MUH442 Bilişimde Güvenlik – 2

Prof. Dr. Hasan Hüseyin BALIK

(2. Hafta)

İçerik

- 2.Yönetim Sorunları
  - 2.1. BT Güvenlik Yönetimi ve Risk Değerlendirmesi
  - 2.2.BT Güvenlik Kontrolleri, Planları ve Prosedürleri
  - 2.3.Fiziksel ve Altyapı Güvenliği
  - 2.4. İnsan Kaynakları Güvenliği
  - 2.5. Güvenlik Denetimi
  - 2.6. Bilişim Güvenliğinde Yasal ve Etik Hususlar

2.1.BT Güvenlik Yönetimi ve Risk Değerlendirmesi

2.1.İçerik

- BT Güvenlik Yönetimi
- Kurumsal Bağlam ve Güvenlik Politikası
- Güvenlik Riski Değerlendirme
- Detaylı Güvenlik Riski Analizi
- Vaka Çalışması: Gümüş Yıldız Madenleri

BT Güvenlik Yönetimine Genel Bakış

Soruları cevaplamanın resmi süreci:

Hangi varlıkların korunması gerekir? → Bu varlıklar nasıl tehdit ediliyor? → Bu tehditlere karşı ne yapılabilir?

- Kritik varlıkların uygun maliyetli bir şekilde yeterince korunmasını sağlar
- Kuruluşta koruma gerektiren her varlık için güvenlik riski değerlendirmesi gereklidir.
- Belirlenen riskleri azaltmak için hangi yönetimsel, operasyonel ve teknik kontrollerin gerekli olduğuna karar vermek için gerekli bilgileri sağlar.

BT Güvenlik Tekniklerine İlişkin ISO/IEC 27000 Standartları Serisi

27000:2016	"Bilgi güvenliği yönetim sistemleri—Genel bakış ve Kullanılan Terimler", bilgi güvenliği yönetim sistemlerine genel bir bakış sağlar ve 27000 standart ailesinde kullanılan terim ve tanımları sağlar.
27001:2013	"Bilgi güvenliği yönetim sistemleri—Gereksinimler", belgelenmiş bir Bilgi Güvenliği Yönetim Sisteminin kurulması, uygulanması, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve iyileştirilmesi için gereksinimleri belirtir.
27002:2013	"Bilgi güvenliği yönetimi için uygulama kuralları", bir kuruluşta bilgi güvenliği yönetimi için yönergeler sağlar ve en iyi uygulama güvenlik kontrollerinin bir listesini içerir. Eskiden ISO17799 olarak biliniyordu.
27003:2010	"Bilgi güvenliği yönetim sistemi uygulama kılavuzu", bir Bilgi Güvenliği Yönetim Sistemi spesifikasyonunun ve tasarımının başlangıcından uygulama planlarının üretilmesine kadar olan süreci detaylandırır.
27004:2009	"Bilgi güvenliği yönetimi—Ölçme", kuruluşların Bilgi Güvenliği Yönetim Sistemi süreçlerinin ve kontrollerinin etkinliğini ölçmelerine ve raporlamalarına yardımcı olmak için rehberlik sağlar.
27005:2011	"Bilgi güvenliği risk yönetimi", bilgi güvenliği risk yönetimi sürecine ilişkin yönergeler sağlar. ISO13335-3/4'ün yerini almıştır.
27006:2015	"Bilgi güvenliği yönetim sistemlerinin denetimini ve belgelendirmesini sağlayan kuruluşlar için gereklilikler" bu kuruluşlar için gereksinimleri belirtir ve rehberlik sağlar.

BT Güvenlik Yönetimi

BT GÜVENLİK YÖNETİMİ: Uygun düzeyde gizlilik, bütünlük, kullanılabilirlik, hesap verebilirlik, özgünlük ve güvenilirlik elde etmek ve sürdürmek için kullanılan bir süreçtir. BT güvenlik yönetimi işlevleri şunları içerir:

Kurumsal BT güvenlik hedeflerinin, stratejilerinin ve politikalarının belirlenmesi	**Kurumsal BT güvenlik gereksinimlerinin belirlenmesi**	**Kuruluş içindeki BT varlıklarına yönelik güvenlik tehditlerini belirleme ve analiz etme**	**Riskleri belirleme ve analiz etme**	**Uygun güvenlik önlemlerinin belirtilmesi**	**Kuruluş içindeki bilgi ve hizmetleri maliyet etkin bir şekilde korumak için gerekli olan koruma önlemlerinin uygulanmasının ve işleyişinin izlenmesi**	**Bir güvenlik farkındalık programı geliştirme ve uygulama**	**Olayları algılama ve tepki verme**

