Bilgi Güvenliğinde Risk Yönetimi

Tahsin TÜRKÖZ
tahsin.turkoz@tubitak.gov.tr

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

11 Ekim 2013

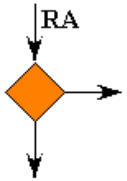
Temel Kavramlar

Risk

Varlık üzerindeki bir **açıklığın** bir **tehdit** tarafından kullanılmasına bağlı **zarar beklentisidir**.

Risk = f(Varlık, Açıklık, Tehdit)

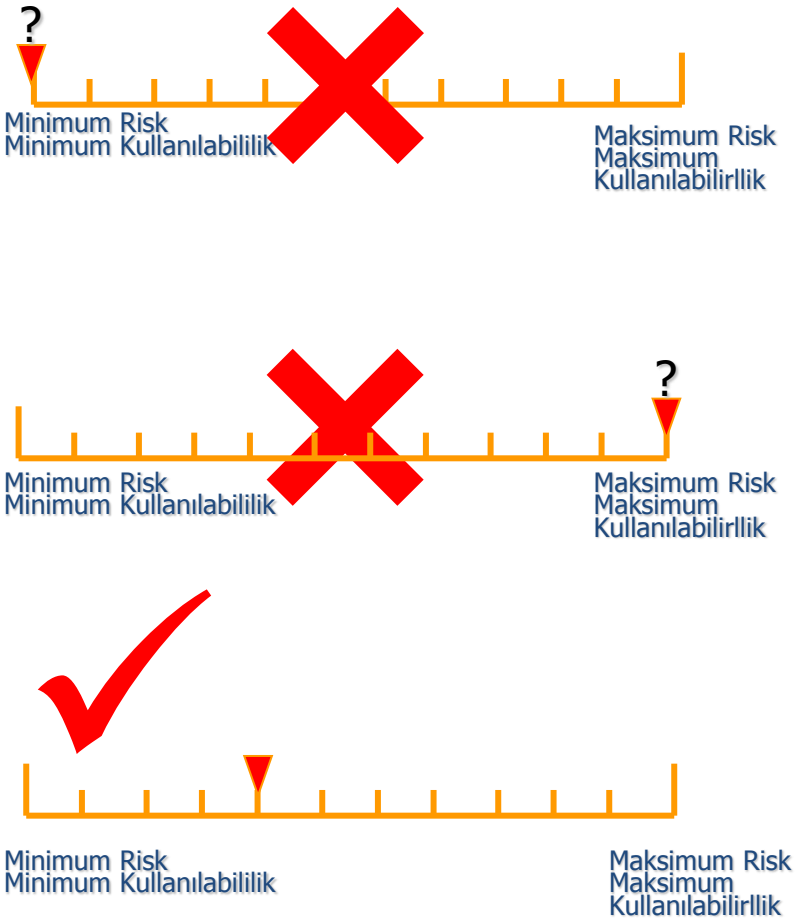
Risk Yönetimi

- Risk Yönetimi 
  - Risklerin Belirlenmesi (Identification) 
  - Risk Değerlendirme (Assessment)
    - Risk Analizi (Analysis)
    - Risk Derecelendirme (Evaluation) 

      
  - Risk Tedavisi (Treatment) 

Neden Risk Yönetimi?

Kullanılabilirlik & Güvenlik



Risklerin Belirlenmesi

- **Varlıkların ve** varlık **sahiplerinin** belirlenmesi
- Varlığa yönelik **tehditlerin** belirlenmesi
- Bu tehditlerin kullanabileceği **açıklıkların** belirlenmesi
- Tehdit ve açıklıkların varlığın gizlilik, bütünlük veya erişilebilirliğine **etkisinin belirlenmesi**

Varlıklar (“Assets”)

- İnsanlar *(personel, müşteriler, tedarikçiler..)*
- Bilgi *(kağıt ve elektronik ortamdaki)*
- Yazılım varlıkları
- Fiziksel varlıklar *(bilgisayar ve iletişim donanımı, altyapı varlıkları)*
- Hizmetler *(bilişim, ısıtma, havalandırma..)*
- Kurum imajı ve itibarı

Varlık Sahipleri

- **Varlık sahibi** = Birey veya birim

  Varlığın üretilmesinden, geliştirilmesinden, bakımından, kullanımından ve güvenliğinden sorumludur.

