İLLER BANKASI ANONİM ŞİRKETİ

BİLGİ TEKNOLOJİLERİ ALANINDA RİSK YÖNETİMİ VE UYGULAMASI

Merve ATAR

UZMANLIK TEZİ

HAZİRAN 2018


İLBANK
TÜRKİYE'NİN YAPICI GÜCÜ

İLLER BANKASI ANONİM ŞİRKETİ

BİLGİ TEKNOLOJİLERİ ALANINDA RİSK YÖNETİMİ VE UYGULAMASI

Merve ATAR

UZMANLIK TEZİ

Tez Danışmanı (Kurum)
Mehmet ALPA

Tez Danışmanı (Ankara Üniversitesi)
Prof. Dr. Fazıl GÖKGÖZ

Merve ATAR tarafından hazırlanan “Bilgi Teknolojileri Alanında Risk Yönetimi ve Uygulaması” adlı tez çalışması aşağıdaki Yeterlik Sınav Kurulu tarafından OY BİRLİĞİ / OY ÇOKLUĞU ile UZMANLIK TEZİ olarak kabul edilmiştir.

	Unvanı	Adı ve Soyadı	İmzası
Başkan	Genel Müdür Yardımcısı	Salih YILMAZ	
Üye	Daire Başkanı	Hüseyin TÖREN	
Üye	Daire Başkanı	Hakkı ÇIRAK	
Üye	Daire Başkanı	Orhan IŞIK	
Üye	Daire Başkanı	Doç. Dr. Birol KAYRANLI	

Tez Savunma Tarihi: 19.06.2018

ETİK BEYAN

İLLER BANKASI ANONİM ŞİRKETİ Uzmanlık Tezi Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Merve ATAR
19 Haziran 2018

Bilgi Teknolojileri Alanında Risk Yönetimi ve Uygulaması

(Uzmanlık Tezi)

Merve ATAR

İLLER BANKASI ANONİM ŞİRKETİ

Haziran 2018

ÖZET

Son yıllarda bilgi teknolojilerinin hızla gelişimi dünyamızı yeni bir çağa taşırken, tüm kurumları değişen koşullara hazırlanmak zorunda bırakmaktadır. Günümüzde bilgi teknolojilerinden yararlanmayan kurumların varlığını sürdürmesi çok zordur. Bilgi teknolojilerinin gelişimiyle birlikte riskler de ortaya çıkmaktadır. Bilgi teknolojileri alanında risk yönetiminin yeterince gelişim gösterememesi, risk öngörüsünün gelişmemiş olması, risklerin önceliklendirilmeden ve fayda/maliyet düşünülmeksizin çözümlenmeye çalışılması, proaktif kontroller yerine reaktif kontrollerin uygulanması nedeniyle tehdit ve zafiyetlerin olumsuz etkilerine maruz kalınmaktadır. Bu çalışmada, bilgi teknolojileri alanında özellikle bankalarda risk yönetiminin nasıl olması gerektiği, risk yönetimi süreçleri, risk yönetimi için var olan yaklaşımlar, metodolojiler, yazılımlar ve risk yönetimi uygulamasına yönelik örnekler incelenerek verilmektedir.

Anahtar Kelimeler : Risk yönetimi, COBIT, ISO 27001

Sayfa Adedi : 115

Tez Danışmanı : Mehmet ALPA (Kurum)
Prof. Dr. Fazıl GÖKGÖZ (Ankara Üniversitesi)

Risk Management and Practice in Information Technologies

(Expertise Thesis)

Merve ATAR

ILLER BANKASI ANONIM SIRKETI

June 2018

ABSTRACT

In recent years, while the rapid development in information technologies is carrying out the world into a new era, it forces all organizations to be prepared for changing conditions. Today, it is very hard to maintain the existence of organizations which is not using information technologies. Also, risks arise with the development in information technologies. In the area of information technology, organizations are exposed of negative effects of threats and vulnerabilities; due to underdeveloped risk management and prediction, trying to solve without considering cost/benefit and prioritization of risks, and applying reactive controls instead of proactive ones. This study examines, especially in banks, how should be the risk management, the risk management processes; and the present approaches, methodologies, softwares and examples for the application of the risk management in the area of information technologies.

Key Words : Risk management, COBIT, ISO 27001

Page Number : 115

Supervisor : Mehmet ALPA (Corporate)
Prof. Dr. Fazıl GÖKGÖZ (Ankara University)

TEŞEKKÜR

Uzmanlık tezimin yazım sürecinde yardımlarını esirgemeyen üniversite danışmanım Sayın Prof. Dr. Fazıl GÖKGÖZ'e ve kurum danışmanım Sayın Mehmet ALPA'ya teşekkürlerimi sunarım. Her anlamda yanımızda olan ve destek veren başkanım Yasin ÖZEN'e, müdürüm Hüseyin ODABAŞI'na ve tüm Test-Kalite-COBIT grubuna teşekkür ederim. Bu günlere gelmemde en büyük destekçim olan aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklamalar**
%	Yüzde
*****	Çarpım
<	Küçüktür
>	Büyüktür
≤	Küçük eşit
≥	Büyük eşit

Kısaltmalar	**Açıklamalar**
AI	Edinim ve uygulama
APO	Hizala, planla ve düzenle
AR-GE	Araştırma ve Geliştirme
BAI	Kur, edin ve uygula
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BGRY	Bilgi güvenliği risk yönetimi
BGYS	Bilgi güvenliği yönetim sistemi
BİT	Bilgi ve iletişim teknolojileri
BKZ.	Bakınız
BS	Bilgi sistemleri
BSI	Bilgi Güvenliği Federal Ofisi
BT	Bilgi teknolojileri
CCTA	Merkezi Bilgisayar ve Telekomünikasyon Ajansı
CLUSIF	Fransa Bilgi Güvenliği Kulübü
COBIT	Bilgi ve ilgili teknolojiler için kontrol hedefleri
COBRA	Danışma, nesnel ve çift fonksiyonlu risk analizi
CORA	Risk analizinin maliyeti
CORAS	Kritik güvenlik sistemlerinin risk değerlendirmesi
COSO	Sponsor Organizasyonlar Birliği

Kısaltmalar	Açıklamalar
CRAMM	Risk analizi ve yönetimi yöntemi
DS	Hizmet ve destek
DSS	Tedarik, hizmet ve destek ver
E-	Elektronik
EA	Avrupa Akreditasyon Birliği
EDM	Değerlendir, yönlendir ve izle
FAIR	Bilgi güvenliği riskleri için faktör analizi
GSYİH	Gayrisafi yurtiçi hasıla
ICT	Bilgi ve iletişim teknolojileri
IEC	Uluslararası Elektroteknik Komisyonu
ISACA	Bilgi Sistemleri Denetim ve Kontrol Derneği
ISO	Uluslararası Standardizasyon Organizasyonu
ISRAM	Bilgi güvenliği risk analizi yöntemi
IT	Bilgi teknolojileri
ITGI	Bilgi Teknolojileri Yönetişim Enstitüsü
ITIL	Bilişim Teknolojileri Altyapı Kütüphanesi
ITU	Uluslararası Telekomünikasyon Birliği
İLBANK	İller Bankası
İVO	İç verimlilik oranı
ME	İzleme ve değerlendirme
MEA	İzle, tespit et ve değerlendir
MEHARI	Uyumlaştırılmış risk analizi yöntemi
NBD	Net bugünkü değer
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü
OCTAVE	Operasyonel kritik tehdit, varlık ve zafiyet değerlendirmesi
OECD	Ekonomik İşbirliği ve Kalkınma Teşkilatı
PMBOK	Proje yönetimi bilgi tabanı
PO	Planlama ve organizasyon
PUKÖ	Planla, uygula, kontrol et, önlem al
RISK IT	Bilgi teknolojileri için risk çerçevesi
ROI	Yatırım getirisi
SDP	Hizmet tasarım paketi

Kısaltmalar	Açıklamalar
SOX	Sarbanes-Oxley yasası
SWOT	Güçlü yönler, zayıf yönler, fırsatlar, tehditler
TBD	Türkiye Bilişim Derneği
TEİAŞ	Türkiye Elektrik İletim Anonim Şirketi
TIRM	Toplam bilgi risk yönetimi
TL	Türk lirası
TSE	Türk Standardları Enstitüsü
TUENA	Türkiye ulusal enformasyon altyapısı ana planı
TURKAK	Türk Akreditasyon Kurumu
UML	Birleşik modelleme dili
VAL IT	Bilgi teknolojileri için değer
VB.	Ve benzeri
YBS	Yönetim bilgi sistemi
YGG	Yönetim gözden geçirme

GİRİŞ

Bilgi geçmişten günümüze en önemli kaynaktır. Bu kaynağı daha verimli kullanan ve nitelikli bilgiye sahip olan ülkeler daha ileri refah düzeylerine ulaşmıştır. Yine aynı şekilde bilgi teknolojilerinden yeterince faydalanmayan ülkeler ise çağa uyum sağlamadıkları için gerilemeye mahkûm kalacaktır.

Teknolojiyle birlikte gelişim her alanda olmakla birlikte özellikle bankacılık alanında teknolojinin önemi büyüktür. Teknolojinin hızlı gelişimi, sunulan hizmetlerin çeşitlenmesi, yasal düzenlemelerin yapılması ve küreselleşmenin etkileriyle geçmişten günümüze bankaların faaliyet ve politikalarında değişiklikler meydana gelmiştir (Teker, 2006: 11).

Teknoloji kullanımı yarar sağlamakla birlikte bilişim sistemlerinin sürekliliğini tehdit eden güvenlik problemlerini de beraberinde getirmektedir. Sistemde oluşan zafiyetler; kurum bilgilerinin ve kişisel bilgilerin çalınması, yetkisiz değiştirilmesi, yok edilmesi hatta sistemin çalışamaz duruma gelmesi gibi risklere sebep olmaktadır. Bankacılık sektöründe riske yönelik çalışma olan Sarbanes Oxley kanun reformu (SOX), Amerika'da yatırımcıları tehlikelerden uzak tutmak amacıyla muhasebe, denetim, finans vb. alanlar ile ilgili düzenlemeleri ile 2002'de yürürlüğe girmiştir. Sarbanes Oxley ile birlikte Türkiye'deki kamu kurumlarının ve özellikle bankaların güvenlik konusundaki standartların yürürlüğe girmesi ve bu standartların uygulamasının yapılması sonucunu doğurmuştur ve bu sayede bilgi teknolojileri risk yönetimi için BS7799, Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri (COBIT) vb. standartların uygulanması öngörülmüştür. Bu uygulamaların başarıya ulaşması için çalışanların uygulamaların gerekliliğine inanması bilgi güvenliğine yönelik davranışları açısından önemlidir (Kuyumcuoğlu ve Başoğlu, 2008).

Gelişmiş ülkeler başta olmak üzere, bütün ülkeler gün geçtikçe bilgi toplumu olma yolunda ilerlemektedir. Bilgi ve iletişim teknolojileri; elektronik (e) bankacılık, e-imza, e-devlet vb. uygulamalarda kullanılmakta olup toplum yaşamında önemli yer edinmiştir. Elektronik uygulamaların güvenli bir şekilde işleyebilmesi için bilgilerin gizliliği, bütünlüğü, erişilebilirliğinin sağlanması için teknik ve hukuki anlamda her türlü önlem alınmalıdır (Özenç, 2007).

Türkiye'de bankacılık sektörü hızlı bir şekilde gelişmektedir. Bu hızlı gelişimle birlikte oluşabilecek risklerinde hızlı bir gelişim ve değişime uğraması nedeniyle bankalarda riskin belirlenmesi, ölçülmesi, değerlendirilmesi ve yönetilmesi ihtiyacı ortaya çıkmıştır. İç kontrol sisteminin ortaya çıkmasıyla risk yönetimi, geleneksel yaklaşımlardan uzaklaşarak daha çağdaşlaşmıştır (Koç ve Çelik, 2015).

Bilgi teknolojileri ile ilgili standartların çokluğuna rağmen uygulama ile ilgili kaynakların yetersiz olduğu görülmektedir. Risk yönetimi ile ilgili son gelişmeler konunun gittikçe daha fazla önem kazandığının göstergesidir. Bilgi teknolojileri alanında risk yönetimi ve uygulamasının açıklandığı bu tez çalışması dört bölümden oluşmaktadır. Birinci bölümde; bilgi, bilgi teknolojileri, bilgi güvenliği ve risk kavramları açıklanmaktadır. İkinci bölümde; bilgi teknolojileri risk yönetimi yaklaşımları, metodolojileri ve yazılımları açıklanmaktadır. Üçüncü bölümde; bilgi teknolojilerinde risk yönetimi ve risk analizi açıklanmaktadır. Dördüncü bölümde; bilgi teknolojilerinde risk yönetimi örnek uygulaması ve risk yönetimiyle ilgili daha önceki çalışmalar yer almaktadır.

1. BİLGİ, BİLGİ TEKNOLOJİLERİ, BİLGİ GÜVENLİĞİ VE RİSK

Bilgi yaşamın en gündelik faaliyetinden en karmaşık faaliyetine kadar kullanılmaktadır. Bilgi toplumundaki en büyük gelişme, emek, sermaye, doğa ile birlikte işlenmiş bilginin üretim faktörü olarak kullanılmasını sağlayan bilgi ve iletişim teknolojilerinin (BİT) yaşamın her alanında kullanılmasıdır. Yönetim bilgi sistemlerinin ve bilgi yönetiminin gelişmesini sağlayan bilginin üretim faktörü olarak kullanılmasıdır (Tutar, 2010: 31). Bilgiyi üretmek bilgi teknolojileri (BT) olmadan da mümkündür; fakat BT bilginin üretilmesini ve kullanılmasını artırarak kuruma daha çok iş yapabilme işlevselliği kazandırmaktadır.

Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) ülkelerinde yapılan araştırmalara göre elde edilen katma değerin yüzde elliden fazlasını bilgi sektörü oluşturmaktadır. OECD ekonomilerinde üretimin temel faktörü bilgidir. Bilgi üretimini sağlamak için uzun ve detaylı araştırma geliştirme faaliyetlerinde bulunmak gerekmektedir (Tutar, 2010: 45).

Kurum için değer oluşturmada bilgi sistemlerinin rolü çok büyüktür. Bilgi sistemleri, yöneticilerin daha iyi kararlar vermesine yardımcı olarak veya iş süreç uygulamalarının gelişmesini sağlayarak gelir artırıcı ya da maliyet azaltıcı etki etmektedir (K. Laudon ve J. Laudon, 2014). Ülke olarak düşünüldüğünde ülkelerin gelişmişlik düzeyi bilgiyi ve teknolojiyi yönetme kapasitelerine bağlıdır (Öztürk, Tekerek ve Yılmaz, 2016).

1.1. Bilgi Kavramı

Bilgi kavramı üzerinde ilk düşünür Aristo'dur daha sonra Bacon, insan zekâsının ortaya koyduğu yöntemler bütünü olarak bilgiyi tanımlar. Türk Dil Kurumu (TDK), insan aklının ereceği olgular, gerçekler ve ilkelerin tümü olarak tanımlamaktadır. İngilizcede "knowledge" ve "information" kelimelerinin karşılığı Türkçede bilgi olarak tanımlansa da information kelimesinin karşılığı, malumattır. Knowledge kelimesinin karşılığı ise anlama, öğrenme, aşina olma olarak tanımlanır. İmgeden fonksiyonel bilgiye erişim süreci Şekil 1.1'de gösterilmiştir (Tutar, 2010: 51-55).

Şekil 1.1. İmgeden fonksiyonel bilgiye erişim süreci (Tutar, 2010: 53)

Şekil 1.1'de belirtildiği üzere veri, bilgi göstergesinin imgeden sonraki basamakta işlenmemiş ham değer anlamına gelir. Enformasyon ise bilgi ve veri arasında yer alarak işlenmiş veri anlamına gelir. Üst bilgi ise işlenmiş, akıl süzgecinden geçmiş, algı, duyu, sezgi, deneyim, gözlem ve üretim sonuçları ile birleştirilmiş iş süreçlerinde kullanılmaya hazır bilgidir.

1.2. Bilgi Teknolojileri Kavramı

Bilgi teknolojileri: Bilginin toplanmasını, işlenmesini, muhafaza edilmesini, istenilen yere iletilmesini, istenilen yerden bu bilgiye erişilmesini, elektronik vb. yollar ile sağlayan teknolojiler bütünü olarak tanımlanmaktadır (Türk Dil Kurumu, 2011). Farklı bir tanımda ise; bilginin toplanması, kullanılması, depolanması, iletişim kaynaklarıyla bir yerden bir yere ulaştırılması, yönetilmesi, saklanması ve güvenliğinin sağlanmasında yararlanılan donanım ve yazılım gibi araçlara bilgi teknolojileri denilmektedir (Kamu İç Denetim Koordinasyon Kurulu, 2014: 276).

