

TBD Kamu-BİB
Kamu Bilişim Platformu VIII

BİLİŞİM TEKNOLOJİLERİNDE RİSK
YÖNETİMİ

2. ÇALIŞMA GRUBU

Özet:

Bu raporda, Bilişim Teknolojilerinde Risk Yönetimi sistematik olarak incelenmekte ve uluslar arası standartlardan yararlanılarak ulusal bir plan çıkartılması için yapılması gerekenler anlatılmaktadır.

Çalışma Planı:

Aylık toplantılar ve Çevrimiçi Çalışmalar yapılacaktır.

Hazırlayanlar:

Oturum Başkan: Ali YAZICI

ÇG Başkanı: Mustafa OKAY

Ahmet PEKEL

Oktay YAMAN

Dicle SOYER

Nezih KULEYİN

Adnan METE

Belge No:

ÇG2/Sürüm2

Tarihi:

27 Mart 2006

Durumu:

2. Ara Rapor

İÇİNDEKİLER

1. GİRİŞ	3
2. TANIM VE KAVRAMLAR	3
2.1. Risk Yönetimi	3
2.2. Bilişim Teknolojilerinde Risk Yönetimi	3
2.3. Bilişim Teknolojileri Boyutuyla Olası Tehditler	4
2.4. Muhtemel Kayıplar ve Etkileri Üzerine Örnek Senaryolar	7
2.5. Bilişim Teknolojilerinde Risk Değerlendirme	9
2.5.1. Risk Değerlendirmesi ve Risk haritasının çıkarılması	9
2.5.2. Risk Yönetiminde Kullanılan Araçlar ve Yöntemler	12
2.5.3. BT Risk Yönetiminde Roller	13
3. BİLİŞİM TEKNOLOJİLERİNDE RİSK DENETİMİ	14
4. ÖRNEK RİSK ANALİZ ÇALIŞMASI	15
4.1. Risk Analizi Yöntemi	15
4.1.1. Risk Analizi Amaçları ve Kullanılan İlkeler	15
4.1.2. Risk Analizi Yaklaşımı	15
4.1.3. Hesaplama Kuralları	16
4.1.4. Kullanılan Değerler	16
4.1.5. CobiT BT Süreç Önceliklendirmesi	18
4.2. Sonuçlar - Risk/Tehdit Senaryoları Analizi	18
5. İŞ SÜREKLİLİĞİ VE OLAĞANÜSTÜ DURUM YÖNETİMİ	22
6. TÜRKİYE'DEKİ UYGULAMALAR	24
6.1 Ulusal Acil Durum Yönetimi Sistemi	24
6.2. Ulusal Acil Durum Yönetimi Bilgi Sistemi	26
7. SONUÇ VE ÖNERİLER	27
EK A- STANDART UYGULAMALAR VE YÖNTEMLER	29
Hükümler	31
PCAOB (Özel Şirketler Muhasebe Gözetim Kurulu) 'nun Gereksinimleri	31
BT Kontrolleri, BT Denetimi ve SOX	31
Uygulamadaki Anlaşma	32
COBIT Yapısı	33
DS2 Üçüncü taraf Hizmetlerin Yönetilmesi	40
EK B – RİSK SENARYOLARININ VE COBIT BT SÜREÇLERİNİN DETAYLI İNCELEMESİ	45

1. GİRİŞ

“Tüm Kamu Kurum ve Kuruluşları Bilgi İşlem Birimlerinin sorunlarına ortak çözümler aramak, üretmek ve Bilgi İşlem Birimleri arasındaki mesleki dayanışmayı sağlamak ve geliştirmek, ülke yönetimine öneriler oluşturmak ve takipçisi olmak” amacıyla Türkiye Bilişim Derneği (TBD) çatısı altında kurulmuş olan TBD-Kamu-BİB (Türkiye Bilişim Derneği Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği); Kamu Bilişim Platformu VIII. Dönem çalışma konuları içerisinde “Bilişim Teknolojilerinde Risk Yönetimi” başlığına da yer vererek, bir çalışma başlatmıştır.

Günümüz toplumlarının günlük yaşamlarında vazgeçilmez bir unsur olmaya başlayan bilişim teknolojileri, yeni ekonomi ve yönetim modellerinin önemli işlem araçları olmuştur. Bilgi ve İletişim teknolojileri alanındaki gelişmeler ile çeşitlenmeler her geçen gün konunun önemini daha da artırmakta, daha kaliteli, sürekli ve güvenilir hizmetlerin sağlanmasını gerektirmektedir.

Kaliteli, sürekli ve güvenilir hizmetlerin sağlanması için amaca yönelik stratejik hedeflerin belirlenmesi bu hedeflere göre de süreçlerin iyi yönetilmesi kaçınılmaz hale gelmektedir. Kurumların temel stratejilerini gerçekleştirebilmesi için Bilgi İşlem Sistemleri ile Bilgi İşlem çalışanlarının rolleri son derece kritik bir hale gelmiş, kurumların bilgi işlem platformlarının çalışabilirliği (availability), platformlar üzerinde işlenen bilginin doğruluğu (accuracy), bütünlüğü (integrity) ve sürekliliği (continuity) gittikçe önem kazanmıştır.

Yukarıda belirtilen nedenlerle, küreselleşen dünyada, bilişim teknolojileri gittikçe önemli hale gelerek, paylaşılan doğru bilgi bir “değer” ve gelişim için kullanılan en önemli “meta” haline gelmiştir. Kurumların bu alanda çalışabilirliğini ekileyecek, hizmetlerini aksatacak ve güvenilirliğini zedeleyecek faktörlerin belirlenerek, yönetilmesi de kaçınılmaz olmuştur. Bu yaklaşım sonucunda da “Risk Yönetimi” kavramı ortaya çıkmıştır.

Ülkemizde Risk Yönetimi anlayışı henüz farkına varılmaya başlanmış bir konudur. Konuyla, uluslararası platformda bankaların sermayelerinin değerlendirilmesine yönelik olarak devam eden düzenlemeler paralelinde, yeni yeni tanışmaktayız. Risk yönetimi finans dünyasında ve bankalarımızca yasal düzenlemeler çerçevesinde ele alınmaya başlanan bir konu olmakla birlikte kar amacı gütmeyen kurum ve kuruluşlarımızda da aynı konuda etkin bir çalışmanın başlatılmasında yarar görülmektedir. Bu çalışma, konunun tanımlanması ve öneminin vurgulanması ile kamu kurum ve kuruluşlarında konuyla ilgili eksikliklerin giderilmesi yönünden bilişim alanında risk yönetimi ile ilgili farkındalık yaratma amacını taşımaktadır.

2. TANIM ve KAVRAMLAR

2.1. Risk Yönetimi

Risk, sözlük anlamı olarak zarara uğrama tehlikesidir ve öngörülebilir tehlikeleri ifade eder. Risk Yönetimi ise bir kurumun ya da kuruluşun çalışabilirliği, ticari müesseseler içinse öncelikle karlılığını olumsuz yönde etkileyebilecek risk faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir. Finans dünyası başlıca risk faktörlerini Piyasa Riski, Kredi Riski ve Operasyonel Risk olarak üç ana başlık altında toplamaktadır. Bu raporda, Bilişim Teknolojilerinde Risk Yönetimi başlığı altında Operasyonel Risk konusunda yoğunlaşıyor olacağız.

2.2. Bilişim Teknolojilerinde Risk Yönetimi

Yukarıda Operasyonel Risk'den bahsedileceği ifade edilmiştir. Öncelikle Operasyonel Risk'den ne anlaşılması gerektiğini netleştirmemiz gerekmektedir. Genel literatür taramasında, Kredi ve Piyasa Riskleri dışındaki tüm risklerin Operasyonel Risk olarak tanımlandığı görülmektedir. Diğer taraftan, yetersiz ya da sorunlu iş süreçleri, personel ve sistemlerden kaynaklanabilecek doğrudan ya da dolaylı kayıpları da operasyonel riskler olarak tanımlamak mümkündür.

Teknolojinin hızlı gelişmesi, ürün ve hizmetlerdeki çeşitliliğin artması, iş süreçlerinin buna bağlı olarak karmaşıklaşması sistem ya da sistemler üzerindeki denetimi zorlaştırmaktadır. Bunun sonucunda hata ve dolandırıcılığa karşı tedbirlerin önceden alınması zorunlu hale gelmektedir. O nedenle, kurum ve kuruluşlar olası bir zarara karşı gerekli altyapı yatırımlarını önceden yapmış olmalıdırlar.

Kurum ve kuruluşlar için Bilişim Teknolojilerine dayalı süreçler, artık kurum ve kuruluşların varlıklarını devam ettirebilmeleri açısından vazgeçilmezler arasında önemli bir yer tutmaktadır. Bilişim Teknolojilerine dayalı iş süreçlerinin herhangi bir sebeple olumsuz yönde etkilenmesi aynı zamanda kurum ya da kuruluşların asli işlevlerini sürdürememesi anlamına gelmektedir.

2.3. Bilişim Teknolojileri Boyutuyla Olası Tehditler

Bilişim Teknolojileri hizmetlerini olumsuz yönde etkileyerek kurum ya da kuruluşları, asli görevlerini kısmen veya tamamen yerine getiremez duruma getirebilecek olası tehditleri beş ana başlık altında toplamak mümkündür.

- (a) **Personel riski** (çalışan sorunları, insan hataları, eksik bilgi ve yetkinlikler),
- (b) **Teknolojik riskler** (hatalı tasarlanmış sistem mimarileri, hatalı modellemeler, güvenlik zaafiyetleri, iletişim problemi, yazılım ve/veya donanım hataları, veri ve sistem kayıpları),
- (c) **Organizasyon riski** (BT ve iş birimleri arasında yetersiz iletişim, yetersiz bütçeleme/planlama, projelendirme hataları, yanlış kaynak kullanımı),
- (d) **Yasal riskler** (Üçüncü şahıs (firma) iflasları veya anlaşmazlıkları),
- (e) **Dış riskler** (Doğal afetler, sabotaj, terörist saldırılar, siber saldırılar, savaş hali, yangın, su basması gibi fiziksel tehditler).

• Yazılım ve/veya donanım hataları

Yazılım geliştirici firmalar piyasaya sundukları kodlar için garanti verememekte, ancak, belli bir süre içinde hatalı kodu düzeltme yoluna gidebileceklerini taahhüt etmektedirler. Bazı donanımlarda ise ilgili firmalar, gelişen üretim teknikleri sayesinde en az bir en fazla üç yıl garanti verebilmektedirler. Ancak, sonuç itibariyle üretimden kaynaklanan, gözden kaçan hatalar her zaman için bir risk unsurudur.

• Telekomünikasyon sistemlerinden kaynaklanabilecek iletişim sorunları

Bilgisayarları birbirine bağlayan, veri iletişimini sağlayan telekomünikasyon sistemlerinde altyapı problemlerinden, işletim hatalarından, doğal olaylardan kaynaklanabilecek sorunlar sağlıklı veri iletişimini engelleyebilmektedir. Alternatif telekomünikasyon yöntemleri kullanılarak riskleri azaltmak mümkün olabilmektedir (Örneğin, iletişim kablolarının yedeklenmesi, mümkün ise farklı rota üzerinden yedek kablolanın yapılması, uydu iletişim altyapısı kullanılarak yedekleme yapılması gibi).

• Veri kayıpları

Veri, bir kurum veya kuruluşun varlığını sürdürebilmesi için hayati önem taşıyan değerdir. Bu bölümde anılan tüm risk noktaları veri kayıplarına neden olabilir. Bu durumda veri alışverişi engellenebilir. Verilerin saklandığı manyetik ortamlar zarar görebilir, veri kısmen veya tamamen okunamaz duruma gelebilir. Böyle bir durumda operasyonun devam edebilmesi açısından kısa sürede veriyi yeniden kazanabilmek önemlidir. Bunun için veriyi farklı bir ortamda yedeklemek ve güvenli bir şekilde yeniden kazanmak gerekir. Bu da ancak muhtemel bir kayıp öncesinde yapılacak iyi bir planlamayla mümkündür.

• Sistem kaybı

Verilerin saklandığı, işlendiği, üzerinde uygulamaların çalıştığı sistemler de yine burada

bahsedilen sebeplerden zarar görebilirler. Bu durum işletmenin, kurum ya da kuruluşun asli görevlerini yerine getirmesine bir engel teşkil edebilir. Bu durumun da önceden öngörülüp, bizzat sistemleri de yedeklemek suretiyle muhtemel bir sistem kaybında normal çalışma durumuna nasıl hızlı bir şekilde gelineceği konusunun çok iyi planlanması gerekir.

- **İnsan hataları**

İnsan hatası olarak risk yaratabilecek unsurlar, yanlış bir kaydın oluşturulması ve bu kaydın örneğin muhasebe kayıtlarında yanlış sonuçlar doğurması şeklinde olabileceği gibi eksik eğitim nedeniyle donanım ve yazılımın hatalı kullanımından kaynaklanan ve görevin yerine getirilmesini etkileyen, engelleyen veya geciktiren sorunlar da olabilir. Bu durum işletmenin nakit akışını da engelleyebilir. İnsan hatalarından kaynaklanan olumsuz sonuçları en aza indirmenin etkin yolu operasyonların mümkün olduğu kadar bilgisayar uygulamalarına taşınması ve insan kaynaklı müdahalelerin azaltılması olacaktır. İnsan bağımlı noktalar içinse periyodik eğitim ve tatbikatlar en azından bilgi eksikliğinden kaynaklanan hataları azaltacaktır.

- **Hatalı tasarlanmış sistem mimarileri**

Bilgisayar sistemleri seçilirken, işletmenin gereksinimleri göz önünde bulundurulmalıdır. Örneğin, işlem kapasitesi, kullanıcı sayısı, sonraki yıllardaki tahmini büyüme hızı gibi unsurlar iyi çözümlenmeli ve işlemci hızı, bellek, veri saklama kapasitesi işletmenin gereksinimine uygun olarak belirlenmelidir. Bu noktalara dikkat edilmediği takdirde eğer işletmenin kullanacağı uygulamalar yoğun işlemci gücü gerektiriyorsa ve bilgisayarın işlemci gücü buna uygun değilse kullanıcıların zamanında hizmet almaları mümkün olmayacaktır. Aynı durum bellek yoğun işlemler için de geçerlidir.

- **Güvenlik zaafiyetleri**

Güvenlik açıkları nedeniyle işletmeler para ve itibar kaybına uğrayabilir ve hizmetleri aksayabilir. Bilişim Teknolojilerinde güvenlik idari ve teknik anlamda ele alınması gereken uzun soluklu bir süreçtir. Güvenlik zaafiyetleri yazılım-donanım bazında alınması gereken teknik tedbirlerin yetersizliğinden kaynaklanabileceği gibi, fiziki güvenliğin zayıflığından veya kullanıcıların bilinçsizliğinden de kaynaklanabilir. O nedenle alınan tedbirler sık aralıklarla gözden geçirilmeli, gerekli düzeltmeler yapılmalı ve işletme çalışanları güvenlik konusunda eğitilmelidir.

- **Hatalı modelleme**

Modelleme bir işi nasıl yaptığımızla ilgilidir. Örneğin bir işletmedeki muhasebe servisinde kayıtların tablolama yazılımlarında saklandığını ve işlem gördüğünü varsayalım. Küçük bir işletmede parasal işlemlerin bu şekilde yürütülmesi belki başlangıçta çok sorun yaratmıyor gibi görünebilir. Ancak işletme büyüdükçe, birimler arası veri alışverişi ihtiyacı arttıkça her birim kendi verisini yaratmaya çalışacak, bu yöntemle tutulan kayıtlarda birimler arasında farklılık olma olasılığı yükselecektir. Artık veri (redundant data) denilen durum ortaya çıkacak ve tutarsızlıklara neden olacaktır. Yanlış üretilen, hatalı işlenen veriler nedeniyle işletmenin büyük maddi zararlara uğrama olasılığı vardır. Veri artıklığını ve farklı formülasyonların kullanılmasını önlemek ve tüm birimlerin doğru ve son bilgiye ulaşabilmesini sağlamak için anılan model bırakılmalı ve merkezi kayıt oluşturma, sorgulama, yetkili birimlerin güncellemesini sağlama gibi olanakları olan, örneğin, web tabanlı bir modele geçilmesi sağlanmalıdır.

- **Doğal afetler**

Doğal afetlerden kaçmamız mümkün olmayabilir ancak, hasarı en az seviyede atlatmak için önlemler alınabilir. Örneğin bilgisayar sistemlerinin kurulacağı mekanın depremlere dayanıklı olarak inşa edilmesi, bir yedeğinin bulunması, alternatif iletişim sistemlerinin kullanılması, afet öncesi, afet sonrası için idari ve teknik anlamda çok iyi planlama yapılmış olması, olası bir kayıp sonrası işletmenin kısa sürede normal işleme geçmesini kolaylaştıracaktır.

- **Çalışan sorunları**

Ücret düşüklüğü, verilen görevden duyulan memnuniyetsizlik, çalışma şartları gibi unsurlar dikkate alındığında çalışanların bu gibi nedenlerle işletmenin aleyhine bilgisayar suçları kapsamına girebilecek işleme zarar verici davranışları görülebilmektedir. Bu nedenle verilerde kötü niyetli değişiklik yapılması, bilgisayarları kısmen veya tamamen çalışamaz duruma getirme ve yetkisiz kullanım girişimleri ile karşılaşma olasılığı göz ardı edilmemelidir.

- **Çalışma yöntem ve yöntemlerinde eksiklik veya yanlışlık**

İyi bir BT yönetimi, doğru yöntemlerin güçlü bir yönetim desteğinde kararlılıkla uygulanması ile mümkündür. Değişen gereksinimler çerçevesinde iş gerekliliklerine uygun teknolojilerin uygulanması beraberinde buna uygun örgütlenme gereksinimini de birlikte getirmektedir. Önceden uygulanmakta olan bir çok yöntemin de değişen koşullara uygun olarak yeniden ele alınması, eksikliklerinin giderilmesi ve yeni duruma uyarlanması gerekmektedir.

- **Yetersiz bütçeleme/planlama**

Teknoloji hızla değişmekte, iş yapış şekillerine uygun teknolojilerin kullanılması günümüz rekabet ortamında zorunluluk arz etmektedir. Gerek işe uygun teknoloji yatırımlarının yapılmasında gerekse mevcut teknolojilerin güncellenmesinde öncelikle gereksinimler doğru olarak belirlenmeli, ardından iyi bir planlama yapılmalı ve bunun için yeterli bütçe ayrılmalıdır.

- **Bilişimden sorumlu birimler ve iş birimleri arasında yetersiz iletişim**

BT birimlerinin en çok karşılaştığı durumlardan biri de işletme yönetimi ile zaman zaman düşünce ayrılıklarına düşmeleri olmaktadır. Bu nedenle gereksinimler yönetimler tarafından doğru algılanamamakta, bunun sonucunda yatırımlar gecikebilmektedir. Bunun nedeni işletme üst yönetimlerinin teknik konulara yabancı oluşlarıdır. BT birimleri ile işletme yönetimleri arasında köprü vazifesi görece bir ara kademeye ihtiyaç duyulmasının sonucunda BT Yönetişim (IT Governence) kavramı doğmuştur. Bu kavram aslında yeni bir yapılanmayı da beraberinde getirmektedir. Buna göre BT birimi ile birlikte iş birimlerinin temsilcilerinden oluşan bir grup oluşturulmakta ve önemli kararlar bu grupta tartışıldıktan sonra alınmaktadır. Ayrıca bu yapılanma BT birimleri ile iş birimleri arasında sürekli bir bilgi alışverişini de sağlayabilmekte iş gereksinimlerinin doğru algılanabilmesine yardımcı olmaktadır.

