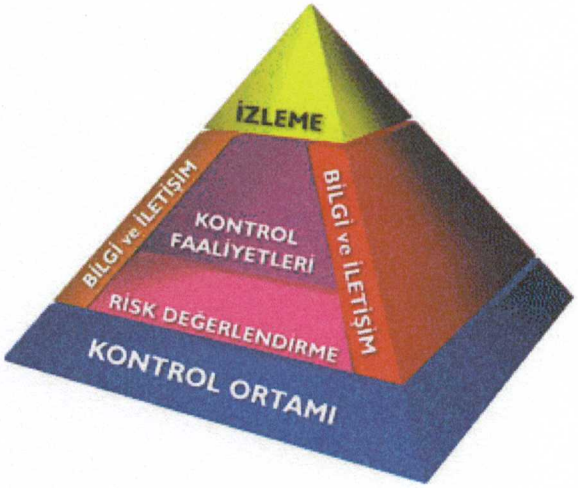
B. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS)

Ülkemizde Kamu Mali Yönetim ve Kontrol Sistemini yeniden düzenleyen 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ve buna ilişkin ikincil mevzuat COSO modelini esas alan İç Kontrol Sisteminin kurulmasını hedeflemektedir.

COSO Küpü (COSO Cube): İç kontrol unsurlarının, iç kontrolün amaçları ve idarenin faaliyetleriyle ilişkisini gösterir. Birimler, hedefler ve iç kontrolün unsurları, bir küpün farklı yüzeylerini oluşturur ve ayrılmaz bir bütündür. Tüm faaliyet ve birimler; faaliyetlerin etkinliği ve verimliliği, bilgilerin güvenilirliği, mevzuata uygunluk ve kurum varlıklarının korunmasını hedeflerine ulaşmak amacıyla COSO modelinde yer alan iç kontrolün beş unsurundan yararlanır.



COSO PİRAMİDİ

Şekil 1 (COSO MODELİ)

COSO Modeli (COSO Model): COSO (The Committee of Sponsoring Organisations of the Treadway Commission) tarafından hazırlanan ve bir kurumun günlük faaliyetleri sırasında kurum içerisindeki mevcut ve olması gereken asgari iç kontrol uygulamalarının sistematik bir şekilde değerlendirilmesine imkân sağlayan bir iç kontrol modelidir. COSO Modeli iç kontrol sistemlerine ilişkin standartların temelini oluşturmaktadır. Modele göre iç kontrol sisteminin ana hedefleri; organizasyonun günlük işlemlerinde etkinlik ve verimliliği, kurum içerisinde üretilen her türlü bilginin doğruluğu ve güvenilirliğini, gerçekleştirilen işlemlerin mevzuata uygun olmasını ve kurum aktiflerinin ve varlıklarının korunmasını sağlamaktır.

COSO Pramidi (COSO Pyramid): İç kontrol unsurlarının birbirleriyle ilişkisini gösterir. Kontrol ortamı kurumun içerisinde faaliyet gösterdiği ana kontrol yapısı olup diğer unsurlara temel teşkil eder. Kontrol faaliyetleri ve risk değerlendirme yapılırken bilgi ve iletişim kanalları kullanılarak gözetimin ihtiyaç duyduğu bilgiler sağlanır. Sistem yönetim, personel ve iç denetçiler tarafından izleme yapılarak geliştirilir.

B.1.RİSK NEDİR

İşletme yönetiminde, iş süreçlerinde ve pay ve menfaat sahipleri ile ilişkilerde; eşitlik, şeffaflık, hesap verebilirlik ve sorumluluk yaklaşımıyla işletme faaliyetlerinin etkinlik ve verimliliği, raporlama güvenilirliği, düzenlemelere uygunluk, pay ve menfaat sahiplerinin hak ve çıkarlarının korunması için güvence sağlayan yaklaşım ve ilkeleri ifade eder.

B.1.1. Riskin Tanımı

- Risk, tehditlerin bir organizasyonun strateji ve hedeflerine ulaşmasında engel teşkil etmedeki etkisi ve olasılığıdır.
- Risk potansiyel bir değer kaybı ya da kazancın optimum sınırların altında kalmasıdır.
- Kısacası, risk bir şirketi mevcut varlıklarını korumaktan ya da hisse değeriniarttırmaktan
- Alıkoyan her şeydir.
- Risk pozitif ve negatif sonuçları kapsar. Pozitif sonuçlar doğuran risk fırsatları,negatif sonuçlar doğuran risk tehditleri olarak değerlendirilir.
- Kurum getiri için riskleri göze almalıdır.

B.1.2. Risk Türleri

- Getirisi olmayan risk (Unrewardedrisk)
- İyi yönetildiğinde herhangi bir getiri sağlamayan, ancak kurumların özellikle yasalarla düzenlenmiş yükümlülüklere uyması ve belirli sorumlulukların yerine getirilmesi ile ilgili risklerdir. Finansal tabloların yanlış oluşturulması ya da mevzuata aykırı hareket edilmesi bu tür risklere örnektir.
- Getirisi olan risk (Rewardedrisk)
- Gerektiği gibi yönetildiğinde kuruma fayda ya da çıkar sağlayan risklerdir. Birleşme ve devralmalar, yeni ürün geliştirme, yeni piyasa ve iş modelleri bu risk tipine örneklerdir.

B.1.3. Risk ve Risk Yönetimi

RİSK
Risk kurum genelindeki seçimler ve kararlar sonucunda karşılaşılacak kayıp ve kazançlara ilişkin belirsizliklerdir.

RİSK YÖNETİMİ
Alınan kararların etkilerini belirleme,ölçeklendirme,azaltma ve ölçmeyi mümkün kılarak organizasyonlarda istikrar sağlayan bir mekanizmadır..

B.1.4. Risk Yönetimi Nedir / Ne Değildir?

Risk Yönetimi:

Kontrol fonksiyonudur

- İcranın bir parçasıdır
- Stratejik karar almanın ilk adımıdır
- Kültür değişimidir
- Aynı zamanda bir fırsat yönetimidir

Ancak,

- Yeni veya bir ölçüye kadar yapılmayan
- Sadece olumsuzlukları öne çıkaran
- Pratik olmayan öneriler geliştiren
- İmaj maksatlı yapılan
- Kendi başına problemleri çözebilecek bir fonksiyon

DEĞİLDİR.