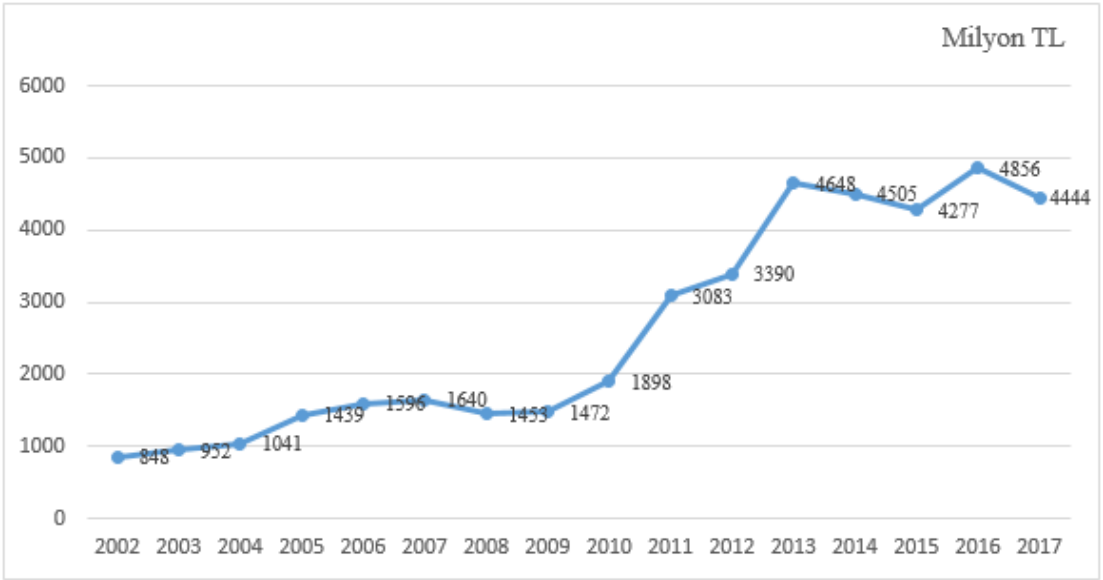
Kurumsal bilgi teknolojileri başarısının sağlanması için kapsamlı bir bilgi teknolojisi planı olması gerekmektedir. Plan, çevresel değişimleri dikkate alan uzun dönem odaklı olmalıdır. Planlamanın içeriğinde işe ve başarıya odaklanma, imkân ve alternatifleri ölçülü bir şekilde değerlendirme, risk tanımlamaları yapma, alternatif ve fırsat maliyetlerini değerlendirme yer almalıdır (Tutar, 2010: 145).

Risk yönetimi, bilgi teknolojileri ve mevzuata uygunluk yönünden iç içedir. Şekil 1.2'de risk yönetimi, BT ve mevzuat uygunluğu arasındaki ilişki gösterilmiştir (Grünendahl ve Will, 2006).

Şekil 1.2. Risk yönetimi, BT ve mevzuat ilişkisi (Grünendahl ve Will, 2006)

Şekil 1.2'de görüldüğü üzere operasyonel riskleri bertaraf etmek ve mevzuata uygunluğu sağlamada bilgi teknolojileri önemli rol oynamaktadır. Uygunluğu sağlamak adına yapılan her şey tamamlayıcı bir risk yönetimiyle mümkündür. İç kontrol çerçevesi mevzuata uygunluğu gerektiren tanımlanmış risklere dayanmaktadır.

Türkiye Bilişim Derneği'nin (TBD) taslak raporunda, Kalkınma Bakanlığı tarafından hazırlanan 2016 yılı Kamu Bilgi ve İletişim Teknolojileri Yatırımları raporu içeriğinde 233 bilgi ve iletişim teknolojileri projeleri için 4,5 milyar ödenek ayrılmıştır bilgisi yer almaktadır (TBD, 2016). Kalkınma Bakanlığı tarafından hazırlanan başka bir rapora göre ise merkezi yönetim kurumlarının bilgi ve iletişim teknolojilerine olan 2002-2017 yıllarındaki yatırımları Şekil 1.3'te gösterilmektedir (Kalkınma Bakanlığı, 2017).



Şekil 1.3. Bilgi teknolojileri yatırımları (2002-2017) (Kalkınma Bakanlığı, 2017)

Şekil 1.3'te görüldüğü üzere yatırımların genellikle yıldan yıla arttığı ve 2011 yılı itibariyle yatırımların önceki yıllara göre ivme kazandığı anlaşılmaktadır.

Bilgi sistemlerine yapılan yatırımlar akıllıca olursa rakiplere karşı üstünlük elde edilebilir; fakat yatırım planlaması kötü yapılırsa sermayenin boşa harcanması gibi bir sonuçla karşılaşılmaktadır (K. Laudon ve J. Laudon, 2014). Yatırım payı ayırmak kadar yatırım planlamasının en iyi şekilde yapılması organizasyonun günümüz koşullarına uyum sağlaması adına gereklidir.

1.3. Yönetim Bilgi Sistemi Kavramı

Yönetim Bilgi Sistemi (YBS) insanların ortak hedeflerine ulaşmak için bir arada bulunmalarından itibaren vardır. YBS, yöneticilerin ihtiyaç gördüğü bilgiyi etkin bir şekilde elde etmek, işlemek, düzenlemek ve erişilmek istenilen hedefe muvafık hale getirmek üzere kurulan sistemdir. Yönetim bu şekilde daha az emek ve maliyet ile kaliteli ve hızlı kararlar alabilmektedir. YBS; farklı ortamdaki bilgileri tek bir yerde birleştirir böylece detaylı bilgiye hızlı bir şekilde ulaşılır, karar alma süresi azalır, risk yönetimi kapasitesi yükselir ve raporlama olanakları artar gibi faydaları sağlamaktadır (Polat, 2007).

1.4. Risk Kavramı

Türk Standardları Enstitüsü (TSE), risk kavramını dünyanın her geçen gün daha fazla fırsatlar evrenine dönüşmesi daha fazla tehdit unsuru içermesine sebep olmaktadır. Risk, belirsizlik (beklenenden sapmanın negatif veya pozitif) etkisi olarak tanımlamaktadır (TSE, 2016).

Risk eski tanımlamalarda; belirsizlik, zarar görme tehlikesi ve maruz kalınabilecek tehditler şeklinde tanımlanmıştır. Günümüz tanımlarında ise gelecekte çıkması olağan tehdit ve fırsatlar şeklinde tanımlanmıştır. Umulmayan vakalardan doğan riskler tehlikeyi, değişimden doğan riskler belirsizliği, kurum yararına kullanılabilecek riskler ise fırsatları barındırmaktadır (Koç ve Uzay, 2015).

Risk ikiye ayrılır. Birincisi: Doğal risk (yapısal/içsel); hiçbir önlem alınmadığında ortaya çıkan risktir. Durum ya da olayın doğasında olan risklerdir. İkincisi: Kalıntı risk (artık); durum ya da olay için alınan önlem ve aksiyonlardan sonra kalan risktir (Acar, 2013).

On yıl öncesine kadar BT'ye ait riskler sınırlı ve BT kaynaklarının kilitli odalarda tutulmasıyla önlenebilecek hırsızlık gibi tehlikeler varken BT hizmetlerinin gelişmesiyle birlikte bilgi teknolojileri yönetiminin uzaktan yapılabilmesinin sağlanmasıyla çok farklı güvenlik tehditleri oluşmuştur.

1.5. Bilgi Güvenliği Kavramı

Bilgi güvenliği, bilginin bir varlık olarak zararlardan korunması, doğru teknolojinin, doğru hedefle ve biçimde kullanılmasıyla her türlü ortamda, yetkisiz kişiler tarafından ele geçirilmesini önleme olarak tanımlanmaktadır (Canbek ve Sağıroğlu, 2006).

Bilgi güvenliği faaliyetleri yirminci yüzyılın ikinci yarısında Amerika'da başlamıştır. İlk virüs 1982 yılında bilgisayarın her 50. açılışında ekrana çıkan bir şiirdir. Bilgi güvenliğini tehdit eden virüsler başlangıçta eğlence veya şaka amaçlı olarak kodlanan yazılımlar iken zamanla illegal olarak ve hızla yayılım sağlayacak şekilde gelişmeye başlamıştır. Dünyada 2015 yılı bilgi güvenliği sektöründe bulunan firma sayısı, eğitim sistemi kalitesi, kişi başına düşen Gayrisafi Yurtiçi Hasıla (GSYİH) ve araştırma-geliştirme (AR-GE) yatırımlarına ayrılan verilere bakıldığında başta Amerika, İngiltere, İsrail, Almanya ve Kanada güvenlik yazılımı ve teknolojinin en fazla üretildiği ülkeler olarak sıralanmaktadır. Türkiye'de bilgi güvenliği ve yönetimi alanında şirketler bulunsa da yeterli düzeyde değildir. Ulusal güvenlik alanında siber güvenlik en önemlisidir. Siber güvenliği sağlamanın yolu ise milli güvenlik yazılımlarının üretilmesi, teknolojik altyapının geliştirilmesi ve üniversite-sanayi-kamu kuruluşlarının ortak hareket ederek bilgi toplumu yapılandırmasına yönelik faaliyetleri ile sağlamaktır (Öztürk ve diğerleri, 2016).

Dünyanın her yerindeki bir bölgeye çok az maliyetle ataklar yapılabilmektedir, bu durumun şirketleri ve hatta ülkeyi zarara uğratması olasıdır. Bilgi güvenliğinin sağlanmasında en önemli faktör kişidir. Kişiler, yalnızca bilgi seviyeleri ile orantılı önlem alabilecekleri için bilgi güvenliği farkındalığının sağlanması amacıyla eğitim almaları gerekmektedir. Karşılaşılacak tehditler kişi, kurum veya ulusal kaynakları hedef alacak nitelikte olduğu için alınacak önlem ve önlem derecelerinin de bu üç duruma uygun olacak şekilde farklılaşması gerekmektedir (Erol, Ceyhan ve Sağıroğlu, 2015). Tehdit ve zafiyetler riskleri oluşturmaktadır. Zafiyetlerin bulunmadığı bir tehdit risk oluşturmaz veya tehdidin

bulunmadığı bir zafiyet risk oluşturamaz. Riskin oluşması için her ikisinin bulunması gereklidir (OECD, 2015).

Operasyonel riske örnek olarak Citibank'ın 2001 yılında Amerika'da meydana gelen saldırılar sonrasında ATM sistemindeki yedekleme ile ilgili sorunlar yüzünden bankanın bu hizmeti iki gün boyunca çalışmaması verilebilir (Ertürk, 2010).

Türkiye'de siber saldırı örneği olarak Türkiye Elektrik İletim Anonim Şirketi (TEİAŞ) verilebilir. TEİAŞ'nin 2014 yılında uğradığı siber saldırı sonucunda kurumun saygınlığı azalmıştır (Türkiye Elektrik İletişim A. Ş.'ye Siber Saldırı). Türkiye'de bilgi toplumu alanında ilk çalışma 1999 yılında yapılan Türkiye Ulusal Enformasyon Altyapısı Ana Planı (TUENA)'dır. 2000 yılında e-Türkiye Girişimi Eylem Planı, 2003-2004 yılında e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı, 2005 Eylem Planı, 2006-2010 yılları için Bilgi Toplumu Stratejisi ve Eylem Planı ve 2015-2018 yılları için Bilgi Toplumu Stratejisi ve Eylem Planı hazırlanmıştır. Bu planlardan TUENA ve e-Türkiye Girişimi Eylem Planı uygulanamamıştır (Kalkınma Bakanlığı, 2015).

Bilgi sistemleri güvenliği; insan güvenliği, teknoloji güvenliği, ağ güvenliği, veri güvenliği ve bilgi sistemleri faaliyetleri güvenliği olarak beş ana unsurdan oluşsa da aslen bilgi güvenliği; bilginin gizliliği, bilginin bütünlüğü ve bilginin kullanılabilirliği ile kullanım yönünden ifade edilmektedir (Raggad, 2010: 11).

Bilgi güvenliği konusunda Uluslararası Standardizasyon Organizasyonu (ISO), Uluslararası Elektroteknik Komisyonu (IEC), Uluslararası Telekomünikasyon Birliği (ITU) ve Bilgi ve İletişim Teknolojileri (ICT) tarafından standartlar oluşturulmuştur (Evrin ve Demirer, 2011).

2. BİLGİ TEKNOLOJİLERİ RİSK YÖNETİMİ YAKLAŞIMLARI VE METODOLOJİLERİ

Bilgi teknolojilerinde riskin öneminin her geçen gün artmasıyla yasal düzenlemeler ile birlikte COBIT, ISO 27001 gibi standartlar benimsenmiş ve denetim mekanizmaları kurulmuştur.

Risk yönetimi yaklaşımlarının benimsenmesiyle risk yönetimi daha bütünleşik bir yapı haline gelmiştir. Organizasyonun yapısına uygun olan yazılım ve metodolojilerin seçimiyle risk yönetiminde otomasyona gidilmiştir.

2.1. Yasal Düzenlemeler

5411 sayılı Bankacılık Kanunun'da risk yönetimiyle ilgili, bankalardaki risklerin izlenmesi ve kontrolü için bankalar; kurum yapısıyla uyumlu etkin bir risk yönetimi, iç kontrol ve denetim sisteminin kurulmasından ve işletilmesinden sorumludur. Risk yönetimi, iç kontrol ve iç denetim sistemi ile ilgili usul ve esaslar Bankacılık Düzenleme ve Denetleme Kurumunca (BDDK) belirlenir ifadesi yer almaktadır (Bankacılık Kanunu, 2005: Madde 29).

BDDK'nın yayımladığı tebliğe göre; bankanın, bilgi teknolojilerini kullanmasıyla oluşabilecek riskleri izlemesi, ölçmesi, kontrolünü ve raporlamasını sağlaması gerekmektedir. Risk değerlendirmesinde bankanın dikkat edeceği unsurlar; teknoloji gelişimine uyumda karşılaşılabilecek zorluklar, yeni hata ve dolandırıcılıkların gelişimi, destek hizmeti alınan kuruluşlara bağlılığın artması, iş sürekliliğinin çoğunlukla bilgi sistemlerine dayanması, veri güvenliğinin sağlanmasına yönelik tedbirlerin zorlaşmasıdır. Bilgi teknolojilerinde oluşabilecek risklerin bankanın diğer faaliyet alanları da göz önünde bulundurularak bütünsel bir çerçeveyle operasyonel risk kapsamında değerlendirilmesi gerekir. Planlanan değişikliklere ilişkin risk analizi yapılır ve prosedürler hazırlanır. Bilgi sistemleri risk yönetimiyle ilgili oluşturulan politika ve prosedürlerin banka içinde işlerliğinin izlenmesi, bankanın yapısına, risk profiline, kurum kültürüne ve mevzuata uygun olarak risk yönetimi süreçlerini geliştirmesi ve BT kaynaklı riskleri değerlendirmesi ifadeleri yer almaktadır (BDDK, 2007: Madde 5).

Sermaye Piyasası Kurulu (SPK) tarafından yayımlanan tebliğde; kurum, kuruluş ve ortaklıkların bilgi sistemleriyle ilgili olan riskleri ölçmek, takip etmek, uygulamak ve raporlamak için süreç ve prosedürler tesis etmesi ve güncelliğine dikkat etmesi gerekir. Risklerin yönetilmesinde dikkate alınacak konular; bilgi teknolojilerindeki gelişmelere uyum zorlukları ve yasal mevzuattaki değişiklikler, tahmin edilemeyen hata ve hileli işlemler, dış kaynak bağımlılığı, iş ve hizmetlerin bilgi sistemlerine olan bağlılığı, işlem, veri ve denetim izlerinin güvenliğinin zorlaşmasıdır. Risk analizi gerektiğinde tekrarlanır veya yılda en az bir kez yapılır. Teknik zafiyetlere zamanında tedbir alınır, yılda en az bir kez ulusal veya ülkeler arası belgesi bulunan kişiler tarafında sızma testi yapılır, ifadeleri yer almaktadır (Bilgi Sistemleri Yönetimi Tebliği, 2018: Madde 8).

BDDK, Türkiye için; süreç odaklılığı, bütüncül yaklaşıma sahip olması, ölçme ve derecelendirme sisteminin bulunması, ITIL, SOX, COSO yaklaşımlarına uyumlu ve Avrupa Birliği mevzuatında uygunluğuna onay verilen bilgi sistemleri yönetişim çerçevelerinden biri olması nedeniyle COBIT'i benimsemiştir. Çizelge 2.1'de Norveç, Portekiz, Almanya vb. ülkelerde benimsenen denetim yaklaşımları belirtilmiştir (Varlı, 2007).

