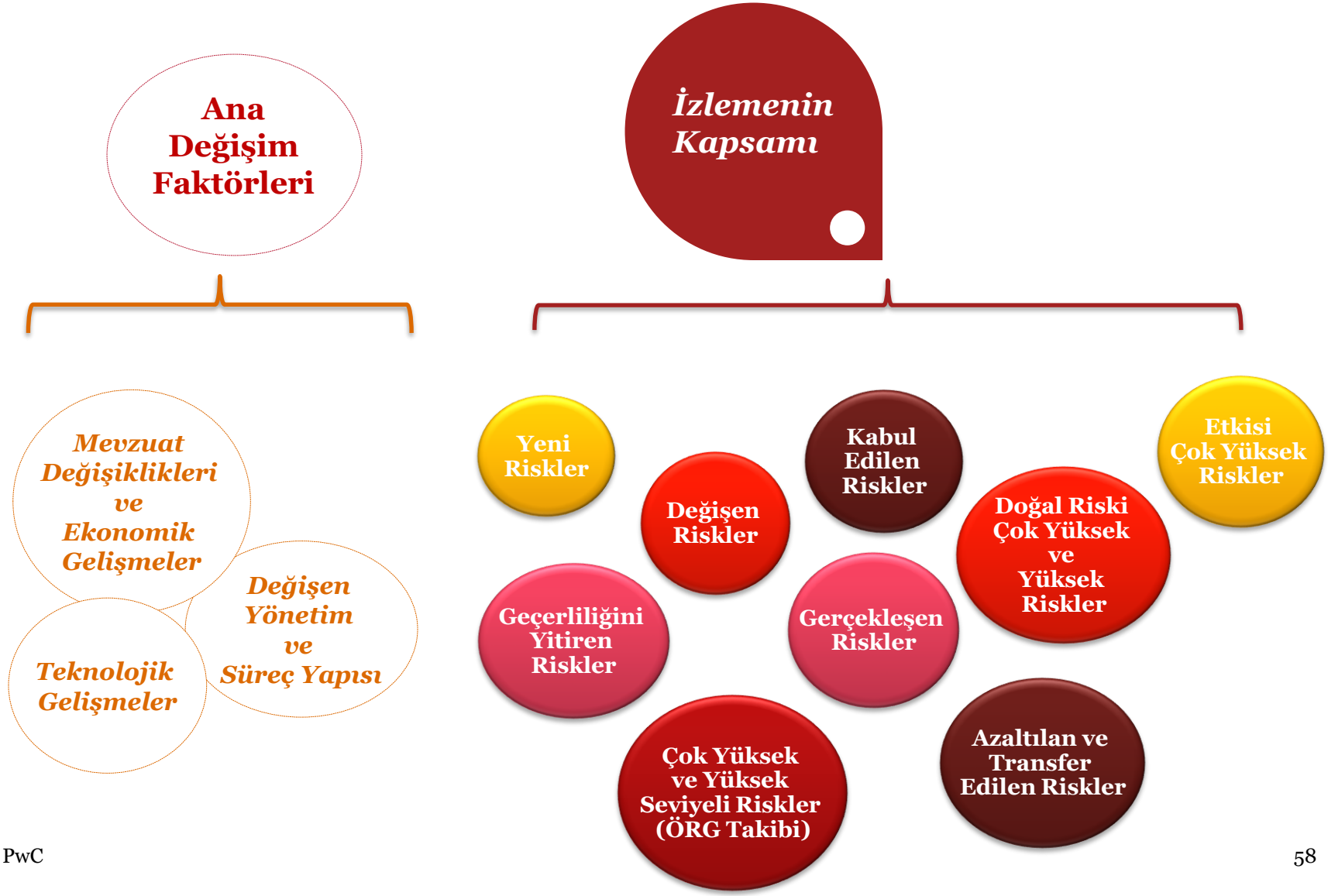
4

Riskleri izle ve raporla

- Yönetim raporlamasına dahil edilmesi
- Aksiyon planlamalarının takibi
- Riske yönelik öncü göstergelerin ve diğer bilgilerin takibi

"Yönetim kurulu ve üst yönetime değer katacak risk bilgisi nedir?"