- **Eksik bilgi ve yetkinlikler**

Eksik bilgi ve yetkinlikler nedeniyle yapılabilecek hatalı uygulamalar, işletmeler açısından birer zaafiyet noktası sayılmalıdır. Örneğin sistemin bilgi güvenliği yöneticisinin yeterli bilgi ve yetkinliğe sahip olmayışı kurum için bir tehdittir. Bilgi eksikliğinden kaynaklanabilecek yanlış bir ayarlama yapması kurumun gizli bilgilerinin çalınması için güvenlik zaafiyeti yaratabilir. Çalışanların yapacakları işe uygun olarak eğitilmeleri ve eğitimlerinin belli dönemlerde yinelenmesi kurum açısından risk olarak sayılabilecek unsurların azaltılmasını sağlayacaktır.

- **Projelendirme hataları**

En sık yapılan hatalardan biri de projelendirme safhasında gerçekleşmektedir. Gereksinimlerin doğru belirlenmemesi, gereksinimlere uygun olmayan çözümlere yönelmesi, projenin çözümlenme safhasında yapılan yanlışlar, hatalı zamanlama, eksik kaynak kullanımı, yönetim desteğinin eksik oluşu, yanlış tasarım ve uygulamalar, uygun örgütsel yapıların olmayışı projelerden istenen sonucu almamızı önleyebilmektedir.

- **Yanlış kaynak kullanımı (yazılım, donanım, insan)**

Kaynak kullanımının uygun yapılabilmesi için iş ihtiyaçlarının doğru belirlenmiş olması, bu ihtiyaçları karşılayabilecek uygun teknolojilerin tespit edilmesi ve uygulama safhasında eğitimli insan gücünün doğru yerde doğru olarak kullanılması kurumun BT hizmetlerinden en üst düzeyde yararlanması için gerekli aşamalar olarak kabul edilmektedir.

- **Üçüncü şahıs (firma) iflasları veya anlaşmazlıkları**

BT hizmetleri açısından herhangi bir şekilde dışarıdan destek hizmeti alınmış ise hizmetin alındığı firmanın veya taşeron firmanın iflas edebileceği veya verilen hizmetlerle ilgili ihtilafa düşülebileceği düşünülerek kontratlarda karşılıklı yükümlülükler ve ihtilaf vukuunda işletmeyi en az zararla bu durumdan kurtarabilecek hususlar açıkça belirtilmelidir.

- **Sabotaj, terörist saldırılar, siber saldırılar**

Stratejik önemi haiz kurum ve kuruluşlarla çevrimiçi alışveriş sitelerine sahip firmaların bilgisayar sistemleri muhtemel bir sabotaj, terörist veya siber saldırıların tehditi altındadır. Bu sistemlerin zarar görmesi olasılığına karşı sistemler farklı bir yerleşkede yedeklenmeli ve muhtemel bir saldırı sonrası normal işleyişe dönüş için önceden planlama yapılmalıdır.

- **Savaş hali**

Ülke olarak herhangi bir savaşa girilmesi halinde stratejik kurum ve kuruluşlarla birlikte bilgisayar sistemleri de tehdit altındadır. Yukarıda açıklandığı üzere yerleşke bazında yedekleme yapılmalıdır. Aynı zamanda, savaş halinde kurumlararası bilgi alışverişinin güvenli bir şekilde devamını sağlayacak önlemlerin alınması gerekmektedir. Savaş hali, aynı zamanda bir ülkenin savaş halinde olduğu ülkenin üretimi olduğu yazılım, donanım ve sunduğu hizmetlerin de aksamasına veya hiç alınmamasına yol açabilir. O nedenle, ürün ve firma bazında da çeşitlendirme söz konusu olmalıdır.

- **Yangın, su basması gibi fiziksel tehditler**

Bilgisayar sistemlerinin kurulduğu mekanların yangın ve su basması gibi tehditlere açık ortamlar olmamasına dikkat edilmeli, bu tehditlerle ilgili erken uyarı ve bilgisayar destekli önleme sistemleri kurulmalıdır. Sistemlerin zarar görmesi olasılığına karşı yedekleme yapılmalı ve olası felaket durumundan geri dönüş planları yapılmış olmalıdır.

Yukarıda ifade edilen tehditlere zaman içinde gelişen teknolojiler ve bu doğrultuda değişen iş süreçleri bağlamında ekler de yapılabilir.

Bir kurum veya kuruluşun yukarıdaki tehditlere göre önceden tedbirlerini almış olması, buna yönelik planlama yapması muhtemel bir tehditin vukuunda asli görevlerini en kısa sürede en az zararla atlatmış olarak yerine getirmeye devam etmesini sağlayacaktır.

Bunun için kurum ya da kuruluş düzeyinde bir Risk Yönetimi anlayışının benimsenmesi, organizasyonel anlamda bu yapının tesis edilmesi gerekir. Risk yönetiminde birinci aşama ilgili kurum ya da kuruluş için riskin tanımlanmasıdır. İkinci aşama ise bunun ölçümüdür. O nedenle risklerin sayısallaştırılmasına ihtiyaç duyulmaktadır. Bunun içinse zarar potansiyelinin tahmini ve gerçekleşme olasılığının belirlenmesi gerekir. Ancak bu şartlar tüm tehditler için uygulanamaz. Aşağıda konuyla ilgili örnekler verilmektedir.

2.4. Muhtemel Kayıplar ve Etkileri Üzerine Örnek Senaryolar

Bölüm 2.3'de ifade edilen olası tehditler dikkate alınarak, "Tehdit gerçekleşirse ilgili kurum ya da kuruluşun kaybı ne olur? Bu kayıpları ve/veya olayın etkilerini en aza indirgeyebilmek için önceden ne tür tedbirlerin alınması gerekir?" şeklindeki sorularının netleştirilmesi amacıyla aşağıdaki senaryolar verilmiştir:

Senaryo 1:

Stratejik önemi haiz bir kurumu referans noktası olarak alalım ve gerçekleşme olasılığı en yüksek tehdit olarak da olası bir terörist saldırıyı belirlemiş olalım. Buna göre ilgili kurum için olası riski yendiden tanımlayalım. Terörist saldırılar nereden geleceği, kimin tarafından ne zaman ve ne şekilde yapılacağı belli olmayan bir saldırı türüdür. Bu bağlamda, olası bir bombalama eylemi, bilişim hizmetlerinin verildiği sistemleri çalışmaz duruma getirebilir, kurumun veri alışverişinde bulunduğu diğer kurum ve kuruluşlarla iletişimini engelleyebilir,

bilişim hizmeti veren birimde çalışan insanların hayatlarını kaybetmelerine sebep olabilir, hizmetlerin verilmekte olduğu bina tamamen kullanılamaz hale getirilmiş olabilir.

En kötü senaryoya göre bu örnekte tüm altyapı kullanılamaz duruma gelmekte, bu hizmeti vermekte olan personel zarar görmektedir.

Örneğimizde, ilgili kurumun, olası bir terörist saldırının sonucundaki parasal kayıplarını, operasyona etkilerini ve kurumun kamuoyu nezdinde yaşayabileceği itibar kaybını sayısallaştırması gerekir.

Örneğin,

- A Kurumu için terörist eylemin olma olasılığı yüksektir.
- Böyle bir olayın meydana gelmesi halinde A Kurumunun olası maddi zararı yaklaşık olarak 22 Milyon YTL'dir.
- Bilişim hizmetleri durursa A Kurumu asli görevlerini yerine getiremez duruma gelir.
- Böyle bir durumda A Kurumu kamuoyu nezdinde güven kaybeder.

Örneğe göre devam edecek olursak, A Kurumu olası tehdit değerlendirmesini gerçekleştirme olasılığını en yüksek bulunduğu terörist eylemlere göre yapacaktır. Böyle bir saldırıya maruz kaldığında kurum yönetimi maddi kaybın mali portresini önceden biliyor olacaktır. A Kurumunun stratejik konumu nedeniyle asli fonksiyonlarını olası saldırı sonrasında devam ettirebilmesi karlılık, nakit akışı ve itibar açısından önemlidir.

Bu durumda, bilişim hizmetleri ikinci bir merkezden, gerek donanım gerekse insan kaynağı açısından kısa süre içinde yeniden devreye alınabilir olmalıdır.

Bunun için A Kurumu organizasyon düzenlemelerini yapmalı; gerekli yatırımları gerçekleştirmeli; olası bir riskin gerçekleşmesinden sonraki adımları planlamalı ve test etmelidir.

Senaryo 2:

Yine stratejik önemi haiz bir B kuruluşumuzu örnek alalım. Bilişim sistemlerinde çok gizli bilgiler tutulmaktadır. Bu bilgilerin kötü amaçlı kişilerce açıklanması halinde B Kurumu kamuoyu nezdinde çok büyük itibar kaybına uğrayacaktır.

Olası bir bilgi sızmasına karşı Bilişim Güvenliği boyutunda her türlü idari ve teknik önlem alınmalı, alınan önlemler için denetim noktaları oluşturulmalı, bu denetimler belli periyotlarda yapılmalıdır. Bu tedbirlerin alınmasında ve uygulanmasında uluslararası Güvenlik Standartlarına uyum gözetilmelidir. B Kurumu, organizasyonunda bilişim güvenliğinden sorumlu bir birim oluşturmalı, güvenlikle ilgili rol ve sorumlulukların tanımlandığı bir Güvenlik Politikası hazırlamalı, bu belge B Kurumunun üst makamınca onaylanmalı ve kurumun tüm çalışanlarına duyurulmalıdır. Bu politika, kurallara uyulmaması halindeki yaptırımları da açıklamalıdır. Düzenli aralıklarla, kurum içi ve bağımsız denetim kurumlarınca güvenlik tedbirlerinin alındığının ve kararlılıkla uygulandığının denetimi uluslararası denetim metodolojileri baz alınmak suretiyle yapılmalıdır. Bu denetimler, kurumun olası riskleri görmesini, risk noktalarında gerekli düzeltmeleri yapmasını sağlayacaktır. Bu şekilde B Kurumu olası kayıplara hazırlıklı olacak ve riskleri en aza indirmiş olacaktır.

Senaryo 3:

C Kurumu deprem kuşağında yer alan bir ilimizde faaliyet göstermektedir. Olası bir deprem felaketinde C Kurumunun bilişim hizmetlerini sürdürebilmesi için iletişim faaliyetlerine devam etmesi hayati öneme sahiptir. Deprem olması halinde kablolu hatların (telefon, fiber vb.) zarar göreceğinden hareketle iletişimin, uydu haberleşme imkanları ile yedeklenmiş olması gerekecektir. Yerleşke kaybı göz önüne alınarak, ikinci bir merkez kurulması (Olağanüstü durum Merkezi) ve olağanüstü durum planlamasının yapılması, iş süreçleri göz önüne alınarak veri kaybını önleyecek yedekleme yöntemlerinin oluşturulması zorunlu olacaktır. Bu kapsamda oluşturulan tüm altyapının da yılda en az bir kez önceden belirlenen senaryolara göre test edilmesi gerekecektir.

2.5. Bilişim Teknolojilerinde Risk Değerlendirme

Risk yönetiminde esas olan, riskin tümüyle engellenmesi değil, sorunlara sistematik ve dikkatli bir şekilde yaklaşılması ve almaya karar verilen risklerin dikkatli yönetimi yoluyla gereksiz kayıpların engellenmesidir. Başarılı bir risk yönetimi için, kurumun varlıklarına ve hedeflerine yönelik riskleri belirlemek, analiz etmek, denetim altında tutmak ve izlemek gereklidir.

Riski yönetmenin en doğru yolu, gerçekleşmesi ve vereceği zarar en yüksek olma olasılığı bulunan riskleri azaltacak resmi bir BT risk yönetim sürecinin oluşturulmasıdır. Risk yönetim sürecinin oluşturulması kararı sonrası yapılması gereken ilk iş bir risk yönetimi lideri atanmasıdır. Bu liderin kim olacağı veya işi nasıl yürüteceği, kurumun büyüklüğüne ve gereksinimlere göre değişecektir. Büyük kurumlarda risk yönetimi için ayrı bir bölümün oluşturulması da söz konusu olabilmektedir. Bu birim anahtar bilgiyi toplayacak ve kararlar verecektir. Aynı zamanda risk yönetim politikalarını ve kılavuzlarını/dokümanlarını oluşturacak ve belki de özel amaçlı risk yönetim sistemlerini devreye alacaktır. Daha küçük çaplı kurumlarda, mevcut birimlerden bir yönetici risk yönetimi çalışmalarının liderliğini yürütebilir. Buradaki önemli nokta, bu işlerin tek bir kişinin görevi olmadığı ve kurum içi ortak bir çalışma gerektiğinin bilincine varılması gerekliliğidir.

Önemli diğer bir nokta iletişim kanallarının düzgün oluşturulmasıdır. BT risk yönetimi hedeflerini oluştururken öncelikle üst yönetimle iyi bir iletişim kurulması gereklidir. Risk yönetimi çalışmalarının, mümkün olan en üst düzey yöneticilerle birlikte planlanması risk yönetiminin başarı şansını artıracaktır. Başarı şansını artıracak bir konu da, risk yönetiminin iş hedefleriyle uyumudur. Üst yönetimden iş hedeflerinin net bir şekilde ortaya konması istenmelidir. BT risk yönetiminden sorumlu yönetici, yürüteceği çalışmanın amaçlarını belirlerken diğer birimlerin risk yöneticilerini de sürece dahil etmeli ve zaman içinde risk değerlendirme bulgularını kurumsal risk çerçevesi içine koymalıdır.

Risk yönetimi ile ilgili destek sağlandıktan sonra işleyiş yöntemlerinin oluşturulması gerekecektir. Bunun için öncelikle kurumun uzun vadeli hedefleri üzerinde çalışılmalıdır. Daha sonra bu hedefleri tehlikeye atacak risklerin tanımlanması ve bu riskler için denetimlerin oluşturulması gerekecektir. Her kurumun bir risk yönetim planı olmalı ve bu plan daima güncel tutulmalıdır.

Risk yönetimi hedefleri, kayıp öncesi ve kayıp sonrası olmak üzere iki kategoride ele alınabilir: Kayıp öncesi hedefler, risklerin gerçekleşmesi beklenmeden alınması gereken önlemleri ve denetimleri (etkin çalışma ortamının sağlanması, belirsizliklerin ortadan kaldırılması, yasal ve diğer resmi düzenlemelere uyum, etik yaklaşımların sağlanması gibi) tarif edecektir. Üretim ortamındaki verilerin bütünlüğünün korunması kayıp öncesi hedeflere iyi bir örnektir. Bu hem yasal ve resmi düzenlemelere uyumu sağlayacak, hem de bu verileri kullanan iş birimlerinin risklerini azaltacaktır. Bu örnek hedefin gerçekleştirilebilmesi amacıyla, üretim ortamlarında değişiklik yönetimi uygulaması devreye alınmalıdır. Bu yöntem verinin keyfi bir şekilde değiştirilmesini engelleyecek, dolayısıyla da olası bir risk faktörünü ortadan kaldıracaktır.

Kayıp sonrası hedefler ise, işletimin hatadan kurtarılması ve devamlılığının sağlanması çerçevesinde değerlendirilmektedir. Soruna müdahale, iş devamlılığının sağlanması ve olağanüstü durumdan kurtulma yöntemleri bu kapsamda oluşturulmalı ve sorun anında gecikmeksizin uygulanmalıdır.

Burada önemle üzerinde durulması gereken konu etkinliktir. Risklerin ortadan kaldırılması veya azaltılması için denetimlerin oluşturulması gereklidir, ancak çok fazla denetim sebebiyle iş yapılamaz duruma gelmesi de kurumlar için bir risk faktörü olabilmektedir. Risk yönetimi işleyiş yöntemleri oluşturulurken getiriler ve etkinlik iyi değerlendirilmelidir.

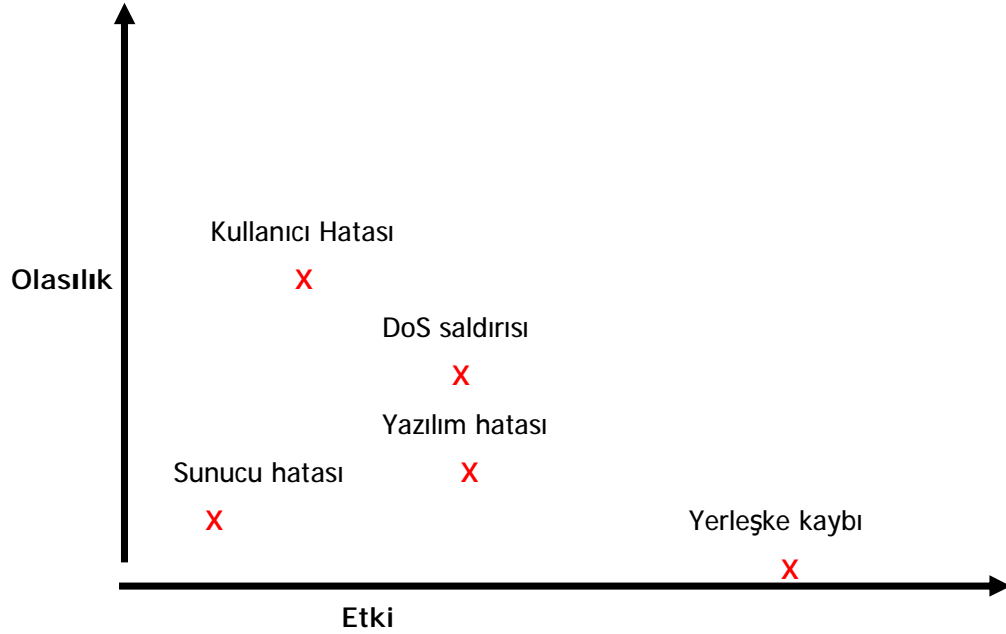
2.5.1. Risk Değerlendirmesi ve Risk haritasının çıkarılması

Risk değerlendirme işlemi BT risk yönetimi hedeflerine ulaşmak için gerçekleştirilmesi gereken bir çalışmadır. Bu çalışmada aşağıdaki adımlar olmalıdır:

- a. **Kayıpların hangi noktalarda oluşabileceğinin belirlenmesi:** Bunun için iş birimleriyle görüşülmesi, mevcut olanakların, süreçlerin, program kodlarının, sistem

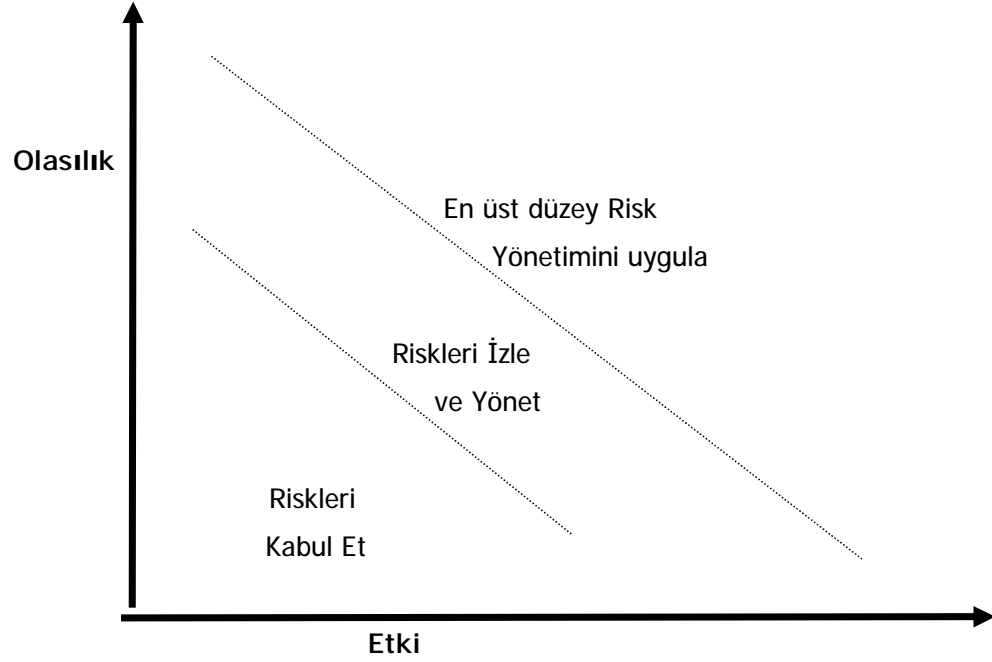
tasarımlarının incelenmesi, açık noktaların ve tehditlerin araştırılması, ağ ve sistem güvenlik tarayıcıları gibi teknik araçların kullanılması gerekebilecektir. Ancak değerlendirme yapılırken, kritik olmayan sistem ve süreçlerle vakit kaybedilmemesi gerekir. Örneğin, yemek listesinin verildiği bir intranet sistemine öncelik tanımak doğru bir yaklaşım olmayacaktır.