Çizelge 2.1. Farklı ülkelerde benimsenen denetim yaklaşımları (Varlı, 2007)

Ülkeler	**Benimsenen Yaklaşımlar**
Finlandiya	İç Kontrol ve Risk Yönetimi İle İlgili Geliştirdikleri Standartları
Norveç	COBIT Standartları
Macaristan	COBIT Standartları
Çek Cumhuriyeti	IT Yönetişimi ve Operasyonel Risk Kapsamındaki Düzenlemeler
Makedonya	ISO 17799 Standartları
Slovakya	Yıllık Bilgi Sistemleri Güvenliğini Kapsayacak Denetim Raporu
Danimarka	Finansal, Sistem, Operasyon, Veri ve İş Devamlılığı Denetimi
Portekiz	Üç Yılda Bir Bilgi Sistemleri (BS) Denetimi
İsrail	ISO 17799 Standartları
Hollanda	Sınırlı Alanda BS Denetimine Referansta Bulunan Standartlar
İtalya	Sınırlı Alanda Kontrolleri İçeren Düzenlemeler
Slovenya	ISO 17799 Standartları
Yunanistan	BS Denetimiyle İlgili Bankacılık Kanunu
Almanya	Almanya Denetim Kuruluşu (IDW) PS 330 Standardı

Çizelge 2.1'de belirtildiği üzere, Norveç ve Macaristan COBIT standartlarını benimserken, Makedonya, İsrail ve Slovenya ISO 17799 standartlarını benimsemiştir.

Sayıştay tarafından BT denetimi 2003 yılında Hazine Müsteşarlığı'nda başlamış ve İngiltere ve İspanya Sayıştayı ile Sayıştay'ın Denetim Kapasitesinin Güçlendirilmesi projesinde, mali ve performans denetimine ek olarak bilişim sistemleri denetimi de ele alınmıştır bu sayede ülkeler arası standartlar ve Avrupa Birliği uygulamalarına kaynak oluşturabilecek önemli katkılar sağlanmıştır. Denetimde ISO 17799, ISO 27001, Bilgi Sistemleri Denetim ve Kontrol Derneği (ISACA) standartlarından yararlanarak risk tabanlı denetim yaklaşımı oluşturulmuştur. Yaklaşım; BT kaynaklı risklerin belirlenmesi, riskleri kontrol edecek mekanizmaların belirlenmesi, kontrol mekanizmalarının kurum içinde varlığının tespit edilmesi, inceleme sonrası zafiyet değerlendirilmesi ve raporlanması aşamalarını içermektedir (Yıldız, 2007).

2.2. Risk Yönetimi Yaklaşımları

Riskler sistemlerin güvenliği ve erişilebilirliğinin yanı sıra iş organizasyonuyla ilgili riskleri de içerdiği için bilgi teknolojileri riskleri belirlenirken iş bazında risk yönetimi olarak ele alınmalıdır. Bilgi teknolojileri risklerini yönetmek ve dengeyi sağlamak amacıyla uygulanan yaklaşım ve metodolojilere bilgi teknolojileri risk yönetimi denilmektedir (Bağcı, 2007).

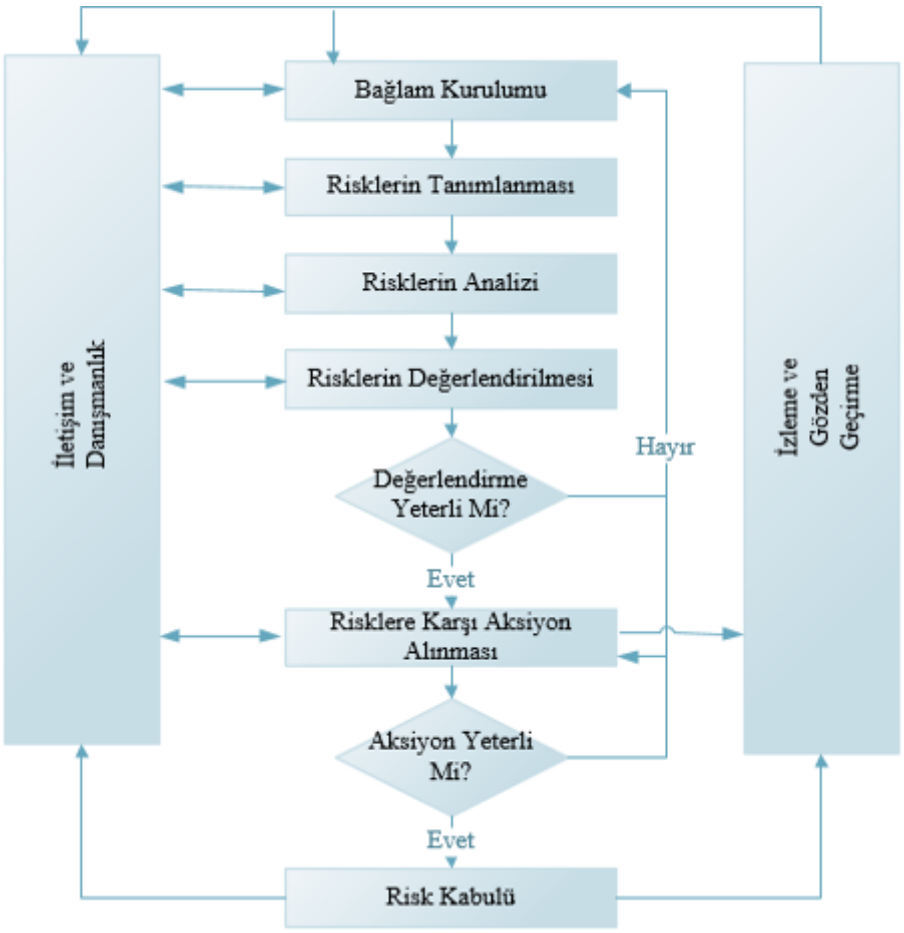
Bilgi teknolojileri risk yönetimi yaklaşımları olarak ISO 27005, ISO 27001, COBIT, ISO 31000, NIST SP 800 gibi yaklaşımlar incelenmiştir.

2.2.1. ISO 27005

ISO/IEC 27005 ilk olarak 2008 yılında yayınlanmış ve Türkçe tanımlaması ise "bilgi teknolojisi-Güvenlik teknikleri-Bilgi güvenliği risk yönetimi" dir. İkincisi, 2011 yılında yayınlanmış ancak Türkiye de TSE tarafından kabul tarihi 2014'tür (Türk Standardı 27005). Bu standartla ISO/IEC 27001 standardı, bilgi güvenliği uygulamasını risk yönetimi yaklaşımıyla desteklemektedir.

ISO/IEC 27005'e göre risk yönetimi aşamaları aşağıda açıklanmıştır. Risk yönetimi süreci ve riske tepki faaliyetleri tekrarlanabilirdir. Bilgi Güvenliği Yönetim Sistemi (BGYS) içindeki Planla, Uygula, Kontrol et, Önlem al (PUKÖ) döngüsünde planla aşamasında; bağlam kurulumu, risk değerlendirmesi, riske tepki planı geliştirilmesi ve risk kabulü yer

almaktadır. Uygula aşamasında, riske tepki planının uygulaması yer almaktadır. Kontrol et aşamasında, risklerin sürekli kontrol edilmesi ve izlenmesi yer almaktadır. Önlem al aşamasında, Bilgi Güvenliği Risk Yönetimi (BGRY) iyileştirilmesine yönelik aktiviteler yer almaktadır. Şekil 2.1'de ISO 27005 risk yönetimi süreci verilmiştir (ISO, 2011).



Şekil 2.1. ISO 27005 risk yönetimi süreci (ISO 2011)

Şekil 2.1'de görüldüğü üzere süreç ilk olarak bağlam kurulumu aşamasından başlamaktadır. Bağlam kurulumu; kapsam ve hedeflere uygun olan risk yönetimi yaklaşımının belirlenmesi, risk değerlendirme kriterlerinin belirlenmesi, bilgi güvenliği olayları sonucunda meydana gelebilecek zarar ve maliyetlerin etki kriterlerinin belirlenmesi, organizasyonun belirlediği risk kabul kriterleri, kapsam ve limitler ve organizasyon içindeki sorumlulukların belirlenmesi maddelerinden oluşmaktadır.

Bilgi güvenliği risklerinin değerlendirmesi; risk belirleme, risk analizi ve risk değerlendirme ana maddelerinden oluşmaktadır. Risk belirleme; risklerin, varlıkların, tehditlerin, mevcut kontrollerin, zafiyetlerin, sonuçların belirlenmesidir. Risk analizi;

niteliksel veya niceliksel olarak risk analizi yönteminin belirlenmesi, olasılıkların değerlendirilmesi, risk seviyelerinin belirlenmesidir. Risk değerlendirme; risk önleme, paylaşma, azaltma gibi aksiyonların belirlenmesi, risk yönetimi sürecinin tüm aşamasında paydaşlar ve karar vericiler arasında iletişim ve danışmanlık sağlanması, risklerin, varlıkların, tehditlerin, zafiyetlerin, olasılıkların organizasyon içindeki tüm değişimlerinin izlenmesi ve gözden geçirilmesi maddelerini içermektedir.

2.2.2. ISO 27001

Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri – Gereksinimler anlamında olan ISO/IEC 27001 standardı, ISO/IEC 17799 standardının genişletilmiş halidir. TS 17799-2 iptal edilerek 2 Mart 2006 tarihinde, Bilgi Teknolojileri ve İletişim İhtisas Grubu tarafından hazırlanan TS ISO/IEC 27001 kabul edilmiştir. 18 Aralık 2013 tarihinde Teknik kurul tarafından hazırlanan ISO/IEC 27001 güncellemesi yapılmıştır. Son güncel hali 22 Mayıs 2017 tarihinde kabul edilmiştir (Türk Standardı 27001; Türk Standardı 17799).

Standardın güçlü yönleri, zayıf yönleri, fırsatları ve tehditlerinden oluşan niteliksel analizi Çizelge 2.2'de SWOT matrisinde gösterilmiştir (Bahtit ve Regragui, 2013).

Çizelge 2.2. SWOT matrisi (Bahtit ve Regragui, 2013)

Güçlü Yönler	BGYS uygunluklarını kontrol edilmesi, iletişimin kolay olması, güvenlik bütçesinin en iyi şekilde kullanılması
Zayıf Yönler	Önlemlerin sağladığı verimlilikten emin olunmaması, dokümantasyon fazlalığı
Fırsatlar	ISO güvencesinin olması
Tehditler	Akreditasyon kuruluşlarının az tecrübeye sahip olması

Çizelge 2.2'de görüldüğü üzere BGYS uygunlukların kolaylıkla kontrol edilmesi ve bütçe yönetimini sağlaması yönünden güçlüdür. Dokümantasyonun çokluğu yönünden zayıftır. ISO güvencesini sağlaması yönü fırsatı oluştururken ve yeterli tecrübeye sahip olunmaması bir tehdit oluşturmaktadır.

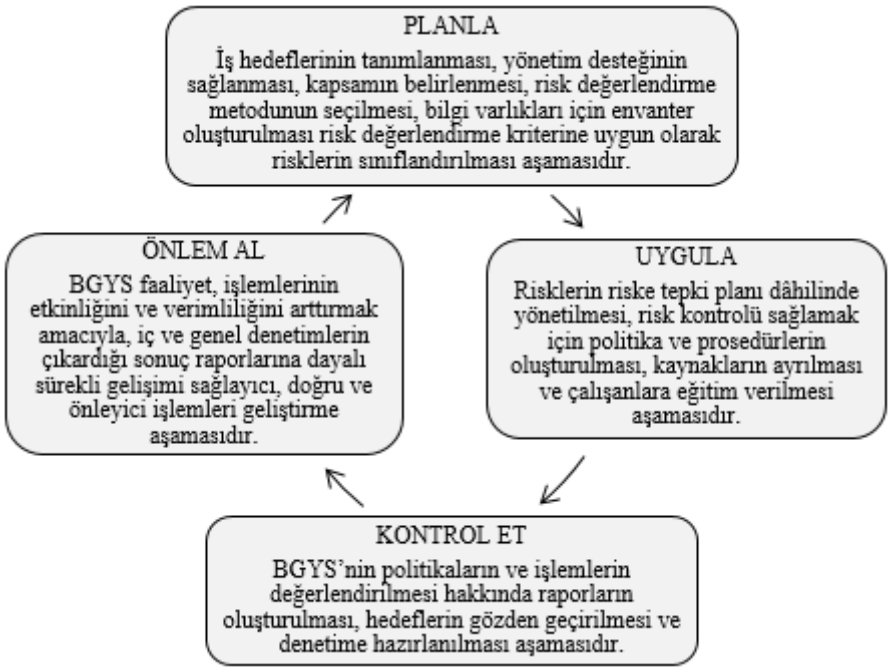
ISO/IEC 27001 belgesi TSE veya bazı özel şirketler tarafından verilmektedir. Türk Standardları Enstitüsü, TS ISO/IEC 27001 konusunda Avrupa Akreditasyon Birliği (EA) üyesi olan Türk Akreditasyon Kurumu (TURKAK) tarafından akredite edilmiştir. Bilginin gizliliğini, bütünlüğünü, kullanılabilirliğini sağlamak için, kurallar çerçevesinde,

planlanmış, sürdürülebilir, yönetilebilir, dokümantasyonu sağlanmış, uluslararası güvenlik standartlarını da temel alarak oluşturulan sisteme BGYS denilmektedir. Kurum için BGYS'nin sağladığı faydalardan bazıları aşağıda verilmiştir (Ersoy, 2012: 8-18).

- Tehdit ve risklerin tanımlanarak risklerin verimli bir şekilde yönetilmesi,
- Kurumsal saygınlığın oluşturulması ve sürdürülmesi,
- Güvenlik standartlarına ve mevzuata uyumun sağlanması,
- Bilgi sistemleri ve varlıklarının ayrıntılı bir şekilde envanterinin tutulmasının sağlanması,
- Bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliğinin sağlanması,
- Tüm paydaşların bilgilendirilerek, personele eğitim aldırılarak bilgi açıklığı oluşturulabilecek davranışların önüne geçilmesidir.

ISO/IEC 27001 ölçülebilirlik, tekrarlanabilirlik ve ölçeklenebilme kavramlarını içerir. Ölçülebilirlik: Varlık değerlendirmesinin somut bir şekilde yapılmasını sağlar. Tekrarlanabilirlik: İstenilen bölümler yönetim tarafından sürekli tekrarlanabilir (PÜKO döngüsü gibi). Ölçeklenebilme: BGYS kapsamının gerektiği takdirde daraltılıp genişletilmesine olanak sağlamasıdır. Bilgi güvenliği kapsamının belirlenmesi aşamasında mevcut olan bilgi sistemi varlıklarına ve süreçlerine öncelik verilmektedir. Standardın getirdiği ölçeklenebilirlik özelliği sayesinde zamanla gereksinim duyulan diğer alanları içine alan BGYS uygulanabilir veya gerekmediği durumlarda Yönetim Gözden Geçirmesi (YGG) toplantılarında geri çıkartılabilir (Ersoy, 2012: 8-20).

Bilgi güvenliğini sağlarken PÜKO döngüsü kullanılmaktadır. Deming'in PÜKO döngüsü ile BGYS ilişkisi Şekil 2.2'de gösterilmiştir (Pelnekar, 2011).



Şekil 2.2 PUKÖ döngüsü ve BGYS (Pelnekar, 2011)

Şekil 2.2'de görüldüğü üzere planla aşamasında, risk yönetimi için yapılması gerekenler planlanır. Uygula aşamasında, riske tepki dâhilinde uygulama yapılır. Kontrol et aşamasında, risk yönetimi ile ilgili performans gösterici raporlar oluşturulur. Önlem al aşamasında, sonuç raporlarına dayanan gelişimi sağlayıcı önlem faaliyetlerinde bulunulur.

ISO/IEC 27001 standardı 11 ana ve 133 alt başlıktan oluşmaktadır. Standardın ana maddeleri şunlardır:

Güvenlik Politikası: Kurum içinde bir güvenlik politikasının oluşturulması ve üst yönetimin bu politikanın kullanımını yaygınlaştırmak için destek ve teşvik etmesinin sağlanmasıdır.

Bilgi Güvenliği Organizasyonu: Kurum içinde bilgi güvenliği grubunun kurulması ve BGYS uygulamasının yapılmasıdır. Yönetim kurum içinde yapılacak güvenlik kontrollerini desteklemeli ve sorumlulukları atamalıdır.

Varlık Yönetimi: Kurumun varlık olarak tanımlayabileceği donanım, yazılım, bilgi varlıkları, fiziksel varlıklar, personel, ağ vb. varlıkların envanterinin periyodik olarak yapılması ve varlığa ait sahiplik ve sorumlulukların belirlenmesidir.

İnsan Kaynakları Güvenliği: Kurum içinde insan kaynaklı ortaya çıkabilecek hatalara karşı önlem alınması, işe alımda gerekli nitelikte personel sağlanması, işten ayrılma durumunda erişim haklarının kaldırılması ve çalışan ile üçüncü taraflar arasında güvenlik anlaşmalarının yapılmasını kapsamaktadır.