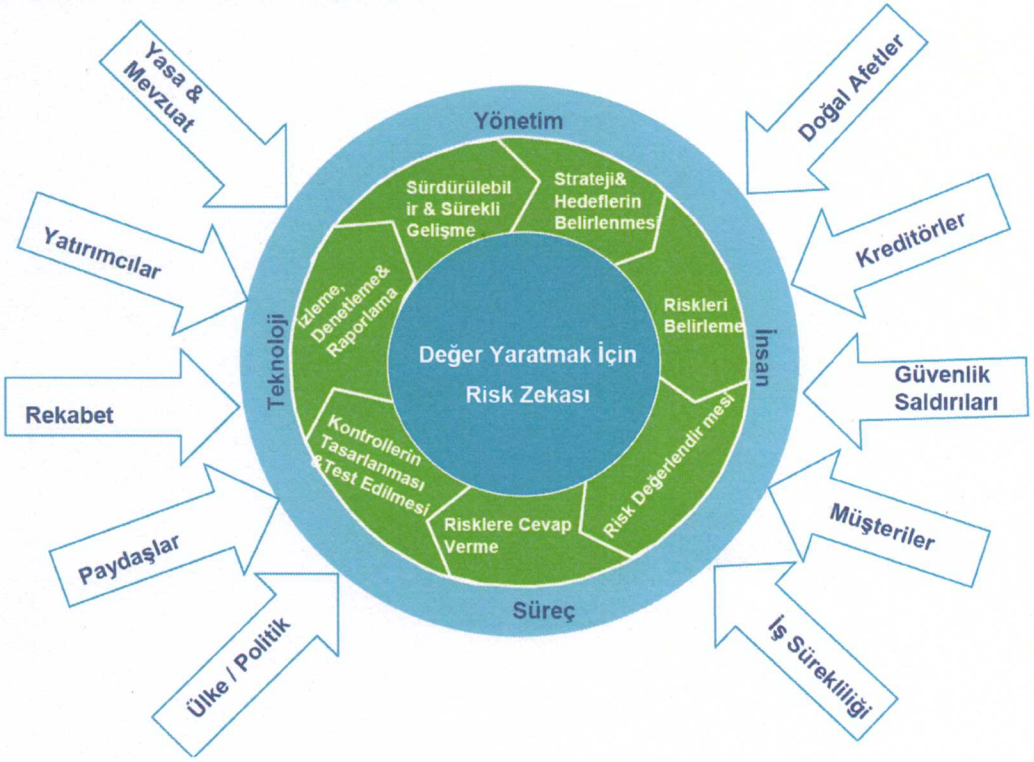
B.1.5. Kurumsal Risk Yönetimi

"Kurumsal Risk Yönetimi, kurumu etkileyebilecek potansiyel olayları tanımlamak, riskleri kurumun risk alma iştahına uygun olarak yönetmek ve kurum hedeflerine ulaşması ile ilgili olarak makul bir derecede güvence sağlamak amacı ile oluşturulmuş; kurumun yönetim kurulu, üst yönetimi ve diğer tüm çalışanları tarafından etkilenen ve stratejilerin belirlenmesinde kullanılan ve kurumun tümünde uygulanan sistematik bir süreçtir."

Kurumsal Risk Yönetimi

- Kurumsal risk yönetimi kurumlarda süregelen ve devam eden bir süreçtir.
- Sadece fonksiyon bazında değil, kurumun tamamında uygulanır.
- Tüm aksiyonların hissedarlarının risk alma isteği ile uyumlu olmasını sağlar.
- Sadece tehlikelerden korunma değil, değer yaratma odaklıdır.
- Strateji belirlemede kullanılır.
- Tüm risklerin uygun bir şekilde yönetildiğine dair makul bir güvence sağlar.
- Sonuç değil, sonuca ulaşmak için kullanılan bir araçtır.

Kurumsal Risk Yönetimi Çerçevesi



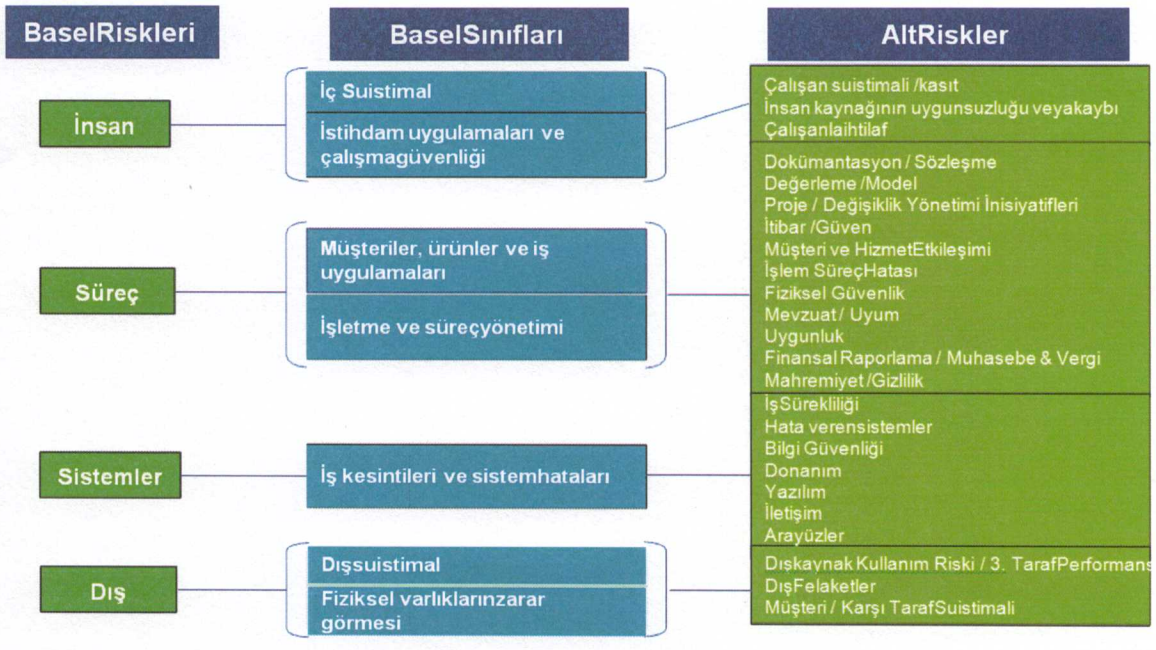
B.2 BT RİSK YÖNETİMİ

Bilişim Teknolojileri riski,BT ortamındaki durumdan kaynaklanan (BT varlıkları,organizasyonu, süreçleri, yönetişimi) herhangi bir hatadan organizasyonun zarara maruz kalma potansiyelidir.

Finansal Riskler	Operasyonel Riskler		Dış Çevre Riskleri
Kur	Müşteri Memnuniyeti	Hukuki Sorunlar	Rakip
Faiz Oranı	İnsan Kaynakları	Bilgi Teknolojileri	Yasa ve Düzenlemeler
Likidite	Ürün Hizmet Geliştirme	Bilgi Güvenliği	Hissedar
Kredi	Verimlilik	Ürün Hizmet	Politik
Finansal Enstrümanlar	Kapasite	Fiyatlandırma	Ekonomik
Yatırım Portföyü	Süreç Yönetimi	Çalışan Bağlılığı	Müşteri Trendleri
Sigorta	Ortaklık	Vergi	Değişim Yönetimi
Hisse Değeri	Konsantrasyon	Yetki ve Limit	Doğal Afet
Emtia Değeri	İş Durması	Tedarik	Sektör
	Ürün Hizmet Kalitesi	Performans Yönetimi	
	Çevre Sağlığı	İletişim	
	Çalışan Sağlığı ve Güvenliği		
	Marka Yönetimi		

Stratejik Riskler	
Yatırım Değerlendirme	Bütçe ve Planlama
İş Modeli	Organizasyonel Yapı
İş Portföyü	

B.2.1 Standart Risk Sınıfları



B.2.2. Risk Yönetim Stratejisi

B.2.2.1. Engeller

- İç BT Politikaları
- Kurumsal Risk Yönetimi vizyonu eksikliği – BT'e yer verilmemesi
- BT Risk Yönetimi Tanımı

B.2.2.2. BT Risk Yönetimi Stratejisi

- BT Risk Yöneticisi (IT CRO) atama
- Bu kişiyi CIO ve CRO'a bağlama
- BT Risk Yönetimi için tüzük oluşturulması
- BT Risk Gösterge Tablosu & Raporlama – BT KPI ile KRI Dengesi
- Risk Yönetimi – Risk analizi, kabulü, sahipliği ve bakımı

B.2.2.3. Zayıflık-Tehdit Örnekleri

Zayıflık	Tehdit-Kaynak	Tehdit–Aksiyon
İşten ayrılan personelin kullanıcı adlarının sistemden silinmemesi/bloke edilmemesi	İşten ayrılanpersonel	Kurum ağına ulaşması ve kurumsal bilgilereerişmesi
Kurum güvenlik duvarlarının gelen telnet'lere izin vermesi ve XYZ sunucusuna "misafir" kullanıcı adı ile ulaşılabilmesi	Yetkilendirilmemiş kullanıcılar (hacker'lar, işten ayrılan çalışanlar, bilişim suçluları,teröristler)	XYZ sunucusuna telnet ile erişim ve "misafir" kullanıcı adı ile sistem dosyalarınaulaşması
Tedarikçinin, sistem güvenlik tasarımında açıklar belirlemesi, yeni yamaların sistemeuygulanmaması	Yetkilendirilmemiş kullanıcılar (hacker'lar, memnun olmayan çalışanlar, bilişim suçluları, teröristler)	Bilinen sistem zayıflıklarını kullanarak kritik sistem dosyalarına yetkisiz erişimler