  - Varlığın ***sınıflandırılması***
  - Erişim haklarının belirlenmesi ve ***gözden geçirilmesi***

  İş sürecine, bir uygulamaya veya veri setine sahip atanabilir.

Varlık Envanteri

Personel	Sahibi	Değeri	Konum
Bilgi (Elektronik/Basılı)	Sahibi	Değeri	Konum
Yazılım varlıkları	Sahibi	Değeri	Konum
Donanım Bilgisayar, Modem, vb.	Sahibi	Değeri	Konum
Hizmetler	Sahibi	Değeri	Konum

Uygulama-1

Bir kurumsal iş sürecinin;

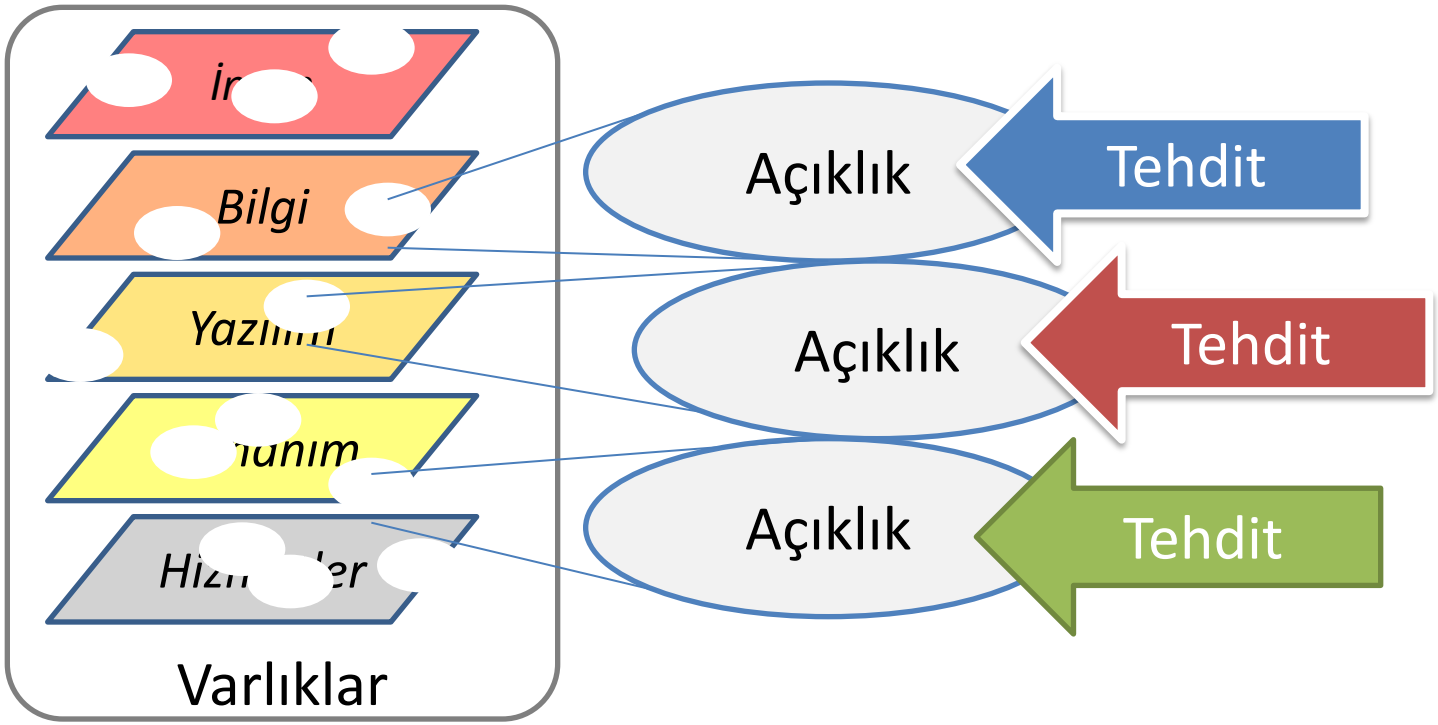
- Bilgi
- Yazılım
- Donanım, altyapı
- İnsan
- Alınan hizmet

varlıklarını ve varlık sahiplerini Risk Belirleme Tablosu.xls dosyasına listeleyiniz.