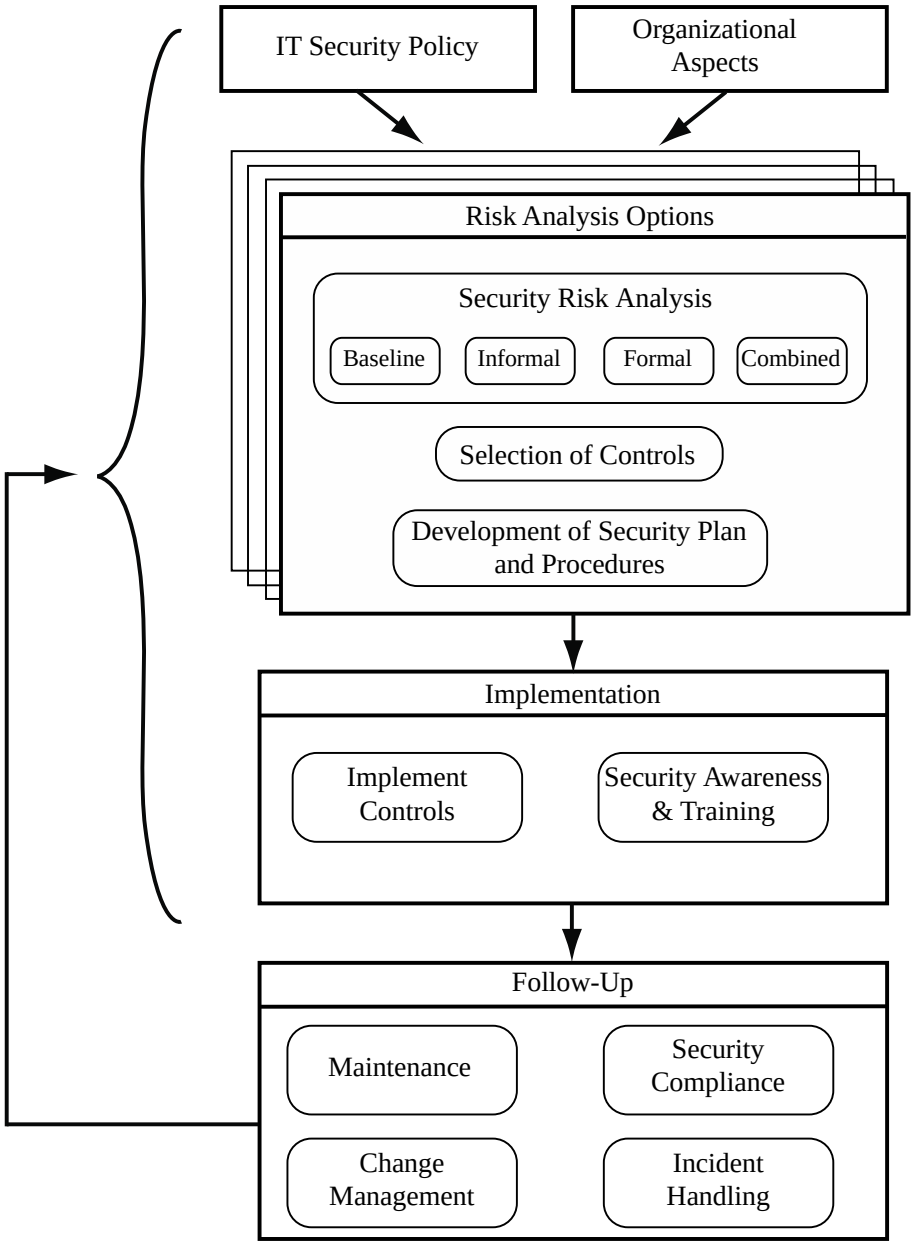


Figure 14.1 Overview of IT Security Management

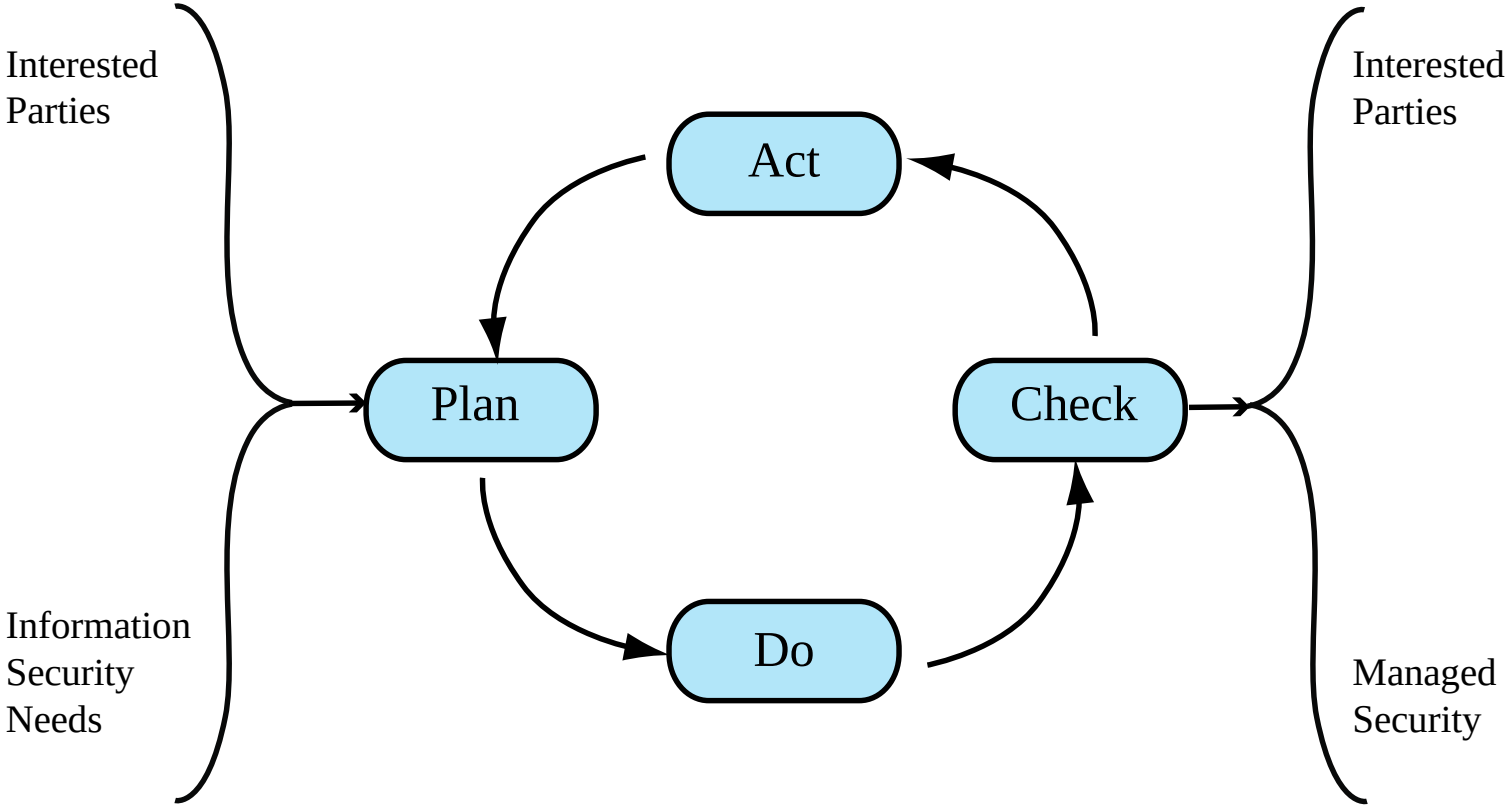


Figure 14.2 The Plan - Do - Check - Act Process Model

Kurumsal Bağlamda Güvenlik Politikası

- Düzenli olarak sürdürülür ve güncellenir
  - Periyodik güvenlik incelemelerini kullanma
  - Değişen teknik/risk ortamlarını yansıtın
- BT sistemlerinin organizasyondaki rolünü ve önemini incelemek

Önce kuruluşun BT güvenliğini inceleyin:

Hedefler - istenen BT güvenliği sonuçları

Stratejiler - hedeflere nasıl ulaşılır

Politikalar - yapılması gerekenler

Güvenlik Politikası

Adreslenmesi gerekenler:

- Hedeflerin iş, yasal ve düzenleyici gerekliliklerle ilişkisi dahil olmak üzere kapsam ve amaç
- BT güvenlik gereksinimleri
- Sorumlulukların atanması
- Risk yönetimi yaklaşımı
- Güvenlik bilinci ve eğitimi
- Genel personel sorunları ve yasal yaptırımlar
- Güvenliğin sistem geliştirmeye entegrasyonu
- Bilgi sınıflandırma şeması
- Acil durum ve iş sürekliliği planlaması
- Olay algılama ve işleme süreçleri
- Politika nasıl ve ne zaman gözden geçirilir ve kontrolü ona göre değiştirir

Yönetim Desteği

- BT güvenlik politikası üst yönetim tarafından desteklenmelidir
- BT güvenlik personeline ihtiyaç var
  - Tutarlı genel denetim sağlamak
  - Üst yönetim ile irtibat
  - BT güvenlik hedeflerinin, stratejilerinin, politikalarının sürdürülmesi