- b. **Kayıp ihtimali olan noktaların analiz edilmesi:** Bu zaman alıcı bir çalışma olabilir. Analizlerde, riskin gerçekleşme sıklığı, yaşanabilecek kaybın önem ve şiddeti, toplam kayıpların hesaplanması ve riskin gerçekleşme zamanı konuları üzerinde durulmalıdır. Bunlarla ilgili veri mevcutta tutulmuyor olabilir ama zaman içinde sağlıklı analiz için bu bilgilerin tutulmaya başlanması önemlidir. Risk değerlendirme ve kayıp analizi Şekil 1 benzeri bir grafikte de yapılabilir (Şekil 1).



Şekil 1. Risk değerlendirme grafiği (örnek)

Şekil 1 benzeri oluşturulacak bir grafiğin risk yönetimi tarafından yorumlanabilmesi için kurumun yapısı ve hedefleri paralelinde oluşturulacak Şekil 2'deki gibi bir değerlendirme yöntemi izlenebilir.



Şekil 2. Risk derecelendirme (örnek)

Bu değerlendirme çerçevesinde, kurum için müdahale gerektiren en önemli riskler ortaya çıkarılabilir ve öncelikle bu riskler üzerine odaklanılması sağlanabilir. Bu çalışmalar sonucunda ortaya çıkacak BT risk haritası ilgili tüm taraflarla da paylaşılarak bilinçlendirme sağlanmalıdır.

- c. **Bir risk yönetim tekniğinin seçilmesi:** Risk yönetimi değişik tekniklerle yapılabilir. Bunlardan birisi riskleri dışarıya transfer etmektir. Bu yöntem, bilişim hizmetlerinin ve varlıklarının dış kaynak kullanımıyla farklı kurumlarca yürütülmesini veya sigortalamayı içerir. Sigortalama konusu, her şeyin ölçülebilir olmadığı BT işlemlerinde pek fazla benimsenmemektedir. Bilişim hizmetlerinin bir dış kuruluş tarafından yürütülüyor olması ise riski ortadan kaldırmamakta, yine kurumun kendisi tarafından da bir risk yönetiminin uygulanmasını gerekli kılmaktadır. Risklerin tamamıyla kurum içinde tutulması durumunda, risk denetimlerinin oluşturulması gerekmektedir. Bu denetimler, olasılıkları düşürmek veya kayıpların etkisini azaltmak amacıyla yönelik olacaktır.

En etkin risk denetim yöntemi riskli durumun tamamen engellenmesidir. Örneğin bir işletim sisteminin güvenlik açıklarının olduğu biliniyorsa, o sistemi hiç kullanmamak kurum için riski tümüyle sıfırlayacaktır. Ancak BT ortamlarında bu çözüm genellikle uygulanabilir olmamaktadır. Bu durumda risk yönetimi, riski kabul etmeli ve dikkatli bir izleme ve uygun denetimlerle riski azaltma yoluna gitmelidir. Risklerin gerçekleşmesi durumunda izlenecek yöntemler için de bir çalışma yapılmalı ve kapsamlı olağanüstü durum planları hazırlanmalıdır. Bu planlarda yer alacak hatadan kurtulma yöntemleri sayesinde kayıplar en alt düzeyde tutulabilecektir. Olağanüstü durum planları daima güncel tutulmalı ve gerektiğinde sorunsuz kullanılabilir olmalıdır. Bu amaca yönelik olarak belli dönemlerde olağanüstü durum tatbikatlarının yapılması faydalı olacaktır. Risk yönetimiyle ilgili olarak devreye alınan yenilikler için eğitim ve/veya kurum içinde bilinçlendirme çalışması da unutulmamalıdır.

Risk yönetiminde önemli konulardan bir diğeri de tespit ve kabul edilen risklerin izlenmesi için bir yöntemin devreye alınması gerekliliğidir. Risk denetimleri, işlevsel yöntemlerle veya

periyodik denetim ve gözden geçirmelerle izlenebilir. Bu izleme, denetimlerin etkililiğini ölçme olanağı sağlayacaktır. Tüm denetimlerin bir sahibi ve sorumlusu olmalıdır.

Kurumların oluşturacakları ve her varlık ve aktivite için riskli durumları tanımlayan ve risk değerlendirmesi sonucu oluşturulan risk haritası üzerinde bir eşik belirlenmeli ve bu eşik üzerindeki aktiviteler çok dikkatli izlenmelidir. Denetimler devreye alındıktan sonra riskler yeniden değerlendirilmeli ve bu risklerin kurumsal risk yaklaşımı içindeki yeri ile kurumsal risk yönetimine katkısı net bir şekilde ortaya konmalıdır.

BT risk yönetiminin amacı, tehditlerin belirlenmesi ve denetim altında tutulması yoluyla kurumun gereksiz tehlikelerle karşılaşmasının önlenmesi, önceden görülebilen kayıpların engellenmesi veya uygun bir şekilde planlanması ve etkili/verimli risk denetimlerinin ortaya konmasıdır. Tüm olağanüstü durumların engellenmesi mümkün olmamakla birlikte iyi bir planlama ile kayıplar en düşük seviyede tutulabilir.

BT risk yönetiminin devreye alınması için gereken adımlar aşağıda listelenmiştir.

- Risk yönetimi hedeflerinin iş hedefleri ile uyumu sağlanmalıdır
- Kurum içinde şeffaf olunmalı ve diğer birimlerin katkısı istenmelidir
- Küçük hedeflerle başlanmalı ve böylece erken gelen başarılarla güvenilirlik sağlanmalıdır
- Tüm taraflarla etkin iletişim sağlanmalıdır
- Üst yönetim desteği sağlanmalıdır
- Süregiden risklerin izlenmesi için bir yöntem oluşturulmalıdır.

Risk yönetimi devreye alındıktan sonra bu süreç kapsamında yürütülmesi gereken aktiviteler ise aşağıda listelenmiştir:

- (a) Riskin tanımlanması, çerçevenin oluşturulması
- (b) Risk alanlarının belirlenmesi ve değerlendirilmesi
- (c) Risklerin gerçekleşme olasılığının ve etkilerinin ölçülmesi
- (d) Risklerin derecelendirilmesi
- (e) Belirlenmiş riskler için kabul edilebilir veya istenen sonuçların tanımlanması
- (f) Tehditlerin azaltılması ve fırsatların artırılması için yöntemler geliştirilmesi
- (g) Bir risk yönetim yöntemi ve stratejisinin seçilmesi
- (h) Stratejinin uygulanması, bir risk yönetim planının oluşturulması
- (i) Risklerin izlenmesi, denetim sonuçlarının analiz edilmesi ve gerekli olması durumunda denetimlerde ve risk yönetim planında değişiklik yapılması

2.5.2. Risk Yönetiminde Kullanılan Araçlar ve Yöntemler

Teknik düzeyde riskin yönetilmesi için değişik araç ve yöntemler kullanılabilir. Aşağıda bazı örnekler sunulmuştur:

Risk haritaları: Risklerin kaynağını ve önem derecelerini göstererek, kurumların riskleri tanımlamasını, anlamasını ve önlem almasına yardımcı olan özet grafik ve çizimlerdir.

Modelleme araçları: Risklerin sonuçlarını ve etkilerini göstermek amacıyla senaryo analizleri ve tahmin yöntemleri sunan araçlardır.

İnterne0t ve intranet: Risk farkındalığının artırılması ve yönetimi için bilginin kurum içi ve gerektiği şekilde kurum dışıyla paylaşılması için kullanılabilir araçlardır.

Diğer teknikler: Risklerin belirlenmesi için kurum içi çalıştaylar ve değerlendirme teknikleridir.

2.5.3. BT Risk Yönetiminde Roller

Risk yönetimi kapsamında kurumdaki tüm çalışanların bir rolü bulunmaktadır. BT risk yönetimindeki roller de bu genel çerçevede değerlendirilmektedir. Bu bölümde, kurum içinde risk yönetiminde değişik grupların üstlenebilecekleri sorumluluklar ve roller incelenmektedir.

Üst yönetimin sorumlulukları:

- Risk yönetiminin kurum stratejilerine entegrasyonu
- Risk yönetiminin yakından izlenip gerekli desteğin sağlanması.
- Risk yönetim çalışmalarının etkililiğinin sorgulanması.
- Risk yönetimi eğitimlerinin sağlanması.
- Risk yönetiminin daha sistematik hale getirilmesi için gerekli yatırımların yapılması

Birim Yönetimlerinin sorumlulukları:

- Risk yönetim stratejilerinin kurum içinde uygulanmasının sağlanması
- Risklerin önceliklendirilmesi
- Risk yönetiminin performansının değerlendirilmesi
- Risk yönetimi prensiplerinin karar verme sürecinin bir parçası haline getirilmesi
- Risk yönetiminde yeterli planlama, gerçekleştirme, eğitim, kontrol, izleme ve dokümantasyon çalışmasının yapılması

Risk Yönetimi Uzmanlarının sorumlulukları :

- Risk yönetimi ile ilgili öneri, yönlendirme ve yardımların tüm kurumun risk politikalarıyla ve üst yönetimin hedefleri doğrultusunda yapılması
- Birimlerin riskleri belirlemelerine ve risk değerlendirmesi yapmalarına yardımcı olunması
- Birimlere, daha etkili bir risk yönetimi için yardımcı araçlar sağlanması veya bu tür araçların tasarım ve gerçekleştirimine yardımcı olunması

İç Denetim ve Kontrol uzmanlarının sorumlulukları:

- Risk Yönetimi kuralları çerçevesinde üst yönetime birimlerin performansı konusunda raporlama yapılması

Tüm çalışanların sorumlulukları:

- Risk yönetimi konularına karşı ilgili ve bilgili olunması
- İşlerin risk değerlendirmesi çerçevesinde yürütülmesi
- Bilgi ve doküman sağlanması

3. BİLİŞİM TEKNOLOJİLERİNDE RİSK DENETİMİ

Bilişim sistemlerinin belirli aralıklarla gözden geçirilmesi, risk noktalarında gerekli düzeltmelerin yapılmasını sağlayacaktır. Bilişim sistemlerinin gözden geçirilmesinde, Dünya genelinde yaygın olarak, Bilgi Teknolojisi ve İlgili Teknolojilere İlişkin Kontrol Hedefleri (*COBIT : Control Objectives for Information Technology*) olarak adlandırılan belge kullanılmaktadır. Gözden geçirmeler belli periyotlarda kurum içi ve kurum dışı bağımsız denetçilerle yapılabilmektedir. Denetim sonuçlarına göre yapılacak düzeltmelerle riskler kabul edilebilir bir seviyede minimize edilebilmektedir.

Risklerin azaltılmasına yönelik başka çalışmalar da bulunmaktadır. Bunlardan biri de *BASEL II (Basel committee on Banking Supervision)* belgesidir. Bankacılık sistemini ilgilendiren ve bankaların sermaye yeterliliklerinin ölçülmesinde ve değerlendirilmesinde Avrupa Birliği'nce uygulanması öngörülen *BASEL II Sermaye Uzlaşısı Belgesinde* yer alan standartlara uyum süreci, ülkemizde de, 2005 yılı itibarıyla başlamış ve bunun için üç yıllık bir geçiş süreci öngörülmüştür. *BASEL II*'de, risklerden biri olarak operasyon riski başlığı altında teknoloji riski ve bunu azaltmaya yönelik olarak gerçekleştirilmesi gereken adımlar yer almaktadır.

ABD'de, 2004 yılı sonunda uygulanmaya başlanan *Sarbanes Oxley (SOX)* ise şirket hissedarlarını korumak amacıyla borsaya kayıtlı şirketlerin yönetimlerine ve çalışanlarına bir takım yükümlülükler getiren uyumluluk yasasının bir parçasıdır. SOX yasasına göre birçok işlemin ve iletişimin kayıt altına alınması gerekmektedir. Örneğin e-postalar, telefon konuşmaları ve işlem kayıtlarının arşivlenmesi gerekmektedir. Halihazırda sadece ABD'deki şirketler için geçerli olan denetime tabi bu yükümlülüğün, dünya genelinde de kabul görmesi ve yaygınlaşması beklenmektedir.

Yukarıda ifade edilen standartlar, belgeler ve yükümlülükler yönetimlerin, bilinmezlerin çok olduğu bir ortamda, daha iyi ölçülebilir ve yönetilebilir bir yapı kurabilme arayışlarının bir sonucudur. En iyi deneyimlerden yola çıkılarak hazırlanmış belgelerdir ve bugün bu alanda bilinen en iyi referanslar olarak kabul görmektedirler (Kaynak : Bilişim Güvenliği, Ahmet PEKEL, Türkiye Cumhuriyet Merkez Bankası Bülteni : Lira, Ocak 2006, Sayı : 37).

Anılan kurallara uyumluluk, bu konuda uzmanlaşmış bağımsız denetçiler tarafından yapılmaktadır. Bu hizmet ya dış hizmet yoluyla temin edilebilmekte veya kurum ya da kuruluş içinde oluşturulan ve doğrudan kuruluşun üst yönetimine bağlı olarak çalışan iç denetim yapısı kapsamında gerçekleştirilebilmektedir. Kuruluşlar içerisinde oluşturulan iç denetim birimlerinin görevi, kuruluşun her türlü etkinliğini denetlemek - ki buna operasyonel risk başlığı altındaki bilişim teknolojileri de dahildir- , geliştirmek, iyileştirmek ve kuruluşa değer katmak amacıyla bağımsız ve tarafsız bir şekilde güvence ve danışmanlık hizmeti vermektir. İç denetim birimleri, bu yönleriyle klasik teftiş anlayışından ayrılmaktadır. Bu anlayışta, finansal, operasyonel ve yönetsel riskler ele alınmakta, mevcut durum en iyi uluslararası uygulamalarla karşılaştırılmakta ve iyileştirme çalışmalarının başlatılması sağlanmaktadır.

4. ÖRNEK RİSK ANALİZ ÇALIŞMASI

Bu bölümde bir kurum için Servis ve Destek hizmetleri kapsamında COBIT yöntemi çerçevesinde örnek bir risk analizi çalışması anlatılmaktadır. Risk senaryolarının ve COBIT BT süreçlerinin detaylı incelemesi EK-A 'da verilmiştir.

Temel yaklaşım, örneğin A Kurumu'nun iş süreçlerini BT ortamı ile eşleştirme, eşleştirme neticesinde belirlenen her alan için birbiri ile uyumlu bir risk değerlendirme yöntemini uygulamaktan oluşmaktadır.

Risklerin gerçekleşme olasılığı ve tüm BT ortamında geçerli olumsuz etkilerinin tanımlanması ve değerlendirilmesi veya bütün ortam için geçerli olan tek bir tehdit/etki değerinin belirlenmesi imkânsızdır. Bu nedenle gerçekleşme olasılığı ve etkilerinin ölçülebilmesi için öncelikle BT'nin bu çalışmaya uygun olarak daha rahat yönetilebilir ve ölçülebilir bir sınıflandırmasının yapılması gerekmektedir.

4.1. Risk Analizi Yöntemi

4.1.1. Risk Analizi Amaçları ve Kullanılan İlkeler

Risk analizinin genel amacı A Kurumu'nun en çok hangi risk senaryolarına maruz kaldığını saptamaktır. Bu bilgi en kritik senaryolara ilişkin riskleri azaltmak için yeterli kontrol önlemlerinin var olduğunu doğrulamak için gerekmektedir.

Tehdit senaryolarını tehditlerin önüne geçmek için uygulanan kontrollerle ilişkilendirmek için değişik yöntemler mevcuttur. Bu yöntemlerden ikisi aşağıda özetlenmektedir:

Her tehdit senaryosunu önleyici kontroller ile ilişkilendirmek – bu ISF (Information Security Forum) SPRINT yöntemi tarafından uygulanan çözümdür. Bu çözümde her bir tehdit senaryosu için önceliklendirilmiş kontrol önlemleri mevcuttur;

Risk senaryolarının olası tehditlerinin etkileri göz önünde bulundurularak, hangi BT süreçlerinin bu riskleri azaltmak için önemli olduğu ve bu süreçler içinde kilit kontrol önlemlerinin hangileri olduğu belirlenir. Bu yaklaşım BT kontrollerine yönelik CobiT yaklaşımıdır. CobiT, risk senaryoları ve BT süreçleri arasında doğrudan bir ilişki kurmadığı için, bu ilişkiyi kurmak amacıyla bilgi ölçütleri ara basamak olarak kullanılacaktır.

Analizin bütünlüğünü ve tutarlılığını sağlamak amacıyla, aşağıdaki adımlar gerçekleştirilmiştir:

- Genel risk senaryolarına dayanarak bu senaryoların A Kurumu'nun ortamında hangi koşullarda gerçekleşebileceğinin belirlenmesi,
- Risk senaryoları gerçekleştiğinde oluşacak finansal, operasyonel ve itibar etkilerinin belirlenmesi ve değerlendirilmesi,
- Mevcut kontrol önlemlerini göz önüne almadan risk senaryolarının gerçekleşme olasılığının tahmin edilmesi.