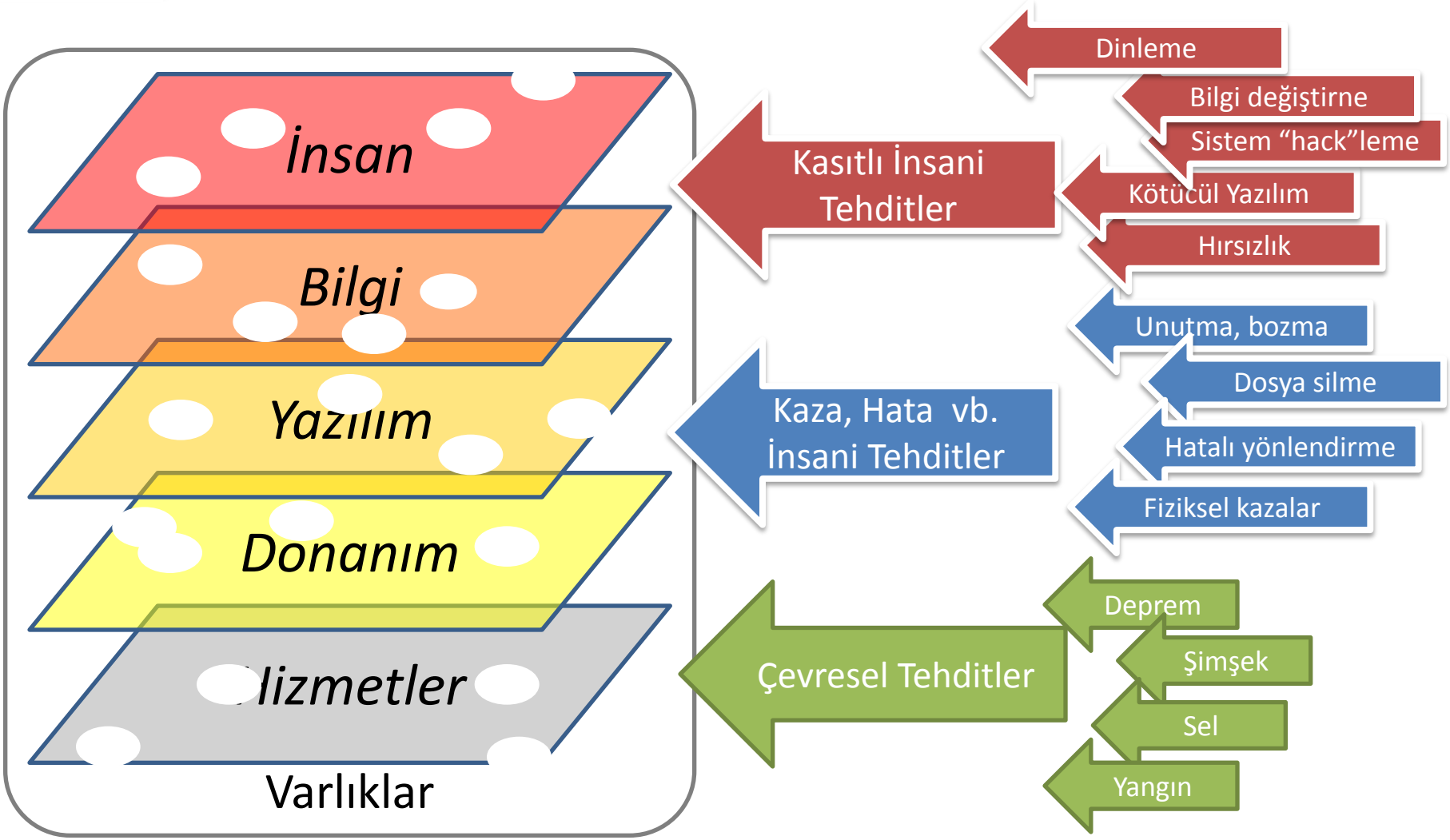
Açıklık – Tehdit – Karşı Önlem

- **Açıklık:** Varlıklarda bulunan kusurlardır.
- **Tehdit:** Varlıklardaki açıklıkları kullanarak zarar veren etkenlerdir.
- **Karşı Önlem:** Riski azaltmak amacıyla alınan tedbirler.
  - Varlığın değerini düşürücü
  - Açıklığın derecesini düşürücü
  - Tehdidin etkisini/olma ihtimalini düşürücü