Fiziksel ve Çevresel Güvenlik: Yetkisiz erişim kaynaklı oluşabilecek zafiyetlere karşı yapılması gerekenlerin belirlenmesi, koruma yöntemlerinin geliştirilmesi ve çevresel kaynaklı oluşabilecek zafiyetlere karşı önlem alınmasını kapsamaktadır.

İletişim ve İşletme Yönetimi: Donanım, yazılım ve ağ sistemlerinin güvenliği sağlanması hususunda alınacak önlemler, uygulanacak prosedürler ve yaptırımları içermektedir.

Erişim Kontrolü: Yetkisiz erişimleri önlemek adına erişim kısıtlamaları ve alınabilecek önlem ve düzenlemeleri kapsamaktadır.

Bilgi Sistemleri Edinim, Geliştirme ve Bakımı: Bilgi işlem altyapısı, uygulama ve süreçlerin güvenliğini sağlamaya yönelik edinimlerin kazanılması ve bu alanlardaki geliştirme ve bakım süreçlerinin yapılmasını kapsamaktadır.

Bilgi Güvenliği İhlal Olayı Yönetimi: İhlal olayı sürecinde, ihlalin nasıl gerçekleştiği, ihlalin raporlanması ve ihlal sonrası tespit ve önlemlerin alınmasını kapsamaktadır.

İş Sürekliliği Yönetimi: Bir olay anında kurumun aksayan işlerini kontrol altına alabilmek için iş etki analizleri ve iş sürekliliği planları yapılmasını kapsamaktadır.

Uyum: Bilgi sistemleri kullanımı sürecinde yasal düzenlemelere sözleşmelere veya mevzuata bağlı kalınmasını ve gerekli dokümantasyonun yapılmasını kapsamaktadır (Ersoy, 2012; Şen ve Yerlikaya, 2013).

ISO 27001'e göre risk yönetimi aşamaları aşağıda maddeler halinde gösterilmiştir (Eskiyörük, 2007):

- Kapsamın Belirlenmesi: Organizasyon amaçlarına uygun olarak kapsam belirlenir.

- Varlıkların Belirlenmesi: Organizasyon için değeri olan her şey varlıktır. Varlıklar bilgi, donanım, yazılım gibi kategorilere ayırarak gruplandırılır. Varlıkları belirlerken anket, birebir görüşmeler, sistem dokümanlarının incelenmesi yöntemleri kullanılabilir.
- Tehditlerin Belirlenmesi: Tehdit kaynağının zafiyetleri kullanarak varlıklara zarar verme durumudur. İnsan kaynaklı, doğal ve çevresel tehditler olarak sınıflandırılabilir.
- Zafiyetlerin Belirlenmesi: Tehditlerin mevcut olması durumunda zarar oluştururlar. Başka bir deyişle bir tehdit ile ortaya çıkabilecek zayıflıktır. Zafiyetleri belirlerken geçmiş dönem risk değerlendirme ve denetim raporları, güvenlik analizleri, sızma testi sonuçları gibi veriler incelenerek zafiyetler altyapı, donanım, yazılım, haberleşme, doküman, personel ile ilgili zafiyetler olarak kategorilere ayrılmaktadır.
- Kontrollerin Belirlenmesi: Risklerin gerçekleşme olasılıklarını düşürmek için kontrol planlaması yapılır.
- Olasılık Değerlendirmesi: Tehdit, zafiyet ve kontroller değerlendirilerek olasılık değerlendirmesi yapılır.
- Etki Analizi: Açıklığın meydana gelmesi durumunda olumsuz etki seviyesi belirlenir.
- Risk Derecelendirmesi: Olasılık ve etki değerlendirmesi sonucuna göre yüksek, orta, düşük gibi risk derecelendirmesi yapılır.
- Uygun Kontrollerin Belirlenmesi: Riskleri tamamen yok etmek veya azaltmak için organizasyon politikaları dikkate alınarak teknik, yönetimsel ve operasyonel kontroller belirlenir.
- Sonuçların Dokümantasyonu: Risk analizi sürecinin raporlanarak paydaşlar ile paylaşılması gerekmektedir. Riske Tepki; riskin kabulü, kaçınma, azaltılması, transferi gibi risk işleme yöntemi belirlenir.
- Kontrollerin Uygulanması: Risk işleme yöntemi belirlendikten sonra fayda/maliyet analizi yapılarak ve bulunan riskin kabul edilebilir riskten büyük olması durumunda uygun kontroller belirlenir ve uygulanır. Kontroller uygulanırken kaynak dağılımını verimli bir şekilde sağlamak için yüksek risk derecelerine öncelik verilerek sorumluluklar atanır.
- Artık Risk: Kontroller neticesinde riskin tamamen ortadan kalkmaması durumudur. Kabul edilebilir seviyesinin altındaki riskler yönetim tarafından kabul edilmelidir.

- İzleme: Risk yönetimi döngüsü değişen koşullar altında veya periyodik olarak yapılmalıdır.

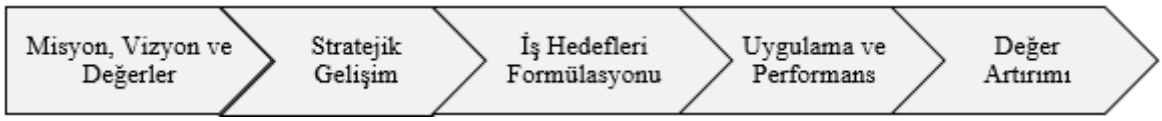
2.2.3. COSO

Sponsor Organizasyonlar Birliği (COSO), hileli finansal raporlamanın önüne geçmek için iç kontrol, risk değerlendirmesi, kurum faaliyetlerinin değerlendirmesi amacıyla 1985 yılında Amerika'da beş örgütün desteğiyle kurulmuştur. İlk yayınını 1992 yılında yapmıştır. Değişen koşullar (mevzuat, teknoloji, kurumsallaşma, risk vb.) doğrultusunda gerekli güncellemeler yapılmıştır.

COSO'ya göre iç kontrol; kontrol ortamı, risk değerlendirme, bilgi ve iletişim, izleme ve kontrol faaliyetleri olmak üzere beş ana maddeden oluşmaktadır (Tarantino, 2006):

- Kontrol Ortamı: Her bir iş süreci için kurum kritikliği göz önünde bulundurularak kontrol ortamı geliştirmeli ve sürdürülebilirliği sağlanmalıdır.
- Risk Değerlendirme: Her bir iş süreci için farklı riskler bulunmaktadır ve kontrol ortamı bu riskler göz önünde bulundurularak oluşturulmalıdır.
- Kontrol Faaliyetleri: Kontrol faaliyetleri iş süreçlerindeki riskleri azaltmak ve risk yönetimini sağlamak için belirlenmelidir.
- Bilgi ve İletişim: İş süreçlerini yönetmek ve kontrolünü sağlamak için bilgi ve iletişim sistemleri kurulmalıdır.
- İzleme: İç kontrol süreci, yapılan değişikliklerin izlendiğinden emin olunarak yönetilmelidir.

Kontrol kapsamını belirlerken risk değerlendirmesi önemli bir adımdır. Kritik ve öneme sahip olan alanlar belirlendikten sonra kontrol faaliyetleri uygulanmalıdır. Sürekli izleme ve test yöntemiyle eksik olan alanlar ve etkin olmayan kontroller ortaya çıkartılarak gerekli raporlamalar yapılmalıdır. Etkin bir iç kontrol sistemi oluşturmak adına yönetim kontrol mekanizmalarının geliştirilmesinden sorumludur (Tarantino, 2006). COSO çerçevesi 2017 yılında güncellenmekle birlikte yeni çerçevede misyon, vizyon ve değerler, stratejik gelişim, iş hedefleri formülasyonu, uygulama ve performans, değer artırımı ana ilkeleri Şekil 2.3'te gösterilmektedir (COSO, 2017).



Şekil 2.3. COSO çerçevesi (COSO, 2017)

Şekil 2.3'te COSO çerçevesi; yönetişim ve kültür, strateji ve hedef belirleme, performans, gözden geçirme ve revizyon, bilgi iletişim ve raporlama olmak üzere beş bileşenden oluşmaktadır.

Yönetişim ve Kültür: Kuruluş içindeki sorumlulukların oluşturulması ve riskin anlaşılmasına ilişkin etik değerlerin kurulmasıyla ilgilidir. Yönetimin risk gözetim faaliyetleri, operasyonel yapının kurulması, istenilen kültür ortamının kurulması, temel değerlere bağlılık, geliştiren ve yetenekli bireylerin devamını sağlama maddelerini kapsamaktadır.

Strateji ve Hedef Belirleme: Strateji planlama sürecinde; kurumsal risk yönetimi, strateji ve hedef belirleme alanları birlikte çalışmaktadır. İşin analizi, risk iştahının tanımlanması, alternatif stratejilerin değerlendirilmesi, iş hedeflerinin formülasyonu maddelerini kapsamaktadır.

Performans: Strateji ve iş hedeflerinin gerçekleşme başarısını etkileyecek risklerin tanımlanması, risk iştahının belirlenmesi, riske karşı aksiyonların alınması ve raporlanmasıdır. Riskin belirlenmesi, risk şiddetinin değerlendirilmesi, risklerin önceliklendirilmesi, riske karşı tepkiler ve risk portföyü geliştirme maddelerini kapsamaktadır.

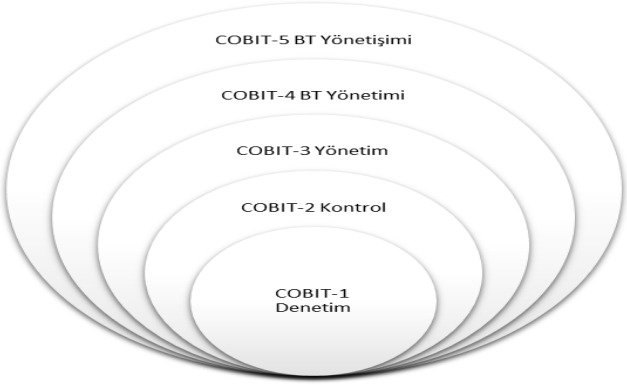
Gözden Geçirme ve Revizyon: Organizasyonun kurumsal risk yönetimindeki performansının gözden geçirilmesi ve değişiklikler karşısındaki hangi revizyonların yapıldığıyla ilgilidir. Önemli değişiklikleri değerlendirme, risk ve performansı gözden geçirme, kurumsal risk yönetimini geliştirme maddelerini kapsamaktadır.

Bilgi, İletişim ve Raporlama: İç ve dış kaynaklardan kurumsal risk yönetimini sağlamak için gerekli bilgiyi elde etme ve paylaşma sürecidir. Bilgi ve teknolojinin geliştirilmesi, riske dair bilgi iletişiminin sağlanması, risk, kültür ve performansın raporlanması maddelerini kapsamaktadır (COSO, 2017).

2.2.4. COBIT

COBIT, ISACA tarafından geliştirilmiş ve BT Yönetişim Enstitüsü (ITGI) devralmıştır. COBIT-1'in 1996 yılında kuruluşundaki alanı sadece denetim iken, 1998 yılında COBIT-2'ye kontrol eklenmiştir. 2000 yılında yönetim güncellemesi eklenerek COBIT-3 yürürlüğe girmiştir.

2005 yılında COBIT-4 ve 2007 yılında COBIT-4.1, Val IT 2.0 ve Risk IT'nin eklenmesiyle BT yönetimi ortaya çıkmıştır. Son olarak 2012 yılında ITIL ve ISO 27001 gibi standartlardan yararlanarak BT'ye yönetişim kavramı eklenmiş ve COBIT-5 yürürlüğe girmiştir. Şekil 2.4'te COBIT'in tarihsel gelişimi gösterilmiştir (Cantürk, 2013; Brand ve Boonen, 2007: 21-36).



Şekil 2.4. COBIT'in tarihsel gelişimi (Cantürk, 2013)

Şekil 2.4'te görüldüğü üzere COBIT'e yıllar içinde denetim, kontrol, yönetim, BT yönetimi ve BT yönetişimi kavramları eklenerek gelişim göstermiştir.

BDDK, başlangıçta birkaç bankada COBIT esaslı denetim faaliyetinde bulunmuştur. 2006 yılından sonra tüm bankalara her iki yılda bir COBIT bazlı denetim zorunlu tutulmuştur. Bankacılık haricinde, diğer sektörlerde de COBIT prensipleri etkili süreç yönetiminin sağlanması amacıyla kullanılabilmektedir. COBIT'in özellikle finans kuruluşlarında kullanılmasının sebebi; bankalarda havale, provizyon, şifre vb. işlemlerin güvenlik tehlikesi içerdiği için kontrol altında tutulmasının gerekmesidir (Güneş, Kızıldeniz, Selçuk, Suna ve Coşkun, 2013). COBIT bazlı bilgi kriterleri (etkinlik, verimlilik, gizlilik, bütünlük, kullanılabilirlik, uyum, bilginin güvenilirliği) ve açıklamaları Çizelge 2.3'te gösterilmiştir (Brand ve Boonen, 2007).

Çizelge 2.3. COBIT bilgi kriterleri (Brand ve Boonen, 2007)

Etkinlik	Bilginin iş ve iş süreçleriyle ilgili zamanında, doğru, sürekli ve kullanılabilir bir şekilde olması
Verimlilik	Kaynakların en iyi şekilde kullanılması
Gizlilik	Hassas bilgilerin yetkisiz kişilerden korunması
Bütünlük	İş değerleri ve beklentilerine uygun olarak bilginin doğruluğunun ve eksiksizliğinin sağlanması
Kullanılabilirlik	Bilginin şimdi veya gelecekte istenilen zamanda ulaşılabilir olması
Uyum	İş sürecinin maruz kaldığı yasalar, düzenlemeler ve sözleşmeye uyum sağlanması
Bilginin Güvenilirliği	Yönetişim sorumluluklarının yerine getirilmesi adına organizasyon için en uygun bilginin sağlanması

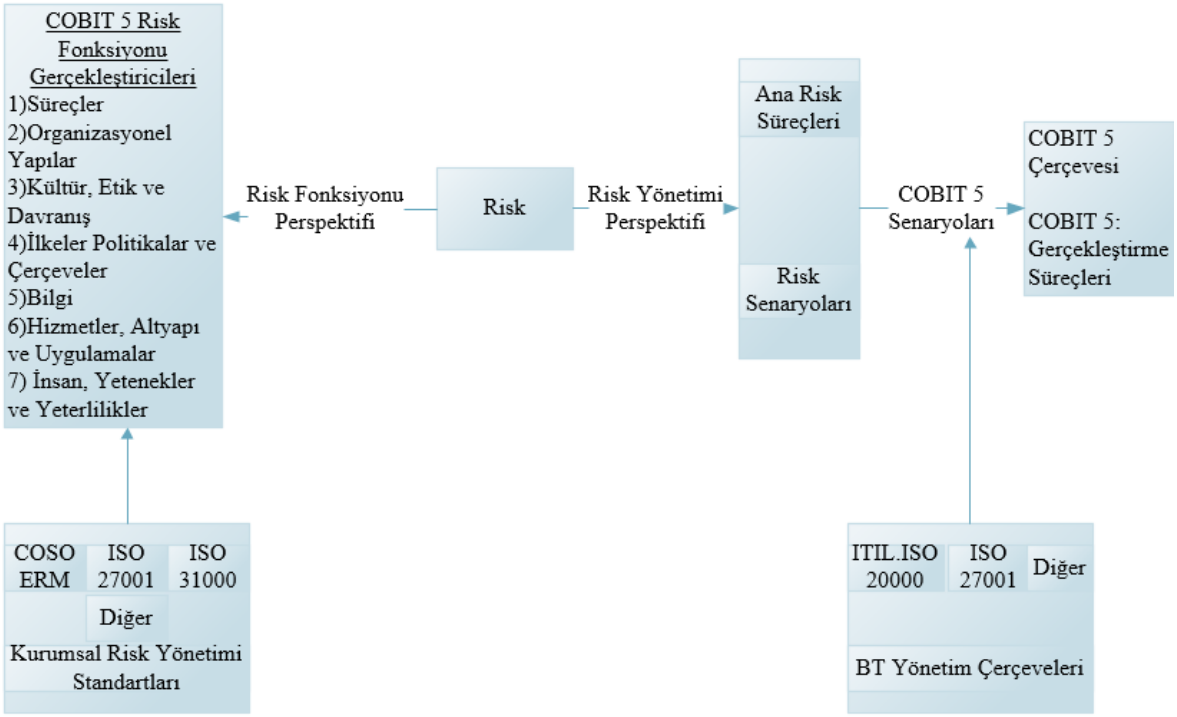
Val IT; BT için değer anlamına gelmektedir. Değer yönetişimi, portföy yönetimi ve yatırım yönetimi olmak üzere üç ana süreci ve yirmi iki alt süreci bulunmaktadır (ISACA, 2010). Risk IT; BT için risk çerçevesi anlamına gelmektedir. Risk-getiri oranının hesaplanmasına yardımcı olmakla birlikte kurumsal risk yönetimine BT risk yönetimini entegre etmek için kullanılmaktadır. Risk IT; risk yönetişimi, risk değerlendirmesi ve riske tepki olmak üzere üç sürece sahiptir (ISACA, 2009). COBIT, süreç sahiplerinin bilgi teknolojileri alanındaki sorumluluklarını kontrol kriterlerine uygun olarak yerine getirmelerini sağlayan bir düzenlemedir. Misyonu, bilgi teknolojisi kontrol hedeflerini geliştirmektir. Amacı, kar maksimizasyonu, fırsat optimizasyonu, kontrol gereklerini yerine getirmeyi sağlamaktır. Bilgi teknolojilerinin kurumun ihtiyaçlarını sağlama konusunda başarılı olmasını amaçlamaktadır. COBIT uygulaması zaman alıcı ve maliyetli olduğu için tüm organizasyonlara uygulamak güç olabilmektedir (Uzunay, 2007).