  - Olayları ele alma
  - BT güvenliği farkındalığı ve eğitim programlarının yönetimi
  - BT proje güvenlik personeli etkileşim
- Büyük kuruluşlar, büyük projeler ve sistemlerle ilişkili ayrı BT proje güvenlik görevlilerine ihtiyaç duyar
  - Alan içi güvenlik politikalarını yönetin

Güvenlik Riski Değerlendirmesi

Sürecin kritik bileşeni

İdeal olarak her kurumsal varlığı inceleyin

- Pratikte pek mümkün değil

Bir kuruluşun BT altyapısına yönelik riskleri belirleme ve azaltmaya yönelik yaklaşımlar:

- Temel
- Gayri resmi
- Ayrıntılı risk
- Bütünleşik

Temel Yaklaşım

- Amaç, en yaygın tehditlere karşı koruma sağlamak için üzerinde anlaşmaya varılan kontrolleri uygulamaktır.
- Daha fazla güvenlik önlemi için iyi bir temel oluşturur
- "Endüstrinin en iyi uygulamasını" kullanın
  - Kolay, ucuz, çoğaltılabilir
  - Riske maruz kalmadaki değişikliklere özel bir önem vermez
  - Çok fazla veya çok az güvenlik sağlayabilir
- Genellikle daha yapılandırılmış yaklaşımları uygulamak için kaynakları olmayan küçük kuruluşlar için önerilir

Gayri Resmi Yaklaşım

Kuruluşun BT sistemleri üzerinde resmi olmayan, pragmatik bir risk analizi yürütmeyi içerir.

Analistin bilgi ve uzmanlığından yararlanır

Oldukça hızlı ve ucuz

Temel yaklaşımın ele almadığı güvenlik açıkları ve riskler hakkında yargıda bulunulabilir.