4.1.2. Risk Analizi Yaklaşımı

Bu bölüm, kullanılan bilgi toplama ve toplanan bilginin değerlendirilmesi konusundaki yaklaşımı içermektedir.

Öncelikle BT ile ilgili risk senaryolarının genel bir listesi derlenmiştir. Bu senaryolar belirlenirken konuyla ilgili aşağıdaki kaynaklardan yararlanılmıştır:

- COSO çerçevesi
- ISF SPRINT risk senaryoları
- Risk senaryo envanteri

Sonuç olarak 21 potansiyel senaryoyu kapsayan aşağıdaki liste oluşmuştur:

BT ile İlgili Risk Senaryoları	
Ref	Olay
S01	Yetersiz sistem & ağ kapasitesi
S02	3. şahıs iflası ve/veya anlaşmazlığı
S03	Doğal Felaket
S04	Şirket kaynaklarının yanlış kullanımı
S05	İnsan hatası
S06	Çalışan sorunları (dahili ve harici)
S07	Veri/işlem gizliliğini tehlikeye sokacak kötü niyet ve sabotaj
S08	Çalışma yöntemleri ve prosedürleri (şimdiki ve geçmişteki) yetersiz tanımlanmış veya belgelenmiş
S09	Yazılım hatası
S10	Yetersiz bütçe & planlama
S11	Veri bozulması
S12	İletim hatası
S13	Veri/işlem bütünlüğünü tehlikeye sokacak kötü niyet ve sabotaj
S14	Veri/işlem erişilebilirliğini tehlikeye sokacak kötü niyet ve sabotaj
S15	Dahili fiziksel olay (kablo, yangın, ...)
S16	Yetersiz altyapı/mimari
S17	Proje & Program Yönetim Başarısızlıkları
S18	BT ve hizmet sağladıkları kişiler arasındaki yetersiz iletişim
S19	Eksik veya yanlış yönlendirilmiş bilgi birikimi & beceriler
S20	BT için artan düzenleyici uyum gereklilikleri
S21	Yetersiz veri modelleme

Tablo 1. BT ile İlgili Risk Senaryolarının Listesi

4.1.3. Hesaplama Kuralları

Risk senaryolarını değerlendirirken her senaryo için "en kötü durumun" göz önünde bulundurulduğunu ve "ortalama değerlerin" kullanılmadığını anlamak önemlidir. Örneğin bir senaryo için üç farklı boyutta tehdit ve etki belirlendiğinde, en yüksek etki derecesine sahip tehdit o senaryonun genel etki seviyesinin belirlenmesinde kullanılmaktadır.

Benzer şekilde, bir servis alanı farklı alt alanlardan oluştuğunda ve bu alt alanlarda aynı senaryo için farklı etki seviyeleri ortaya çıktığında, yalnızca en yüksek etki ve olasılık derecesine sahip alt alana ait olan tehdit ve etki, servis alanının tamamı için ilgili senaryoya ait genel etki seviyesini belirlemekte kullanılmaktadır.

Son olarak, her senaryonun CobiT BT süreçleriyle ilişkilendirilmesinde, aynı şekilde en yüksek etki değerine sahip senaryo CobiT sürecinin A Kurumu açısından önem derecesini belirlemektedir.

4.1.4. Kullanılan Değerler

Her senaryo için etki ve olasılık aşağıdaki tabloya göre değerlendirilmiştir:

- **Olasılık Dereceleri**

Olasılık Dereceleri Açıklamaları	
1	İmkansız veya olması hiç muhtemel değil
2	Olması muhtemel değil
3	Olması muhtemel veya seyrek olarak gerçekleşmiş
4	Olması oldukça muhtemel veya zaman zaman gerçekleşmiş
5	Olması kesin veya sık sık gerçekleşmiş

Tablo 2. Olasılık dereceleri

- **Etki Dereceleri**

A Kurumu'nda yapılan risk değerlendirmesi üç farklı boyutta değerlendirilmiştir. Bu üç boyut finansal, operasyonel ve itibar etkileridir. Belirlenen üç etki boyutuna ilişkin kullanılan ölçütler ve derecelendirme seviyelerinin açıklamaları aşağıda listelenmiştir.

- **Finansal Etki Boyutu**

- 1.50,000 YTL'den az potansiyel kayıp
- 2.50,000 - 200,000 YTL arasındaki potansiyel kayıp
- 3.200,000 - 1,000,000 YTL arasındaki potansiyel kayıp
- 4.1,000,000 - 5,000,000 YTL arasındaki potansiyel kayıp
- 5.5,000,000 YTL'den daha fazla potansiyel kayıp

- **Operasyonel Etki Boyutu**

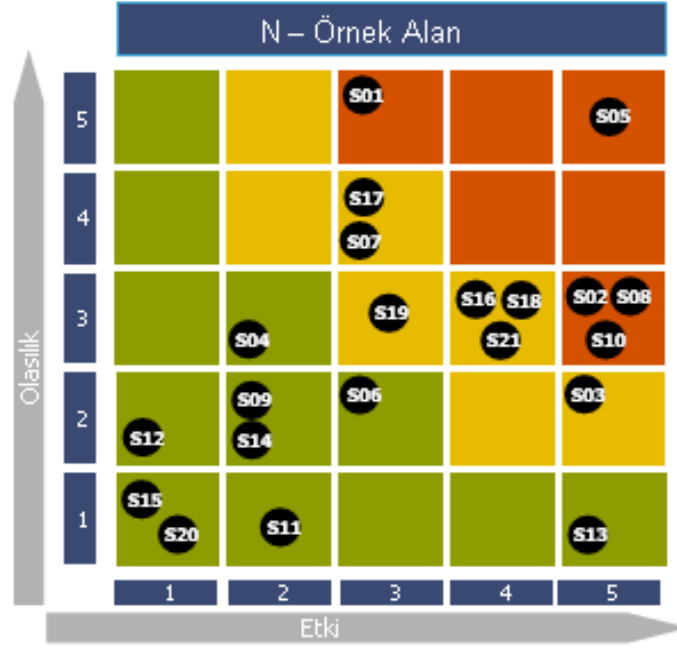
1. İşlemler hiç etkilenmeyecektir.
2. Etki iş süreçlerinin verimliliği ile sınırlı olacaktır.
3. Etki belirgin olur ama iş ile ilgili işlemler devam eder ve başarısızlık tolere edilebilir düzeyde olur.
4. İş süreçleri üzerinde ciddi bir etki olacaktır ve kurumda önemli bir zararlar sonuçlanacaktır.
5. Etki kurumun faaliyetlerinin sürdürülebilirliğini tehdit edecektir.

- **İtibar Etki Boyutu**

1. Kurumun saygınlığına bir etkisi olmaz.
2. Kurumun saygınlığına az bir etkisi olur.
3. Kurumun saygınlığına orta derecede bir etki olacaktır.
4. Kurumun saygınlığına ciddi bir etkisi olacaktır.
5. Kurumun faaliyetlerinin sürdürülebilirliği etkilenecektir.

Risk senaryosunun önem derecesi, gerçekleşme olasılığı ve etki değerlerinin çarpımı ile belirlenmiştir. Bir alandaki senaryonun genel önem derecesi belirlenirken, her senaryo için farklı alt değerlendirmeler sonucu oluşan en büyük önem derecesinin değeri kullanılmaktadır.

Bir alanın genel risk haritası her bir senaryo ile ilgili olasılık ve etkinin Şekil 3'deki grafik üzerinde yerleştirilmesi ile oluşturulmaktadır.



Şekil 1. Genel Risk Haritası

Kırmızı alandaki risk senaryoları en kritik senaryolardır. Bu senaryolar ile belirlenen riskler uygun kontroller ile kabul edilebilir düzeye indirilmelidir.

4.1.5. CobiT BT Süreç Önceliklendirmesi

Risk senaryo çalışması aşamasında edinilen bilgi ve değerlendirmeler sonucu belirlenen önem dereceleri kullanılarak CobiT BT süreçleri de önceliklendirilmiştir.

4.2. Sonuçlar - Risk/Tehdit Senaryoları Analizi

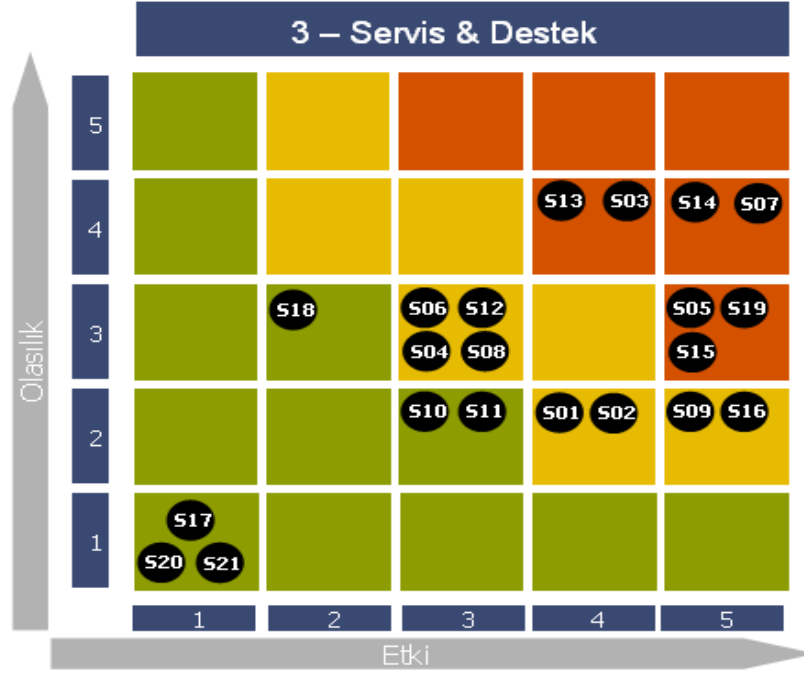
Analiz Sonuç bölümü aşağıdaki bilgileri içermektedir:

- Risk analizi sonuçlarına dayanılarak hazırlanan ve servis alanlarına göre CobiT BT süreçlerinin önem derecelerini içeren genel bir tablo,
- Her servis alanı detayında yüksek risk senaryolarını içeren risk haritası ile risk düzeyi en yüksek senaryolarının kısa bir tanımı ve etkilerini içeren tablo.

Raporun bu kısmında eşleştirme esnasında belirlenen bir servis alanı için risk değerlendirmesinin sonuçları sunulmaktadır. Risk seviyeleri, kullanılan risk senaryolarının önem derecelerini gösteren risk haritaları yoluyla yapılmaktadır.

- **Risk Haritası**

“Servis ve destek” alanı A Kurumu'ndaki BT faaliyetlerinin çoğunu kapsamaktadır.



Şekil 2. Servis & Destek Genel Risk Haritası

- Bu alan için tanımlanmış en kritik senaryolar

Risk haritasının kırmızı bölgelerinde yer alan risk senaryoları bu alan için en kritik senaryolar olarak belirlenmiştir.

Başlık	Tanım	Olayın tanımı	Etki
Doğal Felaket	Doğal felaketler sonucu sistemin kullanım dışı kalması ve/veya servisin ulaşım dışı olması (örneğin deprem, sel, vb.)	Deprem, sel gibi doğal felaketler	İşlemlerde kesinti yaşanabilir
İnsan hatası	Personel hatası yüzünden meydana gelebilecek herhangi bir olay (yanlış konfigürasyon, işlemsel hatalar, kazara ifşa etmek)	Güvenlik araçlarının yanlış konfigürasyonu	Kurum yerel ağına yetkisiz erişim kritik kurumsal verilere ve sistemlere erişimi sağlayabilir. Sonuç olarak da gizlilik ihlali, bütünlüğün bozulması ve verinin erişilemiyor olması gibi durumlar meydana gelebilir.
Veri/işlem gizliliğini tehlikeye sokacak kötü	(Daha önceki) çalışanlar ve/veya harici kişiler tarafından yapılan kasıtlı hareketlerden	- Kritik kurumsal verilere kötü niyetli erişim - Ağ trafiğinin	- Saklanan kritik kurumsal bilgilerinin gizliliğinin bozulması - Şifre veya diğer gizli

Başlık	Tanım	Olayın tanımı	Etki
niyet ve sabotaj	kaynaklanan kayıplar. Örneğin gizlice dinleme, hırsızlık, belgeleri ele geçirme.	dinlenmesi	bilgiler ağ üzerinde dinlenebilir
Veri/işlem bütünlüğünü tehlikeye sokacak kötü niyet ve sabotaj	Şirket içindeki veya dışındaki kişiler tarafından yapılan veri/işlem bütünlüğünü tehlikeye düşürmeye yönelik sahtekarlık, işlemlerin değiştirilmesi gibi kasıtlı hareketler	Saklanan kritik kurumsal verilere kötü niyetli erişim	Saklanan kritik kurumsal verilerin bozulması
Veri/işlem erişilebilirliğini tehlikeye sokacak kötü niyet ve sabotaj	Şirket içindeki veya dışındaki kişiler tarafından yapılan veri/işlem/servis erişilebilirliğini tehlikeye düşürmeye yönelik kasıtlı hareketler(sabotaj, servis girişimlerini geri çevirmek, ...)	Saklanan kritik kurumsal verilere kötü niyetli erişim	Saklanan kritik kurumsal verilere erişilemiyor olması
Dahili fiziksel olay (kablo, yangın, ...)	Potansiyel işletim sorunlarıyla (erişilebilirlik, bütünlük) sonuçlanan fiziksel altyapı olayları	Tesis ve ekipmanları etkileyen zararlar	Veri ve donanıma kalıcı zarar
Eksik veya yanlış yönlendirilmiş bilgi birikimi & beceriler	Gereken sistemlerin ve uygulamaların geliştirilmesinin ve işletilmesinin imkânsızlığı. Teknolojinin gelişimi izlenmiyor ve BT stratejisine dâhil edilmiyor.	Gerekli eğitime sahip olmamak ve takım içinde bilgi birikiminin paylaşılmaması	Yeni tehditler ve/veya değişen BT ortamı ile ilgili uygun faaliyetleri yerine getirememe.

Tablo 3. Servis & Destek için kritik senaryolar

- Risk Analizi Sonuçları**

A Kurumu için bilgi ölçütlerinin önem dereceleri, kullanılan tehdit senaryolarının önem dereceleri, CobiT çerçevesine ait önem dereceleri kullanılarak hesaplanan BT süreç önem değerleri çok önemli görüşler kazandırmaktadır, ancak nihai sonuç değildir. Bu bilgiler kullanılarak A Kurumu aşağıdaki konularda önceliklendirmeler yapılabilir:

- En kritik süreçler üzerinde BT denetimleri;
- BT riskleri ve bu risklere ilişkin süreçleri göz önünde bulundurarak süreç olgunluk değerlerinin artırılması.

Servis ve Destek alanı için, beklenildiği gibi, CobiT DS alanı yüksek önem taşımaktadır. Bunların arasında servis seviyelerinin belirlenmesi, üçüncü şahıslardan alınan servislerin yönetilmesi, kesintisiz servis sağlanması ve sistem güvenliği, yapılandırma yönetimi gibi süreçler en önemlileri olarak belirlenmiştir. Ayrıca CobiT izleme alanındaki süreçler de önemli süreçler olarak belirlenmiştir,

Risk değerlendirme süreci sistematik bir şekilde, her servis alanı için yüksek önem taşıyan bir süreç olarak ortaya çıkmıştır. Bu sonuç CobiT'in doğal değerlerinden kaynaklanmakla birlikte gerçek hayatta da tüm BT ortamlarında önem verilmesi gereken bir süreçtir.

5. İŞ SÜREKLİLİĞİ VE OLAĞANÜSTÜ DURUM YÖNETİMİ

Bilişim Teknolojilerinde risk yönetimi, temelde işin sürekliliğini etkileyebilecek, bilişim sistemlerinde kesintiye yol açabilecek risklerin kontrol altında tutulabilmesini hedeflemektedir. Ancak risk yönetimi çalışmalarının yanısıra, risklerin gerçekleşmiş olacağı olağanüstü durumlar için de iş sürekliliğini ve kesintisiz çalışmayı sağlayabilecek planların ve hazırlıkların yapılmış olması gerekmektedir. Herhangi bir nedenle Bilişim Sistemleri'nin hizmet veremez duruma gelmesi ihtimali, kurum ve kuruluşları iş kritik işlerinin devamlılığını sağlamak üzere bilişim sistemlerini farklı bir yerleşkede yedeklemeye yöneltmektedir.

Bir kuruluşta olağanüstü durum; deprem, yangın, su basması, sabotaj, terörist saldırılar ve savaş hali gibi nedenlerle bilişim sistemleri altyapısının kullanılamayacak derecede zarar görmesi sonucunda ilan edilebilir. Olağanüstü Durum İlanı'nı takiben kurum ya da kuruluşun daha önceden hazırlanmış olan bir yerleşkeye olağanüstü durum öncesinden belirlenmiş bir plan doğrultusunda gidilmek suretiyle iş kritik işlemlerini yönetmesi, Olağanüstü Durum Yönetimi olarak ifade edilmektedir.

Olağanüstü durumda, Bilişim Teknolojileri açısından iki tür önlem söz konusudur. Bunlardan birincisi doğrudan bilişim hizmeti veren teknik birimin alması gereken önlemler, diğeri ise idari anlamda alınması gereken önlemlerdir. Teknik önlemleri, sistem bazında kayıpların ne şekilde giderilebileceği, olağanüstü durum sonrası ikincil sistemden kritik işlerin işletimine nasıl geçileceği ve birincil sistem ayağa kaldırıldıktan sonra normal çalışma düzenine geçiş adımlarının ne olacağı oluşturmaktadır. İdari önlemler ise, özellikle yedek yerleşkeye personelin sevki ve bu mekanın idaresi anlamında önceden planlanmış ve olağanüstü durum ilanı sonrasında uygulamaya alınacak idari önlemlerdir.

Teknik önlemlerin uygulanması daha çok bilişim teknolojileri birimlerinin sorumluluğunda iken, idari önlemler, ilgili kurum ve kuruluşların üst yönetimlerinden iş kritik birimlerine uzanan geniş bir yelpazede ele alınmalıdır.