COBIT 5

COBIT 5; çerçeve, yönetişim prensipleri ve süreç tasarımı olmak üzere üç kitaptan oluşmaktadır (Akay, 2014). Şekil 2.5'te COBIT 5 gerçekleştiricileri ve COBIT kapsamı açıklanmıştır. Kurumsal risk yönetimi standartları, BT yönetim çerçevesi ve senaryoları dikkate alınarak COBIT 5 kapsamı oluşturulmuştur (ISACA, 2013).

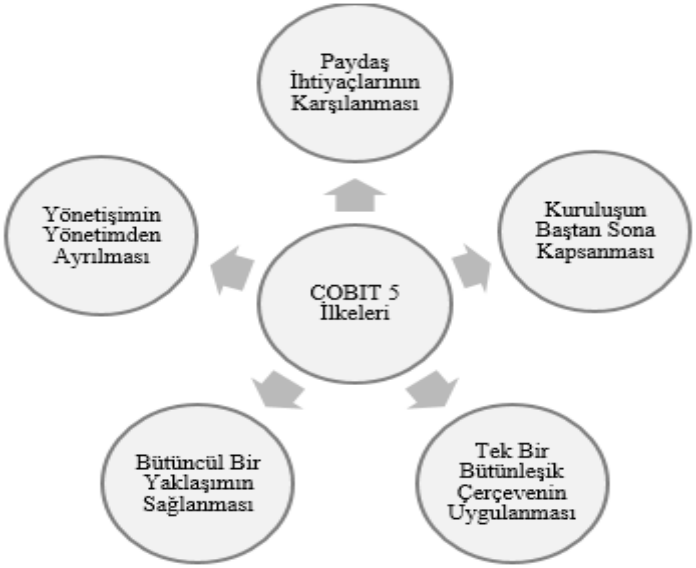
- Süreçler: EDM (değerlendir yönlendir ve izle) ve APO (hizala, planla ve düzenle) başta olmak üzere risk fonksiyonunu etkileyen diğer süreçler oluşturmaktadır.
- Organizasyonel Yapılar: Kurumsal risk yönetimi komitesi vb. karar vericilerdir.
- Kültür Etik ve Davranış: Kurum çapında davranışlar, yöneticilerin davranışları vb.

- İlkeler Politikalar ve Çerçeveler: Risk ilkeleri, risk politikaları vb. istenilen davranışlarda bulunulması için geliştirilen kılavuzlardır.
- Bilgi: Risk profili, risk senaryoları, risk haritası vb. kuruluş tarafından üretilen bilgilerdir.
- Hizmetler Altyapı ve Uygulamalar: Risk danışmanlığı hizmetleri vb. bilgi teknolojileri hizmetlerini sağlayıcılarıdır.
- İnsanlar, Yetenekler ve Yeterlilikler: Başarılı olmak, doğru kararlar almak için gereklidir.



Şekil 2.5. COBIT 5 kapsamı (ISACA, 2013)

Şekil 2.5'te görüldüğü üzere COBIT 5 risk kapsamında risk fonksiyonu gerçekleştiricileri daha çok kurumsal risk yönetimi standartlarıyla ilişkilendirilirken, COBIT 5 kısmı BT yönetim çerçeveleriyle ilişkilendirilmiştir. COBIT 5'te farklılık olarak risk senaryoları ele alınmaktadır. COBIT 5 çerçevesi beş ana ilkeden oluşmaktadır. Süreç uygulamaları gerçekleştiriciler tarafından yapılmaktadır. Şekil 2.6'da COBIT 5 ilkeleri gösterilmektedir.



Şekil 2.6. COBIT 5 ilkeleri (ISACA, 2012)

Şekil 2.6'da görüldüğü üzere paydaş ihtiyaçlarının karşılanması, kurumsal hedeflere uygun bir risk yönetimi uygulanmasıdır. Kuruluşun baştan sona kapsanması, tüm yönetişim ve yönetici olanaklarını kapsamına alarak ve gerekli tüm risk yönetim ve yönetim aşamalarını açıklamasıdır. Tek bir bütünleşik çerçevenin uygulanması, COBIT 5 için riskin tüm ana risk yönetimi çerçeveleriyle uyumlu olmasıdır. Bütüncül bir yaklaşımın sağlanması ve yönetişimin yönetimden ayrılması diğer ilkeleridir

COBIT-5 yönetişim süreçleri; EDM (Değerlendir, Yönlendir ve İzle), APO (Hizala, Planla ve Düzenle), DSS (Tedarik, Hizmet ve Destek Ver), BAI (Kur, Edin ve Uygula) ve MEA (İzle, Tespit Et ve Değerlendir) olmak üzere beş yönetişim süreci ve bunlara bağlı olan 37 alt süreçten oluşmaktadır. COBIT 5 için ana ve alt süreçler Çizelge 2.4'te gösterilmiştir (ISACA, 2012).

Çizelge 2.4. COBIT 5 süreçleri (ISACA, 2012)

EDM-Değerlendir, Yönlendir ve İzle		**APO-Hizala, Planla ve Düzenle**	
EDM01	Yönetimi Çerçevesi Kurulumunu ve Sürdürülmesini Sağla	APO01	BT Yönetim Çerçevesini Yönet
EDM02	Fayda Yaratımı Sağla	APO02	Stratejiyi Yönet
EDM03	Risk Optimizasyonu Sağla	APO03	Kurumsal Mimariyi Yönet
EDM04	Kaynak Optimizasyonu Sağla	APO04	Yeniliği Yönet
EDM05	Paydaş Şeffaflığını Sağla	APO05	Portföyü Yönet
BAI-Kur, Edin ve Uygula		APO06	Bütçe ve Maliyeti Yönet
BAI01	Program ve Projeleri Yönet	APO07	İnsan Kaynaklarını Yönet
BAI02	Gereksinimlerin Tanımlanmasını Yönet	APO08	İlişkileri Yönet
BAI03	Çözüm Belirleme ve Oluşturmayı Yönet	APO09	Hizmet Anlaşmalarını Yönet
BAI04	Kullanılabilirliği ve Kapasiteyi Yönet	APO10	Tedarikçileri Yönet
BAI05	Organizasyonel Değişimin Olabilirliğini Yönet	APO11	Kaliteyi Yönet
BAI06	Değişiklikleri Yönet	APO12	Riski Yönet
BAI07	Değişiklik Kabulü ve Geçişini Yönet	APO13	Güvenliği Yönet
BAI08	Bilgiyi Yönet	**DSS-Tedarik, Hizmet ve Destek Ver**	
BAI09	Varlıkları Yönet	DSS01	İşlemleri Yönet
BAI10	Yapılandırmayı Yönet	DSS02	Hizmet Taleplerini ve Olayları Yönet
MEA-İzle, Tespit Et ve Değerlendir		DSS03	Problemleri Yönet
MEA01	Performans ve Uyumu İzle, İncele ve Değerlendir	DSS04	Sürekliliği Yönet
MEA02	İş Kontrol Sistemini İzle, İncele ve Değerlendir	DSS05	Güvenlik Hizmetlerini Yönet
MEA03	Dış Gereksinimlere Uygunluğu İzle, İncele ve Değerlendir	DSS06	İş Süreç Kontrollerini Yönet

Çizelge 2.4'te görüldüğü üzere değerlendir, yönlendir ve izle ana başlığında; yönetim çerçevesi, risk optimizasyonu, fayda, kaynak kullanımı gibi organizasyon için önemli olan değerlere yer verilmiştir. Hizala, planla ve düzenle alt başlığında; strateji, kurumsal mimari, portföy, bütçe ve maliyet, kalite gibi konular yer almaktadır.

Kur, Edin ve Uygula alt başlığında; proje, varlık, değişiklik ve bilgi yönetimi konuları yer almaktadır. İzle, tespit et ve değerlendir alt başlığında; performans, iş kontrolü ve dış gereksinimlere uyum yer almaktadır. Tedarik, hizmet ve destek ver alt başlığında; olay, problem ve iş sürekliliği yönetimi konuları yer almaktadır.

COBIT 5'in içeriğinde bulunan risk yönetimiyle ilgili olan süreçler açıklanmıştır (ISACA, 2012):

EDM03-risk optimizasyonunu sağlama

Kurumun risk iştahı ve risk kabulü seviyesinin belirlenmesidir. Kod ile ilgili hedefler; BT ile ilgili iş risklerinin verimli bir şekilde yönetilmesi, BT harcamaları, faydaları ve riskleriyle ilgili şeffaflık, bilgi, altyapı ve uygulamaların güvenliği, kurum politikalarına BT'nin uyumu, risk eşiklerinin tanımlanması ve risklerin belirlenmesidir.

Ölçüm kriterleri olarak; risk değerlendirmesi kapsamındaki kritik iş süreçleri ve BT hizmetleri listesi, kurumsal risk içindeki BT risklerinin oranı ve risk profili güncelleme sıklığı, BT ile ilgili operasyonel harcamalar ve fayda/maliyet oranları, paydaşlar ile finansal bilgilerin (mali kayıp, getiri) şeffaf bir şekilde paylaşılması, üstün güvenlik önlemleri gerektiren hizmetlerin sayısı, servis seviye anlaşmalarına, yönergelere ve standartlara uyum göstergeleri ve güncellemelerin sıklığı, BT risk aksiyon planları performans göstergeleri, kurumsal risk toleransını aşan BT risklerinin göstergesi ölçüm kriterleridir.

EDM03.01-risk yönetimini değerlendir

BT'nin mevcut ve gelecekteki risklerini periyodik olarak kurum değerlerine uygun bir şekilde yönetimin incelemesini kapsamaktadır. Bu alanda yapılacak faaliyetlere örnek olarak; kurumun hedeflerini gerçekleştirmek için katlanacağı risk seviyelerinin belirlenmesi, kurum risk stratejisi ile BT risk stratejisi, ülkeler arası standartlar ve mevcut standartlar arasında uyumun sağlanması ve BT risklerinin proaktif bir şekilde değerlendirilmesi yer almaktadır.

EDM03.02-doğrudan risk yönetimi

Yönetimin belirlediği risk iştahını aşmama güvencesini sağlayarak BT risk uygulamalarının yönlendirmesini kapsamaktadır. Bu alanda yapılacak faaliyetlere örnek olarak; BT riskleri ve potansiyel etkilerine karşı kurum içinde risk farkındalığının oluşturulması, risk aksiyon planları kadar risk iletişim planlarının da yönetilmesi, değişen risk koşullarına karşı hızlı bir raporlamanın sağlanacağı sistemin geliştirilmesi, risk ve fırsatların önceden tanımlanmış prosedür ve politikalar ile belirlenmesi, raporlama yapılması ve raporların gerektiğinde üst yönetime sunulması yer almaktadır.

EDM03.03-risk yönetimi izle

Risk yönetimi süreciyle ilgili hedeflerin ve ölçümlerin izlenmesi ve iyileştirmeler için problemlerin ve sapmaların belirlenmesini kapsamaktadır. Bu alanda yapılacak faaliyetlere örnek olarak; risk iştahı eşiği içindeki risk profillerinin izlenmesi, sapmaların sebeplerinin analiz edilmesi altta yatan nedenlere karşı iyileştirici önlemlerin alınması, paydaşların kurumun tanımlanmış hedeflere doğru ilerlemesini gözden geçirmelerinin sağlanması ve yürütme komitesine gerekli raporlamaların yapılması yer almaktadır.

APO12-riskleri yönet

Kurum yürütme komitesi tarafından belirlenen seviyeye uygun olarak BT ile ilgili risklerin belirlenmesi, yönetilmesi ve azaltılması amacını taşımaktadır. Ölçüm kriterleri olarak; BT hizmet sağlayıcıları ile yapılan anlaşmalara uyumsuzluk göstergeleri, risk değerlendirmesine alınmayan BT ile ilgili önemli olayların sayısı, risk profilinin güncellenme sıklığı, paydaşlarla BT'nin finansal durumu ile ilgili bilgi paylaşımı ve memnuniyet anketi değerlendirmesi, finansal zarara ve iş kesintilerine neden olan güvenlik vakalarının sayısı, bütçe içinde ve zaman limitini aşmadan tamamlanan proje sayısı, önemli iş süreçlerinin risk profilinin içinde olması, risk aksiyon planlarının uygulanma oranı yer almaktadır.

APO12.01-veri topla

BT ile ilgili risklerin verimli bir şekilde tanımlanması, analizi ve raporlanması için veri toplanması ve tanımlanmasıdır. Bu alanda yapılacak faaliyetlere örnek olarak; BT ile ilgili risk verisinin toplanması, sınıflandırılması ve analizi için bir yöntemin kurulması ve devamlılığının sağlanması, BT risklerinin yönetiminde önemli rol oynayabilecek ilgili verilerin kaydedilmesi, geçmiş BT risk verilerinin dış kaynaklardan alınarak analiz edilmesi, benzer durumdaki olaylar için toplanan verinin düzenlenmesi ve katkı faktörünün vurgulanması, risk meydana geldiğinde var olan veya olmayan durumların, olayın sıklığına ve kayıp derecesine etkisinin belirlenmesi, yeni veya meydana gelmekte olan riskleri tanımlamak ve iç ve dış risk faktörlerini anlamak için periyodik olarak olay ve risk faktörü analizinin yapılması yer almaktadır.

APO12.02-risk analizi

İş ile ilgili risk faktörlerinin kararlarını desteklemek için kullanışlı bilgi geliştirmektir. Bu alanda yapılacak faaliyetlere örnek olarak; fayda/maliyet analizi yaptıktan sonra risk analizi kapsamının belirlenmesi, BT risk senaryolarının kurulması ve periyodik olarak güncellemelerinin yapılması, BT risk senaryolarıyla ilgili kayıp ve kazançların sıklık ve şiddetinin tüm uygulanabilir risk faktörlerinin hesaba katılarak ve bilinen operasyonel kontroller değerlendirilerek tahmin edilmesi, artık riski ve kabul edilebilir risk seviyesini karşılaştırarak risk tepkisinin tanımlanması, en iyi risk tepki yöntemini (önleme, azaltma, transfer, kabul) bulmak için fayda/maliyet analizi yapılması, risk analizi sonuçlarının karar almada kullanılmadan önce doğrulanması, analizin gereksinimlerle uyumlu olduğunun onaylanması yer almaktadır.

APO12.03-risk profili sürdürülmesi

Bilinen risk ve riskle ilgili olan sıklık, potansiyel etki kapasite ve kontrol faaliyetlerinin sürdürülmesidir. Bu alanda yapılacak faaliyetlere örnek olarak; altyapı, personel, uygulamalar, tedarikçiler gibi bilgileri içeren iş süreçleri envanterini oluşturmak, operasyon ve iş süreçlerinin devamlılığını sağlamak için gerekli olan BT hizmet ve altyapısının belirlenmesi, güncel risk senaryolarının fonksiyonel olarak kategorilere ayrılması, tüm risk verisine dayanarak mevcut risk ve risk eğilimlerinin tanımlanmasına izin veren risk göstergelerinin tanımlanması, risk profilini oluşturmak için risk aksiyon planı durumlarıyla ilgili bilgi edinilmesi yer almaktadır.

APO12.04-risklerin ifade edilmesi

BT ile ilgili mevcut durumun gerektiğinde paydaşlarla zamanında paylaşılmasını gerektirmektedir. Bu alanda yapılacak faaliyetlere örnek olarak; kurumun kararlarını desteklemede yardımcı olacak formatta risk analizi sonuçlarının raporlanması, karar vericiler ile en kötü ve en olası senaryoların, yasal düzenlemelerin paylaşılması, risk yönetimi süreçlerinin ve kontrollerin etkinliğini, iyileştirme yapılan alanları, uyumsuzlukları içeren mevcut risk profilinin paydaşlara raporlanması yer almaktadır.