Bazı riskler yanlış değerlendirilebilir

Analistin görüşlerine göre çarpık, zamana göre değişir

BT sistemlerinin zorunlu olmadığı küçük ve orta ölçekli kuruluşlar için uygundur

Detaylı Risk Analizi

Bütünleşik Yaklaşım

- Temel, resmi olmayan ve ayrıntılı risk analizi yaklaşımlarının unsurlarını birleştirir
- Amaç, mümkün olan en kısa sürede makul düzeyde koruma sağlamak, ardından zaman içinde önemli sistemlerde uygulanan koruma kontrollerini incelemek ve ayarlamaktır.
- Yaklaşım, tüm sistemlerde uygun temel güvenlik önerilerinin uygulanmasıyla başlar.
- Ardından, yüksek risk seviyelerine maruz kalan veya organizasyonun iş hedefleri için kritik olan sistemler, yüksek seviyeli risk değerlendirmesinde belirlenir.
- Daha sonra, kontrollerin gereksinimlerini daha doğru bir şekilde yansıtacak şekilde nispeten hızlı bir şekilde uyarlamak amacıyla, kilit sistemler üzerinde muhtemelen anında gayri resmi bir risk değerlendirmesi yapmak için bir karar verilebilir.
- Son olarak, bu sistemlerin detaylı risk analizlerinin yapılması için düzenli bir süreç başlatılabilir.
- Zamanla bu, en uygun ve uygun maliyetli güvenlik kontrollerinin seçilmesine ve bu sistemlerde uygulanmasına neden olabilir.

Detaylı Güvenlik Riski Analizi

Bir kuruluşun BT sisteminin güvenlik risklerinin en doğru şekilde değerlendirilmesini sağlar

En yüksek maliyetli

Başlangıçta savunma güvenliği endişelerini ele almaya odaklanır

Genellikle devlet kurumları ve ilgili işletmeler tarafından zorunlu kılınır

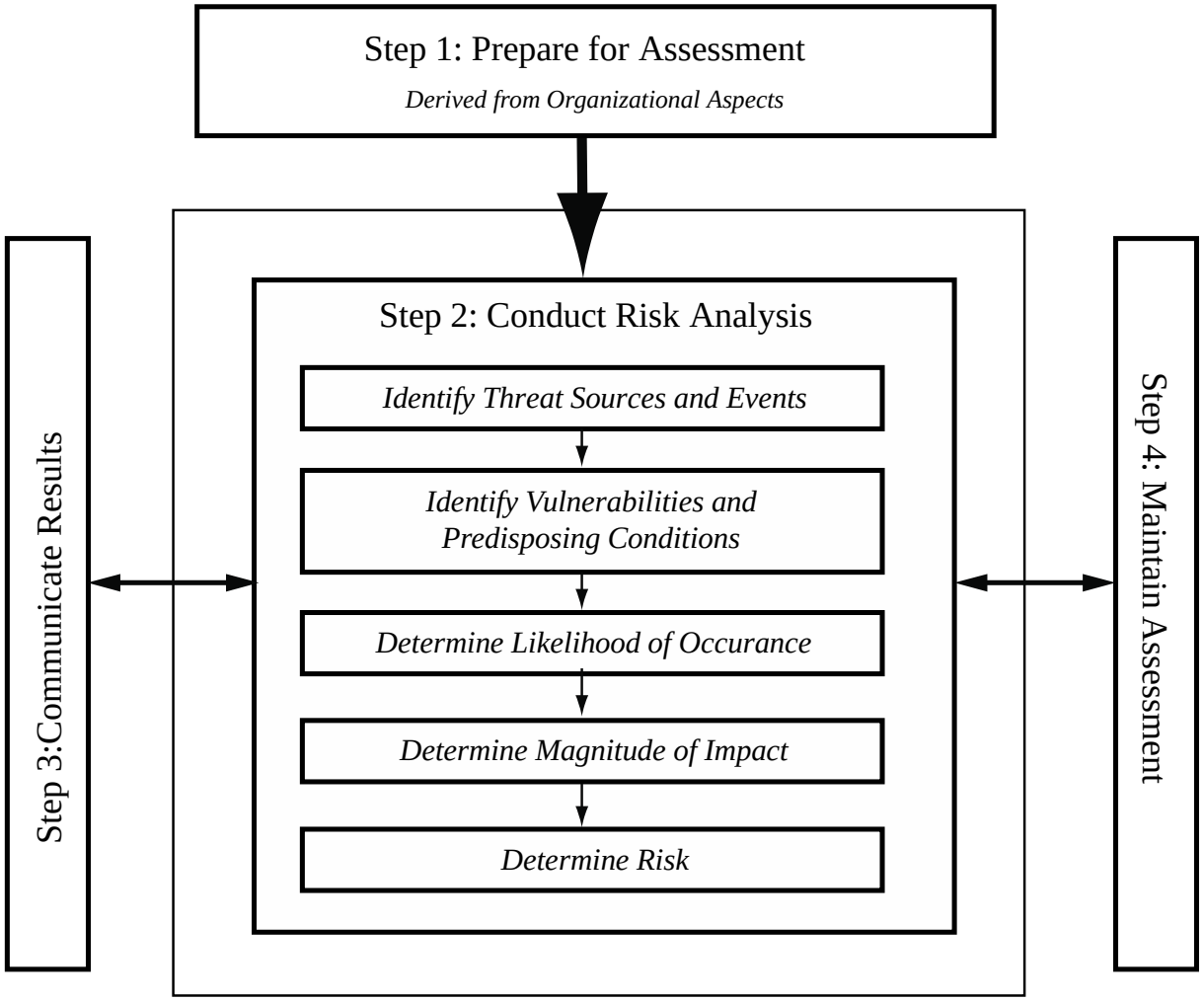


Figure 14.3 Risk Assessment Process

Bağlamı Oluşturma

- İlk adım
  - Risk değerlendirmesinin temel parametrelerini belirleyin
  - İncelenecek varlıkları tanımlayın
- Kuruluşun faaliyet gösterdiği siyasi ve sosyal ortamı araştır
  - Yasal ve düzenleyici kısıtlamalar
  - Kuruluşun riske maruz kalması için temel sağlayın
- Risk arzusu
  - Kuruluşun kabul edilebilir olarak gördüğü risk seviyesi