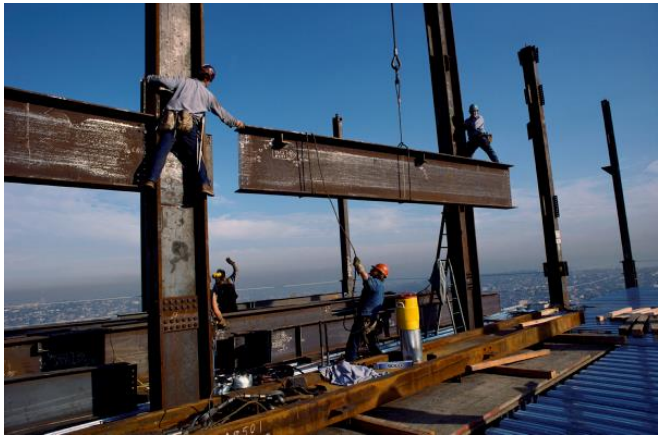
Risklerin izlenmesi ve raporlanması



Riskler nasıl raporlanmalı?

Periyodik raporlamalarda örnek başlıklar:

- **Öncelikli risklerin listesi (ör: Top 10)**
- Kurumu etkileyen kritik dış değişkenlerdeki değişikliklerin değerlendirildiği **senaryo analizleri**
- Kritik riskler için yönetim tarafından **belirlenen politika ve limitlere uyumsuzluklar**
- Kritik risklerin yönetim kapasitesindeki **önemli yetersizlikler ve iyileştirme çalışmalarının mevcut durumu**



Riskler nasıl raporlanmalı?

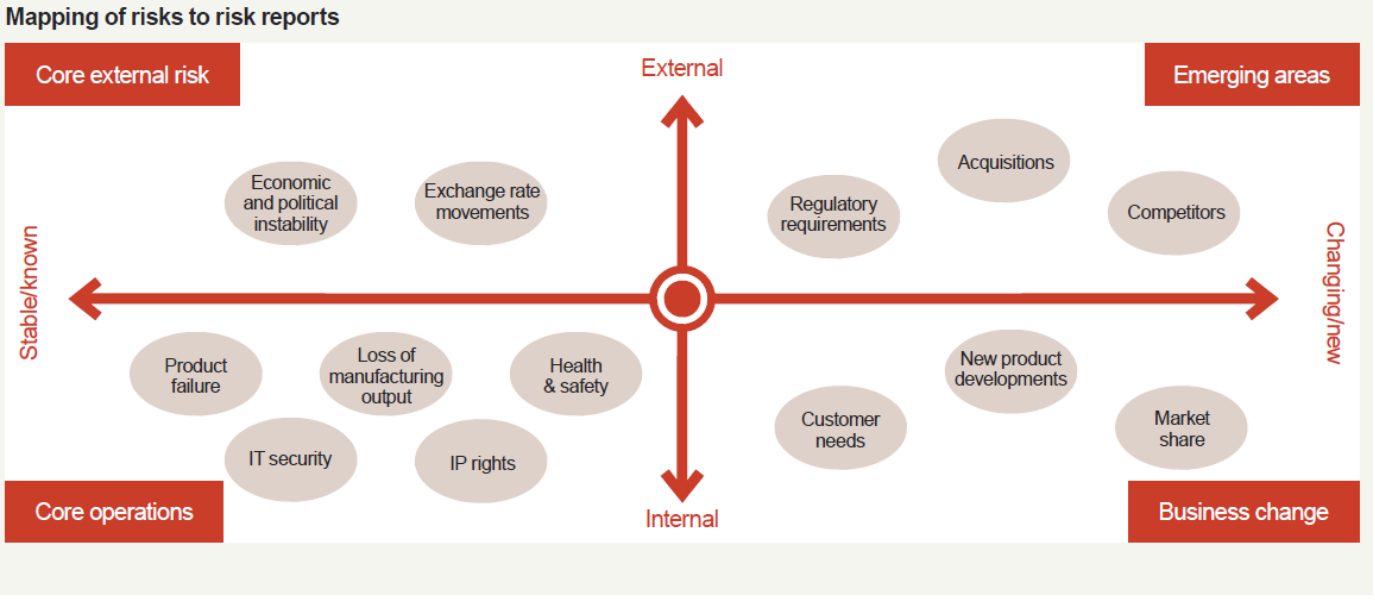
Periyodik raporlamalarda örnek başlıklar:

- **Gelecekte ortaya çıkabilecek ana risklerin listesi** (ör: emerging risks, black swans)
- Yönetim tarafından riski belirleme, değerlendirme, önceliklendirme ve ölçümlemede kullanılan yöntemin açıklaması
- **Kritik risk göstergelerindeki eğilimler**
- **Kritik risk yönetim faaliyetlerinin etkinliğinin değerlendirilmesi**