APO12.05-risk yönetimi portföyünü tanımla

Riskleri kabul edilebilir bir seviyeye indirmek için fırsatların yönetilmesidir. Bu alanda yapılacak faaliyetlere örnek olarak; kontrol faaliyetlerinin sınıflandırılması, her bir organizasyon için bireysel ve portföy tolerans seviyeleri içinde faaliyet gösterdiğinin hesap verilebilirliğinin belirlenmesi, fayda/maliyet, mevcut risk profili ve düzenlemeler göz önünde bulundurularak riskleri azaltıcı proje önerilerinin tanımlanması yer almaktadır.

APO12.06-riske tepki

Zamanında alınacak önlemlerle, BT ile ilgili olaylardan kaynaklı kayıpların büyüklüğünü sınırlandırır. Bu alanda yapılacak faaliyetlere örnek olarak; operasyonel kayıplara neden olabilecek önemli risk durumlarında atılması gereken adımları belgeleyen planların hazırlanması, olayları sınıflandırmak ve gerçek maruz kalmalar ile risk toleransı eşiklerini karşılaştırarak karar vericilerle güncellenen risk profillerinin paylaşılması, risk olayları meydana geldiğinde etkiyi en aza indirmek için uygun müdahale planının uygulanması, geçmişteki olumsuz olayları, kayıpları ve kaçırılmış fırsatların incelenmesi ve kök nedenlerinin belirlenmesi yer almaktadır.

COBIT 4.1

COBIT 4.1 süreçleri; Planlama ve Organizasyon, Edinim ve Uygulama, Hizmet ve Destek, İzleme ve Değerlendirme olmak üzere dört süreçten ve bunlara bağlı olan 34 alt süreçten oluşmaktadır (ISACA, 2007). COBIT içerisinde var olan konu başlıkları Çizelge 2.5'te yer almaktadır.

Çizelge 2.5. COBIT 4.1 süreçleri (ISACA, 2007)

PO-Planlama ve Organizasyon		**DS-Hizmet ve Destek**	
PO1	Stratejik BT Planının Tanımlanması	DS1	Hizmet Seviyelerinin Tanımlanması ve Yönetimi
PO2	Bilgi Mimarisinin Tanımlanması	DS2	Üçüncü Kişilerden Alınan Hizmetlerin Yönetimi
PO3	Teknolojik Yönün Belirlenmesi	DS3	Performans ve Kapasite Yönetimi
PO4	BT Organizasyon ve İlişkilerinin Tanımlanması	DS4	Hizmet Sürekliliğinin Sağlanması
PO5	BT Yatırımlarının Yönetimi	DS5	Sistem Güvenliğinin Sağlanması
PO6	Yönetimin Amaçlarının İletilmesi	DS6	Maliyetlerin Belirlenmesi ve Tahsisi
PO7	BT İnsan Kaynakları Yönetimi	DS7	Kullanıcıların Eğitimi
PO8	Kalite Yönetimi	DS8	Hizmet Sunumu Yönetimi ve Olay Yönetimi
PO9	BT Risklerinin Değerlendirilmesi ve Yönetimi	DS9	Konfigürasyon Yönetimi
PO10	Proje Yönetimi	DS10	Problem Yönetimi
AI-Edinim ve Uygulama		DS11	Veri Yönetimi
AI1	Çözümlerin Belirlenmesi	DS12	Fiziksel Çevre Yönetimi
AI2	Uygulama Yazılımı Edinimi ve Bakımı	DS13	Operasyon Yönetimi
AI3	Teknoloji Alt Yapısının Oluşturulması ve Bakımı	**ME-İzleme ve Değerlendirme**	
AI4	Operasyon ve Kullanımın Sağlanması	ME1	Bilgi Sistemleri Performansının İzlenmesi ve Değerlendirilmesi
AI5	BT Kaynaklarının Satın Alınması	ME2	İç Kontrolün İzlenmesi ve Değerlendirilmesi
AI6	Değişiklik Yönetimi	ME3	Dış Gereksinimler ile Uyumun Sağlanması
AI7	Çözümlerin ve Değişikliklerin Uygulanması ve Akredite Edilmesi	ME4	BT Yönetişiminin Sağlanması

Çizelge 2.5'te görüldüğü üzere planlama ve organizasyon ana başlığı altında; organizasyon için gereken bilgi teknolojileri yönetiminin ana hatları yer almaktadır. Hizmet ve destek alt başlığında; hizmet sürekliliği, sistem güvenliği, olay, problem ve konfigürasyon yönetimi, performans ve kapasite yönetimi gibi kritik süreçler yer almaktadır. Edinim ve uygulama alt başlığında; değişiklik yönetimi, uygulama yazılımı edinimi gibi konular yer almaktadır. İzleme ve değerlendirme kısmında ise bilgi sistemleri güvenliğini sağlamada gerekli olan kontrol, performans izleme ve denetim gibi konular yer almaktadır.

COBIT 4.1'de risk yönetimi, PO9-BT Risklerinin Değerlendirilmesi ve Yönetimi başlığı altında yer almaktadır. BT risklerini ve risklerin iş süreçleri ve hedefleri üzerindeki

potansiyel etkilerini analiz etmek, risk yönetimi çerçevesi, risk değerlendirmesi, risk azaltma ve kalan risk bazında geliştirmek amaçlanır (ISACA, 2007). PO9-BT Risklerinin Yönetimi ve Değerlendirilmesi için örnek iş akışı Şekil 2.7'de gösterilmiştir (Brand ve Boonen, 2007: 80).

Şekil 2.7. COBIT 4.1 risk yönetimi iş akışı (Brand ve Boonen, 2007: 80)

Şekil 2.7'de görüldüğü üzere stratejik, taktik plan, hizmet portföyüde göz önünde bulundurularak risk iştahı belirlenir ve değerlendirilir. Değerlendirme sonuçlarına uygun olan kontroller belirlenerek aksiyonlar alınır. Sonuç değerlendirmesi yapılır uygunsa o varlık için risk değerlendirmesi sonlanır, uygun değilse yeni risk iştahı belirlenerek süreç devam ettirilir.

PO9-BT Risklerinin değerlendirilmesi ve yönetimi sürecinin ana maddeleri aşağıda açıklanmaktadır (ISACA, 2007).

PO9.1. BT Risk Yönetim Çerçevesi: Kurum risk yönetimi çerçevesine bağlı olan bir BT risk yönetim çerçevesinin oluşturulmasıdır.

PO9.2. Risk Bağlamının Oluşturulması: Risk değerlendirme çerçevesi içinde her bir risk değerlendirmesinin iç ve dış bağlamını, değerlendirmenin hedeflerini ve değerlendirilen risklere karşı kriterleri belirleyerek kurulmasıdır.

PO9.3. Olay Tanımlaması: Organizasyonun hedeflerine ve operasyonlarına, negatif etkisi olabilecek potansiyel olayların tanımlanması, olayların etki derecesinin belirlenmesi ve kaydedilmesidir.

PO9.4. Risk Değerlendirmesi: Tüm tanımlı risklerin olasılığı ve etkisi, niteliksel ve niceliksel metotlar kullanılarak periyodik olarak değerlendirilmesi, Artık riskin olasılığının ve etkisinin tanımlanmasıdır.

PO9.5. Riske Tepki**:** Maruz kalınacak riskleri sürekli olarak azaltacak uygun maliyetli kontrollerin tasarımı ile riske tepki sürecinin gelişiminin ve bakımının sağlanması, riske tepki sürecinde sakınma, azaltma, paylaşma veya kabul etme gibi risk stratejilerinin tanımlanması, sorumlulukların paylaşılması ve risk tolerans seviyelerinin belirlenmesi maddelerinden oluşmaktadır.

PO9.6. Risk Aksiyon Planı Bakımı ve İzlenmesi: Maliyetler, yararlar ve yürütme sorumluluğu da dâhil olmak üzere, gerekli olduğu takdirde tanımlanan risk tepkilerini uygulamak için tüm seviyelerdeki kontrol aktivitelerinin önceliklendirilmesi ve planlanması yapılır. Önerilen aksiyonların ve kalan risklerin kabulü için onay alınması ve taahhüt edilen aksiyonların etkilenmiş süreç sahipleri tarafından sahiplenildiğinden emin olunması ve her hangi bir sapmada üst yönetime raporlamalarda bulunulmasıdır.

Aşamalarının kontrolünü sağlamak ve kurumun eksiklerini görmesi adına 0-5 olarak puanlaması kriterlere sahip olmasına göre verilmektedir:

*"*0" Var olmayan: Süreçler ve iş kararları için risk değerlendirmesi yapılmaz. Organizasyon güvenlik açıkları ve geliştirme projesi belirsizlikleri ile ilgili iş etkileri dikkate alınmaz. Risk yönetimi, BT çözümleri elde eden ve BT hizmetleri sunan taraflar ile ilgili olarak tanımlanmamıştır.

“1” Başlangıç: BT riskleri doğaçlama olarak kabul edilir. Proje riskinin informel değerlendirmeleri her bir proje tarafından belirlendiği gibi gerçekleşir. Risk değerlendirmeleri proje planında bazen belirlenmiş olsa da konuyla ilgili yöneticiler nadiren atanır. BT ile ilgili riskler (güvenlik, kullanılabilirlik ve bütünlük) projeden projeye bazen değerlendirilir. Günlük operasyonları etkileyen BT ile ilgili riskler nadiren yönetim toplantılarında ele alınır. Risklerin dikkate alındığı durumlarda, azalma tutarsızdır. BT risklerinin önemi ve dikkate alınması gerekliliği konusunda gelişen anlayış vardır.

“2” Tekrarlanabilir ama sezgisel: Gelişen risk değerlendirmesi yaklaşımı vardır ve proje yöneticilerinin takdirine bağlı olarak uygulanmaktadır. Risk yönetimi genellikle yüksek bir düzeyde ve genellikle sadece büyük projelere veya problemlere yanıt olarak uygulanır. Risk azaltma süreçleri risklerin belirlendiği yerde uygulanmaya başlar.

“3” Tanımlı: Organizasyon geneli risk yönetim politikası risk değerlendirmelerinin ne zaman ve nasıl gerçekleşeceğini tanımlar. Risk yönetimi belgelenen tanımlanmış süreçleri takip eder. Risk yönetimi eğitimi tüm personel için vardır. Risk yönetim sürecinin takibi ve alınacak eğitim kararları bireylerin takdirine bırakılmıştır. Risk değerlendirmesi metodolojisi, akla uygun ve işin ana risklerinin tespit edilmesini sağlar. Önemli riskleri azaltmak için genellikle bir süreç kurulur. İş tanımları risk yönetimi sorumluluklarını dikkate alır.

“4” Yönetilmiş ve ölçülebilir: Risk yönetimi ve değerlendirmesi standart prosedürlerdir. Risk yönetim sürecindeki istisnalar BT yönetimine raporlanır. BT risk yönetimi üst düzey sorumluluğa sahiptir. Risk bireysel olarak proje düzeyinde ve düzenli şekilde tüm BT operasyonunda değerlendirilir ve azaltılır. Üst yönetime, iş ve BT ile ilgili risk senaryolarını önemli ölçüde etkileyen BT çevresindeki değişimler konusunda önerilerde bulunulur. Yönetim risk pozisyonunu izleyebilir ve kabul etmeye istekli olduğu konusunda ilgili bilgiye dayalı kararlar verebilir. Tanımlanan tüm risklerin bir sahibi bulunmaktadır ve üst yönetim ve BT yönetimi organizasyonunun katlanabileceği risk seviyesini belirler. BT yönetimi risk değerlemesi ve risk/getiri oranlarının belirlenmesi için standart ölçümleri geliştirir. Operasyonel risk yönetim projesi için bütçe yönetimi riskleri, düzenli olarak yeniden değerlendirilir. Bir risk yönetimi veri tabanı kurulur ve risk yönetimi süreçlerinin bir kısmı otomasyon edilmeye başlanır. BT yönetimi risk azaltma stratejilerini göz önünde bulundurur.

“5” En uygun: Risk yönetimi, yapılandırılmış, örgütsel bir sürecin uygulandığı ve iyi yönetildiği bir aşamaya kadar gelişir. İyi uygulamalar tüm organizasyon çapında uygulanır. Risk yönetimi verilerinin, analizi ve raporlaması oldukça otomatiktir. Rehberlik bu alanda uzmanlaşmış kişilerden alınır ve BT organizasyonu benzer gruplarla tecrübelerini paylaşır. Risk yönetimi tüm iş ve BT operasyonlarına tümüyle entegredir ve BT hizmetleri kullanıcılarını içerir. Yönetim, büyük BT operasyonel ve yatırım kararlarının, risk yönetim planı dikkate alınmadan verildiğinde algılar ve harekete geçer. Yönetim risk azaltma stratejilerini sürekli değerlendirir (ISACA, 2007).

COBIT 4.1’de PO9-BT Risklerinin Yönetimi ve Değerlendirilmesi başlığında yer alırken COBIT 5’teki karşılığı Çizelge 2.6’da gösterilmiştir (ISACA, 2007; ISACA, 2012).

Çizelge 2.6. COBIT 4.1 ve COBIT 5 risk karşılıkları (ISACA, 2007; ISACA, 2012)

COBIT 4.1 Kodu	**Açıklaması**	**COBIT 5 Kodu**
PO9.1	BT Risk Yönetim Çerçevesi	EDM03.02; APO01.03
PO9.2	Risk Bağlamının Oluşturulması	APO12.03
PO9.3	Olay Tanımlaması	APO12.01; APO12.03
PO9.4	Risk Değerlendirmesi	APO12.02; APO12.04
PO9.5	Riske Tepki	APO12.06
PO9.6	Risk Aksiyon Planı Bakımı ve İzlenmesi	APO12.04; APO12.05

Çizelge 2.6’da ifade edildiği şekilde COBIT 4.1’de PO da yer alırken, COBIT 5’te EDM ve APO olmak üzere iki farklı süreçte yer almaktadır.

COBIT bazlı risk yönetimi uygulanırken aşağıdaki hedeflerin göz önünde bulundurulması gerekmektedir (Grünendahl ve Will, 2006: 87-100).

Çizelge 2.7’de riskin dikkate alınacağı planlama ve organizasyon ile ilgili alt süreçler yer almaktadır.

Çizelge 2.7. PO riskle ilgili alt süreçler (ISACA, 2007; Grünendahl ve Will, 2006: 87-100)

COBIT 3	**COBIT 4.1**	**COBIT 3**	**COBIT 4.1**
PO1.5 BT Fonksiyonları için Kısa Dönem Planlaması	PO1.5	PO6.8 Güvenlik ve İç Kontrol Çerçevesi Politikası	PO6.2
PO2.3 Veri Sınıflandırma Şeması	PO2.3	PO8.4 Gizlilik, Entelektüel Mülkiyet ve Veri Akışı	ME3.1
PO2.4 Güvenlik Seviyeleri	PO2.3	PO9.1 BT Risk Değerlendirmesi	PO9.1 PO9.2 PO9.4
PO4.1 BT Planlama ve Yönlendirme Komitesi	PO4.3	PO9.2 Risk Değerlendirme Yaklaşımları	PO9.4
PO4.2 BT Fonksiyonunun Organizasyon İçindeki Yeri	PO4.4	PO9.3 Risk Tanımlanması	PO9.3
PO4.7 Sahiplik ve Bulundurma	PO4.9	PO9.4 Risk Ölçümleri	PO9.1 PO9.2 PO9.3 PO9.4
PO4.8 Veri ve Sistem Sahipleri	PO4.9	PO9.5 Risk Aksiyon Planı	PO9.5
PO4.9 Gözetim	PO4.10	PO9.6 Risk Kabulü	PO9.5
PO4.15 İlişkiler	PO4.15	PO9.7 Seçimleri Koruma	PO9.5
PO6.1 Olumlu Bilgi Kontrol Ortamı	PO6.1	PO9.8 Risk Değerlendirme Komitesi	PO9.1
PO6.2 Politikalar Üzerine Yönetimin Sorumlulukları	PO6.3 PO6.4 PO6.5	PO11.19 Kalite Güvence Değerlendirme Raporları	PO8.2
PO6.5 Politikaların Sürdürülebilirliği	PO6.3 PO6.4 PO6.5		

Çizelge 2.7'de görüldüğü üzere planlama ve organizasyonda; kısa ve uzun dönem planların birbirleriyle olan ilişkileri periyodik olarak güncellenmelidir. Kısa dönem planları içinde yer alan kaynaklar ve değişen durumlar, uzun dönem planlarıyla uyumluluk içinde olmalıdır. Veri sınıflandırmasına uygun olarak güvenlik seviyeleri belirlenmeli ve belirli periyotlarda gereken güncellemeler yapılmalıdır. Risk yönetiminin takibinin sağlanması için komiteler belirli periyotlar ile toplanmalı ve üst yönetime rapor sunmalıdır. Kurumsal yönetim ilkelerine uyulmalıdır. BT güvenliği için alınacak önlemler fayda/maliyet göz önünde bulundurularak yapılmalıdır. Risk değerlendirmesi sistematik bir şekilde yapılmalıdır. Risk belirlenmesi nitel ve nicel değerlendirme ile beyin fırtınası, stratejik plan ve geçmiş dönem denetim verileri gibi bilgilerden yararlanılarak oluşturulmalıdır. Risk kabul seviyesi fayda/maliyet düşünülerek oluşturulmalı ve risk aksiyon planı risk stratejisini

(önleme, transfer, azaltma, kabul) içerecek şekilde kurulmalıdır. Kalite güvence raporları oluşturulmalı ve üst yönetim tarafından onaylanmalıdır.