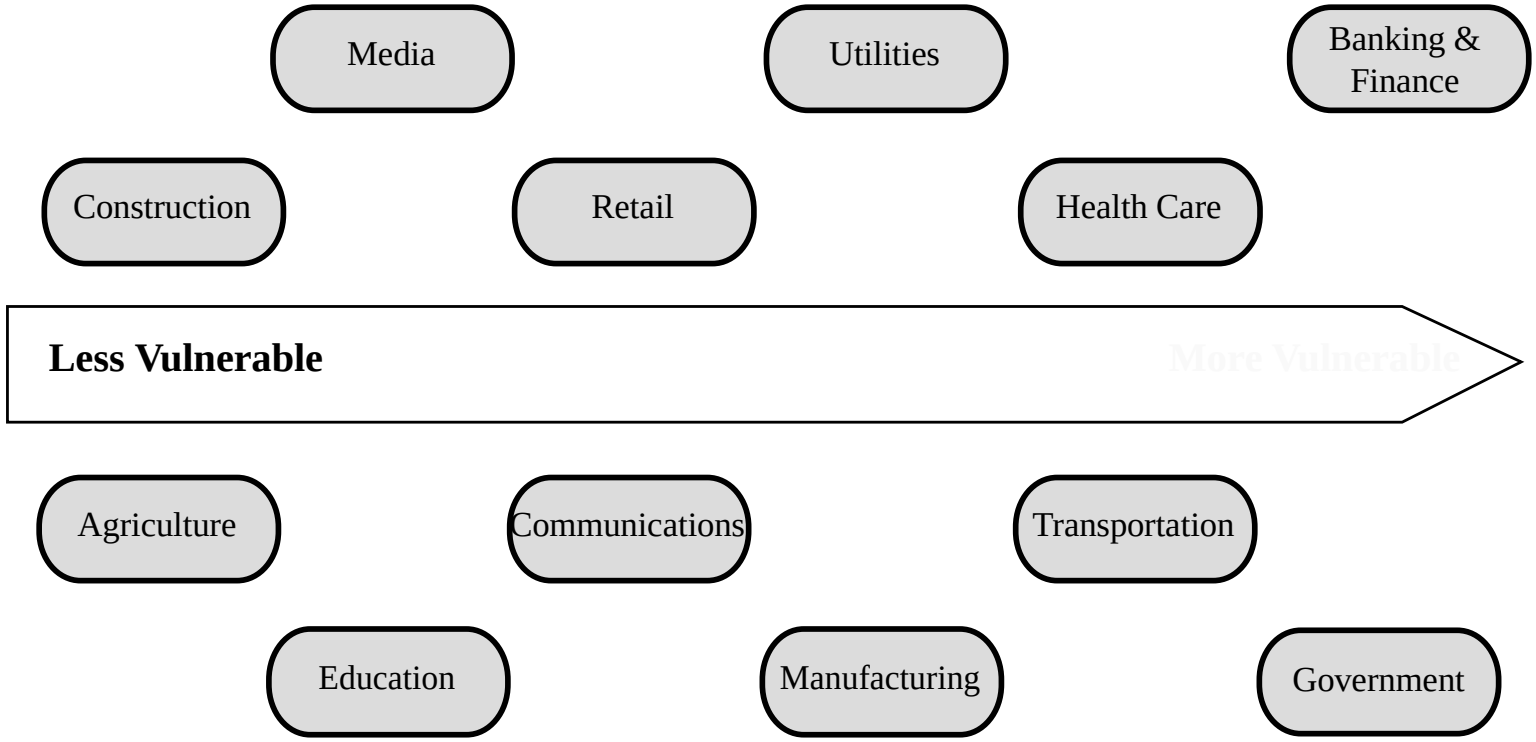


Figure 14.4 Generic Organizational Risk Context

Varlığın Tanımlanması

- Son bileşen, incelenecek varlıkları belirlemektir
- Önemli varlıkları belirlemek için organizasyonun ilgili alanlarındaki kişilerin uzmanlığından yararlanın
  - Bu tür personeli belirleyin ve onlarla görüşün

Varlık
"korunması gereken her şey" çünkü kuruluş için değeri vardır ve kuruluşun hedeflerine başarılı bir şekilde ulaşılmasına katkıda bulunur.