Tehditler ve Açıklıklar



Tehditler*



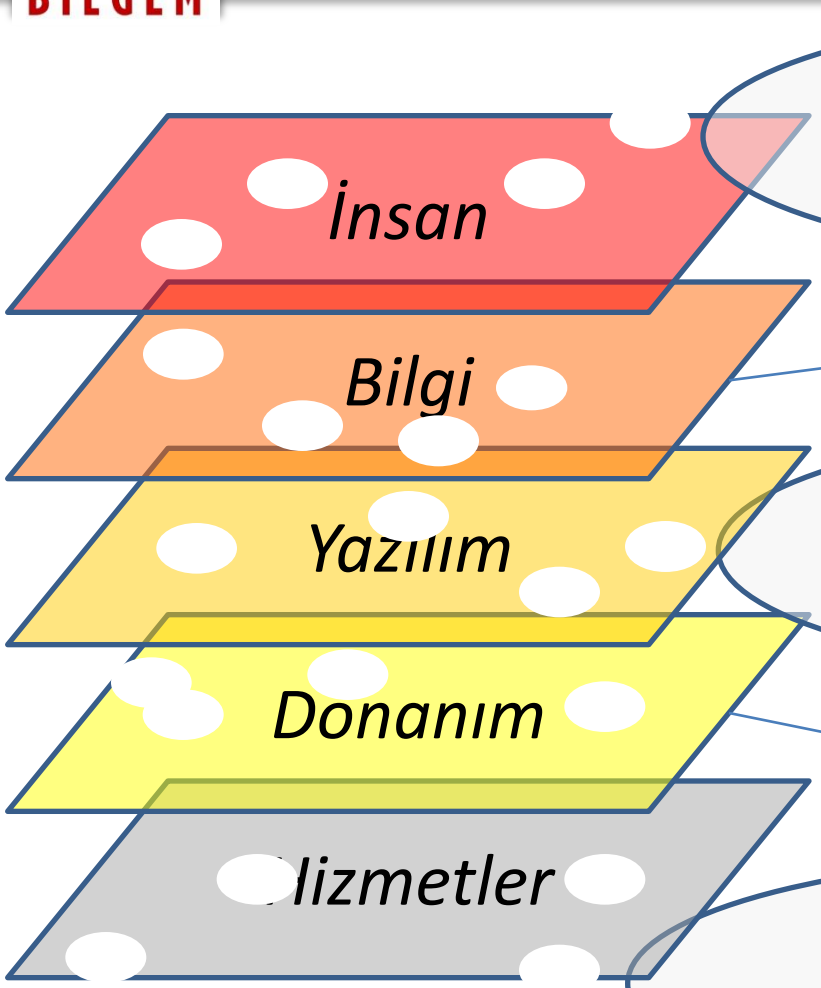
(*) ISO/IEC 13335-1:2004 - Concepts and models for information and communications technology security management – Threats.

Uygulama-2

- Tehdit Listesi dosyasını inceleyiniz.

- Uygulama-1'de listelenen bilgi varlıklarına yönelik *tehditleri* aynı dosyada ilgili varlığın karşısına kaydediniz.