Raporlama örnekleri

Key risks for 2013	Potential impact	Mitigating action	Potential opportunities	Change in risk in the year	
External **Economic environment**	Negative impact on the Group's businesses, largely through a reduction in demand for services. In rail, franchise bids make economic assumptions years into the future. A weaker economy can lead to under performance against bid targets.	• Continue to focus our operations in more resilient geographical areas. • Local management constantly assesses the needs of the local markets and tailors services and products accordingly. • Focus on driving volumes through innovative and targeted marketing. • Generate customer loyalty through smart-ticketing. • Proactive cost control.	• A more challenging economic environment encourages modal shift, as motorists seek value for money alternatives to the private car.	The economic risk was similar in the year as economic growth rates for the year ended June 2013 remained low at 1.4%.	
Political and regulatory framework	Changes in Government or to laws, regulations, policies (e.g. concessionary travel), local authority attitudes towards public transport and reductions in the availability of Government financial support could adversely impact the Group's operations and financial position.	• Limited exposure to local authority funding as 90% of deregulated bus operations are commercial. • Actively participate in key industry, trade and Government steering groups. • Maintain close relationships with key industry partners and stakeholders. • Use internal initiatives across the business to offset external issues.	• Changes in law, regulation or funding could positively impact the Group, potentially leading to increased funding or more flexibility for operators. For example, the potential introduction of Quality Contracts may increase our ability to bid for contracts in new areas. The political and regulatory framework provides us with the opportunity to influence decisions through close dialogue with the Government, local authorities and other key parties.	Two years ahead of the next general election we are mindful of the major political parties' developing policies. Our good levels of engagement with these parties enable us to influence policies impacting on the industry and Go-Ahead. The Tyne & Wear Integrated Transport Authority began a consultation period with a view to introducing Quality Contracts in the North East. In the 2013 Government spending review, TfL's funding was reduced. This could impact on the London bus market. Positively, BSOG has been protected until at least 2016.	
Strategic **Sustainability of rail profits**	The sustainability of rail profits is dependent on a number of factors. The nature of the current rail franchising model leads to high volatility of earnings; failure to retain or win new franchises could impact on the overall profitability of the Group; failure to comply with conditions of rail franchise agreements could lead to financial penalties or even the termination of a rail franchise.	• Flexible and experienced management team which responds quickly and expertly to changing circumstances. • Shared risk through Govia, which is 65% owned by Go-Ahead and 35% by Keolis. • Element of protection through revenue support arrangements. • Significant resource and financial investment in bidding for new franchises. • Regular Board review of rail performance, and Board approval of overall rail bidding strategy. • Compliance with franchise conditions closely monitored.	• Following the review of rail franchising, the Government issued a revised franchise timetable. Fourteen rail franchises are up for tender in the next five years presenting growth opportunities for the Group. There may be the opportunity for increased earnings if the economic climate is stronger than assumed in a franchise bid.	The proposed extensions of the Southeastern and London Midland franchises enable us to renegotiate contract terms with the DfT. Southern qualifies for revenue support in September 2013, providing protection against significant losses. Being shortlisted for two forthcoming franchise competitions gives confidence in our ability to secure future franchises.	

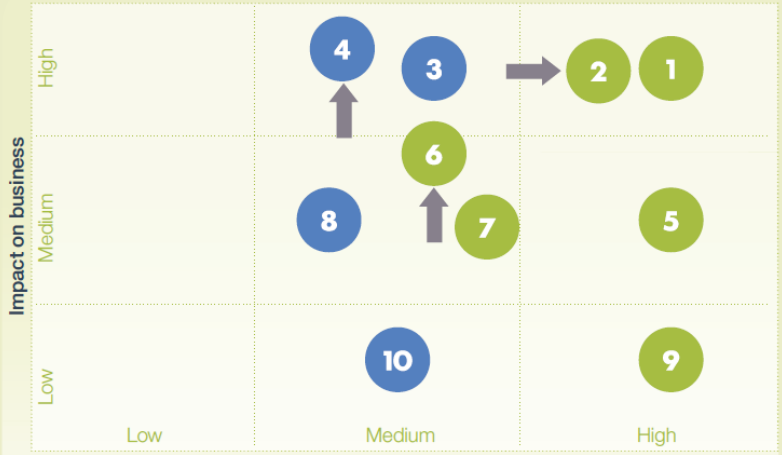
Raporlama örnekleri



Principal risk	Change	Impact	Mitigation	Relevance to strategy
Economic and political instability: The Group operates worldwide. Economic and political instability creates risks for our locally based direct operations. The Group has reviewed country, credit, liquidity and currency risks and, in particular, those arising from European debt issues. The risk has increased as a result of the deterioration in some European economies and the general world economic outlook.	↑	• Fluctuations in profit from significant currency movements • Reduced profit due to impact on customers from economic problems • Potential redenomination of local currency, devaluation and high inflation.	• Compliance with Group Treasury Policy • Strong internal controls with internal audit and appropriate insurance • Resilient business model (as explained in the Business Review on page 17). • Well spread business – approximately 10% of Group sales originate in the higher risk countries of Greece, Ireland, Italy, Portugal and Spain. Sales in Greece are immaterial.	Broaden our global presence