Terminoloji

- **Varlık:** Koruma gerektiren, sahibine değer katan bir sistem kaynağı veya yeteneği
- **Tehdit:** Bir tehdit kaynağının, bazı varlıklardaki bir güvenlik açığından yararlanma potansiyeli; bu, meydana gelmesi durumunda varlığın güvenliğini tehlikeye atabilir ve varlığın sahibine zarar verebilir.
- **Güvenlik Açığı:** Bir varlığın tasarımında, uygulamasında veya işletiminde ve yönetiminde bazı tehditler tarafından kullanılabilecek bir kusur veya zayıflık
- **Risk:** Belirli bir tehdidin bir varlığa yönelik bazı açıklardan yararlanma olasılığı ile varlığın sahibine yol açan zararlı sonuçların büyüklüğünün birleşimi olarak hesaplanan kayıp potansiyeli.

Tehdidin Tanımlanması

- Tehdit:

Tehdit Kaynakları

- Tehditler …… olabilir
  - Doğal "Allah'tan gelen"
  - İnsan yapımı
  - Kazara veya kasıtlı

İnsani tehditlerin değerlendirilmesinde dikkate alınanlar::

- Motivasyon
- Kabiliyet
- Kaynaklar
- Saldırı olasılığı
- Caydırıcılık

- Kuruluş tarafından tecrübe edilen herhangi bir önceki saldırı deneyimi de dikkate alınmalıdır.

Güvenlik Açığı Tanımlama

- Kuruluşun BT sistemlerindeki veya süreçlerindeki istismar edilebilir kusurları veya zayıflıkları belirleyin
  - Tehdidin kuruluşa uygulanabilirliğini ve önemini belirler
- Bir varlığa risk oluşturmak için tehdit ve güvenlik açığı kombinasyonuna ihtiyaç var
- Çıktı, nasıl ve neden meydana gelebileceklerine dair kısa açıklamalarla birlikte tehditlerin ve güvenlik açıklarının bir listesi olmalıdır.

Risklerin Analizi

- Mevcut kontroller göz önüne alındığında, varlığa yönelik olarak tanımlanan her tehdidin gerçekleşme olasılığını belirtin
- Tehdit meydana geldiğinde sonucu belirtin
- Her tehdit için genel risk derecesini türet
  - Risk = olasılık tehdidi oluşur x kuruluş için maliyet
- Kesin olasılıkları ve gerçekçi maliyet sonuçlarını belirlemek zor
- Niceliksel değil niteliksel derecelendirmeler kullanın

Mevcut Kontrollerin Analizi

- Tehditleri en aza indirmeye çalışmak için kullanılan mevcut kontrollerin tanımlanması gerekir
- Güvenlik kontrolleri şunları içerir:
  - Yönetimsel
  - operasyonel
  - Teknik

  süreçler ve prosedürler
- Bilgi almak için mevcut kontrollerin kontrol listelerini kullanın ve önemli organizasyon personeliyle görüşün

Risk Olasılığı

Derece	Olasılık	Genişletilmiş Tanım
1	Nadiren	Sadece istisnai durumlarda ortaya çıkabilir ve "şanssız" veya pek olası görülmeyebilir.
2	Olası olmayan	Mevcut kontroller, koşullar ve son olaylar göz önüne alındığında, herhangi bir zamanda meydana gelebilir ancak beklenmeyen bir durumdur.
3	Mümkün	Bir süre sonra ortaya çıkabilir, ancak olmama olasılığı kadar. Dış etkilerden dolayı oluşumunu kontrol etmek zor olabilir.
4	Büyük ihtimalle	Muhtemelen bazı durumlarda ortaya çıkacaktır ve gerçekleşirse şaşırmamak gerekir.
5	Neredeyse kesin	Çoğu durumda ve kesinlikle er ya da geç gerçekleşmesi bekleniyor

Derece	Sonuç	Genişletilmiş Tanım
1	Önemsiz	Genellikle, tek bir alanda küçük bir güvenlik ihlalinin sonucudur. Etki muhtemelen birkaç günden az sürecektir ve düzeltilmesi için yalnızca küçük harcamalar gerekir. Genellikle kuruluşa herhangi bir somut zararla sonuçlanmaz.
2	Küçük	Bir veya iki alanda güvenlik ihlalinin sonucudur. Etki muhtemelen bir haftadan az sürecektir ancak yönetim müdahalesi olmaksızın segment veya proje düzeyinde ele alınabilir. Genellikle proje veya ekip kaynakları dahilinde düzeltilebilir. Yine, kuruluş için somut bir zarara yol açmaz, ancak geriye dönüp bakıldığında, daha önce kaybedilen fırsatları veya verimlilik eksikliğini gösterebilir.
3	Orta	Sınırlı sistemik (ve muhtemelen devam eden) güvenlik ihlalleri. Etki muhtemelen 2 haftaya kadar sürecektir ve genellikle yönetim müdahalesi gerektirecektir, ancak yine de proje veya ekip düzeyinde ele alınabilmelidir. Üstesinden gelmek için bazı devam eden uyum maliyetlerini gerektirecektir. Müşteriler veya halk bu olaydan dolaylı olarak haberdar olabilir veya sınırlı bilgiye sahip olabilir.
4	Ciddi	Devam eden sistemik güvenlik ihlali. Etki muhtemelen 4-8 hafta sürecek ve üstesinden gelinmesi için önemli yönetim müdahalesi ve kaynakları gerektirecektir. Üst yönetimin, olay süresince devam eden doğrudan yönetimi sürdürmesi gerekecektir ve uyum maliyetlerinin önemli olması beklenmektedir. Müşteriler veya halk, böyle bir olayın meydana geldiğinden haberdar olacak ve bir dizi önemli gerçeğe sahip olacaktır. İş veya organizasyonel sonuçların kaybı mümkündür, ancak özellikle bu bir defaya mahsus ise beklenmez.
5	Katastrofik-felaket	Büyük sistemik güvenlik ihlali. Etki 3 ay veya daha fazla sürecek ve eksikliklerin giderilmesi için üst yönetimin etkinlik süresince müdahale etmesi gerekecektir. Uyum maliyetlerinin çok yüksek olması beklenmektedir. Müşteri iş kaybı veya kuruluşa diğer önemli zararlar bekleniyor. Kuruluşla ilgili önemli kamu veya siyasi tartışmalar ve kuruluşa duyulan güven kaybı muhtemeldir. İlgili personele karşı olası cezai veya disiplin cezası muhtemeldir.
6	Kıyamet günü	Büyük sistemik güvenlik ihlallerinin birden çok örneği. Etki süresi belirlenemez ve üst yönetimin şirketi gönüllü yönetime veya diğer büyük yeniden yapılandırma biçimlerine tabi tutması gerekecektir. Üst yönetime karşı cezai takibat yapılması beklenir ve önemli ölçüde iş kaybı ve kurumsal hedeflere ulaşılamaması kaçınılmazdır. Uyum maliyetlerinin, muhtemelen organizasyonun tasfiyesi ile birlikte, bazı yıllar için yıllık kayıplarla sonuçlanması muhtemeldir.