Herhangi bir kurum ya da kuruluşta Olağanüstü Durum planları hazırlanırken, öncelikle kritik işler belirlenmeli ve bu işlerin olağanüstü durum sonrasında devam etmesi için elverişli uygun altyapılar oluşturulmalıdır. Bu altyapılar oluşturulmadan önce ikincil sistemin kurulacağı yerleşkenin coğrafi yapısı, birincil sistemin bulunduğu yerle olan uzaklığı, depreme dayanıklılığı, yangın ve su basmalarına karşı veya herhangi bir terörist saldırıya karşı alınacak ilave fiziki önlemler doğru analiz edilmelidir. Bunun için teknik birimler operasyonel birimlerle biraraya gelmeli ve iş ihtiyaçlarını belirlemelidir. İş ihtiyaçlarına uygun altyapı oluşturulmalı ve bu altyapının işlerliği yılda en az bir kez iş birimleriyle birlikte eşgüdüm sağlanarak kurum ya da kuruluşun üst yönetimleri bilgisi dahilinde sınanmalıdır. Bu altyapının kurulu olduğu yerleşkede sistemlerle birlikte iletişim altyapısı da yedekli çalışıyor olmalıdır. Hatta eğer kablolu iletişimden yararlanılmış ise mevcut iletişim, alternatif iletişim teknolojisi olarak uydu haberleşmesi ile yedeklenmelidir. Bu yerleşkede, ihtiyaç duyulan, örneğin telefon, faks, telex, internet erişimi gibi olanaklar önceden düşünülmüş olmalıdır. Bu yerleşkeye geliş ve gidişler veya yeme-içme olanakları için kurumun bu işlerden sorumlu birimleriyle eşgüdüm sağlanmalıdır. Diğer taraftan, konunun birden çok birimi ilgilendirmesi nedeniyle genel koordinasyon, kurumun üst yönetimince idari birimlerden birine verilebilir veya üst yönetim düzeyinde ele alınabilir. Ayrıca, bu çalışmalar konusunda kurum çalışanları belli periyotlarda bilgilendirilmeli ve yapılan tatbikatlarla herhangi bir olağanüstü durum sonrasında çalışanlardan beklenenler adeta refleks boyutuna taşınmış olmalıdır.

İş birimleri iş sürekliliğine yönelik olarak, işlemlerini ikincil merkezden yürütmeyi B Planı olarak ele almışlarsa, bilişim hizmetleri olmaksızın da iş sürekliliğini ne şekilde sağlayabileceklerini bir C Planı çerçevesinde ele almalıdırlar. Bu süreç, işlerin daha çok kağıt ortamında nasıl takip edileceğine yöneliktir. İş birimleri, işin kağıt ortamında nasıl gerçekleştirilebileceğini ifade eden genel bir doküman hazırlamış olmalıdırlar. Tüm planlara ilişkin dokümanların bir kopyası ikincil yerleşkede korumalı bir şekilde hazır tutulmalıdır. Ayrıca, bu yerleşkede ihtiyaç duyulacak her türlü ekipman (bilgisayar, yazıcı, toner, kağıt, telefon, faks, telex, kirtasiye malzemeleri v.b.) yedek olarak hazır bulundurulmalıdır.

Yedek merkezden hizmet verilmesi ile ilgili olarak bilgisayar firmalarıyla yapılacak servis ve destek hizmetleriyle ilgili sözleşmelerde ikinci yerleşkede alınacak hizmetlerle ilgili maddeler bulunmalı ve alınacak hizmetlerin kapsamı doğru ve detaylı olarak tarif edilmelidir.

İş sürekliliği ve olağanüstü durum yönetimi, tüm dünyada son yıllarda, özellikle de terör saldırılarının artmasıyla birlikte, üzerinde daha da önemle durulan bir konu haline gelmiştir. Bu kapsamda, kurumlar kendi içlerinde olağanüstü durum organizasyonları oluştururken, tüm ülke boyutuna ulaşan kapsamlı hazırlık ve çalışmalar da gündeme gelmiştir. Türkiye'de de bu çerçevede ulusal boyutta yapılan çalışmalar bir sonraki bölümde detaylandırılmıştır.

6. TÜRKİYE'DEKİ UYGULAMALAR

Olağanüstü Durum Planlaması ve Yönetimi ile Olağanüstü Durum Merkezi kavramları da Risk Yönetimi kapsamında ele alınması gereken bir konu olarak değerlendirilmektedir. Bu nedenle, Ulusal Acil Durum Yönetimi Sistemi ülkemiz için önemli bir proje niteliği taşımaktadır.

6.1 Ulusal Acil Durum Yönetimi Sistemi

Ulusal Acil Durum Yönetimi Sistemi; Türkiye Cumhuriyeti sınırları içerisinde ve bölgede olası her türlü afetlerde/acil durumlarda hükümetin ve çok uluslu kuruluşların bilgi ve haberleşme ihtiyacını karşılamak amacıyla kurulması planlanmıştır. Sistemin başlıca işlevi ise; Acil Durum öncesi hazırlık, Acil Durum anında yönetimin doğru ve hızlı karar verme sürecine destek vermek, Acil Durum sonrası ise normale dönüşün hızlanmasını sağlayan dinamik ve yaşayan bir yapıya sahip olacaktır

Sistem esas itibarıyla, haberleşme, veri şebekesi, uygulama yazılımları ve operasyon merkezleri ve destek sistemleri ile gerekli hizmetlerinin temin edilmesinden oluşmaktadır.

Sistemin çalışacağı ana merkezler:

- (a) Ulusal Acil Durum Yönetim Merkezi;
- (b) Bakanlıklar Acil Durum Yönetim Merkezleri
- (c) Kurumlar Acil Durum Merkezleri
- (d) İl Acil Durum Merkezleri
- (e) Mobil Merkezler

Sistem Ulusal Acil Durum Yönetiminin ihtiyaçlarını karşılayacak şekilde tasarlanmıştır:

- Ulusal acil durum koordinasyon merkezi
- Kurumlar arası koordinasyon
- Kaynak yönetimi
- Güvenilir, beka kabiliyeti yüksek ve emniyetli haberleşme
- Bilgisayar tabanlı karar destek sistemi
- 24 saat 365 gün çalışan bir sistem
- Erken uyarı sistemleri ile iletişim
- Yardım faaliyetlerinin kontrol ve koordinasyonu
- Olay hakkında hızlı, doğru bilgiye ulaşabilme
- Hızlı reaksiyon, arama - kurtarma, yardım, iyileştirme ve mobil bir yönetim
- Afet zararlarının azaltılması
- Afete hazırlık
- Eğitim ve tatbikatların ifası
- Halkın bilgilendirilmesi ve eğitim malzemeleri / dokümantasyon
- Yasal ve idari altyapının oluşturulması / güncellenmesi
- Uluslararası yardım faaliyetleri ve ilişkilerin düzenlenmesi

Sistem Bileşenleri:

- (a) Haberleşme sistemi
- (b) Veri şebekesi
- (c) Acil Durum Yönetim Bilgi Sistemi (Uygulama Yazılımı)
- (d) Operasyon merkezleri
- (e) Destek sistemleri
- (f) İl Acil Durum yönetim sistemleri

Haberleşme sistemi her durumda sistemin çalışmasına imkan vermek amacı ile farklı ortamları kullanacak şekilde tasarlanmıştır.

Ses, Veri ve Video haberleşmesi, iletişimi TT ve TÜRKSAT sistemi üzerinde oluşturulacak WAN yapısı üzerinden sağlanacaktır. Bunun dışında mobil sistemlerden (Uydu telefonları, GSM,3G HF/SSB telsizleri, UHF ve UHF) de yararlanılacak, Merkezler arasında ses iletişimi için mevcut TT telefon şebekesi, telsiz sistemleri esas ortamların yedeği olarak kullanılacaktır. Sadece mobil sistemlerle merkez arasında HF/SSB telsiz sistemi kullanılacaktır. İnternet ise halkın kullanımı dışında gerektiğinde kullanılabilir bir ortam olacaktır.

Haberleşme/İletişim altyapısında kullanılacak Karasal Sistemler:

Karasal hatlar üzerinden sağlanan servislerin tamamının kullanılması amaçlanmakla beraber, maliyet, teknoloji, yaygın kullanım gibi temel nedenlerle bu safhada sistemde 2 adet temel ortam (TT ve TÜRKSAT) kullanılacak şekilde tasarlanmıştır. Diğer ortam imkanları (TAFICS, BOTAŞ, DDY, Enerji İletim hatları, Radyolinkler ve Özel sektör vb.) ve alternatif bağlantılar ilerideki safhalarda değerlendirilecektir.

Uydu Sistemine ilaveten, Bakanlık, kamu kurum ve kuruluşlarındaki acil durum merkezlerinin tamamı Ulusal Acil Durum Yönetim Merkezi'ne noktadan noktaya karasal hatlarla bağlı olacaktır.

Uydu Bağlantılarında ise; Ankara Merkez'e tesis edilecek bir HUB istasyonu ile yönetilecek bir sistem tesis edilecektir. Tüm iller Data, ses ve Video trafiğine bağlı olarak en az VSAT 512 Kbps hızı ile merkeze bağlantı sağlayacaktır. Esnek bant yönetim sistemi vasıtasıyla bant genişlikleri artırılıp – azaltılabilecektir. Mobil merkezlerle ulusal merkez arasında 1024 Kbps hızında bağlantı sağlanacaktır.

Haberleşme Sistemi Bileşenleri:

- (a) Ses haberleşme sistemleri
- (b) Veri haberleşme sistemleri
- (c) Video haberleşme sistemleri

Ses haberleşmesi acil durum yönetiminin en önemli haberleşme unsurlarında birisini oluşturmaktadır. Ses haberleşmesi,

- (a) TT telefon şebekesi,
- (b) GSM operatörleri,
- (c) VSAT ve mobil uydu telefonları
- (d) HF/SSB telsizleri
- (e) Mobil araç VHF/SSB telsizleri

Veri şebekesi haberleşme sistemiyle bütünleşik yapıya sahip olacak; ses, veri ve video iletişimi sağlayacaktır. Veri sistemi, TT ve VSAT ortamını kullanarak oluşturulan WAN üzerinde çalışacaktır. Sistemi oluşturan tüm elemanlar bu hizmetleri sağlayacak şekilde çok servisli bir yapıya sahip olacaklardır.

Veri Sistemi Topolojisi:

- (a) Acil durum ana merkez ađı
- (b) Ulusal Acil Durum Merkezi ađı
- (c) Bakanlık ve kuruluşların ađı
- (d) İl ađları
- (e) Yedek merkez
- (f) Çok Uluslu kuruluşlar

6.2. Ulusal Acil Durum Yönetimi Bilgi Sistemi

Bu bölümde, Ulusal Acil Durum Yönetimi Bilgi Sistemi (UADYBS)'in mimari yapısı, ve genel tasarım ilkelerini açıklanacaktır.

UADYBS, doğal ve insan kaynaklı her tür acil durumlar yönetimi gerektiren olaylara karşı can ve mal kaybını asgariye indirmek amacıyla, yönetim faaliyetlerinin gerçekleştirilebileceđi, bir sistemdir. Genel olarak kullanım ihtiyacı duyulan durumlar ise Deprem, yangın, sel, çığ gibi doğal afetler ile teknolojik/endüstriyel/kimyasal ve benzeri kazaları destekleyecek ancak sayılanlar ile sınırlı olmayacaktır.

UADYBS, bir acil durumun her evresinde(hazırlık, arama ve kurtarma, iyileştirme, zararların azaltılma ve normale dönüş) kullanılabilir. UADYBS, acil durumlarda ihtiyaç duyulan kaynak bilgilerinin hızlı bir şekilde bulunması ve koordine edilmesi maksadıyla, kamu kurumu/kuruluşları ve sivil kuruluşlar gibi birçok farklı kurumun bilgilerini kullanabilecektir.

UADYBS sağlayacağı ana kabiliyetleri ise;

- Kaynak Yönetimi
- Durum Bildirimi
- Planlama ve Operasyon Yönetimi
- Karar Destek ve Yol Gösterim Kılavuzları
- Sistem Yönetimi
- Şehir Acil Durum Yönetimi
- Uluslararası Acil Durum Yönetimi
- UADYBS, hem WEB tabanlı hem de en son bir Java uygulaması olacaktır
- UADYBS, e-devlet kapısı ve e-dönüşüm kapsamındaki olası ilişkileri destekleyecektir.

Yazılım Geliştirme süreci döngüsü ise;

- Yazılım Gereksinimleri Yönetimi
- Yazılım Ön Tasarımı
- Yazılım Detay Tasarımı
- Yazılım Gerçekleştirimi (kodlanması) ve Birim Testler
- Yazılım Birim Entegrasyonu ve Testleri
- Yazılım Kabul Testleri
- Yazılım Kurulumu

7. SONUÇ VE ÖNERİLER

Rapor kapsamında ele alınan konular, senaryolar ve örneklemelerden de görüldüğü gibi "BT Risk Yönetimi" çağdaş kurum/kuruluşlar için temel becerilerinden birisi haline gelmektedir. Maruz kaldıkları riskleri değerlendiremeyen, ölçemeyen veya diğer bir deyişle iyi yönetemeyen kurum/kuruluşlar ile iyi risk yönetimi yapabilenler arasında karşılaşacakları sonuçlar açısından (kazanç-kayıp) keskin ayrımlar olacaktır. **Teknolojik ilerleme ve küreselleşme olgularının yanısıra böyle bir ortamda varlığını sürdürebilme, hizmet kalitesinden ödün vermeden güvenliği ve sürekliliği sağlayabilmek için bu konulara ciddi yatırımlar yapılması ve kurum/kuruluş yönetimlerinden en alt çalışana kadar bu konuya sahip çıkılması zorunlu hale gelmektedir.**

Örneğin, Ülkemizde son yıllarda yaşanan finansal krizler, ekonominin tümünü etkilemiş, en olumsuz etkiye bankacılık sektörü maruz kalmıştır. Uluslararası boyuttaki gelişmeler de aynı zaman dilimlerinde ortaya çıkmış; küreselleşmenin boyutlanması ve teknolojiye olan bağımlılığın giderek artması uluslararası finans kesiminin de temel gündemini oluşturmuştur. Bu gelişmeler sonucunda bankacılıktaki risk yönetimi gittikçe önemli hale gelmiştir.

Ülkemizdeki risk yönetimi düzenlemeleri iç denetim, iç kontrol ve risk yönetimi fonksiyonlarının bağımsız olarak yapılandırılmasını öngörmektedir. Bu çalışma kapsamında yapılan anket çalışmasına göre Risk yönetimi fonksiyonunun nasıl bir organizasyonel yapıda icra edildiğine ilişkin olarak kamuda (ANKET SONUCUNA GÖRE YAZILACAK).....olduğu gözlenmektedir.

Bankalarda risk yönetimi fonksiyonunu icra etmekte olan birimlerin temel görevleri risklerin tespit edilmesi, ölçülmesi, yönetilmesi ve raporlanması şeklinde gözlenmektedir. Türkiye Bankalar Birliği bünyesinde kurulmuş olan bir çalışma grubunun raporunda belirtildiği üzere (Kaynak- "Bankaların Risk Yönetimi Çalışmaları Hakkında Değerlendirme, Nisan 2004 TBB-RYÇG); "risklerin raporlanma süreci, risk yönetimini icra etmekte olan birimlerin üst düzey yönetimlerine yaptıkları dahili raporlamalar ve Bankacılık Düzenleme ve Denetleme Kurumu'na (BDDK) yapılan yasal raporlamalar şeklinde gerçekleştirilmektedir" denilmektedir. Benzer yaklaşımın kamu kurum ve kuruluşları içinde yapılması ve gerekli yasal düzenleme çerçevesinde bir kurumun sorumluluğunda denetlenmesi uygun bir yaklaşım olacaktır.

Yukarıda belirtilen raporda ayrıca, "Risklerin belirlenmesi ve ölçülmesi kapsamında gerçekleştirilen modelleme çalışmaları BDDK ve uluslararası düzenlemelere koşut olarak yürütülmektedir. Bank for International Settlements (BIS) nezdindeki Basel Komitesi tarafından yayımlanan yeni sermaye düzenlemelerinin (Basel-II) 2007 yılında yürürlüğe girmesi beklenmektedir. Basel II'nin Türk bankacılık sistemine olası etkilerinin saptanması amacıyla bankaların büyük çoğunluğunun katılımı ile yapılan Sayısal Etki Çalışmasının (QIR-TR) sonuçları ışığında; Türk Bankalarının, Basel II'ye uyum çerçevesinde başlatmış oldukları risklerin daha duyarlı hesaplanmasına yönelik faaliyetler devam etmektedir" denilmektedir. Benzer yaklaşımın, özellikle AB mevzuatları çerçevesinde tüm kamu kurum ve kuruluşları açısından da ele alınması gerekebilecektir.

Kurumlarda iyi yönetim ortamının kurulması, etkili bir risk yönetimi örgütlenmesi ve etkin iletişim, şeffaflık ve hesap verilebilirliğin sağlandığı yapının oluşturulması ile sağlanabilecektir. Gerek teknik altyapısı, gerekse de örgütsel bağımsızlığı anlamında risk yönetimi sistemine kurumsal anlamda gereken önemin ve desteğin verilmesi, iyi yönetişimin sağlanması bakımından risk yönetimi fonksiyonunun payına düşen bir gereklilik olarak görülmektedir. Etkili risk yönetiminin sağlanabilmesi için gelişmiş risk ölçme ve raporlama tekniklerinin kullanılması, risk ölçüm ve değerlendirmelerinin kurumların karar süreçlerinde dikkate alınması gereklidir.

BT risk yönetimi (operasyonel risk kapsamında) konusundaki metodolojik ve teknik standartların ve sınırların daha net ortaya konulması ve kapsamlı bir çalışma alanının belirlenmesi gerekmektedir. Kurumların faaliyetlerine özgü operasyonel risk noktalarını mümkün olan en geniş çerçevede tanımlamış olmaları zorunlu hale gelmektedir. Kurumların faaliyetlerini her koşulda devam ettirmek için "İş sürekliliği Planına (Business Continuity Plan) sahip olmaları ve bu planlarının uygulanabilir olması gereklidir.

Bu kapsamda Bilgi güvenliği Politikalarının varlığı da önem kazanmakta, bilgi işlem suçlarının

ve bilgi güvenliđi açıklarından kaynaklanan zararların yaygınlaşması nedeniyle, kurumların çalışanlarını eğitici ve uyarıcı nitelik taşıyan yazılı bilgi güvenliđi politikalarına sahip olmaları ve bu politikalarının uygulanmasını sağlamaları büyük önem taşımaktadır.

Bu çalışma kapsamında gerçekleştirilen anket çalışması mevcut duruma ilişkin kesin bilgi vermemesine rağmen bir takım konuların saptanmasında ve farkındalık yaratılması açısından oldukça yararlı olmuştur.

EK A- STANDART UYGULAMALAR VE YÖNTEMLER

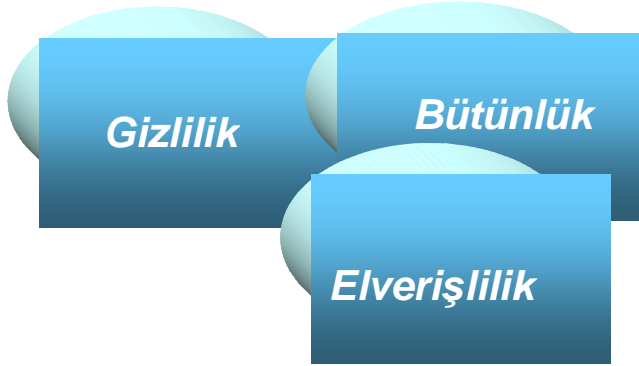
1. BS7799 / ISO17799 / TS 17799 Güvenlik Standartı

ISO 17799, bilgi güvenliği yönetimi için uygulama prensiplerinin ortaya konulduğu dünyada kabul görmüş bir standarttır. ISO 17799 standardı bir kurumda bulunması gereken güvenlik önlemlerine yer vererek temel bir güvenlik çerçevesi çizer.