B.2.2.4. Zayıflık ve Tehditlerin Kontrolle Eşleştirilmesi

(1) Risk (Zayıflık-Tehdit)	(2) Risk Seviyes	(3) Önerilen Kontroller	(4) Aksiyon Önceliği	(5) Seçilen Kontroller	(6) Gereken Kaynaklar	(7) Sorumlu Ekip/Kişiler	(8) Başlangıç BitişTarihi	(9) Bakım Gereksinimi/Görüşler
Kurumgüvenlik duvarlarınıngelen telnet'lereizin vermesi veXYZ sunucusuna "misafir"kullanıcı adı ileulaşılabilmesi	Yüksek	• Gelen telnet'eizin verilmemesi • Hassaskurumsal dosyalara"herkes" erişiminin kaldırılması • "misafir"kullanıcı adınınkaldırılması veyaparolasının zorlaştırılması	Yüksek	• Gelentelnet kaldırılması • Dosyalara "herkes" erişiminin kaldırılması • "misafir" kullanıcı adının kaldırılması	Sistemi tekrar konfigüre etmek vetest etmek için10 saat	• XYZ sunucusu sistem yöneticisi • Güvenlik duvarı yöneticisi	xx.xx.xxxx–xx.xx.xxxx	Sistemgüvenliğinin düzenligözden geçirilmesi veXYZ sunucusunauygun güvenliğin sağlandığınıntest edilmesi

1. Riskler (Zayıflık-Tehdit), risk değerlendirme sürecinin çıktısıdır.

2. Belirlenmiş her bir risk için risk seviyesi risk değerlendirme sürecinin çıktısıdır.

3. Önerilen kontroller risk değerlendirme sürecinin çıktısıdır.

4. Aksiyon önceliği risk seviyesine ve müsait durumdaki kaynaklara (maddi, insan, teknoloji) göre belirlenmektedir.

5. Seçilen kontroller, önerilen kontroller arasından belirlenmektedir.

6. Gereken kaynaklar, seçilen kontrolleri uygulamaya almak üzere belirlenmektedir.

7. Sorumlu ekip ve kişiler, yeni veya geliştirilen kontrolleri uygulayacak kişilerdir.

8. Başlangıç ve bitiş tarihi, yeni veya geliştirilen kontrollerin hangi tarihlerde uygulanacağını belirtir. Bakım gereksinimi, yeni veya geliştirilen kontrollerin uygulanması sonrasında ihtiyaç duyulacak çalışmalardır.

B.3. SORUMLULUKLAR

B.3.1. Üst Yönetim

İş hedeflerine ulaşmak için kaynakların doğru kullanıldığını takip eder ve risk analizi sonuçlarından karar verme sürecinde faydalanırlar.

B.3.2. Bilgi İşlem Müdürlüğü

BT planlamasından, bütçesinden ve performasından sorumludur. Kararları, etkin bir risk yönetim programına dayanarak alırlar.

B.3.3. Sistem ve Bilgi Sahibi

Organizasyonel varlıkların fonksiyonel sahipleri olarak iş birimi yöneticileridir. Varlıkların bütünlüğünün, gizliliğinin ve kullanılabilirliğin temel sorumlularıdır.

B.3.4. İş Yöneticileri

Organizasyonun hedeflerine ulaşması için maliyet etkin kararlar almakla sorumlu kişilerdir. Risk yönetimi sürecindeki sorumlulukları, iş ile ilişkili kontrollerin uygulanmasını sağlamaktır.

B.3.5. Bilgi Güvenliği Yöneticileri

Risk Yönetimi sürecinde bilgi güvenliği ile ilişkili programların gerçekleştirilmesinden sorumludur.

B.4. BT RİSK YÖNETİMİ KATEGORİLERİ

B.4.1. BT Risk Alanları

1. *BT Yönetişim/Strateji Riski*
2. *BT Beceri/İnovasyon Riski*

3. *BT Mimari Riski*
4. *İş Sürekliliği Riski*
5. *Uyum Riski*
6. *BT Kaynak Riski*
7. *Tedarikçi Yönetim Riski*
8. *Üçüncü Taraf İlişkileri Riski*
9. *Proje/Geliştirme Riski*
10. *Değişiklik Riski*
11. *BT İtibar/Müşteri Memnuniyet Riski*
12. *Bilgi Riski*
13. *BT Güvenlik Riski*
14. *Online/Web Riski*

B.4.1.1 BT Yönetişim/ Strateji Riski:

Kurum BT stratejilerinin iş gereksinimleri ile tutarlı olmaması, iş gereksinimlerini karşılamaması, değişikliğe uygun olmaması, düzenli ve sık sık organizasyonla paylaşılmaması, iş ile uyumunda eksiklikler olması riskidir. Bu durumda, BT iş ile ilişkisi olmayan bir birim olarak algılanır.

B.4.1.2 BTBeceri/ İnovasyon Riski:

Kurumun bulunduğu pazar, endüstri ve etkileşim ortamında ilerlemesi için BT'nin yeni hizmet teknolojilerini uygulayamaması riskidir. BT'nin yeni teknolojilere adapte olmakta başarısız olması durumunda, Kurum pazar ve endüstrideki değişikliklere uyum sağlayabilmek için baskı altında kalacak ve rekabetçi ortamda iş performansını en uygun duruma getiremeyecektir.

B.4.1.3 BT Mimari Riski:

İş birimlerinin mevcut ve gelecekteki ihtiyaçlarını etkin bir şekilde desteklemek için, BT'nin etkin, standart hale getirilmiş ve sürdürülebilir bilgi teknolojileri altyapısına (donanım, ağ, yazılım, insan ve süreç) sahip olmaması riskidir.

B.4.1.4 İş Sürekliliği Riski:

BT ile ilişkili kritik operasyonların ve süreçlerin devam ettirilmesi için gerekli organizasyonel beceri riskidir. Kritik bilgi veya sistemlerin erişilebilir olmaması durumunda, Kurum kar eden operasyonlarını devam ettirememe riski ile karşılaşır.

B.4.1.5 Uyum / Yasa Riski:

BT organizasyonunun, dış gereksinimler ve kurumsal yönetişim politikaları/uygulamaları ile uyum sağlayamama riskidir. Bu risklere, hukuksal ve

sözleşmeye dayalı yükümlülükler ve yasal konular dahildir.

B.4.1.6 BT Kaynak Riski:

İnsan ve finansal kaynakların hazır olmaması ve planlanmaması veya verimsiz bir şekilde kullanılması riskidir. Bu riske, BT sistemleri hakkındaki bilgilerin personel değişiklikleri ile korunmaması da dahildir.

B.4.1.7 Tedarikçi Yönetimi Riski:

BT organizasyonunun, BT tedarikçileri, dış kaynak kullanımlar, sözleşmeli personel ve hizmet sağlayıcılar ile ilişki kurarken karşılaştığı risklerdir.

B.4.1.8 Üçüncü Taraflarla İlişki Riski:

Dağınık bir iş ortamında diğer kuruluşlarla ilişki kurarken ve bilgi paylaşırken karşılaşılan risklerdir. İş ortakları ve dış paydaşlarla iletişim kurmak,hassas bilgilerin gizliliğinin ihlal edilmesi ve yasal riskleri oluşturacaktır.

B.4.1.9 Proje/Geliştirme Riski:

BT'nin kötü proje planlama ve yönetimi sebebiyle karşılaştığı risklerdir. Bu risklere, iş ihtiyaçlarını karşılayan uygulamaların geliştirilmesi için bir biri ile ilişkili ve iyi anlaşılmış sürecin bulunmaması veya aksine çok fazla kontrolün olması sebebiyle BT'nin uygulamaları zamanında kullanıma alma becerisinin kaybedilmesi de dahildir.