Açıklıklar*



Personel eksikliği / Bilgi güvenliği farkındalığında eksiklik / Yetersiz işe alma süreci / Kaza ve hastalıklara açık olma

Erişim kontrolü, yedekleme ve güvenli imha prosedürlerinin bulunmaması / Kontrolsuz kopyalama

Yetersiz tasarım, test ve dokümantasyon süreci / Eski yazılım sürümlerini kullanmak

Periyodik yenileme ve bakım eksikliği / Voltaj, sıcaklık ve nemdeki değişikliklere dayanıksızlık

Yetersiz sözleşme yönetimi

(*) ISO/IEC TR 13335-3 - Techniques for the Management of IT Security – Annex D - Common Vulnerabilities

Uygulama-3

- Açıklık Listesi dosyasını inceleyiniz.

- Uygulama-2'de belirlediğiniz tehditlerin kullanabileceği *açıklıkları* aynı dosyaya kaydediniz.

Uygulama-4

Uygulama-2 ve Uygulama-3'te belirlenen tehdit ve açıklıkların bilgi varlıklarının

- Gizlilik,
- Bütünlük ve
- Erişilebilirliğine

etkisini belirleyiniz.

Risk Değerlendirme

- Risk analizi ve risk derecelendirme süreçlerinin bütünü ...
- Risk değerlendirmesi sonucunda:
  - Kabul edilebilir risk seviyesi belirlenir
  - Hangi risk için ne yapılacağı belirlenir:
    - Risk işleme
    - Diğer seçenekler
  - Riskler kritiklik sırasına göre sıralanır.
  - Azaltılacak risk kalemlerinin öncelikleri belirlenir.

Risklerin Analizi ve Derecelendirmesi

- Güvenlik ihlalinin oluşması sonucunda kurumun karşılaşacağı **zararın belirlenmesi**
- Güvenlik ihlalinin oluşma **olasılığın**ın **belirlenmesi**
- Riskin hesaplanması
- Riskin, önceden tanımlanmış olan risk ölçeğine göre değerlendirilmesi

Risk Derecelendirme

Tartışma-1

Zararın belirlenmesinde kullanılabilecek ölçek gözden geçirilir ve tartışmaya açılır.

Zarar Belirleme Ölçeği

Zararın Etki Derecesi		Zararın Açıklaması
4	Çok yüksek	•Kurumun itibarının kaybolması •Hayati tehlike / can kaybı •Çok yüksek düzeyde maddi kayıp
3	Yüksek	•Kurumun itibarının ciddi düzeyde zarara uğraması •Belirgin hayati tehlike / can kaybı olasılığı •Yüksek düzeyde maddi kayıp
2	Orta	•Kurumun itibarının orta düzeyde zarara uğraması •Orta düzeyde hayati tehlike •Orta düzeyde maddi kayıp
1	Düşük	•Kurumun itibarının hafif düzeyde zarara uğraması (durum kurtarılabilir) •Düşük düzeyde hayati tehlike •Düşük düzeyde maddi kayıp

Uygulama-5

Güvenlik ihlallerinin oluşması halinde kurumun karşılaşacağı **zararı belirleyiniz.**

Tartışma-2

Olasılığın belirlenmesinde kullanılabilecek ölçek gözden geçirilir ve tartışmaya açılır.