Raporlama örnekleri

How we see our principal risks



- Longer term risks
- Shorter term risks

1. Waste volumes
2. Financial risk
3. Market/legislative drivers
4. Long-term contracts
5. Price competition
6. Project management
7. Succession planning
8. Plant availability and insurance
9. Fuel pricing
10. SHE (safety, health, environmental)

Strategic priorities

1. Invest in new sustainable opportunities that build on our core capabilities and generate attractive returns
2. Deliver outstanding operational performance from existing businesses and investments
3. Develop world-class capabilities and technologies in a cohesive Group culture
4. Actively manage Shanks' portfolio and use bolt-on acquisitions to accelerate profitable growth

External drivers

- **A.** Macro market drivers
- **B.** Regulatory and legislative
- **C.** Economic pressures and limited capital

Strategic priorities/ External drivers	Risk/impact	Our response	Progression
2, 4, C	1 – Waste volumes		
	The inability to attract sufficient waste volumes due to external economic factors including over capacity of incineration in the Netherlands, limiting the availability of waste by commercial and municipal customers. If facilities are working at below full capacity, there is the likelihood of increased unit costs.	Regular reporting and monitoring of volumes both at local and Board level through the use of performance measures. Dedicated sales teams. Innovative action taken to increase volumes through the sourcing of new waste streams such as waste importation into the Netherlands and increasing presence in household waste markets in Belgium. • Reorganising the processing and disposal of waste to optimise asset utilisation and reduce costs with a higher focus on energy production.	No change due to the continuing macro-economic environment.

Ülkemizdeki düzenlemelere yansımalar…

Türk Ticaret Kanunu

SPK Kurumsal Yönetim İlkeleri

Yönetim kurulunun işlevine yönelik beklentiler…

Yönetim kurulu, alacağı stratejik kararlarla, ***şirketin risk, büyüme ve getiri dengesini en uygun düzeyde tutarak akılcı ve tedbirli risk yönetimi anlayışıyla şirketin öncelikle uzun vadeli çıkarlarını gözeterek****, şirketi idare ve temsil eder.*

Yönetim kurulu şirketin stratejik hedeflerini tanımlar, şirketin ihtiyaç duyacağı insan ve finansal kaynaklarını belirler, ***yönetimin performansını denetler****.*

Yönetim kurulu, ***şirket faaliyetlerinin mevzuata, esas sözleşmeye, iç düzenlemelere ve oluşturulan politikalara uygunluğunu gözetir****.*

SPK Kurumsal Yönetim İlkeleri

Yönetim kurulunun işlevi

Devredilemez görev ve yetkiler

Yönetim kurulunun devredilemez ve vazgeçilemez görev ve yetkileri şunlardır:
a) ***Şirketin üst düzeyde yönetimi*** *ve bunlarla ilgili talimatların verilmesi.*
b) Şirket yönetim teşkilatının belirlenmesi.
c) Muhasebe, finans denetimi ve şirketin yönetiminin gerektirdiği ölçüde, ***finansal planlama için gerekli düzenin kurulması****.*
d) Müdürlerin ve aynı işleve sahip kişiler ile imza yetkisini haiz bulunanların atanmaları ve görevden alınmaları.
e) Yönetimle görevli kişilerin, özellikle kanunlara, esas sözleşmeye, iç yönergelere ve yönetim kurulunun yazılı talimatlarına uygun hareket edip etmediklerinin ***üst gözetimi****.*
f) Pay, yönetim kurulu karar ve genel kurul toplantı ve müzakere defterlerinin tutulması, ***yıllık faaliyet raporunun ve kurumsal yönetim açıklamasının düzenlenmesi*** *ve genel kurula sunulması, genel kurul toplantılarının hazırlanması ve genel kurul kararlarının yürütülmesi.*
g) Borca batıklık durumunun varlığında mahkemeye bildirimde bulunulması.

Türk Ticaret Kanunu, Madde 375

Riskin erken saptanması komitesinin işlevi…

Riskin erken saptanması ve yönetimi

(1) Pay senetleri borsada işlem gören şirketlerde, yönetim kurulu, **şirketin varlığını, gelişmesini ve devamını tehlikeye düşüren sebeplerin erken teşhisi, bunun için gerekli önlemler ile çarelerin uygulanması ve riskin yönetilmesi amacıyla, uzman bir komite kurmak, sistemi çalıştırmak ve geliştirmekle yükümlüdür**. Diğer şirketlerde bu komite denetçinin gerekli görüp bunu yönetim kuruluna yazılı olarak bildirmesi hâlinde derhâl kurulur ve ilk raporunu kurulmasını izleyen bir ayın sonunda verir.
(2) Komite, yönetim kuruluna her iki ayda bir vereceği raporda durumu değerlendirir, varsa tehlikelere işaret eder, çareleri gösterir. Rapor denetçiye de yollanır.