B.4.1.10 Değişiklik Gerçekleştirme Riski:

BT' de teknoloji ortamının değiştirilmesini yönetmek için uygun olmayan gözetim ve süreçlerin bulunması riskidir. Buradaki en büyük risk,BT sistemleri ve uygulamaları üzerinde yetkilendirilmemiş veya kötü test edilmiş değişikliklerin oluşturacağı bütünlük ve erişilebilirlik problemidir.

B.4.1.11 BT İtibar/Vatandaş Memnuniyet Riski:

BT' nin iş taleplerini, hizmet seviye anlaşmalarını ve müşteri destek çağrılarını uygun olmayan bir şekilde karşılaması riskidir. BT itibar riski, nasıl hizmet verildiğidir.

B.4.1.12 Bilgi Riski:

BT'nin hassas ve düzenlenmiş kurumsal bilgiyi uygun olmayan bir şekilde kontrol etmesidir. Bilgi risk yönetimi, risk ve fırsatların yönetilmesi amacıyla organizasyonel bilginin belirlenmesi, sınıflandırılması ve kontrol edilmesi için çabalamaktadır.

B.4.1.13 BT Güvenlik Riski:

BT' nin teknik mimari zayıflığı ve organize suç,hacker, zararlı yazılım (virüs, solucan vb.) gibi saldırılara maruz kalmasıdır.

B.4.1.14 Online / Web Riski:

BT' nin Web varlığını oluşturma, işletme ve koruma için karşılaştığı risklerdir. Bu risklere web dünyasındaki itibar, hackleme, mahremiyet, markalaşma ve uyum dahildir.

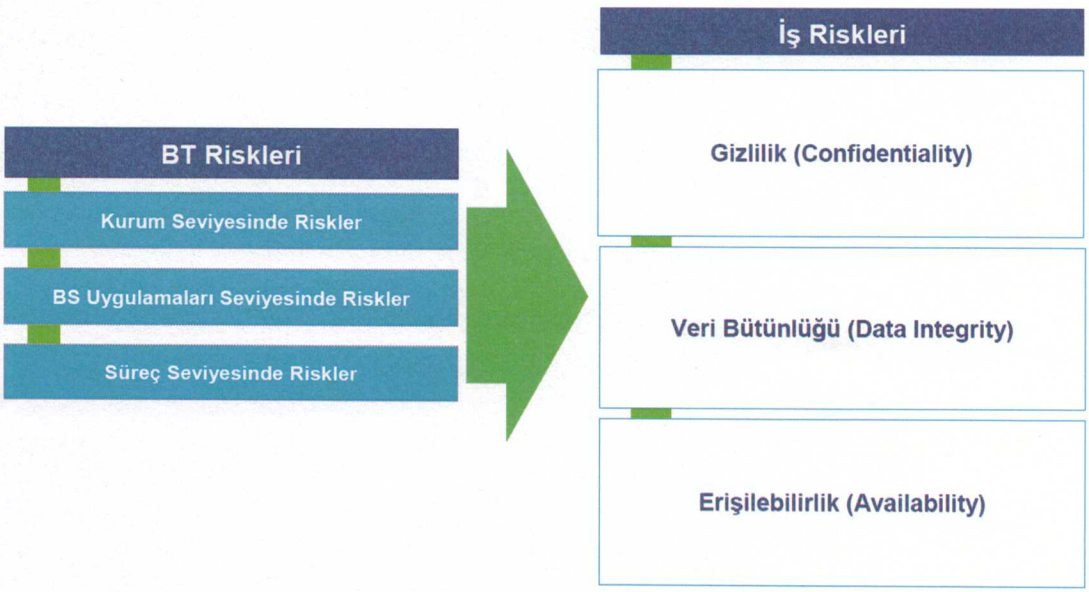
B.5. BT RİSK KATEGORİLERİ

BT riskleri üç seviyede düşünülmelidir:

- Kurum seviyesinde (organizasyonun geneli için),
- Bilgi sistemleri uygulamaları seviyesinde (uygulamalar tarafından desteklenen iş süreci işlemleri için), Süreç seviyesinde (uygulama ve veri bütünlüğünü destekleyen genel bilgisayar kontrol alanları için)

B.6. BT RİSKLERİNİN İŞ RİSKLERİ İLE İLİŞKİLENDİRMESİ

BT riskleri iş risklerini doğurmakta ve iç kontrol ortamına etki etmektedir.



B.6.1. Risk Etki Kategorileri

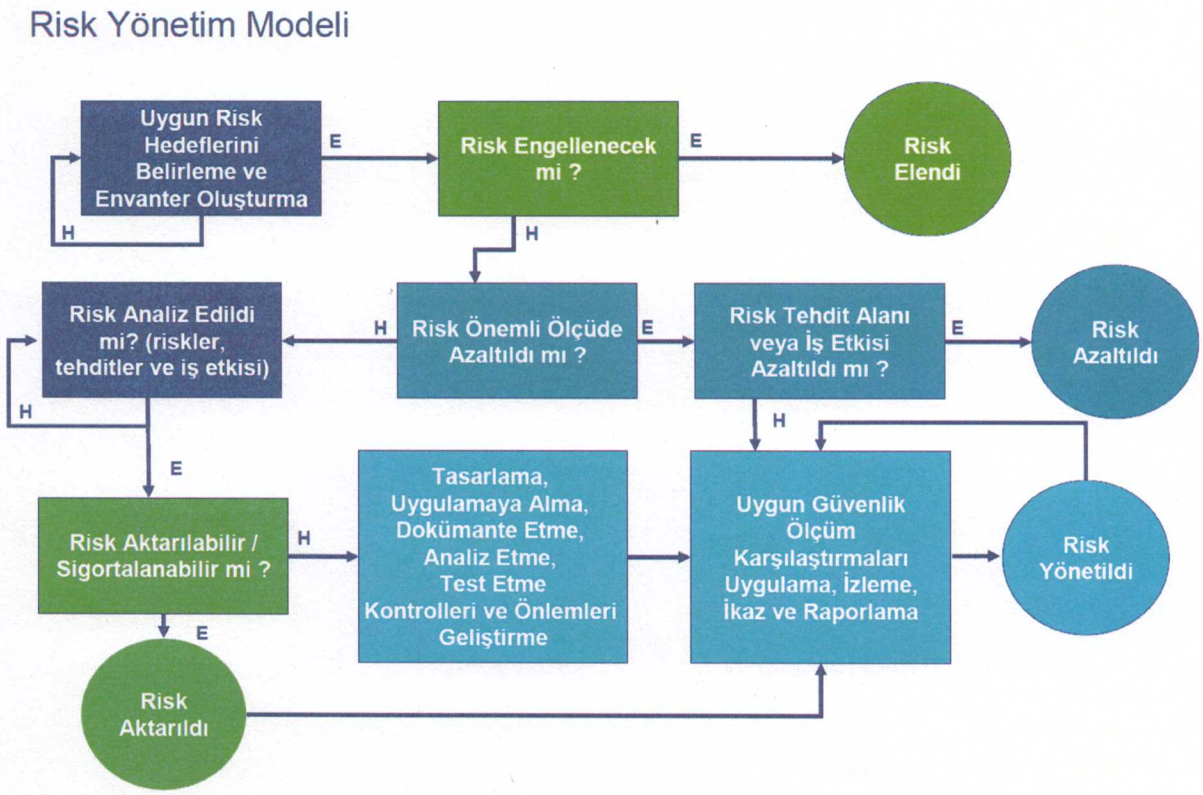
B.6.1.1. Operasyonlar: İş hizmetleri sunumunu destekleyen fonksiyonlar (mekan veya alan tahsisi, personel, satınalma, finansal, iletişim vb.)