Risk Sonuçları

Risk Seviyesi Belirleme ve Anlamı

	SONUÇ					
Olasılık	**Kiyamet günü**	**Katastrofik-felaket**	**Ciddi**	**Orta**	**Küçük**	**Ömensiz**
Neredeyse kesin	E	E	E	E	Y	Y
Büyük ihtimalle	E	E	E	Y	Y	O
Mümkün	E	E	E	Y	M	D
Olası olmayan	E	E	Y	O	D	D
Nadiren	E	Y	Y	O	D	D

Risk	**Tanım**
Extrim (E)	Bir yönetici/direktör düzeyinde ayrıntılı araştırma ve yönetim planlaması gerektirecektir. Düzenli incelemelerle sürekli planlama ve izleme gerekli olacaktır. Maliyetleri muhtemelen orijinal tahminleri aşan riskleri yönetmek için kontrollerde önemli ayarlamalar yapılması bekleniyor.
Yüksek (Y)	Yönetimin dikkatini gerektirir, ancak yönetim ve planlama üst düzey proje veya ekip liderlerine bırakılabilir. Düzenli gözden geçirmelerle devam eden planlama ve izleme olasıdır, ancak kontrollerin ayarlanması muhtemelen mevcut kaynaklardan karşılanacaktır.
Orta (O)	Mevcut özel izleme ve müdahale prosedürleri ile yönetilebilir. Çalışanlar tarafından yönetim, uygun izleme ve incelemelerle uygundur.
Düşük (D)	Rutin prosedürlerle yönetilebilir.

Risk Kaydı

Varlık	Tehdit/ Güvenlik Açığı	Var olan Kontroller	Olma olasılığı	Sonuç	Risk Seviyesi	Risk Önceliği
İnternet yönlendiricisi	Dışarıdan hacker saldırısı	Yalnızca yönetici şifresi	Mümkün	Orta	Y	1
Veri merkezinin zarar görmesi	Kaza sonucu yangın veya su basması	Yok (felaket kurtarma planı yok)	Olası olmayan	Ciddi	Y	2