Türk Ticaret Kanunu, Madde 378

Riskin erken saptanması komitesi

Riskin erken saptanması komitesi:
a) *Şirketin varlığını, gelişmesini ve devamını tehlikeye düşürebilecek risklerin erken teşhisi, tespit edilen risklerle ilgili gerekli önlemlerin uygulanması ve riskin yönetilmesi amacıyla çalışmalar yapar.*

b) Risk yönetim sistemlerini en az yılda bir kez gözden geçirir.

SPK Kurumsal Yönetim İlkeleri

Faaliyet raporu ve riskin erken saptanması…

Yönetim kurulunun yıllık faaliyet raporu, şirketin, o yıla ait faaliyetlerinin akışı ile her yönüyle finansal durumunu, doğru, eksiksiz, dolambaçsız, gerçeğe uygun ve dürüst bir şekilde yansıtır. Bu raporda finansal durum, finansal tablolara göre değerlendirilir. Raporda ayrıca, ***şirketin gelişmesine ve karşılaşması muhtemel risklere de açıkça işaret olunur. Bu konulara ilişkin yönetim kurulunun değerlendirmesi de raporda yer alır****.*

Türk Ticaret Kanunu, Madde 516

Şirketin, finansal performansı ile finansal durumunun genel özellikleri ve karşı karşıya bulunduğu temel riskler yıllık faaliyet raporunda değerlendirilir. Şirketin finansal durumuna ilişkin bu değerlendirmeler finansal tablolara dayandırılır. Ayrıca ***finansal olmayan risklere de faaliyet raporunda yer verilir****.*

Şirketlerin yıllık faaliyet raporunun asgari içeriğinin belirlenmesi hakkında yönetmelik, Madde 4

Yıllık faaliyet raporlarında:
b) ***Yönetim kurulu komitelerinin*** *komite üyeleri, toplanma sıklığı, yürütülen faaliyetleri de içerecek şekilde* ***çalışma esaslarına ve komitelerin etkinliğine ilişkin yönetim kurulunun değerlendirmesine*** *yer verilir.*

SPK Kurumsal Yönetim İlkeleri

(1) Yıllık faaliyet raporunun ***riskler ve yönetim organının değerlendirmesi*** *bölümünde aşağıda belirtilen hususların yer alması zorunludur:*
a) Varsa şirketin öngörülen risklere karşı uygulayacağı risk yönetimi politikasına ilişkin bilgiler,
b) Oluşturulmuşsa riskin erken saptanması ve yönetimi komitesinin çalışmalarına ve raporlarına ilişkin bilgiler,
c) Satışlar, verimlilik, gelir yaratma kapasitesi, kârlılık, borç/öz kaynak oranı ve benzeri konularda ileriye dönük riskler.

Şirketlerin yıllık faaliyet raporunun asgari içeriğinin belirlenmesi hakkında yönetmelik, Madde 13