B.6.1.2. Teknoloji: BT altyapısını destekleyen bilgi varlıkları (güvenlik, donanım, yazılım, ağ veya iletişim sistemleri)

B.6.1.3. Yasal: Kanunlara dayalı zorunluluklardan oluşan parametreler, mevzuat, politika veya üst yönetim kararları

B.6.1.4. İtibar: Hizmetlerin nasıl sunulduğu hakkında genel kamuoyu düşüncesi (bütünlük, kredibilite, güven, müşteri memnuniyeti, imaj, medya ilişkileri)

B.7. BT RİSK YÖNETİMİ YAŞAM DÖNGÜSÜ



B.7.1. 1. Aşama BT Altyapı Süreçlerinin Anlaşılması

Ana Aktiviteler

- Bilgi Toplama:
  - Kurumsal hedef ve stratejiler
  - Organizasyonel yapı ve değişiklikler
  - Kritik iş süreçleri ve merkezler
  - Geçmiş dönem denetim bulguları
  - Mevcut risk analiz dokümanları
  - Sektörel riskler ve sorunlar
- Kurumsal yapının toplanan veriler ışığında değerlendirilmesi

Çıktılar

- Profil
  - İş Hedefleri
  - Organizasyonel yapı
  - İş ve BT süreçleri, lokasyonları
- Ön risk bilgileri
  - Mevcut analizler
  - Sektörel riskler

Ana Aktiviteler	**Aktivite 1:** İstenecek Dokümanların Listelesinin Hazırlanması	**Aktivite 2:** BT Hedef, Amaç ve Stratejisinin Anlaşılması	**Aktivite 3:** BT Genel Kontrol Yapısının Anlaşılması	**Aktivite 4:** BT Süreç ve Altyapısının Anlaşılması	**Aktivite 5:** Trend / Endüstriyel Risklerin Belirlenmesi	**Aktivite 6:** Altyapı – BT Süreçlerinin Eşleştirilmesi
Dokümanlar / Çıktılar	Doküman Listesi Ön Bilgiler Talep Edilen Dokümanlar için Takip Listesi	BT Profili BT Strateji Dokümanı BT Yıllık Plan BT Bütçesi Büyük Projeler	Kurumsal Kontrol Noktaları BT Yönetişim Dokümanları BT Politika Prosedürler BT Risk Kontrol Matrisleri	Temel BT Süreçleri Uygulama Listesi Altyapı Envanteri Veri Merkezleri	Risk & Kontrol Dokümanları Yasal Zorunluluklar Sektörel Riskler	BT Süreçleri-Altyapı Eşleştirilmesi

B.7.2. 2. Aşama BT Risk Modelinin Geliştirilmesi

Ana Aktiviteler

- İş süreçleri sahipleri ile birlikte risk çerçevesinin belirlenmesi:
  - Risk çerçevesi kapsamının belirlenmesi
  - Etki, olasılık ve zafiyet kriterlerinin belirlenmesi
- Risk çerçevesinin onaylanması

Çıktılar

- Risk çerçevesi
  - BT yönetişimi
  - BT süreçleri
  - Operasyon
- BT risk tanımları
- Risk değerlendirme kriterleri:
  - Etki
  - Olasılık
  - Zafiyet

Ana Aktiviteler	**Aktivite 1:** BT Risk Çerçevesinin Belirlenmesi	**Aktivite 2:** Kriterlerinin Belirlenmesi	**Aktivite 3:** Risk Çerçevesinin Onaylanması	**Aktivite 4:** Risklerinin Belirlenmesi
Dokümanlar / Çıktılar	BT Risk Çerçevesi Kategoriler: • Yönetişim / Strateji Planlama • BT Süreçleri • Altyapı	Kriterler (Etki, zafiyet, olasılık) Risk Değerlendirme Yaklaşımı	BT Risk Modeli	Risk Kataloğu

BT Risk Çerçevesi, öngörülen risklerin belirli kategoriler altında toplanarak, tüm BT süreçleri ile ilgili risklerin değerlendirilmesini sağlar.

- BT Risk Değerlendirme Yöntemi üzerinde anlaşılır.
- Paydaşlar ile BT risk değerlendirmesi sonuçları paylaşılır.
- Tüm riskleri içeren bir risk kataloğu hazırlanır.

Risk Kataloğu				
#	Sahibi	Sınıfı	Risk İfadesi	Olasılığı
1	Bilgi Güvenliği Sorumlusu	Bilgi Varlıkları	Sistem yöneticisinin CEO e-postalarını okuması ve rakiplere bilgi vermesi	Düşük
2				

ÖRNEK BT RİSKLERİ –YÖNETİŞİM SEVİYESİ

B.7.2.1. BT Yönetişimi:

B.7.2.1.1. Misyon: BT misyonu dokümante edilmemiştir veya mevcut değerleri korumaya ve yeni katma değer yaratmaya yönelik değildir.

B.7.2.1.2. BT–İş Birimleri Uyumu: BT ile iş birimleri arasındaki hedefler uyumlu olmadığı için BT etkin bir katma değer sağlayamamaktadır.

B.7.2.1.3. Politika: Politika ve prosedürler tanımlanmamış ya da dokümante edilmemiştir. Mevcut yazılı politika ve prosedürler etkin bir dağıtım mekanizmasıyla birimlerle paylaşılmamıştır. Politika ve prosedürlerin farkındalığında eksiklikler bulunmaktadır.

B.7.2.2. BT Strateji Planlama:

B.7.2.2.1 BT Planlama: Bilgi sistemleri strateji ve planları kurumsal stratejik hedeflerle tam uyumlu değildir.

B.7.2.2.2 Bütçe, Metrik ve Kontroller: BT bütçeleri yönetim tarafından onaylanmamaktadır. Bütçedeki gerçekleşme farklılıkları kontrol edilmemekte ve sebepleri araştırılmamaktadır. Metrik ve kontroller tanımlanmamıştır.

B.7.2.3. Mimari:

B.7.2.3.1 Teknoloji Planlama: BT organizasyonu, kuruma ve süreçlere katma değer sağlayacak teknolojileri takip edememekte ve zamanında kullanmaya başlayamamaktadır.

B.7.2.3.2 Gelişen Teknolojiler: BT organizasyonu gelişen teknolojileri takip edememekte, ortaya çıkan yeni fırsat ve önerileri değerlendirememektedir.

B.7.2.3.3 Tedarikçi / Ürün Seçimi: BT tedarikçi ve ürünlerinin seçimi,yönetimin belirlediği standartlar dahilinde yapılamamaktadır.

B.7.2.3.4 Entegrasyon &Konsolidasyon: Sistemlerin entegrasyonu etkin değildir, sistemlerin etkileşimi istenilen düzeyde değildir.

B.7.2.4. Proje Yönetimi:

B.7.2.4.1 Proje Yönetim Hayat Döngüsü: Projelerin planlamasında, kaynak ayrılmasında, yürütülmesinde ve zamanında tamamlanması için belirli bir metodoloji geliştirilmemiştir.

B.7.2.4.2 Yazılım Geliştirme Hayat Döngüsü: BT yazılım geliştirme projeleri yönetimin belirlediği standartlara göre yürütülmemektedir.

B.7.2.4.3 Proje Risk (Geçiş Öncesi) Değerlendirme: BT projeleri, Kalite Güvence birimleri, İç Denetim ve/veya Yönetim tarafından geçiş öncesi incelenmemektedir.

B.7.2.5. BT Operasyonları

B.7.2.5.1 Çevre Yönetimi: İş ve BT hedeflerininin kullanılabilirlik ve performans değerleri için diğer tüm BT ihtiyaçları (donanım, yazılım, bilgisayar ağı, veri merkezleri, araçların) izlenmemektedir.

B.7.2.5.2 Veri Saklaması/Yedeklemesi: Üst Yönetim ve kullanıcılar veri yedeklemesi ve saklanması ile ilgili uygun planlama yapmamaktadır. Veri kaybolması riskinin azaltılması amacı ile yedeklemeler uzak bir lokasyonda tutulmamaktadır.