Çizelge 2.8'de riskin dikkate alınacağı edinim ve uygulama ile ilgili alt süreç yer almaktadır.

Çizelge 2.8. AI riskle ilgili alt süreçler (ISACA, 2007; Grünendahl ve Will, 2006: 87-100)

COBIT 3	**COBIT 4.1**
AI1.8 Risk Analizi Raporu	AI1.2

Çizelge 2.8'de görüldüğü üzere sistem geliştirme yaşam döngüsü metodolojisi; tehditleri, zafiyetleri, bilgi sistemleri gelişimi üzerindeki etkisini, uygulamaları ve iç kontrol sistemini tanımlanan riskleri azaltmayı sağlayacak şekilde oluşturulmalıdır.

Çizelge 2.9'da riskin dikkate alınacağı izleme ve değerlendirme ile ilgili alt süreçler yer almaktadır.

Çizelge 2.9. ME riskle ilgili alt süreçler (ISACA, 2007; Grünendahl ve Will, 2006: 87-100)

COBIT 3	**COBIT 4.1**	**COBIT 3**	**COBIT 4.1**
ME1.4 Yönetim Raporlaması	ME1.5	ME2.3 İç Kontrol Seviye Raporlaması	ME2.2 ME2.3
ME2.1 İç Kontrol İzlenmesi	ME2.2	ME2.4 Operasyonel Güvenlik ve İç Kontrol Güvencesi	ME2.4
ME2.2 İç Kontrollerin Zamanında İşletilmesi	ME2.1		

Çizelge 2.9'da görüldüğü üzere; kurumun hedefleri, planlanan hedeflerin ulaşılabilirliği, performans durumlarını içeren raporlar oluşturulmalıdır. İç kontrol verimliliğini sağlamak için periyodik olarak raporlar oluşturulmalı sapma olan durumlarda iletişim sağlanmalı ve önemli sapmalar üst yönetime raporlanmalıdır.

Çizelge 2.10'da riskin dikkate alınacağı hizmet ve destek ile ilgili alt süreçler yer almaktadır.

Çizelge 2.10. DS riskle ilgili alt süreçleri (ISACA, 2007; Grünendahl ve Will, 2006: 87-100)

COBIT 3	**COBIT 4.1**	**COBIT 3**	**COBIT 4.1**
DS2.6 Hizmet Sürekliliği	DS2.3	DS11.8 Veri Girişi Hata İşleme	AC2 AC4
DS3.5 Proaktif Performans Yönetimi	DS3.3	DS11.10 Veri İşleme, Doğrulama ve Düzenleme	AC4
DS3.6 İş Yükü Tahmini	DS3.3	DS11.11 Veri İşleme, Hata İşleme	AC4
DS5.1 Güvenlik Yönetimi	DS5.1	DS11.12 Çıktı İşleme ve Saklama	AC5 DS11.2
DS5.2 Tanımlama, Doğrulama ve Erişim	DS5.3	DS11.14 Çıktı Dengeleme ve Mutabakatı	AC5
DS5.4 Kullanıcı Hesapları Yönetimi	DS5.4	DS11.15 Çıktı Gözden Geçirmesi ve Hata İşleme	AC5
DS5.7 Güvenlik Gözetimi	DS5.5	DS11.16 Çıktı Raporları İçin Güvenlik Sağlama	DS11.6
DS5.8 Veri Sınıflandırması	PO2.3	DS11.17 İletim Süresince Hassas Bilgilerin Korunumu	AC6 DS11.6
DS5.10 İhlal ve Güvenlik Faaliyetleri Raporları	DS5.5	DS11.18 Hassas Bilgi İmhasının Korunumu	DS11.4 AC6
DS5.12 Yeniden Akreditasyon	DS5.1	DS11.19 Depolama Yönetimi	DS11.2
DS11.2 Yetki Prosedürleri Kaynak Dokümanı	AC1	DS11.20 Saklama Süreleri ve Depolama Koşulları	DS11.2
DS11.3 Veri Koleksiyonu Kaynak Dokümanı	AC1	DS11.23 Yedekleme ve Restorasyon	DS11.5
DS11.4 Hata İşleme Kaynak Dokümanı	AC1	DS11.28 Doğrulama ve Bütünlük	AC6
D11.5 Saklama Kaynak Dokümanı	DS11.2	DS11.30 Depolanmış Verinin Bütünlüğünün Sağlanması	DS11.2
DS11.6 Veri Girişi Yetkilendirme Prosedürleri	AC2	DS12.6 Kesintisiz Güç Arzı	DS12.5
DS11.7 Doğruluk, Tamamlama ve Yetkilendirme Prosedürleri	AC3	DS13.3 İş Çizelgesi	DS13.2

Çizelge 2.10'da görüldüğü üzere; hizmet sürekliliğini sağlamak için tedarikçilerle olan anlaşmalara, yasal düzenlemelere uyulmalıdır. Kapasite tahminleri, problemler ortaya çıkmadan önce periyodik olarak yapılarak oluşturulmalı ve yönetilmelidir. BT Güvenlik Planı değişen koşullar altında sürekli güncellenmeli ve takibi sağlanmalıdır. Veriler için yetki doğrultusunda gizlilik, bütünlük, erişilebilirlik kurallarına uygun olarak yönetimini sağlayacak prosedürler ve geri dönüşüm planları oluşturulmalıdır. İş, süreç, görev planlamaları yetkili kişiler tarafından yönetilmeli ve düzenlenmelidir.

2.2.5. ISO 31000

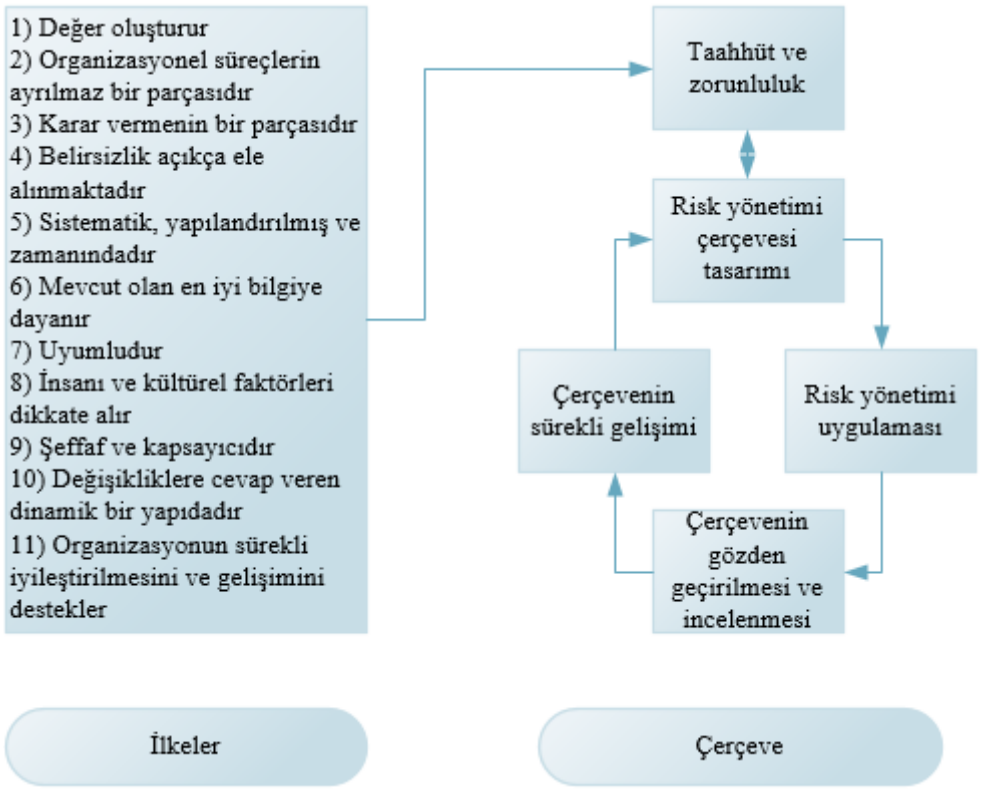
ISO 31000 risk yönetimi genel bir rehber niteliğindeki ülkeler arası bir standarttır. Kamu veya özel sektör fark etmeksizin herhangi bir kuruma uygulanabilmektedir. ISO 31000 ilkeler, çerçeve ve süreç olmak üzere üç bölümden oluşmaktadır (ISO, 2009).

ISO 31000 risk yönetimi ilkeleri, çerçevesi ve süreci Şekil 2.8 ve Şekil 2.9'da gösterilmiştir.

ISO 31000'e göre risk yönetimi başarısının sağlanması için uyulması gereken ilkeler bulunmaktadır:

- Risk yönetimi; insan sağlığı ve güvenliği, proje yönetimi ve operasyonel verimlilik, düzenlemelere uyumluluk gibi pek çok alanda değer oluşturur ve korur.
- Risk yönetimi, stratejik planlama, projeler ve değişiklik yönetimi gibi organizasyonel süreçlerin ayrılmaz bir parçasıdır.
- Risk yönetimi; karar vericilerin bilinçli seçimler yapması aksiyon önceliklendirmesi gibi kararları vermelerini sağlamaktadır. Sürekli, karşılaştırılabilir ve güvenilir sonuçlar elde etmek için sistematik, yapılandırılmış ve zamanında bir yaklaşıma sahiptir.
- Risk yönetimi; girdiler, geçmiş veriler, gözlem ve tahminler gibi konularda mevcut olan en iyi bilgilere dayanmaktadır.
- Risk yönetimi, insan faktörünü dikkate almaktadır.
- Risk yönetimi, değişime karşı duyarlı ve dinamik bir yapıdadır ve organizasyonun sürekli gelişimini desteklemektedir.

Çerçeve yapısında ise; taahhüt ve bağlılık, verimli bir risk yönetim süreci geçirmek için yönetim güçlü ve devamlı bir taahhüt vermelidir.

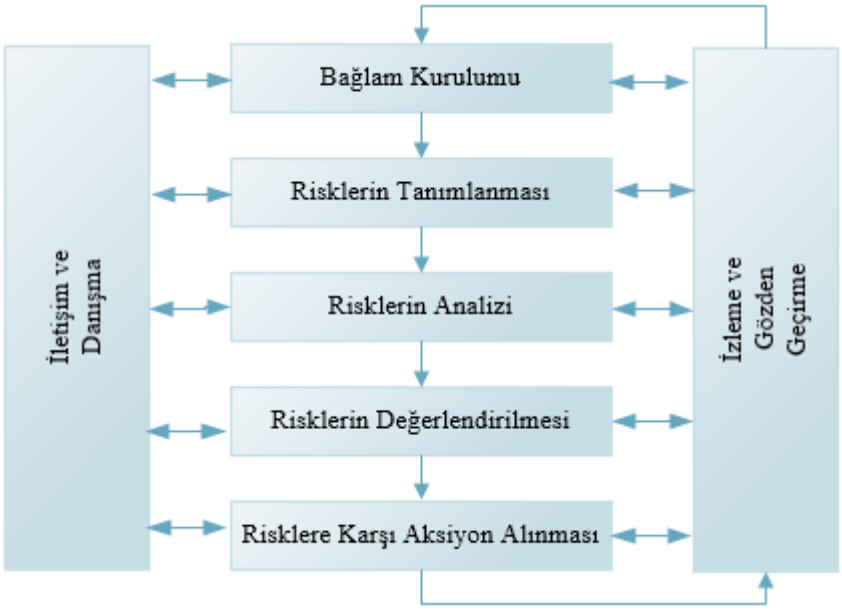


Şekil 2.8. ISO 31000 çerçevesi ve ilkeler (ISO, 2009)

Şekil 2.8'de görüldüğü üzere risk yönetimi çerçevesi tasarımı yedi bölümden oluşmaktadır.

Yönetim çerçevesi tasarımı bölümleri; organizasyonu ve organizasyonun iç ve dış kapsamının belirlenmesi, organizasyonun hedefleriyle uyumlu risk yönetimi politikasının oluşturulması, risk yönetimi süreçlerini yönetirken yapılan kontrol faaliyetlerinin hesap verilebilirliğinin sağlanması, tüm organizasyon uygulamalarının ve süreçlerinin entegrasyonunun sağlanması, organizasyonun risk yönetimi için uygun kaynak tahsis etmesi, risk sahipliği ve sorumluluğu sağlamak adına kurum içi iletişim ve raporlama yöntemlerinin kurulması, planların uygulanabilirliği için dış paydaşlarla olan iletişimin kurulmasıdır.

Risk yönetiminin uygulanması risk yönetimi çerçevesi ve süreçlerinin uygulanması olmak üzere ikiye ayrılmaktadır. Organizasyonel performansı desteklemek için çerçevenin sürekli gözden geçirilmesi ve izlenmesi ve çerçevenin sürekli gelişimi sağlanmalıdır.



Şekil 2.9. Risk yönetimi süreçleri (ISO, 2009)

Şekil 2.9'da görüldüğü üzere risk yönetimi süreci yönetimin ayrılmaz bir parçasıdır. Risk yönetimi sürecinin her aşamasında iç ve dış paydaşlar ile iletişim ve danışmanlık ilişkisi bulunmalıdır. Organizasyonun hedeflerine ulaşmak için iç ve dış çevresini, risk yönetimi süreçlerini, risk kriterlerini belirlemesi gerekmektedir. Risk değerlendirme bölümü riskin belirlenmesi, analizi, ölçümü, riske tepki, izleme ve gözden geçirme ve raporlama aşamalarından oluşmaktadır.

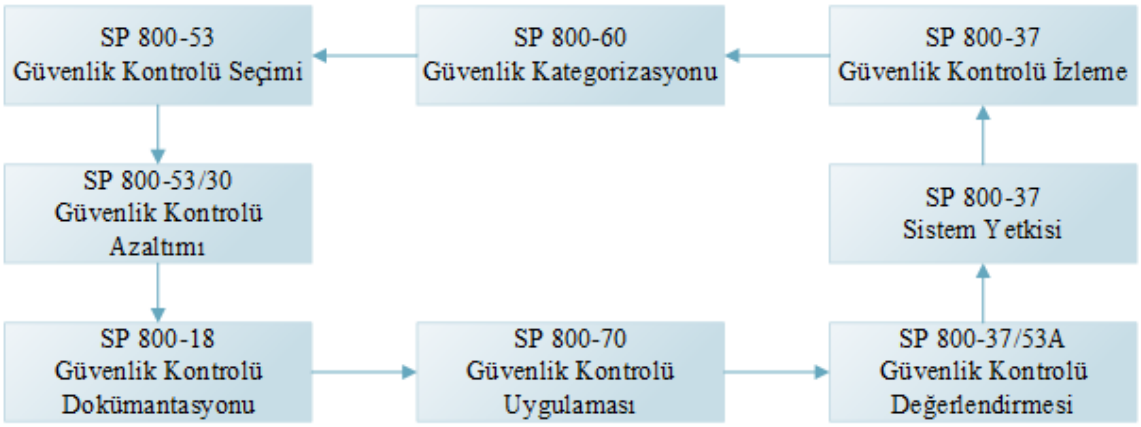
2.2.6. NIST SP 800

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), risk yönetimi sürecini detaylı olarak üç yayınında açıklamıştır. NIST SP 800-30, Risk Değerlendirmesi için Kılavuz, sistem gelişimi yaşam döngüsüne risk yönetiminin nasıl uyumlu olacağı ve risk değerlendirmenin ve risk azaltmanın nasıl olacağı ile ilgilidir.

NIST SP 800-37, Bilgi Sistemleri ve Organizasyonlar için Risk Yönetimi Çerçevesi, organizasyonel riskler ve risk değerlendirme süreci anlatılmaktadır. NIST SP 800-39, Bilgi Güvenliği Risklerinin Yönetimi, kurumlara organizasyon çapında çok katmanlı (organizasyon, hedef ve iş süreçleri, sistem) risk yönetimini sunmaktadır (Broad, 2013: 24).