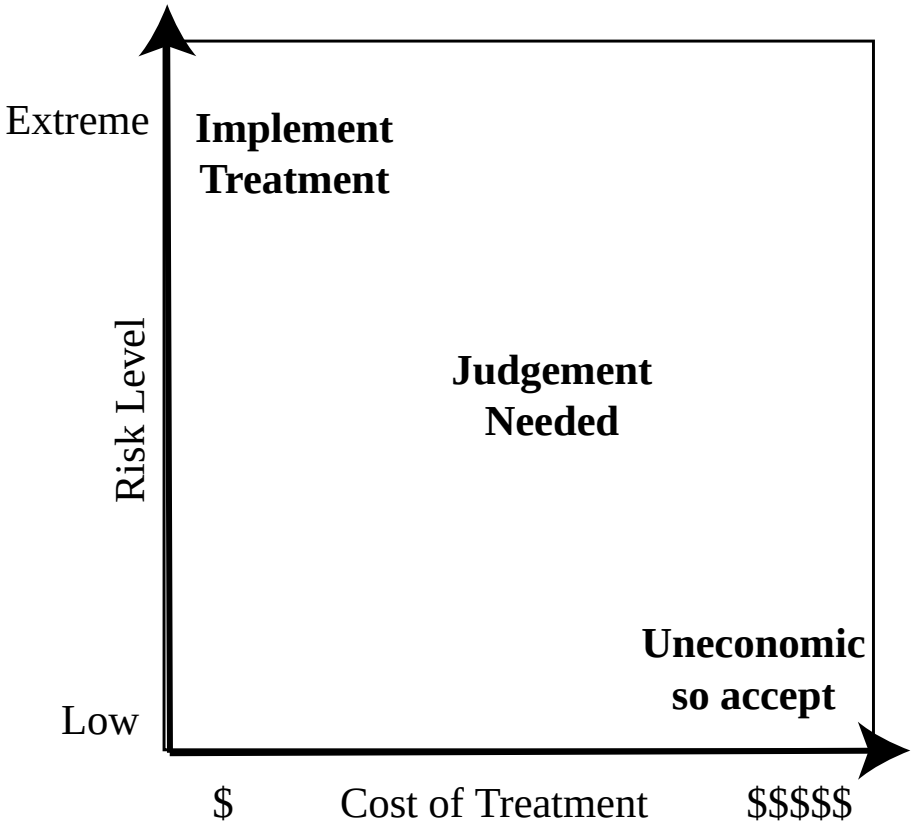


Figure 14.5 Judgment About Risk Treatment

Risk Çözümleme Alternatifleri

Risk kabulü	İş nedenleriyle normalden daha yüksek bir risk düzeyini kabul etmeyi seçmek
Riskten kaçınma	Bu riski oluşturan faaliyet veya sistemle devam etmemek
Risk transferi	Riskin sorumluluğunu üçüncü bir tarafla paylaşmak
Sonucu azaltın	Riskin gerçekleşmesi durumunda kuruluş üzerindeki etkiyi azaltmak için risk altındaki varlıkların yapısını veya kullanımını değiştirmek
Olasılığı azaltın	Güvenlik açığından yararlanma olasılığını azaltmak için uygun kontroller uygulayın

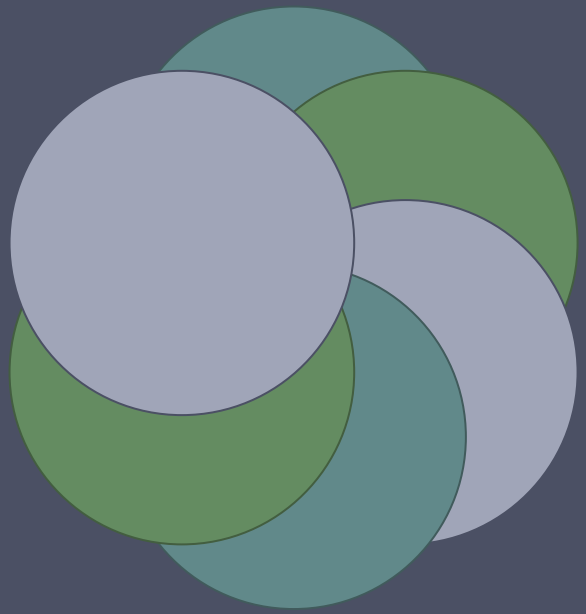
Vaka Çalışması: Gümüş Yıldız Madenleri

- Küresel madencilik şirketinin hayali operasyonu
- Geniş BT altyapısı
  - Hem yaygın hem de özel yazılım
  - Bazıları doğrudan sağlık ve güvenlikle ilgilidir
  - Önceden izole edilmiş sistemler artık ağa bağlı
- Bütünleşik yaklaşıma karar verildi
- Madencilik endüstrisi, spektrumun daha az riskli tarafında
- Yasal/düzenleyici gerekliliklere tabi
- Yönetim orta veya düşük riski kabul ediyor

Varlıklar

SCADA düğümlerinin
ve ağın güvenilirliği
ve bütünlüğü

Posta hizmetlerinin
kullanılabilirliği,
bütünlüğü ve
gizliliği



Depolanan dosya ve
veritabanı
bilgilerinin
bütünlüğü

Bakım/üretim sisteminin
kullanılabilirliği ve
bütünlüğü

Finansal sistemin
kullanılabilirliği ve
bütünlüğü

Tedarik sisteminin
kullanılabilirliği ve
bütünlüğü

Gümüş Yıldız Madenleri Risk Kaydı

Varlık	Tehdit/ Güvenlik Açığı	Var olan Kontroller	Olma olasılığı	Sonuç	Risk Seviyesi	Risk Önceliği
SCADA düğümlerinin ve ağının güvenilirliği ve bütünlüğü	Kontrol sisteminde yetkisiz değişiklik	Katmanlı güvenlik duvarları ve sunucular	Nadiren	Ciddi	Yüksek	1
Depolanan dosya ve veritabanı bilgilerinin bütünlüğü	Bozulma, hırsızlık ve bilgi kaybı	Güvenlik duvarı ve politikalar	Mümkün	Ciddi	Ekstrim	2
Finansal sistemin kullanılabilirliği ve bütünlüğü	Sistemi etkileyen saldırılar/hatalar	Güvenlik duvarı ve politikalar	Mümkün	Ciddi	Yüksek	3
Tedarik sisteminin mevcudiyeti ve bütünlüğü	Sistemi etkileyen saldırılar/hatalar	Güvenlik duvarı ve politikalar	Mümkün	Orta	Yüksek	4
Bakım/üretim sisteminin kullanılabilirliği ve bütünlüğü	Sistemi etkileyen saldırılar/hatalar	Güvenlik duvarı ve politikalar	Mümkün	Küçük	Orta	5
Posta hizmetlerinin kullanılabilirliği, bütünlüğü ve gizliliği	Sistemi etkileyen saldırılar/hatalar	Güvenlik duvarı, harici posta ağ geçidi	Neredeyse kesin	Küçük	Yüksek	6