B.7.2.6. Süreklilik Yönetimi

B.7.2.6.1 İŞ-Etki Analizi: Kurum geneli için geçerli olan bir süreklilik planı hazırlanmamış yada iş-etki analizine göre yapılmamıştır.

B.7.2.6.2 Süreklilik Planı Geliştirme/Güncelleme: Süreklilik Planı mevcut değildir yada gözden geçirilmemekte veya iş ortamındaki değişiklikleri yansıtmamaktadır.

B.7.2.6.3 Test Edilmesi: Üst Yönetim süreklilik planını düzenli olarak test etmemekte, test sonuçlarını dokümante etmemekte ya da planı geliştirmemektedir.

B.7.3. 3. Aşama - Riskin Ölçeklendirilmesi

Ana Aktiviteler

- Mülakat, çalışma toplantıları ve anketlerle risklerin değerlendirilmesi:
  - Üst yönetim
  - Orta seviye yönetim
  - İş birimleri ve BT birimleri yöneticilerine anketler yapılması
- Risk derecelendirmesi ve haritasının çıkarılması

Çıktılar

- Risk Haritası ("MARCI")
  - Risklerin etki ve zafiyetlere göre değerlendirilmesi
- Mülakat toplantı notları
- Anket sonuçları

Ana Aktiviteler	**Aktivite 1:** Risk Değerlendirme Süreci Katılımcıların Belirlenmesi	**Aktivite 2:** Mülakat, Çalışma Toplantıları ve Anketlerin Yapılması	**Aktivite 3:** BT Risklerinin Önceliklendirilmesi	**Aktivite 4:** Risklerin Yönetim Tarafından Değerlendirilmesi
Dokümanlar / Çıktılar	Mülakat, Çalışma Toplantıları ve Anket Katılımcılarının Belirlenmesi Anket ve Mülakat Formlarının Belirlenmesi	Duyuru e-postaları Mülakatlar Çalışma Toplantıları Materyalleri Anketler Anket, Mülakat ve Formların Belirlenmesi	Risk Değerlendirme Sonuçları Risk Haritası	Uyarlanmış Risk Değerleri

B.7.3.1. Risk Faktörleri

Varlıkların ve sahiplerinin belirlenmesi, gizlilik, bütünlük ve erişilebilirlik değerlerinin verilmesi

Varlık Grubu	Varlık	G	B	E
Bilgi / veri	Maaş bilgileri			
Donanım	Domain Controller			
Yazılım ve uygulamalar	Ana bankacılık uygulaması			
İletişim cihazları	Güvenlik Duvarı			
Taşınabilir veri saklama ortamları	Yedekleme kartuşları			
Dokümanlar	Faturalar			
Personel	Veritabanı Yöneticisi			
Bilgi işlem merkezleri	Olağanüstü Durum Merkezi			

Zayıflık	Bir varlık üzerinde gizlilik, bütünlük ve/veya erişilebilirliğin kaybedilmesine neden olabilecek açıklık	Kullanıcılar ve sunucular aynı ağ içerisinde yer almaktadır ve kullanıcılar sunuculara erişebilmektedir.
Tehdit	Varlığın gizlilik, bütünlük ve/veya erişilebilirliğinin kaybedilmesine neden olabilecek olay	Kullanıcılar bilinçli veya bilinçsiz olarak kritik servislere müdahale edebilir.
Risk	Tehditin zayıflığı istismar etmesiyle ortaya çıkabilecek sonuç	Hizmet kesintisi gerçekleşebilir.
Kontrol	Riskin etkisini azaltan düzenleme ve/veya aksiyonlar	Güvenlik duvarı ve sanal ağlar kullanılarak erişim kısıtlaması sağlanmalıdır.

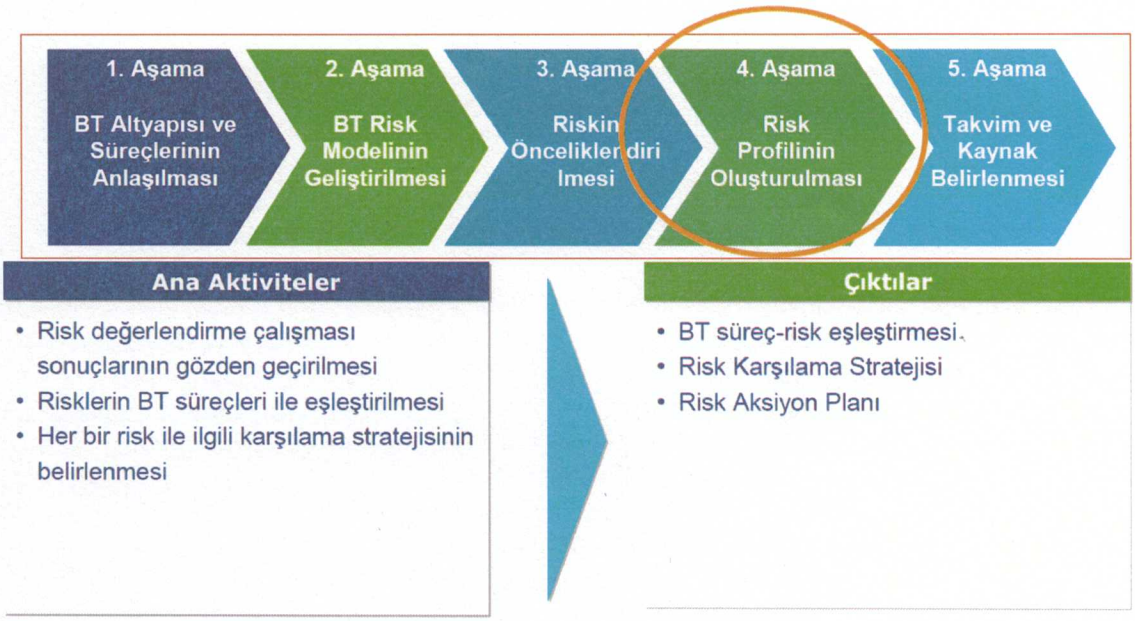
B.7.3.2. Risk Değerlendirmesi

Riske Maruz Kalma Olasılığı (Tehdit)	Zayıflık: Düşük	Zayıflık: Orta	Zayıflık: Yüksek
Düşük	Çok Düşük	Düşük	Orta
Orta	Düşük	Orta	Yüksek
Yüksek	Orta	Yüksek	Çok Yüksek

Risk Seviyesi (İş Etkisi)	Riske Maruz Kalma Olasılığı: Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
Düşük	1	2	3	4	5
Orta	2	3	4	5	6
Yüksek	3	4	5	6	7

Varlık	İş Etkisi (G / B / E)			Zayıflık	Tehdit	Risk
Web Uygulama Sunucusu				Varsayılan kullanıcı hesapları aktif durumdadır.	İnternetteki saldırganlar uygulamaya erişebilir.	Veriler yetkisiz kişilerce değiştirilebilir.
VoIP Telefonlar				Görüşmeler şifrelenmeden iletilmektedir.	Kurum çalışanları görüşmeleri dinleyebilir.	Kişisel ve gizli kurumsal bilgiler ifşa olabilir.

B.7.4. Aşama – Risk Profilinin Oluşturulması



Risk Karşılama, riskin etkisini azaltmak üzere Üst Yönetimin uygulattığı sistematik metodolojidir. **Risk karşılama için seçenekler aşağıdaki gibidir:**

B.7.4.1 Riski Kabullenme: Potansiyel riski kabul ederek devam etmektir. Kontroller uygulanarak risk daha az bir seviyeye getirilmeye çalışılır.

B.7.4.2 Riskten Kaçınma: Riskin oluşmasına neden olan durumu ortadan kaldırarak riskten kaçınmaktır.