ISO 17799 standardının temeli BS 7799 standardına dayanmaktadır. BS 7799 bir İngiliz standardıdır. İlk olarak 1995 senesinde yayınlanmıştır. 1999 senesinde günün ihtiyaçlarına göre büyük ölçüde değişikliğe uğramıştır. BS 7799 standardı 2000 senesinde ISO standardı olarak yayınlanmış ve tüm dünyada ISO 17799 olarak kabul görmüştür.

2002 senesinde çıkartılan BS 7799-2 (Bölüm 2) standardı ile ortaya konan kullanım kılavuzu ile kurumların ISO 17799 sertifikasyonu alması hedeflenmiştir. TSE, ISO 17799'u 2002 senesinde BS 7799-2'yi ise Şubat 2005'te Türkçe olarak yayınlamıştır.

BS7799 standartı kurumlar bünyesinde bilgi güvenliği yönetimi sürecini başlatan, gerçekleştiren ve sürekliliğini sağlayan kişilerin kullanımı için, bilgi güvenliği yönetimi ile ilgili tavsiyeleri kapsar. Bu bağlamda aşağıda belirtilen üç temel prensip çok önemlidir.



- **Gizlilik:** Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunun garanti edilmesi.
- **Bütünlük:** Bilginin ve işleme yöntemlerinin doğruluğunun ve bütünlüğünün temin edilmesi.
- **Elverişlilik:** Yetkilendirilmiş kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara erişime sahip olabileceklerinin garanti edilmesi.

BS7799'u Edinmek

İlk basamak standartın kendisinin bir kopyasını edinmektir. BS7799 tek olarak satın alınabilmekte, ya da ISO17799 ve ISO27001 içeren bir giriş seviyesi kit'in parçası olarak gelmektedir. Bu kit uygulama metodları, yön haritaları, prezentasyon ve pek çok diğer dokümanı içermektedir.

BS7799'a Uyumluluk Sağlamak

BS7799'a uyumluluğu elde edebilmek çok önemli bir iştir. Bilgi sistemleri için uyumluluk seviyelerini tespit etmek, tam uyumlu olmak için gerekli planları oluşturmak ve uygulamak gerçekten çok yoğun ve kapsamlı bir çalışma gerektirmektedir. Buna rağmen, doğru bir yaklaşım ve metotla daha az çabayla gerçekleştirilebilmektedir.

BS 7799-3

“BS7799-3:2005 Bilgi Güvenliđi Yönetim Sistemleri. Bilgi Güvenliđi Risk Yönetimi için Rehber” i ISO27001'deki BGYS (Bilgi Güvenliđi Yönetim Sistemi) risk yönetim döngüsündeki tüm alanlarla ilgili gereksinimleri desteklemek üzere bir kılavuz sağlamayı amaçlamaktadır. BS7799-2 (ISO 27001) standardının uygulanması için destek sağlamakta ve küçük, orta ve büyük kurumlarda kullanılması hedeflenmektedir.

İçeriğinde şunlar bulunmaktadır:

1. Faaliyet Alanı
2. Kurala uygun referanslar
3. Terim ve tanımlar
4. Kurumlardaki bilgi yönetimi riskleri
5. Risk saptaması
6. Risk değerlendirmesi ve yönetim kararının verilmesi
7. Devamlı risk yönetimi aktiviteleri

TS 17799-2 BİLGİ GÜVENLİĐİ YÖNETİM SİSTEMİ (BGYS)

Uluslararası uygulanmakta olan BS7799 / ISO17799 standardı Türkiye'de TS 17799-2 standardı olarak 17.2.2005 tarihinde kabul edilip yürürlüğe girmiştir. Standardın Türkçe adı : “Bilgi güvenliđi yönetim sistemleri – Özellikler ve kullanım kılavuzu” 'dur. Bu standart, belgelenmiş bir BGYS'ni kuruluşun tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, bakımını yapmak ve iyileştirmek için gereksinimleri kapsamaktadır.

TS 17799-2' yi Edinmek

Kuruluşlar TSE Kalite Müdürlüklerine doğrudan, yazı, telefon ve ya faks ile TS 17799-2 Standard edinmek için başvurabilmektedirler. Başvurularında aşağıda belirtilen müracaat formlarının doldurulması, kuruluş yetkilileri tarafından imzalanması ve müracaat aşamasında TSE Kalite Müdürlüklerinden birine talimatlarda belirtilen belgelerle birlikte teslim edilmesi gerekmektedir. Belgelendirme öncesinde talep eden kuruluşlara, TSE Kalite Müdürlükleri tarafından BGYS ile ilgili ön tetkik hizmeti de verilebilmektedir.

Müracaat ile ilgili dokümanlar;

- TSE BGYS Kuruluş Bilgi Formu
- TSE BGYS Müracaat Formu
- TSE Sistem Belgelendirme Talimatı
- TSE Sistem Belgelendirme Ücret Talimatı
- TSE Sistem Belgelendirme Ücret Çizelgesi
- Logo Kullanma Talimatı
- Müşteri Şikayet ve Önerilerinin Deđerlendirilmesi Talimatı
- Müracaatta Gerekli Belgeler Listesi

2. Sarbanes Oxley

Sarbanes-Oxley Yasası, 30 Temmuz 2002'de yürürlüğe girmiş olan, Özel Şirketler Muhasebe Yeniden Düzenlemesi ve Yatırımcının Korunması Yasası olarak da bilinen (genel olarak SOX ya da SarbOX diye adlandırılan) bir ABD federal yasasıdır.

Yasanın içeriğinde Özel Şirket Muhasebe Gözetim Kurulu'nun kurulması, denetçinin bağımsızlığı, şirkete ait sorumluluk ve gelişmiş finansal açıklamalar gibi konular yer almaktadır. Sarbanes Oxley, kanuni denetim gereksinimlerini incelemek üzere planlanmış bir yasa olup 1930lardan beri Amerika güvenlik yasalarında yapılan en büyük deđişiklik olarak görülmektedir. Bu yasa SEC diye bilinen Amerika Menkul Kıymetler ve Borsa Kurulu'na ilave

yetkiler ve sorumluluklar vermektedir.

Yasa, aralarında Enron, Tyco International, Worldcom (MCI) gibi firmalarında etkilendiği bir seri finansal skandalın patlak vermesiyle birlikte doğmuştur. Senatör Paul Sarbanes ve Vekil Michael G. Oxley'nin adlarından oluşmaktadır.

Hükümler

Sarbanes-Oxley Yasasının başlıca hükümleri aşağıda belirtilmektedir.

- Finansal raporların Genel Müdür ve Finans Müdürü tarafından tasdik edilmesi
- Tüm Yönetici ve Müdürlere kişisel kredinin yasaklanması
- İçeriden alınan bilgilerle hisse senedi alışverişinde bulunanların hızlandırılmış raporlanması
- Emeklilik fonlarını karartma zamanlarında içeriden alınan bilgilerle hisse senedi alışverişinde bulunmanın yasaklanması
- Genel Müdür ve Finans Müdürü'nün tazminat ve karlarının halka açıklanması
- İlave açıklamalar yapılması
- Denetim bağımsızlığı; bazı tür işlerden tamamen men edilmesi ve denetime tabii olmayan tüm işlerin Denetim Komitesi tarafından önceden tasdiklenmesi
- Menkul Kıymetler Yasasının çiğnenmesi için kriminal ve medeni cezalar verilmesi
- Bilerek ve isteyerek finansal tablolarını farklı gösteren şirket yöneticileri için çok daha uzun hapis cezaları ve büyük tazminat bedelleri uygulanması
- Müşterilerine hukuksal ve ya danışmanlık gibi denetim işleriyle ilgisi olmayan ekstra 'katma değerli' hizmetler sunan denetim firmalarının yasaklanması
- Halka açık firmaların finansal raporlama ile ilgili iç denetimlerinin varlığı ve durumuyla ilgili yıllık bağımsız raporlar vermeleri gereksinimi

PCAOB (Özel Şirketler Muhasebe Gözetim Kurulu) 'nun Gereksinimleri

- Finansal tablolardaki belli başlı hesaplar ve açıklamalarla ilgili uygun teyitlerin kontrolünün planlanması
- Belli başlı hareketlerin nasıl başladığı, yetkilendirildiği, desteklendiği, yürütüldüğü ve raporlandığı hakkında bilgi
- Yanlışlık ya da kasıtlı olarak oluşmuş yanlış beyanların yerlerinin saptanması için hareketlerin akışıyla ilgili yeterli bilgi
- Sahtekarlığı önlemek ve saptamak için gerekli kontrollerin oluşturulması (kontrollerin kimin tarafından yapıldığı ve düzenlenmiş görev ayrımlarını da içeren)
- Dönem-sonu finansal raporlama işlevinin kontrolü
- Mal varlıklarının korunmasının kontrolü
- Yönetimin testlerinin ve değerlendirmesinin sonuçları

BT Kontrolleri, BT Denetimi ve SOX

Bugünün iş çevresinde, kurumlarının çoğunun finansal raporlama süreçleri bilgi teknolojileri sistemlerinden alınmaktadır. Sadece az miktarda kurum verilerini elle yönetmektedir. Kurumların pekçoğu verinin, dokümanların ve anahtar operasyonel süreçlerin elektronik yönetimine geçmiştir. Bundan dolayı, iç denetimde bilgi teknolojilerinin hayati bir rol oynadığı görülmektedir. PCAOB şöyle demektedir:

„Bir kurumun bilgi sistemleri içinde bilgi teknolojilerini kullanma şekli, içeriği ve özellikleri kurumun finansal raporlama üzerindeki iç kontrolünü etkilemektedir.“

Finansal verilerin yönetildiği ve raporlandığı sistemlerin güvenliği, doğruluğu ve güvenilirliğinden Bilgi Teknolojileri Yöneticileri sorumludur. ERP (Kurumsal Kaynak Yönetimi) gibi sistemler finansal verilerin oluşturulması, yetkilendirilmesi, işletilmesi ve raporlamasıyla derinden entegre edilmiştir. Öyleki, bunlar genel finansal raporlama sürecine ayrılmaz bir şekilde bağlanmıştır ve Sarbanes Oxley Yasasına uyumluluk için diğer önemli süreçlerle birlikte değerlendirilmesi gerekmektedir. Dolayısıyla, Yasanın operasyonel işlerde ve finansal raporlamada çok önemli bir değişikliğe işaret etmesine, ve kurumsal finansal raporlamada sorumluluğu genel müdür (CEO), ve finans müdürü (CFO) ne vermesine rağmen, finansal raporların onaylanmasında bilgi teknolojileri yöneticisi (CIO) önemli bir rol oynamaktadır.

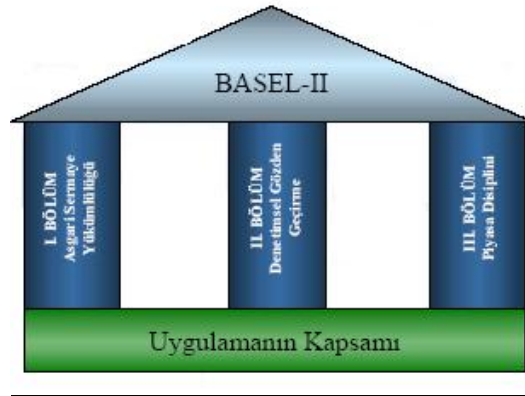
3. Basel II

Basel Sermaye Uyumu adı verilen Basel II, ikinci Basel Anlaşmasıdır ve bankanın sermayesinin kifayetini ölçen uluslararası standartları gözden geçirmek için Bankacılık Denetimi üzerine kurulan 13 ülkeden merkez bankacıların oluşturduğu Basel Komitesi temsil etmektedir. Basel II Basel II, operasyonel risklerin tanımlanması, değerlendirilmesi ve ölçülmesi için geliştirilmiş bir kurallar bütünüdür. Basel II, bankaların ve bankacılık düzenleyicilerinin ulusal sınırlar arasında risk yönetimine yaklaşım yöntemlerindeki tutarlılığı yükseltmek için yaratılmıştır. Yüksek standartlara sahip olan Basel II'ye uyum sağlamak için bankaların pek çok gerekliliği yerine getirmesi gerekmektedir.

Uygulamadaki Anlaşma

Basel II "üç yapısal blok" ("three pillars") kavramını kullanmaktadır - (1) asgari sermaye yükümlülüğü; (2) denetimsel gözden geçirme ; and (3) piyasa disiplini - finansal sistemdeki istikrarı daha da yükseltmek için.

Basel I bu üç yapısal bloğun sadece bazı parçalarıyla ilgilenmiştir. Örneğin: Birinci yapısal blokta riskler ve kredi riskleri basit bir şekilde irdelenmiş, pazar riski sonradan düşünülmüş, operasyonel risk ise hiç irdelenmemiştir.



Birinci Yapısal Blok

Birinci yapısal blok sermaye yükümlülüklerinin bir bankanın karşılaştığı riskin üç parçası ile hesaplandığı şekilde iyileştirilmiş risk hassasiyeti sunmaktadır. Bu parçalar : kredi riski, operasyonel risk ve piyasa riskidir. Sırasıyla, bu parçalardan herbiri iki veya üç değişen karmaşıklik içinde hesaplanmaktadır. Bu aşamada, diğer risklerin tamamen rakamlarla belirtilebilir olduğu düşünülmektedir.

Kredi riskinin daha teferruatlı hesaplanmasında kullanılan teknik terimler EL (Beklenen Kayıp) ile bunun parçaları olan PD (Temerrüt Olasılığı), LGD (Temerrüt Halinde Kayıp) ve EAD (Temerrüt Halinde Kredi Tutarı) 'ni içermektedir. Bu parçaların hesaplanması, ileri düzeyde veri toplama ve teferruatlı risk yönetimi teknikleri gerektirmektedir.

İkinci Yapısal Blok

İkinci yapısal blok Basel I 'de yer alan araçlardan çok daha gelişmiş araçları denetim otoritesine vererek birinci yapısal bloğa düzenleyici cevabı irdelemektedir. Aynı zamanda bu blok bir bankanın karşılaştığı isim riski, likidite riski ve yasal riskler gibi diğer risklerle ilgilenmek için bir çerçeve sağlamaktadır. İkinci yapısal bloğun temel prensipleri; bankaların kendi risk profillerini ve sermaye yeterliliklerini değerlendirmeleri, denetim otoritesinin bankanın risk profilini ve sermaye yeterliliğini değerlendirmesi, bankaların asgari yasal sermayenin üzerinde sermaye ile çalışmalarının sağlanması ve sermayenin asgari sermayenin altına düşmesi riskine karşı gerekli düzeltici tedbirlerin erkenden alınmasıdır.

Üçüncü Yapısal Blok

Üçüncü yapısal blok bankanın yapması gereken açıklamaları (kamuyu bilgilendirme, kamuya açıklama) daha da fazla arttırmaktadır. Bu yapısal blok bankanın genel risk durumunun piyasa tarafından daha iyi görülmesini sağlamaktadır. Birinci yapısal blokta yer alan asgari sermaye yükümlülüklerini ve ikinci yapısal blokta yer alan gözden geçirme sürecini tamamlamak üzere piyasanın banka ile ilgili temel ve önemli bilgilere erişebilmesini sağlayacak bir kamuyu bilgilendirme sürecini oluşturarak piyasa disiplini teşvik etmektedir.

Üçüncü yapısal blok ile bankalar ve finansal kurumların sürekli bazda değişen ve güncellenen detaylı finansal ve ilintili diğer bilgilerin muhtelif formlar vasıtasıyla kamuya açıklanması yoluyla mudilerin, yatırımcıların ve ilgili diğer kişilerin finansal kararlarını belirlemeleri ve sözkonusu kurum ve kuruluşların risklerini sağlıklı bir şekilde değerlendirmeleri amaçlanmaktadır.

4. COBIT

Control Objectives for Information and related Technology (COBIT) 'in Türkçe açılımı Bilgi ve ilgili Teknolojiler için Kontrol Hedefleri'dir. COBIT ISACA ([Information Systems Audit and Control Association](#)) ve ITGI ([IT Governance Institute](#)) tarafından yaratılmış BT bilgi yönetimi riskleri için bir çerçevedir. COBIT BT yöneticileri, denetçiler ve BT kullanıcıları için bir kurumda bilgi teknolojileri kullanımının ve uygun BT yönetişiminin geliştirilmesi ve kontrol edilmesinin faydalarını artırmak için genel olarak kabul edilmiş bilgi teknolojileri kontrol hedef setleri sunmaktadır. Üçüncü basımında COBIT 'te dört alanda sınıflandırılan 318 kontrol hedefini içeren 34 yüksel seviye hedefler bulunmaktadır. Bu dört alan: Planlama ve Organizasyon, İktisap ve Uygulama, Teslim ve Destek, Gözlem ve Değerlendirme.

Altı adet temel esası kapsamaktadır : yönetim klavuzu, kontrol hedefleri, COBIT çerçevesi, yönetim özeti, denetim klavuzu ve uygulama araçları. Hepsi ayrı ciltlerde doküman edilmiştir.

COBIT, IT Governance Institute ve Information Systems Audit and Control Foundation tarafından bilgi teknolojileri ile ilgili kontrol hedefleri ilk belirlendiğinde 1992 yılında geliştirilmiştir. İlk basımı 1996'da, ikincisi 1998'de, üçüncüsü 2000'de yayınlanmış ve 2003'de çevrimiçi olarak yayınlanmıştır. Enron Skandalı ve Sarbanes Oxley 'e geçiş gibi dış gelişmelerle önemi artmıştır. 2005 Aralık'da Cobit Versiyon 4.0 yayımlanmıştır.

COBIT'in misyonu "yöneticiler ve denetçiler için günlük kullanabilecekleri genel olarak kabul edilmiş bilgi teknolojileri kontrol hedeflerinden oluşan geçerli, güncel ve uluslararası bir set araştırmak, geliştirmek, tanıtmak ve teşvik etmektir." COBIT'in geliştirilmesinden yöneticiler, denetçiler ve kullanıcılar faydalanmaktadır çünkü COBIT bir BT yönetim modeli geliştirilmesiyle birlikte onların bilgi teknolojileri sistemlerini daha iyi anlamalarını ve kurumdaki bilgi teknolojileri varlıklarını korumak için gerekli güvenlik seviyesi ve kontrole karar vermelerini sağlamaktadır.

COBIT Yapısı

COBIT yöneticilere, BT kullanıcılarına ve denetçilere faydalar sağlamaktadır. Yöneticiler COBIT'ten faydalanmaktadır çünkü COBIT onlara bilgi teknolojileriyle ilgili kararlarını ve yatırımlarını dayandırabilecekleri bir temel sunmaktadır. Karar alma çok daha etkin bir şekilde

yapılabilmektedir çünkü COBIT yönetime stratejik bir BT planı tanımlama, bilgi mimarisini tanımlama, BT stratejisini uygulamak için gerekli BT donanım ve yazılımını satın alma, hizmet sürekliliğini temin etme ve BT sisteminin performansını kontrol etmek için yardım etmektedir. Bilgi teknolojileri kullanıcıları COBIT'ten faydalanmaktadır çünkü bilgiyi toplamaya, işlemeye ve raporlamaya yardım eden uygulamaların COBIT'e uygun olması, onlara iş süreçlerinin kontrolünün ve güvenliğinin sağlandığına ilişkin güvence vermektedir. COBIT denetçiler için de faydalıdır çünkü kurumun bilgi teknolojileri altyapısındaki BT kontrol sorunlarını belirlemek için yardımcı olmaktadır. COBIT onlara denetim bulgularını doğrulamada da yardımcı olmaktadır.