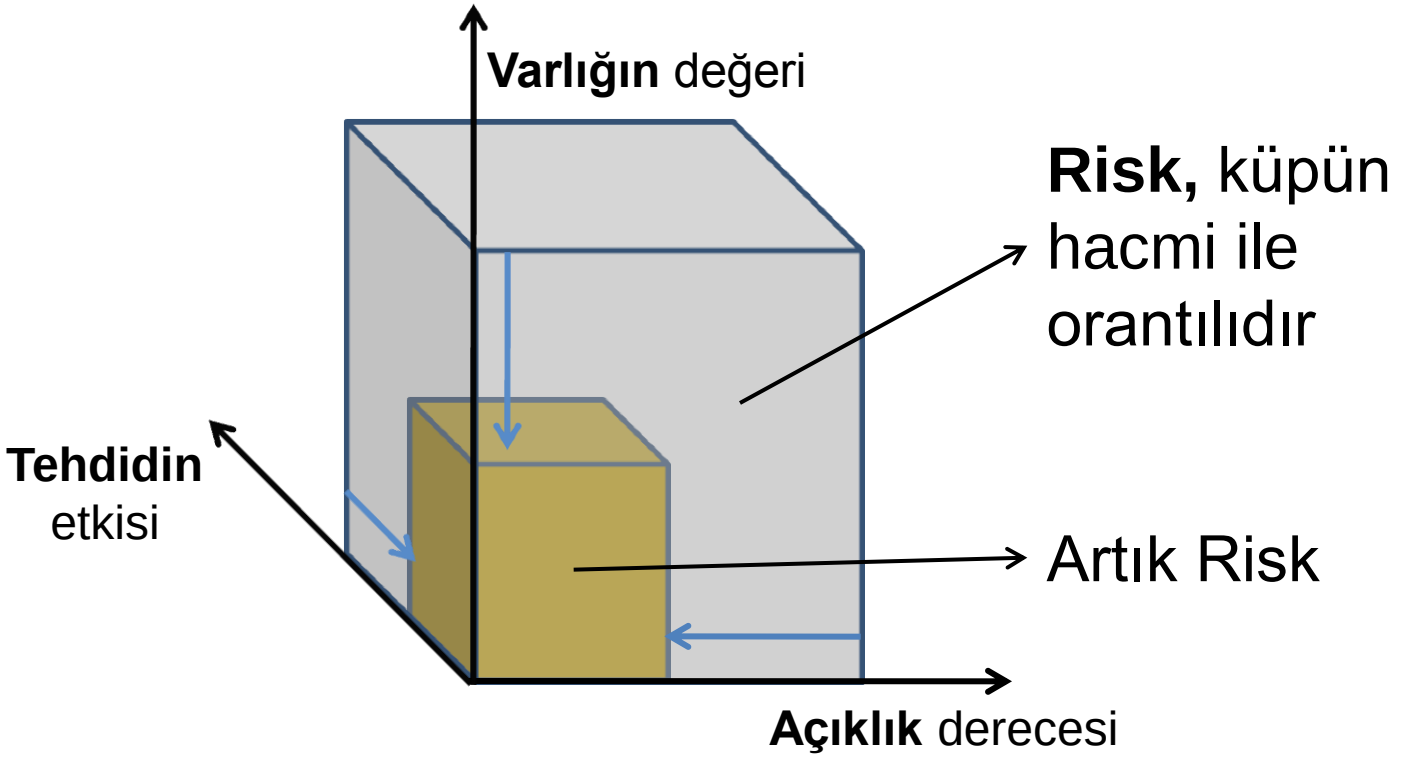
Tehdit Olasılığı Belirleme Ölçeği

Olasılık Değeri	Gerçekleşme sıklığı	Değer Adı
5	Günde en az bir defa	ÇY (Çok yüksek)
4	Haftada en az bir defa	Y (Yüksek)
3	Üç ayda bir defadan çok	O (Orta)
2	Yılda bir defadan çok	D (Düşük)
1	Yılda bir defadan az	ÇD (Çok düşük)

Uygulama-6

Güvenlik ihlallerinin oluşma **olasılıklarını belirleyiniz.**

Riskin Hesaplanması



Risk = F(Varlık, Açıklık, Tehdit)

Zarar x Olasılık

Uygulama-8

Risk değerlerini belirleyiniz.

Terminoloji

Kabul edilebilir risk:

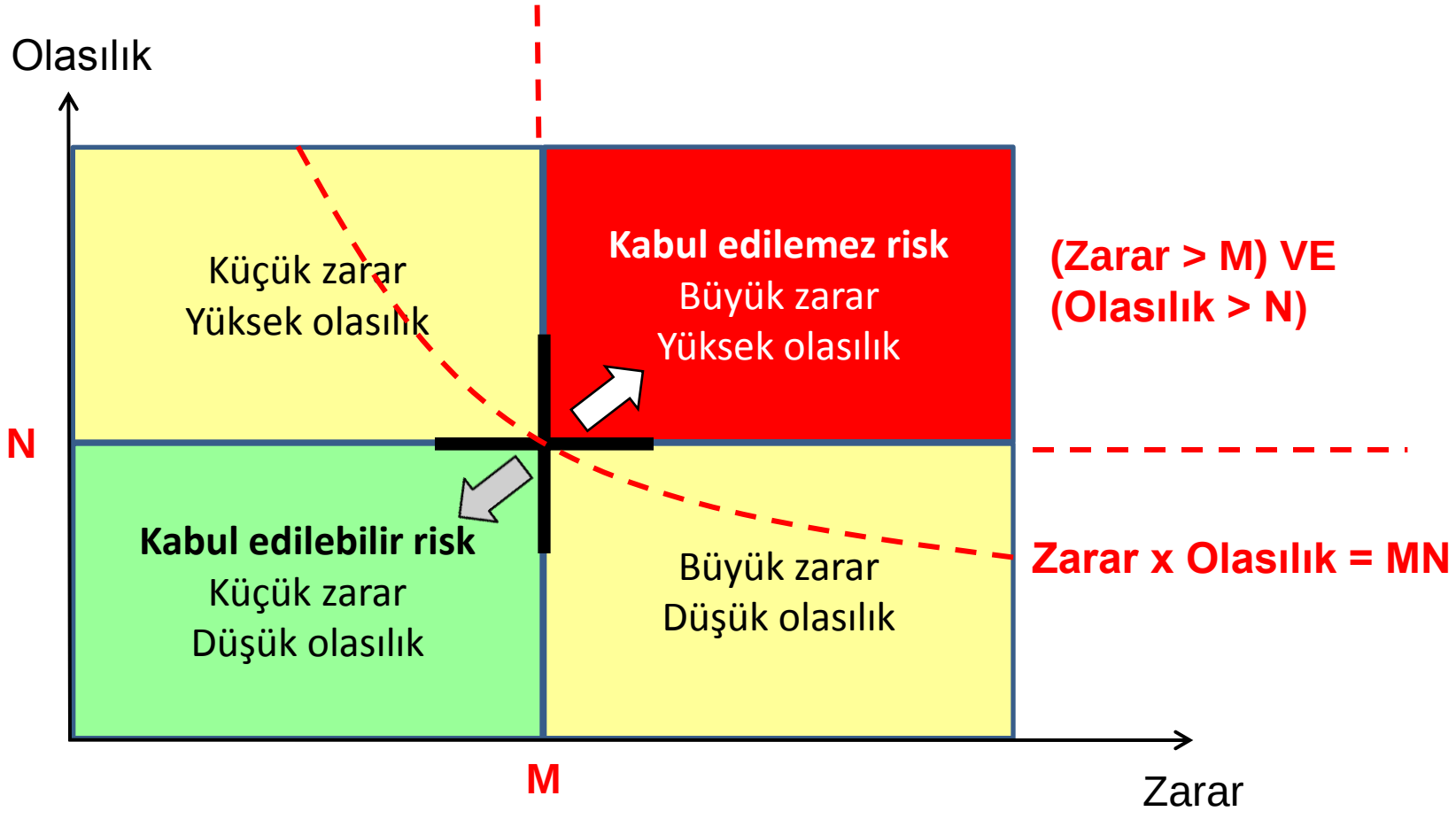
Belli bir sistem veya varlık için kurumun güvenlik ihtiyaçları çerçevesinde kabul edebileceği risk miktarı.

Risk Derecelendirme Kriterleri

- **Kabul edilebilir risk** seviyesinin belirlenmesi
  - Yasal gereksinimler
  - Müşteri ve kontrat gereksinimleri
  - Güvenlik ihtiyaçları
  - Bütçe / Maliyet
  - Uygulama kolaylığı

  göz önünde bulundurulur.

Risk Derecelendirme



Uygulama-9

- Risk değerleri gözden geçirilerek kabul edilebilir risk seviyesinin ne olabileceği tartışılır.

Risk İşleme Seçeneklerinin Tanımlanması ve Derecelendirilmesi

- Risk işleme seçenekleri
  - Uygun kontrollerin uygulanması
  - Risk kabulü
  - Riskten kaçınma
  - Riski transfer etme

Artık Risk

- Risk işleme sonrasında kalan risk (“residual risk”)…
- Artık riski değerlendirin (Kabul edilebilir / edilemez…)
  - Daha fazla kontrol uygulayın
  - Kabul etmek zorunda kalınabilir
- **Yönetim onayı gerekir.**