B.7.4.3 Risk Sınırlama: Bir zayıflık ile ilgili çalışarak tehdidin etkisini azaltmak amacıyla

kontroller uygulamaktır. (Tespit edici veya kurtarıcı kontroller gibi)

B.7.4.4 Risk Planlama: Kontrolleri önceliklendiren, uygulayan ve yürüten bir risk karşılama planı geliştirilmesi ile riskin yönetilmesidir.

B.7.4.5 Risk Aktarımı: Zararın azaltılmasını sağlayacak seçeneklerin kullanılması ile riskin transfer edilmesidir.

Üst Yönetim

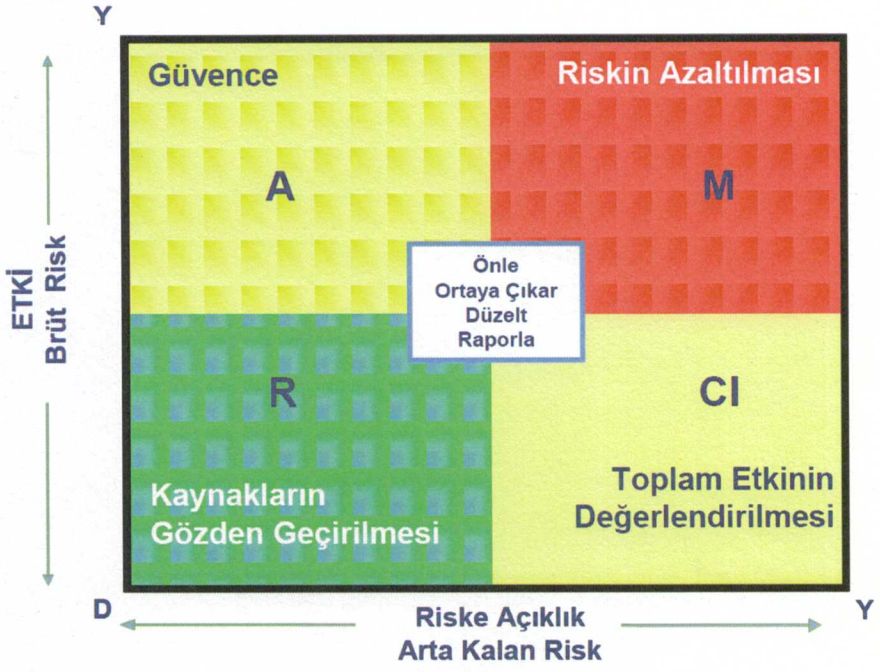
- Öncelikleri ve endişeleri nedir?
- Hangi riskler yüksek önceliklidir?
- Hangi riskler kabul edilmektedir?
- Hangi kontroller etkin değildir?
- Hangi riskler müdahale gerektirir?

RiskProfili

#	Doğal Risk Seviyesi	Kontrol	Kalan Risk Seviyesi	Hedef Risk Seviyesi	Öncelik	Aksiyon
1	Yüksek	Kont1	Düşük	Düşük	Düşük	Kabul
2	Orta	-	Orta	Düşük	Yüksek	Müdahale

Risk Haritası Genel Alanları

Risk Karşılama yaklaşımı "MARCI" şemasında risklerin yerleştiği alana göre belirlenir.



B.7.5. Aşama – Takvim Ve Kaynak Belirlenmesi

Ana Aktiviteler

- İlgili Aksiyon Sorumluları ve Üst Yönetimi ile gerekli niteliklerin, araçların belirlenmesi
- Risk azaltma çalışmaları takviminin oluşturulması ve kaynakların belirlenmesi

Çıktılar

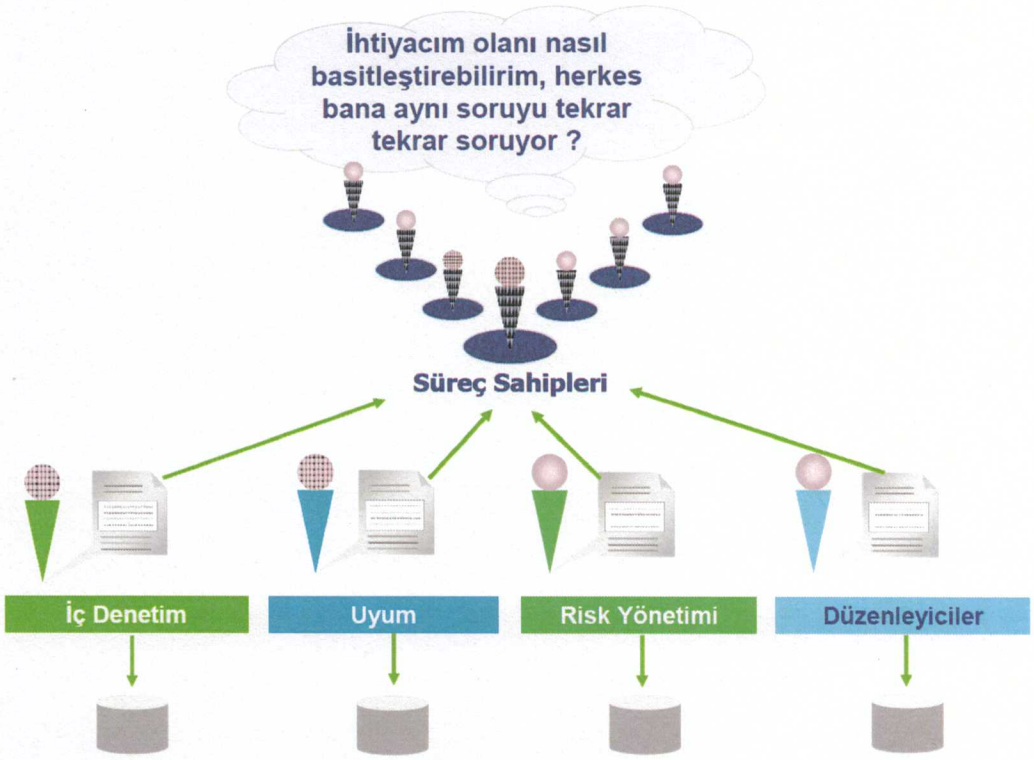
- Detaylı aksiyon planı:
  - Risk değerlendirmesi ile aksiyon planının eşleştirilmesi
  - Takvim
  - Kaynak & Eğitim Listesi