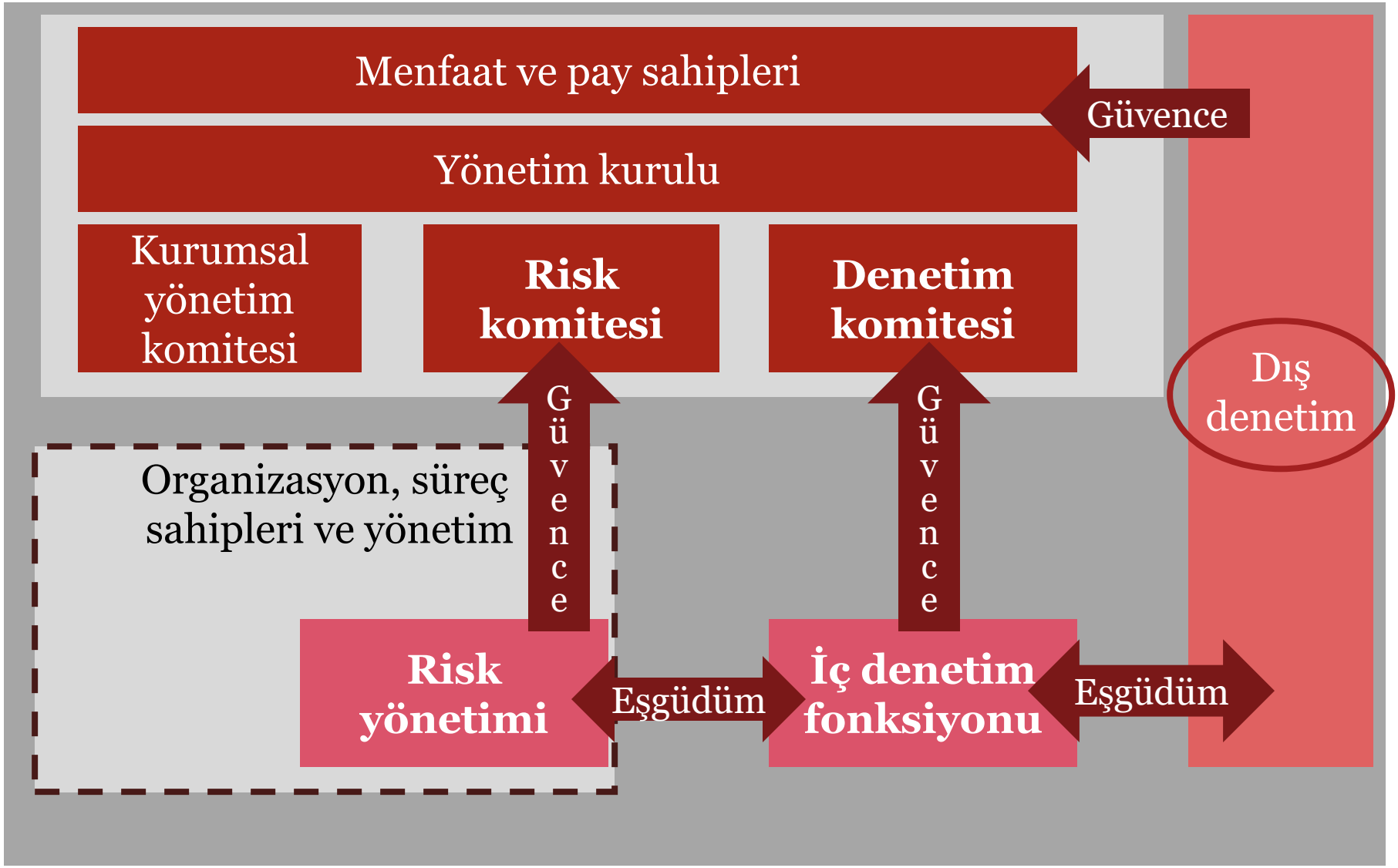
Riskler ve yönetim organının değerlendirilmesi