COBIT dört alandan oluşmaktadır:

- Planlama ve Organizasyon
- İktisap ve Uygulama
- Teslim ve Destek
- Gözlem ve Değerlendirme

Planlama ve Organizasyon

Planlama ve Organizasyon alanı teknoloji kullanımını ve kurumun amaç ve hedeflerini gerçekleştirmeye yardımcı olmak için nasıl en iyi şekilde kullanılabileceğini kapsamaktadır. Bu alan en uygun sonucu elde etmek ve bilgi teknolojileri kullanımından en iyi şekilde faydalanmak için bilgi teknolojilerinin alması gereken organizasyonel ve altyapısal şekli ortaya çıkartmaktadır. Planlama ve Organizasyon alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır:

PO1 Stratejik bir BT Planı Tanımlama
PO1.1 IT Değer Yönetimi
PO1.2 İş ve BT Arasındaki Uyumun Sağlanması
PO1.3 Mevcut Performansın Değerlendirilmesi
PO1.4 BT Stratejik Planı
PO1.5 BT Taktik Planları
PO1.6 BT Portföy Yönetimi
PO2 Bilgi Mimarisini Tanımlama
PO2.1 İşletme Bilgisi Mimarisi Modeli
PO2.2 İşletme Veri Sözlüğü ve Veri Sentaks Kuralları
PO2.3 Veri Sınıflandırma Şeması
PO2.4 Bütünlük Yönetimi
PO3 Teknolojik Yönü Belirleme
PO3.1 Teknolojik Yönün Planlanması

PO3.2 Teknolojik Altyapı Planı
PO3.3 Gelecekteki Eğilimler ve Yönetmenliklerin Takibi
PO3.4 Teknoloji Standartları
PO3.5 BT Mimarisi Kurulu
PO4 BT Prosesleri, Organizasyon ve İlişkilerini Tanımlama
PO4.1 BT Proses Çerçevesi
PO4.2 BT Stratejisi Komitesi
PO4.3 BT Yönetim Komitesi
PO4.4 BT İşlevinin Organizasyon içinde Yerleştirilmesi
PO4.5 BT Organizasyon Yapısı
PO4.6 Rol ve Sorumluluklar
PO4.7 BT Kalite Güvencesi Sorumluluğu
PO4.8 Risk, Güvenlik ve Uyum Sorumluluğu
PO4.9 Veri ve Sistem Mülkiyeti
PO4.10 Denetleme
PO4.11 Sorumlulukların Ayrıştırılması
PO4.12 BT Personel Alımı
PO4.13 Ana BT Personeli
PO4.14 Sözleşmeli Personel Politika ve Prosedürleri
PO5 BT Yatırımını Yönetme
PO5.1 Mali Yönetim Çerçevesi
PO5.2 BT Bütçesi içinde Önceliklerin Tanınması
PO5.3 BT Bütçe Oluşturma Prosesi
PO5.4 Maliyet Yönetimi
PO5.5 Fayda Yönetimi
PO6 Yönetim Hedefleri ve Yönünü Bildirme

PO6.1 BT Politikası ve Kontrol Ortamı
PO6.2 İşletme BT Riski ve İç Kontrol Çerçevesi
PO6.3 BT Politikalarının Yönetimi
PO6.4 Politikanın Yaygınlaştırılması
PO6.5 BT Amaçlarının Bildirilmesi ve Yönlendirme
PO7 BT İnsan Kaynaklarını Yönetme
PO7.1 Personel Alımı ve İstihdam
PO7.2 Personel Yetkinlikleri
PO7.3 Roller için Personel Alımı
PO7.4 Personel Eğitimi
PO7.5 Bireylere Bağlılık
PO7.6 Personel Onay Prosedürleri
PO7.7 Çalışanın İş Performansı Bakımından Değerlendirilmesi
PO7.8 İş Değişikliği ve İşe Son Verilmesi
PO8 Kaliteyi Yönetme
PO8.1 Kalite Yönetim Sistemi
PO8.2 BT Standartları ve Kalite Uygulamaları
PO8.3 Geliştirme ve İktisap Standartları
PO8.4 Müşteri Odağı
PO8.5 Sürekli İyileştirme
PO8.6 Kalite Ölçümü, Takip ve Gözden Geçirme
PO9 BT Risklerini Değerlendirerek Yönetme
PO9.1 BT ve İş Riski Yönetiminin Uyumlaştırılması
PO9.2 Risk Bağlamının Tespiti
PO9.3 Olay Tanımlama
PO9.4 Risk Değerlendirme
PO9.5 Risk Yanıtı
PO9.6 Risk Faaliyet Planının Sürdürülmesi ve Takibi

PO10 Projeleri Yönetme
PO10.1 Program Yönetim Çerçevesi
PO10.2 Proje Yönetim Çerçevesi
PO10.3 Proje Yönetim Yaklaşımı
PO10.4 Paydaş Bağlılığı
PO10.5 Proje Kapsam Beyanı
PO10.6 Proje Aşamasının Başlatılması
PO10.7 Entegre Proje Planı
PO10.8 Proje Kaynakları
PO10.9 Proje Risk Yönetimi
PO10.10 Proje Kalite Planı
PO10.11 Proje Değişiklik Kontrolü
PO10.12 Güvence Yöntemlerinin Proje Planlaması
PO10.13 Proje Performansının Ölçülmesi, Raporlanması ve Takibi
PO10.14 Proje Kapanışı

İktisap ve Uygulama

İktisap ve Uygulama alanı BT gereksinimlerini belirleme, teknolojiyi satınalma ve kurumun mevcut iş süreçlerine uyarlama için kurumun stratejilerini adreslemektedir. Bu alan aynı zamanda bilgi teknolojileri sisteminin ve parçalarının hayatını sürdürebilmesi için kurumun kabulleneceği bir bakım planı geliştirilmesini içermektedir. İktisap ve Uygulama alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır:

A11 Otomatize Edilmiş Çözümleri Tanımlama
A11.1 İşletmenin İşlevsel ve Teknik Şartlarının Tanımlanarak Sürdürülmesi
A11.2 Risk Analiz Raporu
A11.3 Fizibilite Araştırması ve Alternatif Faaliyet Yollarının Oluşturulması
A11.4 Şartlar ve Fizibilite Kararı ile Onayı
A12 Uygulama Yazılımını İktisap Ederek Bulundurma
A12.1 Üst Düzey Tasarım

AI2.2 Ayrıntılı Tasarım
AI2.3 Uygulama Kontrolü ve Denetlenebilirliği
AI2.4 Uygulama Güvenliği ve Kullanılabilirliği
AI2.5 İktisap Edilen Uygulama Yazılımının Konfigürasyon (Yapılandırma) ve Uygulanması
AI2.6 Mevcut Sistemler için Ana Upgrade'ler (Yükseltimler)
AI2.7 Uygulama Yazılımının Geliştirilmesi
AI2.8 Yazılım Kalite Güvencesi
AI2.9 Uygulama İhtiyaçlarının Yönetimi
AI2.10 Uygulama Yazılımının Sürdürülmesi
AI3 Teknoloji Altyapısını İktisap Ederek Sürdürme
AI3.1 Teknoloji Altyapısı İktisap Planı
AI3.2 Altyapı Kaynaklarının Korunması ve Kullanılabilirliği
AI3.3 Altyapının Bakımı (Sürdürülmesi)
AI3.4 Fizibilite Testi Ortamı
AI4 Çalışma ve Kullanımı Etkinleştirme
AI4.1 İşlemsel Çözümleri için Planlama
AI4.2 İşletme Yönetimine Bilgi Transferi
AI4.3 Son Kullanıcılara Bilgi Transferi
AI4.4 İşlemler ve Destek Personeline Bilgi Transferi
AI5 BT Kaynaklarını Elde Etme
AI5.1 İstihsal Kontrolü
AI5.2 Tedarikçi Sözleşmesinin Yönetimi
AI5.3 Tedarikçi Seçimi
AI5.4 Yazılım İktisabı
AI5.5 Geliştirme Kaynaklarının İktisabı
AI5.6 Altyapı, Tesis ve İlgili Hizmetlerin İktisabı

A16 Değişiklikleri Yönetme
A16.1 Standart ve Prosedürleri Değiştiriniz
A16.2 Etki Değerlendirmesi, Önceliklendirme ve Yetkilendirme
A16.3 Acil Durum Değişiklikleri
A16.4 Değişiklik Durumunun İzlenmesi ve Raporlanması
A16.5 Değişikliğin Kapanışı ve Belgelenmesi
A17 Çözüm ve Değişikliklerin Kurulması ve Akreditasyonu
A17.1 Eğitim
A17.2 Test Planı
A17.3 Uygulama Planı
A17.4 Test Ortamı
A17.5 Sistem ve Veri Dönüşümü
A17.6 Değişikliklerin Test Edilmesi
A17.7 Son Kabul Testi
A17.8 Üretim Promosyonu
A17.9 Yazılım Sürümü
A17.10 Sistem Dağıtımı
A17.11 Değişikliklerin Kaydı ve İzlenmesi

Teslim ve Destek

Teslim ve Destek alanı bilgi teknolojilerinin teslim yönüne odaklanmaktadır. Bu alan bilgi teknolojileri sistemindeki uygulamaların hayata geçirilmesi ve sonuçları ile bu BT sistemlerinin etkin ve elverişli uyarlanmasını sağlayan destek süreçlerini de kapsamaktadır. Bu destek süreçleri güvenlik konuları ve eğitimini içermektedir. Teslim ve Destek alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır:

DS1 Servis Düzeyi Yönetimi
DS1.1 Servis Düzeyi Yönetimi Çerçevesi
DS1.2 Hizmetlerin Tanımı
DS1.3 Hizmet Düzeyi Anlaşmaları

DS1.4 İşletim Düzeyi Anlaşmaları
DS1.5 Hizmet Düzeyi Başarılarının İzlenmesi ve Raporlanması
DS1.6 Hizmet Düzeyi Anlaşmaları ve Sözleşmelerinin Revizyonu
DS2 Üçüncü taraf Hizmetlerin Yönetilmesi
DS2.1 Tüm Tedarikçi İlişkilerinin Tanımlanması
DS2.2 Tedarikçi İlişkisi Yönetimi
DS2.3 Tedarikçi Risk Yönetimi
DS2.4 Tedarikçi Performans Gözlemi
DS3 Performans ve Kapasite Yönetimi
DS3.1 Performans ve Kapasite Planlama
DS3.2 Mevcut Kapasite ve Performans
DS3.3 Gelecekteki Kapasite ve Performans
DS3.4 IT Kaynakların Mevcudiyeti
DS3.5 Gözlem Ve Raporlama
DS4 Sürekli Hizmetin Sağlanması
DS4.1 IT Süreklilik Çerçevesi
DS4.2 IT Süreklilik Planları
DS4.3 Kritik IT Kaynakları
DS4.4 IT Süreklilik Planının Korunması
DS4.5 IT Süreklilik Planı Testi
DS4.6 IT Süreklilik Planı Eğitimi
DS4.7 IT Süreklilik Planı Dağıtımı
DS4.8 IT Hizmetlerinin Kurtarılması ve Yeniden Başlatılması
DS4.9 Alan Dışı Yedekleme Belleği
DS4.10 Yeniden başlatma sonrasında revizyon
DS5 Sistem Güvenliğinin Sağlanması

DS5.1 IT Güvenliđi Yönetimi
DS5.2 IT Güvenlik Planı
DS5.3 Kimlik Yönetimi
DS5.4 Kullanıcı Hesabı Yönetimi
DS5.5 Güvenlik Testi, Gözetim ve Gözlem
DS5.6 Güvenlik Olay Tanımı
DS5.7 Güvenlik Teknolojisinin Korunması
DS5.8 Kriptografik Anahtar Yönetimi
DS5.9 Zararlı Yazılım Korunması, Tespiti ve Düzeltilmesi
DS5.10 Ağ Güvenliđi
DS5.11 Hassas Verilerin Deđiřimi
DS6 Maliyetlerin Tanımlanması ve Dađıtımı
DS6.1 Hizmetlerin Tanımı
DS6.2 IT Muhasebesi
DS6.3 Maliyet Modelleri ve tarifeler
DS6.4 Maliyet Modeli Bakımı
DS7 Kullanıcıların Eđitimi ve Öđretimi
DS7.1 Eđitim ve Öđretim Gereksinimlerinin Tanımlanması
DS7.2 Eđitim ve Öđretimin Verilmesi
DS7.3 Alınan Eđitimin Deđerlendirilmesi
DS8 Hizmet Masası ve Olaylar Yönetimi
DS8.1 Hizmet Masası
DS8.2 Müřteri Anketlerinin Kaydı
DS8.3 Olay Yükseltilmesi
DS8.4 Olay Kapatma
DS8.5 Trend Analizi
DS9 Konfigürasyon Yönetimi

DS9.1 Konfigürasyon Havuzu ve Dayanak
DS9.2 Konfigürasyon Maddelerinin Tanımlanması ve Korunması
DS9.3 Konfigürasyon Entegrite Revizyonu
DS10 Sorun Yönetimi
DS10.1 Sorunların Tanımlanması ve Sınıflandırılması
DS10.2 Sorun İzleme Ve Çözüm
DS10.3 Sorun Kapatma
DS10.4 Değişiklik, Konfigürasyon ve Sorun Yönetimi Entegrasyonu
DS11 Veri Yönetimi
DS11.1 Veri Yönetimi için İşletme Gereklilikleri
DS11.2 Saklama ve Elde Tutma Düzenlemeleri
DS11.3 Medya Kütüphane Yönetimi Sistemi
DS11.4 Elden Çıkarma
DS11.5 Yedekleme ve Restorasyon
DS11.6 Veri Yönetimi için Güvenlik Gereklilikleri
DS12 Fiziksel Ortamların Yönetimi
DS12.1 Site Seçimi ve Planı
DS12.2 Fiziksel Güvenlik Önlemleri
DS12.3 Fiziksel Erişim
DS12.4 Çevresel Faktörlere Karşı Koruma
DS12.5 Fiziksel Tesis Yönetimi
DS13 Operasyonların Yönetimi
DS13.1 Operasyonlar Prosedürleri ve Talimatları
DS13.2 İş Cetvelleri
DS13.3 IT İç Yapı Gözlemi
DS13.4 Hassas Belgeler ve Çıktı Cihazları

DS13.5 Donanım için Koruyucu Bakım

Gözlem ve Değerlendirme

Gözlem ve Değerlendirme alanı kurumun ihtiyaçlarını, mevcut BT sisteminin hedefleri karşılayıp karşılamadığını ve yasal gereksinimlerle uyumluluk için gerekli kontrolü tayin etmek için kurumun stratejilerini irdedelemektedir. Gözlem ve Değerlendirme aynı zamanda bilgi teknolojileri sisteminin iş hedeflerini karşılamadaki etkinliği ile iç ve dış denetçilerce yapılan kurumun kontrol süreçlerinin bağımsız değerlendirmesi konularını kapsamaktadır. Gözlem ve Değerlendirme alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır :

ME1 IT Performansının Gözlemi ve Değerlendirmesi
ME1.1 Gözlem Yaklaşımı
ME1.2 Gözlem Verilerinin Tanımı ve Toplanması
ME1.3 Gözlem Metodu
ME1.4 Performans Değerlendirmesi
ME1.5 Yönetim Kadrosu ve Yönetici Raporlama
ME1.6 Çözüm Eylemleri
ME2 İç Kontrol Gözlemi ve Değerlendirmesi
ME2.1 İç Kontrol Çerçevesinin Gözlenmesi
ME2.2 Denetim Revizyonu
ME2.3 Kontrol İstisnaları
ME2.4 Kontrol Öz-değerlendirme
ME2.5 İç Kontrol Güvencesi
ME2.6 Üçüncü Taraflarda İç Kontrol
ME2.7 Çözüm Eylemleri
ME3 Yönetmeliklere Uyumluluğun Sağlanması
ME3.1 BT üzerinde Potansiyel Etkisi Olan Yasa ve Yönetmeliklerin Tanımlanması
ME3.2 Yönetmelik Koşullarının Karşılmasında Optimizasyonun Sağlanması
ME3.3 Yönetmelik Koşullarıyla Uyumluluğun Değerlendirilmesi
ME3.4 Uyumluluğun Olumlu Biçimde Sağlanması
ME3.5 Tümüleşik Raporlama

ME4 BT Yönetimi Sağlanması
ME4.1 BT Yönetimi Çerçevesinin Oluşturulması
ME4.2 Stratejik Uyum
ME4.3 Değer Yaratma
ME4.4 kaynak Yönetimi
ME4.5 Risk Yönetimi
ME4.6 Performans Ölçümü
ME4.7 Bağımsız Denetim/Güvence

EK B – RİSK SENARYOLARININ VE COBIT BT SÜREÇLERİNİN DETAYLI İNCELEMESİ

1. Uyarı ve Sınırlamalar

Bu kısım incelenen alanın en önemli süreçlerini belirlemek için kullanılan ve risk değerlendirmesi sonuçlarına dayanan yöntemi tanımlamaktadır. Bu kısmın amacı, ileride kullanılmak üzere bu süreçlerdeki ana kontrolleri belirlemek ve süreç olgunluk derecesini ölçerken (ve iyileştirirken) potansiyel olarak önceliklendirmektir.

Güvenilebilir sonuçların çıkması için her türlü önlem alınmış olmasına rağmen analizin sonuçları kullanılırken dikkatli olunmalıdır. Uygulanan yaklaşım genel bir yaklaşımdır ve sonuçlar verilen durumda ortama uygunluğu ve uygulanabilirliği açısından her zaman incelenmelidir. Bahsedildiği gibi bu analizin sonuçları kendi başına bir sonuç değil, sonraki ihtiyaçlar - potansiyel ana kontrolleri teşhis etme ve BT süreçlerini etkili kılarken önceliklendirmeyi sağlama - için bir araçtır.

2. İnkeler

CobiT modeli Risk Senaryoları (risk analizi projelerinde genel olarak kullanıldığı şekliyle), BT süreçleri ve ilgili kontrol hedefleri arasında doğrudan bir bağlantı sağlamaz. Bu nedenle aşağıdaki eşleştirme yapılmıştır.

Risk Senaryoları

IT Süreçleri

COBIT

Ref	Olay	Tanım / Etki
S01	Yetersiz sistem & ağ hacmi	Yetersiz sistem hacmi (hafıza, depo, işlemci gücü) program/batch hatalarıyla, yanlış işlem yapılmasıyla, performans sorunlarıyla veya veri bozulmalarıyla sonuçlanabilir. Ağ hacmi sorunları gerekli tüm işlem trafiğinin desteklenmesinde yetersizliğe yol açabilir.
S02	3. şahıs iflası & anlaşmazlığı	3. şahıslardaki istemsiz olaylar (örneğin elektrik sağlayıcı, iletişim sağlayıcı, servis sağlayıcı, vb.) işlemleri şiddetli bir biçimde etkileyebilir.
S03	Doğal Felaket	Doğal felaketler sonucu sistemin kullanım dışı kalması ve/veya servisin ulaşım dışı olması (örneğin deprem, sel, vb.)
S04	Şirket Kaynaklarının yanlış kullanımı	Paranın doğrudan kaybı (örneğin malların çalışanlar veya dışarıdan birileri tarafından zimmete geçirilmesi) veya şirket kaynaklarının uygunsuz amaçlar için yanlış kullanımı (BT, maddi)
S05	İnsan hatası	Teknisyen hatası yüzünden meydana gelebilecek herhangi bir olay (yanlış ayar, işlemsel hatalar, kazara yayma veya ortaya çıkarma...)