Risk Aksiyon Planı

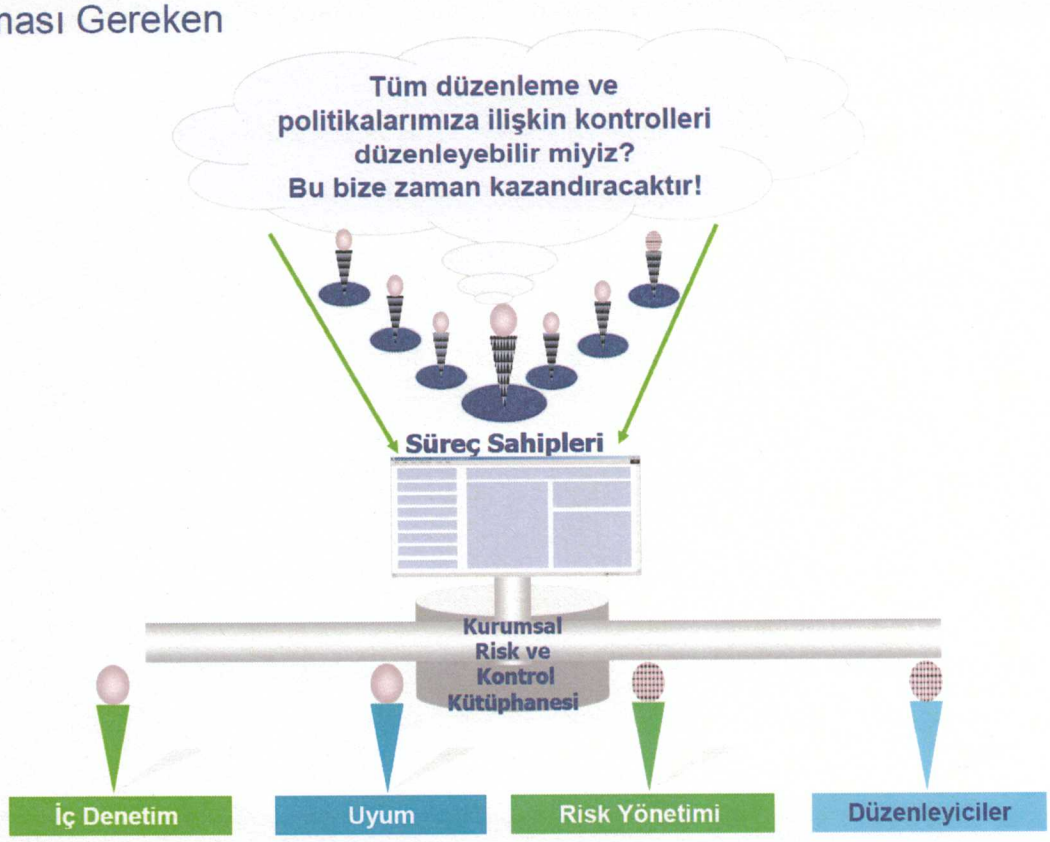
Riskler	Yanıtlar	Sorumlu	Tamamlanma Tarihi	Durum
1,2	Oracle Veritabanında Değişiklik Kontrollerinin Uygulanması	Veritabanı Yöneticisi	XX.XX.XXXX	Açık
3	Sistem odası günlük erişim raporlarının, şüpheli aktiviteler ve anormallikler için gözden geçirilmesi	BT Yöneticisi, Sistem odası Sorumlusu	XX.XX.XXXX	Açık

B.8. BT Risk Yönetiminin Teknolojik Beklentileri

Mevcut Durumun Sebebi



Yapılması Gereken



B.9. Risk Kapsamının Belirlenmesi

Uygun sonuçların elde edilmesi için risk değerlendirme çerçevesinin uygulama kapsamının belirlenmesi amaçlanmaktadır.

- Risk değerlendirmede iç ve dış kapsam, değerlendirmenin hedefi ve hangi risklerin değerlendirileceği kriterleri göz önüne alınmalı
- Risk kapsamı, Kurumun risk yaklaşımı olarak anlaşılmalı
- Prosedürler genel BT risk değerlendirmelerinde ve ayrıca proje risk değerlendirmelerinde kullanılacak standartları içermeli

B.10. Olay Tespiti

Kurumun, iş, yasal, düzenleyici, teknolojik, ticari ortak, insan kaynağı ve operasyonel durum hedeflerine ve operasyonlarına potansiyel negatif etkisi olan olayların (önemli bir zayıflığı kullanan gerçek bir tehdidin) belirlenmesi amaçlanmaktadır.

- Tespit edilen riskler bir risk kütüğüne kaydedilmeli ve buradan yönetilmeli
- BT risk kayıtlarında tehditlerin ilişkisi, tehdide açıklık miktarı ve etkinin önemi bulunmalı
- Tehdit unsuru olabilecek potansiyel olayları belirlemek için kullanılan süreçler oluşturulmalı
- Tüm BT süreçleri risk analizine dahil edilmeli
- Değişik vakalarda ve etki tespit aktivitelerinde uygun işlevler arası ekipler görev almalı

B.11. Risk Yanıtlaması

Düzenli olarak risklerin oluşumunu azaltan maliyet etkin kontroller sağlamak için tasarlanmış bir risk karşılama sürecinin geliştirilmesi ve yönetilmesi amaçlanmaktadır.

Risk yanıtlama süreci kaçınma, azaltma, paylaşma veya kabul etme gibi risk stratejilerini belirlemeli, sorumlulukları atamalı ve risk tolerans seviyelerini göz önüne almalıdır.

Her bir risk için belirlenen strateji Üst Yönetim tarafından onaylanmalıdır.

B.12. Risk Aksiyon Planının Oluşturulması Ve İzlenmesi

Yararlı olarak belirlenmiş risk yanıtlarının gerçekleştirilmesi için maliyetlerin, kazanımların ve sorumlulukların belirlenmesini içeren kontrol aktivitelerinin tüm seviyelerinin önceliklendirilmesi ve planlanması amaçlanmaktadır.

- BT risk aksiyon planı oluşturulmalı, planın sahipliğine ve yönetilmesine ilişkin sorumluluklar belirlenmeli
- Tüm önerilen aksiyonlar ve kabul edilen kalan riskler onaylanmalı
- Onaylanan aksiyonlar uygun süreç sahibi tarafından sahiplenilmeli
- Aksiyon planının işleyişi izlenmeli ve sapmalar Üst Yönetime raporlanmalı

Bu standard, risk değerlendirme, güvenlik tasarımı ve gerçekleştirme, güvenlik yönetimi ve yeniden değerlendirmeyi yöneten bu kılavuzlardaki prensipleri gerçekleştirmek için sağlam bir model sağlar.

- **BGYS'nin kurulması için aşağıdakiler yapmalıdır:**
  - BGYS kapsamını ve sınırlarını tanımlama
  - BGYS politikası tanımlama
  - Risk değerlendirme yaklaşımını tanımlama
  - Riskleri tanımlama
  - Riskleri çözümleme ve derecelendirme
  - Risklerin işlenmesi için seçenekleri tanımlama ve değerlendirmE
  - Risklerin işlenmesi için kontrol amaçları ve kontrolleri seçme
  - Sunulan artık risklere ilişkin yönetim onayı edinme
  - BGYS'yi gerçekleştirmek ve işletmek için yönetim yetkilendirme edinme
  - Uygulanabilirlik Bildirgesi hazırlama

BGYS dokümantasyonu aşağıdakileri kapsamalıdır:

- Risk değerlendirme metodolojisinin bir tanımı
- Risk değerlendirme raporu
- Risk işleme planı

Bilgi Güvenliği Yönetiminde

- Süreç hedefleri arasında BT risklerinin uygun şekilde yönetilmesi de yer almaktadır.
- İş ve BT riskleri ve yönetimi süreç kapsamı içerisindedir.
- Bilgi Güvenliği Yönetişiminin 6 temel çıktısından birisi Risk Yönetimidir:
  - Üzerinde uzlaşılmış bir risk profili
  - Risk Yönetimi önceliklerinin farkındalığı
  - Risk Karşılama
  - Risk Kabul

B.13. Belediye Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler

- Belediye, Belediyecilik faaliyetlerinde bilgi teknolojilerini kullanıyor olmasından kaynaklanan riskleri ölçmek, izlemek, kontrol etmek ve raporlamak üzere gerekli önlemleri alır.
- Bilgi sistemlerine ilişkin risklerin yönetilmesi, bilgi sistemleri yönetiminin önemli bir bileşeni olarak ele alınır.
- Belediye, risk yönetim politika ve süreçlerini, bilgi teknolojilerinin kullanımına bağlı olarak gözden geçirip, buradan kaynaklanacak risklerin yönetimini kapsayacak şekilde yeniler.
- Bilgi teknolojilerinden kaynaklanan risklerin operasyonel risk kapsamında değerlendirilmesinin yanı sıra bu risklerin belediyecilik faaliyetlerinden kaynaklanan diğer risklerin de bir çarpanı olabileceğinden, bilgi teknolojilerinden kaynaklanan riskleri de içeren bütünleşik bir risk yönetim yaklaşımı tüm belediyecilik faaliyetleri için benimsenir, bilgi teknolojilerinin takibi ve gözetimine ilişkin çalışmalardan edinilen verilerin belediyenin bütünsel risk yönetim çerçevesinin bir parçası haline gelmesi sağlanır.
- Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla geliştirilen politika ve prosedürlerin gerekleri, belediyenin organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilir, bunların işlerliğine ilişkin gözetim ve takip gerçekleştirilir.