Risklerin erken saptanması ve yönetimi mekanizması…

3 Ana Odak

1. Gözetim
2. Koordinasyon
3. Yönetim

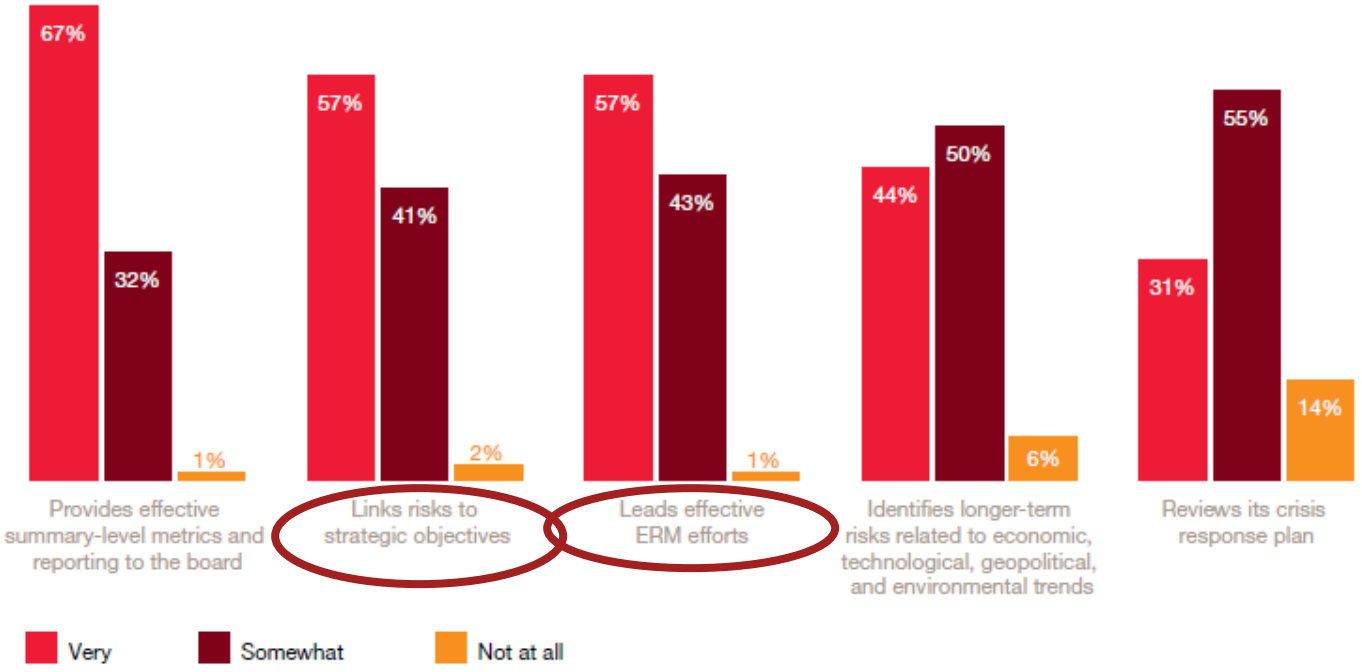
Güvence Mekanizmaları



Riskin Erken Saptanması ve Gözetiminde Sorumluluklar - Örnek

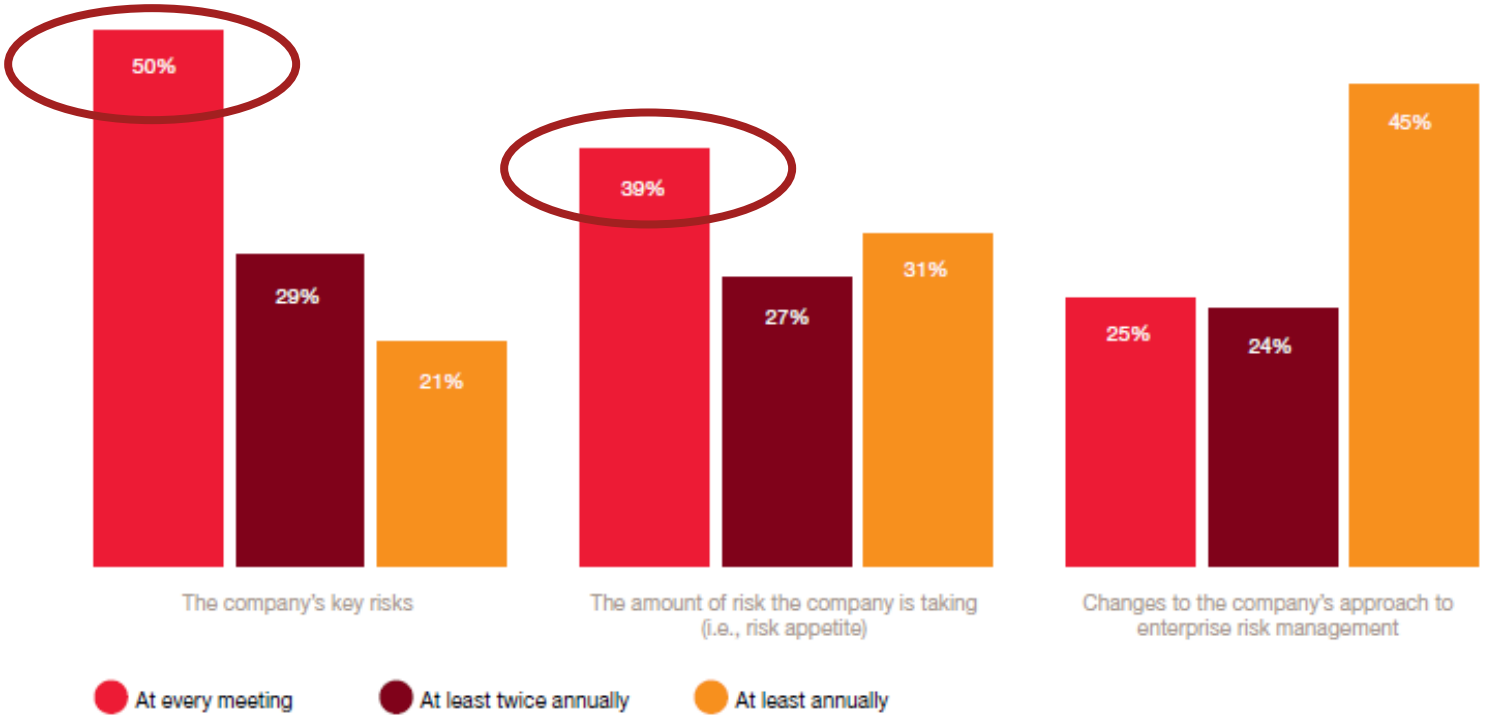
	Rol ve Sorumluluklar
Yönetim Kurulu	▪ Kurumsal yönetim süreçlerinin izlenmesi ve gerekli durumlarda süreç ile ilgili stratejik kararların verilmesi ▪ Organizasyonun öncelikli risklerinin belirlenmesi ve bu risklerin etkin şekilde yönetildiğine ilişkin güvence alınması ▪ Risklerin etkin şekilde yönetimine ilişkin **şeffaf ve hesap verebilir bir yönetim mekanizmasının** tesis edilmesi
Riskin Erken Teşhisi Komitesi	▪ KRY **Yönetmeliğinin** onaylanması ▪ KRY süreçlerinin iyileştirilmesine yönelik önerilerin geliştirilmesi ▪ Risk yönetimi **rehberi ve standartlarının** gözden geçirilmesi ve onaylanması ▪ Grup şirketleri ve iş süreci seviyesinde **raporların onaylanması**
Üst Yönetim	▪ Risk yönetimi **kültürünün** yerleştirilmesi ▪ Risk yönetimi süreçlerinin **entegrasyonu** ▪ Risk değerlendirme süreçlerinin sonuçları hakkında Yönetim Kurulu ve Denetim Komitesi ile iletişim ▪ Karar alma süreçlerinde risk yönetimi çıktılarının göz önünde bulundurulması
Grup Şirketleri	▪ Risk yönetimi kültürünün sürdürülmesi ▪ İş süreçleri seviyesinde **risk değerlendirme raporlarının incelenmesi** ve raporlanması ▪ Risk yönetimi süreçlerinin planlama süreçleri ile entegrasyonunun sağlanması ▪ Yönetim süreçlerinde risk yönetimi çıktılarının göz önünde bulundurulması
İş Süreci Sahipleri	▪ İş süreçlerine ilişkin **risklerin sürekli izlenmesi ve yeni ve değişen risklerin raporlanması** ▪ Yönetim tarafından belirlenen tolerans limitlerinin aşım durumlarının raporlanması
Risk Yönetimi Birimi	▪ KRY uzmanı olarak KRY süreçlerinde koordinasyon rolü üstlenmesi ▪ Yönetim Kurulu ve Üst Yönetime mevcut durum **raporlarının hazırlanması** ▪ KRY metodoloji ve uygulama **eğitimlerinin geliştirilmesi** ▪ KRY **Yönetmeliğinin** hazırlanması ▪ Risk yönetimi **rehberi ve standartlarının** oluşturulması
İç Denetim	▪ KRY programının etkinliğinin değerlendirilmesi ve iç denetim planı ile entegrasyonun sağlanması