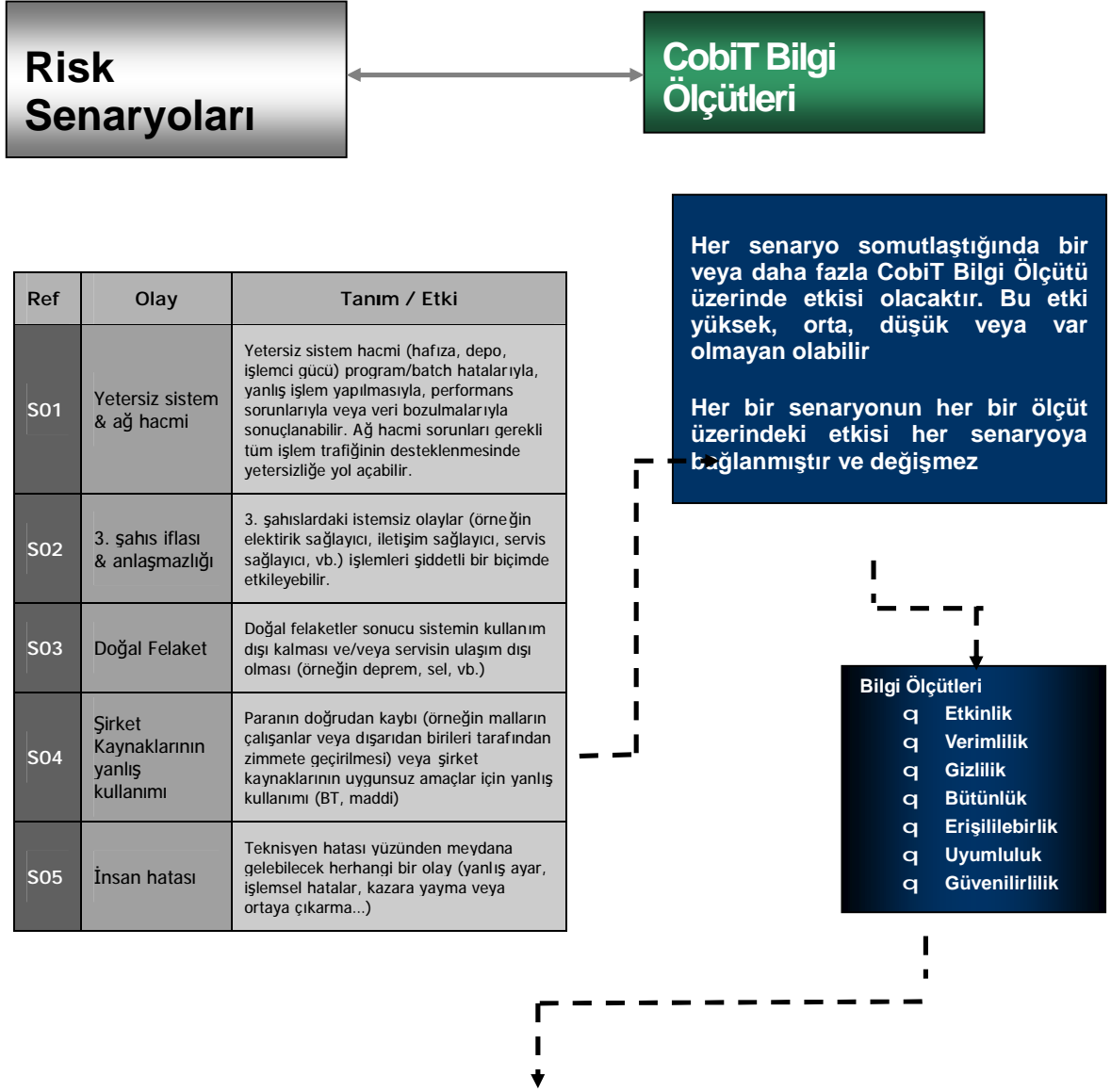


PO 1	Stratejik bir BT planı tanımlamak
PO 2	Bilgi mimarisini tanımlamak
PO 3	Teknolojik doğrultuyu belirlemek
PO 4	Organizasyonu ve ilişkileri belirlemek
PO 5	Yatırımları yönetmek
PO 6	Yönetim amaçlarını ve talimatlarını iletmek
PO 7	İnsan kaynaklarını yönetmek
PO 8	Harici gerekliliklere uyumu garanti etmek
PO 9	Riski değerlendirmek
PO 10	Projeleri yönetmek
PO 11	Kaliteyi yönetmek
AI 1	Otomatik hale getirilmiş çözümleri belirlemek
AI 2	Uygulama yazılımlarını edinmek ve bakımını sağlamak
AI 3	Teknoloji mimarisini edinmek ve bakımını sağlamak
AI 4	Prosedürler geliştirmek ve sürdürmek
AI 5	BT Kaynaklarını temin etmek

AI 6	Değişiklikleri yönetmek
DS 1	Servis düzeylerini belirlemek

A Kurumu için önemli BT süreçlerini belirlemek için izleyen yöntem tanımlanmış ve kullanılmıştır:

Öncelikle her bir risk senaryosu CobiT bilgi ölçütleri ile ilişkilendirilmiştir. Bunun sonucu olarak senaryo bilgi ölçütleri görünümü tanımlanmıştır.

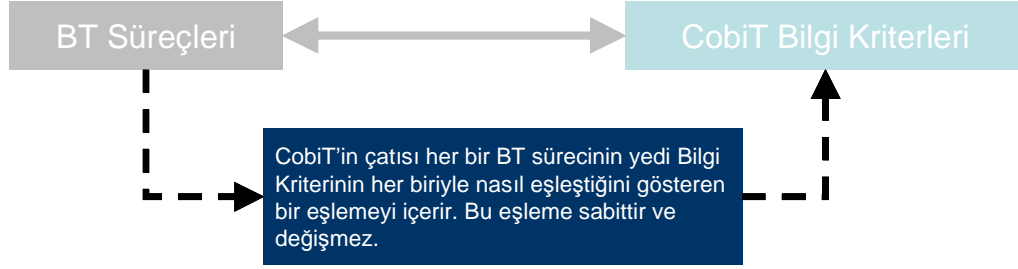


Ref	Olay	Tanım / Etki	Verimlilik	Etkinlik	Gizlilik	Bütünlük	Erişilebilirlik	Uyumluluk	Güvenilirlik
-----	------	--------------	------------	----------	----------	----------	-----------------	-----------	--------------

S01	Yetersiz sistem & ađ hacmi	Yetersiz sistem hacmi (hafıza, depo, işlemci gücü) program/batch hatalarıyla, yanlış işlem yapılmasıyla, performans sorunlarıyla veya veri bozulmalarıyla sonuçlanabilir. Ađ hacmi sorunları gerekli tüm işlem trafiğinin desteklenmesinde yetersizliğe yol açabilir.							
S02	3. şahıs iflası & anlaşmazlığı	3. şahıslardaki istemsiz olaylar (örneğin elektrik sağlayıcı, iletişim sağlayıcı, servis sağlayıcı, vb.) işlemleri şiddetli bir biçimde etkileyebilir.							
S03	Doğal Felaket	Doğal felaketler sonucu sistemin kullanım dışı kalması ve/veya servisin ulaşım dışı olması (örneğin deprem, sel, vb.)							
S04	Şirket Kaynaklarının yanlış kullanımı	Paranın doğrudan kaybı (örneğin malların çalışanlar veya dışarıdan birileri tarafından zimmete geçirilmesi) veya şirket kaynaklarının uygunsuz amaçlar için yanlış kullanımı (BT, maddi)							
S05	İnsan hatası	Teknisyen hatası yüzünden meydana gelebilecek herhangi bir olay (yanlış ayar, işlemsel hatalar, kazara yayma veya ortaya çıkarma...)							

Risk Senaryolarının Bilgi Ölçütleri ile Eşlemesi

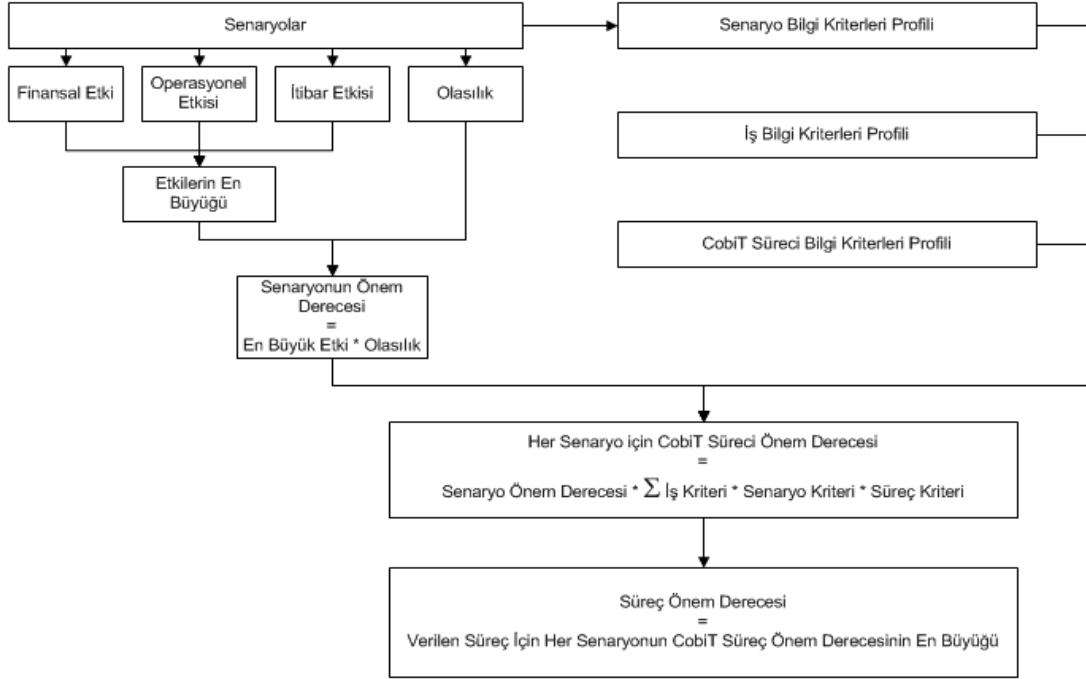
Bu aşamadan sonra CobiT bilgi ölçütleri ve BT süreçleri arasındaki 'standart' eşleme CobiT Çerçevesi'nde yer aldığı şekilde kullanılmıştır:



ALAN	SÜREÇ	Bilgi Kriterleri							BT Kaynakları					
		etkinlik	verimlilik	gizlilik	bütünlük	ulaşılabilirlik	uygunluk	güvenilirlik	insan	uygulamalar	teknoloji	olanaklar	veri	
Planlama & Organizasyon	PO 1	Stratejik bir BT planı tanımlamak	1	2						a	a	a	a	a
	PO 2	Bilgi mimarisini tanımlamak	1	2	1	1				a				a
	PO 3	Teknolojik doğrultuyu belirlemek	1	2							a	a		
	PO 4	Organizasyonu ve ilişkileri belirlemek	1	2						a				
	PO 5	Yatırımları yönetmek	2	2						a	a	a	a	
	PO 6	Yönetim amaçlarını ve talimatlarını iletmek		2					1					
	PO 7	İnsan kaynaklarını yönetmek	2	2						a				
	PO 8	Harici gerekliliklere uyumu garanti etmek		2					2	1				a
	PO 9	Riski değerlendirmek	1	2	2	2	2	1	1	a	a	a	a	a
	PO 10	Projeleri yönetmek	2	2						a	a	a	a	
	PO 11	Kaliteyi yönetmek	2	2		2				1	a	a	a	a
Edinim & Uygulama	AI 1	Otomatik hale getirilmiş çözümleri belirlemek	1	2						a	a	a		
	AI 2	Uygulama yazılımlarını edinmek ve bakımını sağlamak	2	2		1			1	1				
	AI 3	Teknoloji mimarisini edinmek ve bakımını sağlamak	2	2		1					a			
	AI 4	Prosedürler geliştirmek ve sürdürmek	2	2		1			1	1	a	a	a	a
	AI 5	Sistemler yüklemek ve uygunluğu		2		1	1				a	a	a	a
	AI 6	Değişiklikleri yönetmek	2	2		2	2			1	a	a	a	a
Servis & Destek	DS 1	Servis düzeylerini belirlemek	2	2	1	1	1	1	1	1	a	a	a	a

Bu aşamanın sonucunda bütün bileşenler birbiriyle ilişkilendirilmiş bulunmaktadır. Bakıldığında her risk senaryosu birkaç bilgi ölçütünü belli bir düzeye kadar etkilemektedir. Her CobiT BT süreci de bilgi ölçütlerini etkilemektedir. Bilgi ölçütleri yoluyla senaryolar ve CobiT BT süreçleri eşlendiğinde bir senaryonun bir BT süreci üzerindeki etkisi ya da tam tersi durum ölçülebilmektedir.

Model birbirleri ile bağlı hesaplama tabloları yolu ile uygulanmaktadır. Hesaplamaların sonucu, incelenen alanlar için, her BT sürecinin öneminin ortaya konduğu tablolarıdır. Bu önem aşağıdaki şekilde gösterildiği şekilde hesaplanmıştır:



Model üzerindeki son ayarlama A Kurumu iş birimleri ile ilgili yapılan görüşmeler sonucu elde edilen her bilgi ölçütü için (etkinlik, verimlilik, gizlilik, bütünlük, erişebilirlik, uygunluk ve güvenilirlik) 1-5 arasındaki ağırlığın modele tanıtılması gerçekleştirilerek yapılmıştır. Bu ayarlama sonucu Bilgi Ölçütü görünümü her servis alanı için A Kurumu iş süreçlerinin önceliklerine göre uyarlanmıştır.

3. Hesaplamalar

Yukarıda bahsedildiği gibi, senaryo bilgi ölçütleri görünümü her senaryo için tanımlanmıştır. Bu bilgi ölçütleri görünümü bir tehdit senaryosunun gerçekleşmesi halinde etkilenebilecek CobIT bilgi ölçütlerinin listesidir. Ele alınan tehdit senaryoları için her CobIT bilgi ölçütü bir ağırlıkla şu şekilde ilişkilendirilmiştir:

- 2 : bu senaryo bu bilgi ölçütü üzerinde önemli bir etkiye sahiptir
- 1 : bu senaryo orta derecede etkiye sahiptir
- 0 : bu senaryo ihmal edilebilir etkiye sahiptir.

CobIT Bilgi Ölçütleri ve CobIT BT Süreçleri (şu şekilde hesaplanmıştır: $P = 2$, $S = 1$, boş = 0), arasındaki standart ilişki ile bir araya getirildiğinde, belirli bir CobIT BT süreci üzerinde belirli bir senaryonun önem derecesini hesaplamak mümkündür:

- § Her bilgi ölçütü için iş bilgi ölçütleri görünümünden alınan puan, tehdit senaryosu bilgi ölçütleri görünümünün ağırlığı ve CobIT süreci bilgi ölçütleri görünümünün ağırlığı çarpılmaktadır.
- § Her bilgi ölçütü için elde edilen farklı çarpımlar toplanmaktadır.
- § Bu toplam, üzerinde çalışılan tehdit senaryosunun önem derecesiyle çarpılmaktadır.

Son olarak CobIT BT sürecinin önem derecesi tüm farklı senaryolar için bu işlemle hesaplanmış en yüksek önem derecesi olarak tanımlanmıştır. Bu son önem derecesi tüm CobIT BT

süreçlerinin sınıflandırılmasını sağlamaktadır. Bu sınıflandırma A Kurumu'nun iş süreçlerinin devamlılığını sağlamadaki risk seviyesini en aza indirmek için hangi BT süreçlerinin öncelikli olarak kontrol edilmesi gerektiğini göstermektedir.

4. Normalizasyon

Yukarıda bahsedilen yöntem kullanılırken her bir süreç için sonuçtaki önem derecesi puanının bu sürecin etkilediği toplam Bilgi Ölçütleri ile yakından ilişkili olduğu görülecektir. Diğer bir deyişle standart CobiT'te yüksek ağırlığa sahip olan süreçler risk analizinden sonra da yüksek ağırlığa sahip olacaktır. Bu, yöntemin tam anlamıyla mekanik olarak uygulanamayacağı ve sonuçların yorumlanması gerektiği hesaba katılsa dahi, beklentilerden farklı sonuçlara yol açabilir.

Bundan dolayı normalizasyon gerekmektedir ve bu çalışmada aşağıdaki yöntem kullanılmıştır:

- § Etkilenen Bilgi Ölçütlerinin sayısı ve düzeyine dayanan her süreç için standart CobiT ağırlıklarını içeren tablo oluşturulmuştur; (sonuç A)
- § Her süreç için önem derecesini kapsayan tablo ek bir sütun ile "göreceli önemlilik derecesini" kapsayacak şekilde genişletilmiştir. Önemlilik derecesi bu süreç için ortalama önemlilik derecesi ile bölünmektedir; (sonuç B)
- § Normal durumlarda (her yerde eşit risk) göreceli süreç önem derecesi (B) göreceli süreç ağırlığı (A) ile benzer şekilde dağıtılacaktır. Bunun sonucunda eğer belirli bir süreç için (B) (A)'dan daha yüksek ise süreç göreceli olarak daha önemlidir ve inceleme açısından daha ön planda tutulabilir. Ters durumda yani (A) (B)'den daha yüksek ise gözden geçirme süreci altında bulunan alan için süreç az öneme sahiptir;

Yukarıda tanımlanan mantık aşağıdaki örnekte (hayali veri) gösterilmiştir:

Aşama 1	Standart CobiT						
Süreç	IC1	IC2	IC3	IC4	IC5	Mutlak Ağırlık	Göreceli Ağırlık (A)
PR01	2	2		1	1	6	120%
PR02	2		1		1	4	80%
PR03	1	2				3	60%
PR04	2			1	1	4	80%
PR05		2	2	2	2	8	160%

Ortalama Ağırlık 5

Aşama 2	Risk Analizi						
Süreç						Mutlak Önem Derecesi	Göreceli Önem Derecesi (B)
PR01						15	123%
PR02						7	57%
PR03						11	90%
PR04						10	82%
PR05						18	148%

Ortalama Önem Derecesi 12,2

Aşama 3
Süreç Önemi
(B/A)

1,00
0,70
1,50
1,00
0,90

Görüyoruz ki mutlak önem derecesi süreç PR05'i en yüksek dereceye getirirken göreceli süreç önemi puanı süreç PR03'ü muhtemelen en önemli dereceye koyacaktır.