Üst Yönetim aşağıdaki faaliyetleri yönetmek konusunda ne kadar başarılı?



Kaynak: PwC Annual Corporate Directors Survey

Risklerin Yönetim Kurulu'na raporlanması



Kaynak: PwC Annual Corporate Directors Survey

Kurumsal Risk Yönetiminde Kritik Başarı Faktörleri

Kritik Başarı Faktörleri

Yönetişim

Üst Yönetim Desteği ve Risk Kültürü

Var Olan Süreçlere Entegrasyon

Risk Yönetimi Sorumluluklarının Belirlenmesi

Kritik Başarı Faktörleri

Metodoloji

Kök Neden ve Etki

Doğru sınıflama

Hedeflerle ilgili

Kritik Başarı Faktörleri

Metodoloji

Doğru değerlendirme

Doğru önceliklendirme

Doğru ÖRG tanımı

Kritik Başarı Faktörleri

Metodoloji

Doğru cevap

Doğru risk yönetimi faaliyeti

Uygun süre

Uygun sorumlu

Kurumsal risk yönetiminde zorlanılan konu başlıkları ve kritik faktörler

Risk sahiplerinin risklerin takip sorumluluğunu üstlenmek istememesi, Zayıf risk kültürünün KRY süreçlerini olumsuz etkilemesi

Farkındalık

Üst yönetimin KRY ve performans arasındaki bağı kuramaması

Hedef bazlı risk

Üst yönetim için KRY çalışmalarının katma değerinin yeterince ortaya koyulamaması

Etkin raporlama

KRY'nin rutin iş süreçlerine yeterince entegre edilmemiş olması

Var olan süreçlere entegrasyon

Teknolojik altyapının KRY'nin etkin uygulanması için yetersiz olması

Altyapı kurulumu ve entegrasyon

OAiB
ORTA ANADOLU
İHRACATÇI BİRLİKLERİ

Sorularınız?

Teşekkürler

İletişim Bilgileri

Tuğçe Aydoğan, CIA, CCSA,
COSO ERM, ISO 31000 Risk Yöneticisi
tugce.aydogan@pwc.com
+90 530 280 6341
+90 312 457 4501