Potansiyel etki ve kayıplar göz önünde bulundurularak bilgi sistemlerinin kategorilere ayrılması, bilgi sistemlerini korumak için minimum güvenlik kontrollerinin

seçilmesi, organizasyon ihtiyaçlarını ve tehditleri önlemek için en az kontrol seviyesinde risk değerlendirmesinin yapılması, planlanan güvenlik kontrollerinin dokümantasyonu, bilgi sistemlerine güvenlik kontrollerinin uygulanması, güvenlik kontrollerinin doğru şekilde uygulanması ve güvenlik gereksinimlerini gidermedeki etkisinin değerlendirilmesi, bilgi sistemleri süreçlerinin yetkilendirilmesi, güvenlik kontrollerini etkileyen değişikliklerin takibinin yapılmasıdır. NIST SP 800'ün risk yöntemiyle ilgili olan dokümanları Şekil 2.10'da yer almaktadır (Ross, 2004).



Şekil 2.10. NIST risk yönetimi çerçevesi (Ross, 2004)

NIST SP 800-39 risk yönetimini aşamalı bir şekilde tanımlamıştır. Bunlar; bilgi ve bilgi sistemlerinin amaç ve etkilerine göre sınıflandırılması, risk azaltmak için güvenlik kontrollerinin seçilmesi ve dokümantasyon yapılması, altyapıyı destekleyici ve güvenliği sağlayıcı ve etkinliği belirleyici kontrollerin uygulanması, bilgi sistemlerinin ve operasyonel çevrenin yönetilmesi ve izlenmesidir (Kouns ve Minoli, 2010: 35).

NIST SP800-30 risk değerlendirme aşamaları Çizelge 2.11'de gösterilmiştir (Stoneburner, Goguen ve Feringa, 2002).

Çizelge 2.11. NIST SP800-30 risk değerlendirme aşamaları (Stoneburner ve diğerleri, 2002)

	Girdi	Aşama	Çıktı
1	Donanım, yazılım, sistem ara yüzleri, insan, misyon	Sistem Karakteristiğinin Belirlenmesi	Sistem sınırı ve fonksiyonu, sistem ve veri kritikliği, sistem ve veri duyarlılığı
2	Saldırı geçmişi, kitle iletişim araçları	Tehditlerin Belirlenmesi	Tehdit ifadesi
3	Eski risk değerlendirmeleri, denetçi yorumları, güvenlik gereksinimleri, test sonuçları	Zafiyetlerin Belirlenmesi	Potansiyel açıklıkların listesi
4	Mevcut kontroller, planlanan kontroller	Kontrol Analizinin Yapılması	Mevcut ve planlanan kontrollerin listesi
5	Tehdit kapasitesi, zafiyetler, mevcut kontroller	Olasılıkların Belirlenmesi	Olasılıkların derecesi
6	Hassas ve kritik veriler, etkinin derecesi	Etki Analizinin Yapılması (Gizlilik, Bütünlük, Erişilebilirlik)	Etkilerin derecesi
7	Tehdidin olma olasılığı, etki şiddeti, mevcut ve planlanan kontrollerin yeterliliği	Risklerin Belirlenmesi	Riskler ve risk seviyeleri
8		Kontrol Tavsiyelerinin Belirlenmesi	Tavsiye edilen kontroller
9		Sonuçların Raporlanması	Risk değerlendirme raporu

Çizelge 2.11'de görüldüğü üzere NIST SP800-30 girdi, aşama ve çıktı olmak üzere dokuz aşamalıdır. Süreç; sistem karakteristiğinin belirlenmesi, tehdit, zafiyet, kontrollerin belirlenmesi, olasılıkların belirlenmesi, etki analizinin yapılması, riskler, kontrol tavsiyeleri ve sonuçlar aşamalarından oluşmaktadır. Aşamaya uygun girdiler kullanılarak risk yönetimi dokümantasyonu olarak çıktılar meydana gelmektedir. En son olarak risk değerlendirme raporu oluşmaktadır.

2.2.7. ITIL

Bilgi Teknolojisi Altyapı Kütüphanesi (ITIL), BT'yi bir hizmet yönetimi olarak ele almaktadır. Hizmet stratejisi, hizmet tasarımı, hizmet geçişi, hizmet operasyonu, Sürekli hizmet iyileştirme olarak ayırmaktadır (Workman, Phelps ve Gathegi, 2013: 84-85).

Hizmet Stratejisi: Kimlerin hangi hizmetleri alacaklarını ve bu hizmetlerin tedarikinin nasıl ölçüleceğinin tanımlanması, verilen hizmetin değerinin belirlenmesi, hizmet stratejileriyle uyumlu olan kritik başarı faktörlerinin ve stratejileri geliştirenlerin sorumluluklarının tanımlanmasını içermektedir.

Hizmet Tasarımı: Hizmet tasarımı uygularken kullanılacak olan süreçlerin, politikaların ve mimarinin belirlenmesi, hizmet kalitesinin belirlenmesi, tedarikçi gereksinimlerinin belirlenmesi ve Hizmet Tasarım Paketi (SDP) oluşturulması gibi maddeleri içermektedir.

Hizmet Geçişi: SDP'nin uygulanması için gerekli olan kaynakların (değişiklik yönetimi, konfigürasyon, ürün kontrolü, bilgi yönetimi vb.) sağlanmasından oluşmaktadır.

Hizmet Operasyonu; Hizmetlerin destek, bakım işlemlerinin yapılıp kesintilerin ve problemlerin çözümlendiği içinde servis masası gibi mevcut operasyonların yönetildiği yapılar bulunmaktadır.

Sürekli Hizmet İyileştirme: Hizmetlerin sürekli izlenip ölçümlerinin yapılarak uygun değişiklikler ile iyileştirme faaliyetlerinde bulunmaktır.

2.2.8. Basel II

Basel II'de bilgi teknolojilerine yönelik risk yönetimi, operasyonel riskler altında yer almaktadır. Basel Komite operasyonel riski; uygun olmayan ya da işlenmeyen iç süreçler, dış etkenler, insanlar ve sistemler nedeniyle ortaya çıkabilecek zarara uğrama riski olarak tanımlamaktadır. Operasyonel riskler; süreç, dışsal etkenler, insan ve sistem olarak dörde ayrılmıştır.

İnsan faktörü; banka çalışanlarının ve yöneticilerinin eğitim yetersizliği, ihmalkârlık veya görevi kötüye kullanarak zarara uğratma riskidir. Sistem faktörü; teknolojinin gelişimi ve ürün çeşitlendirmesi sonucu bankaların sistemlerini değiştirme ya da mevcut sistemin güncellenmesi sırasında ortaya çıkabilecek risklerdir. Süreç faktörü; bankanın iç kontrol yapılması gerekli olan süreçlerde (satış ve hizmet, proje ve değişiklik yönetimi vb.) karşılaşılabilecek risklerdir. Dışsal faktör; tedarikçilerden, yasa ve politikalardan, doğal afetlerden meydana gelebilecek olan risklerdir. Operasyonel riskler 1990 yılından itibaren fark edilmiş olsa da bankalar kurulumundan itibaren operasyonel risklere maruz kalmaktadır. Basel Komite, bankaların beklenen ve beklenmeyen operasyonel kayıplarının toplamı kadar sermaye ayırmalarını istemiştir (Teker, 2006: 29-38).

Basel II olay çeşitlerinin içinde bilgi teknolojileri ile ilgili vakaların yer aldığı alanlar ve ilgili COBIT süreçleri Çizelge 2.12'de gösterilmiştir (IT Governance Institute, 2007).

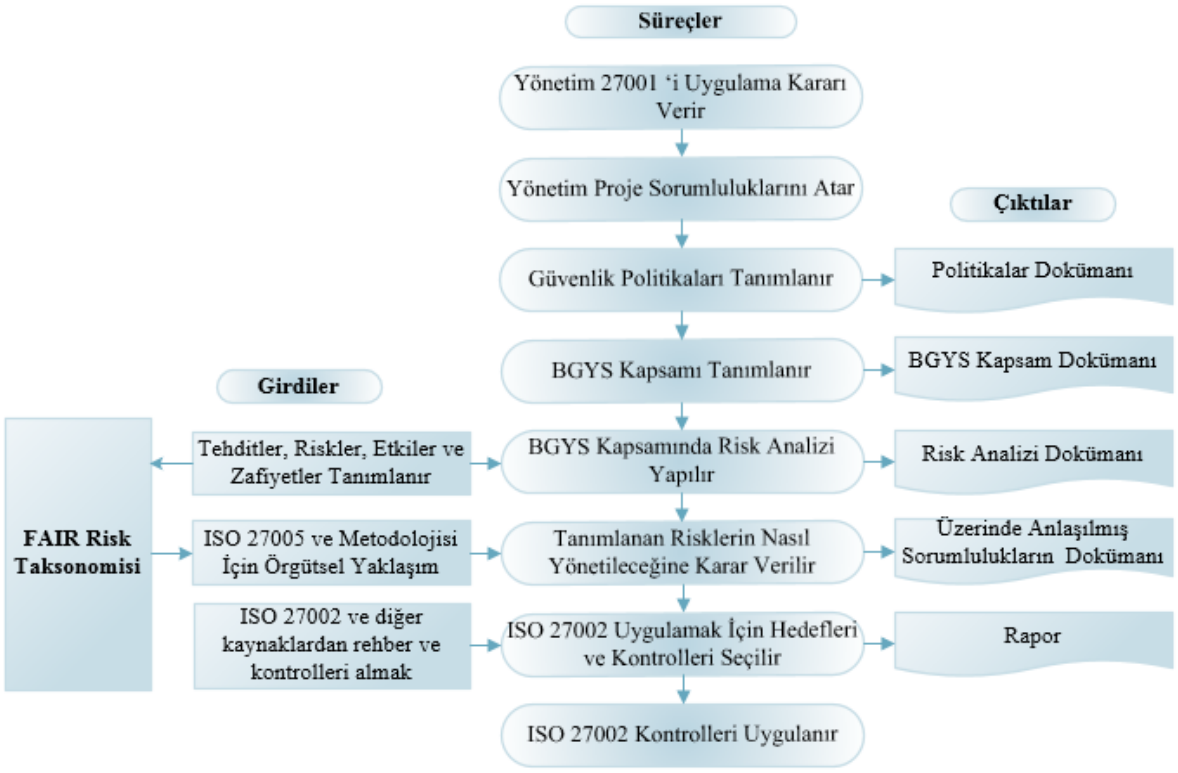
Çizelge 2.12. COBIT ve Basel II ilişkisi (IT Governance Institute, 2007)

Basel II Olay Çeşitleri	BT İle İlgili Alanlar	COBIT Süreçleri
İç dolandırıcılık	o Programların kötü niyetli değişimi o Yetkisiz, değişiklik fonksiyonlarının kullanımı o Kötü niyetli, sistem yönergelerinin değiştirilmesi o Yazılımların lisanssız kullanımı o Yetkisiz erişim verilmesi	PO6 DS5 DS9 DS12
Dış dolandırıcılık	o Uygulama verileri ve sistemin hacklenerek değiştirilmesi o Gizli fiziksel veya elektronik dokümanlara yetkisiz erişim verilmesi o Haberleşme ağlarının dinlenmesi/kesilmesi o Şifrelerin ele geçirilmesi o Virüsler	DS5
İstihdam uygulamaları ve iş ortamı güvenliği	o BT kaynaklarının kötü kullanımı o Güvenlik hassasiyetinin az olması	PO6 DS5
Müşteriler, ürünler ve iş uygulamaları	o Hassas bilginin çalışanlar tarafından yabancılara açıklanması o Üçüncü taraf tedarikçilerin yönetimi	PO6 DS2
Fiziksel değerlerin zarar görmesi	o BT fiziksel altyapısına verilen zararlar	DS12
İş aksamaları ve sistem arızaları	o Donanımda ve yazılımda aksamalar o Haberleşme sorunları o BT çalışanlarının işten ayrılması o Yazılımların/hassas bilgilerin ele geçirilmesi o Bilgisayar virüsleri o Sistemin geri yüklenmesindeki aksaklıklar o Konfigürasyon hatası	AI7 DS3 DS4 DS5 DS9 DS10
Süreç yönetimi	o Elektronik medyaları kullanma hatası o Değişim kontrolünün sağlanamaması o Veri girdi/çıktısında eksiklikler o Operatör hatası o Programlama ve test hatası	AI3 AI6 AI7 DS5 DS10

Çizelge 2.12'de belirtildiği üzere; Basel II'de operasyonel riskler, iç ve dış dolandırıcılık, istihdam, iş ortamı, müşteriler, sistem arızaları, iş aksamaları, süreç yönetimi yönünden ele alınmıştır. COBIT süreçleriyle uyumlu olduğu anlaşılmaktadır.

2.2.9. FAIR

Bilgi Güvenliği Riskleri için Faktör Analizi (FAIR); ISO/IEC 27005, COSO, ITIL, ISO/IEC 27002, COBIT, OCTAVE vb. yaklaşım ve metodolojilerden yararlanarak risk yönetimi çerçevesini oluşturmuştur. Şekil 2.11'de FAIR risk taksonomisi verilmektedir (FAIR, 2010).



Şekil 2.11. ISO 27005, FAIR, ISO 27001 uygulama süreçleri (FAIR, 2010)

Şekil 2.11'de görüldüğü üzere FAIR taksonomisi girdiler, süreçler ve çıktılar olarak işlenmiştir. Girdileri; tehdit, risk, etki, zafiyet, ISO 27005 ve ISO 27002 yaklaşımları ve kontrollerdir. Süreçleri, uygulama kararının verilmesinden kontrollerin uygulanmasına kadar ki aşamalar oluşturur. Çıktılar; süreçlerde raporlanan dokümanlardır.

2.3. Risk Yönetimi Metodolojileri

Risk yönetimi metodolojileri organizasyonun yapısına uygun olarak seçilmelidir. Uygunluğu belirlerken beş noktaya dikkat etmek gerekmektedir (Vorster ve Labuschagne, 2005).

Risk analizinin tek bir varlığa ya da varlık grubuna hitap etmesi: Tek bir varlığın risk analizi zaman alıcı olabilmekte çoğu durumda grup halinde analiz etmek verim sağlamaktadır. OCTAVE yönteminde tek bir varlığın risk analizi yapılırken Risk Analizinin Maliyeti (CORA) yönteminde grup olarak yapılmaktadır.

Risk analizinin uygulandığı yer: Risk analizinin hangi aşamada yapılacağını açıklamaktadır. Risk analizinin yapılabilmesi için yöntemden yönteme farklılık gösteren bilgi değerlendirme süreci vardır. Zaman yönünden kısıtlama yoksa ve risk analizinde doğruluk önemliyse ISRAM kullanılabilir. Zaman yönünden kısıtlama bulunmaktaysa CORA kullanılabilmektedir.

Risk analizini uygulayan insan niteliği: Analizciler iç veya dış kaynaktan karşılanabilir. Dış kaynaktan karşılandığında ek maliyet gerektirir; fakat uzmanlık seviyeleri yüksektir. İç kaynaktan karşılandığında ek bir maliyet gerektirmez; fakat uzmanlık seviyeleri düşük olabilmektedir. OCTAVE yöntemi için iç kaynaktan yararlanılabilir.

Kullanılan ana formül: Basit veya karmaşık formül kullanılarak sonuçların güvenilirlik bakımından değerlendirilmesidir. OCTAVE yöntemi basit hesaplama içerirken ISRAM yöntemi karmaşık hesaplamayı kullanmaktadır.

Yöntem sonucunun yakın ya da tamamen doğru olması: Hesaplamalardaki sayısal değerlerin karşılaştırılmasıyla riski yüksek olanın bulunmasıdır. OCTAVE niteliksel hesaplama yaptığı için sonuçları arasında benzer değerler bulunmaktadır.

Risk analizi için diğer bir yöntem ise; evet(1)/hayır(0) cevapları verilerek en uygun yöntemin bulunmasıdır. Yöntemde; varlıkların önem dereceleri, maliyetin yüksek/düşük olması, güncellenebilirlik, detaylı raporlamaya ihtiyaç olması, zaman gereksinimi, yöntemin satın alma sonrası bakım durumu vb. sorular ile değerlendirilerek organizasyon için en uygun modelin seçilmesidir. Toplam değeri en büyük olan risk analizi metodu seçilmektedir (Aktaş ve Soğukpınar, 2010).

2.3.1. CRAMM

Merkezi Bilgisayar ve Telekomünikasyon Ajansı (CCTA) tarafından Risk Analizi ve Yönetimi Yöntemi (CRAMM) 1980'li yıllarda İngiltere'de geliştirilmiş ve Birleşik

Krallık'ta önemli bir yöntem haline gelmiştir. Yöntem risk azaltmayı amaçlamaktadır. Varlıkların tanımlanması, zafiyetler, tehditler ve olasılıklara uygun olarak risk hesaplamasının yapılmasını sağlamaktadır. Bilgi teknolojileri sistemlerinin çeşitliliği ve karmaşıklığı nedeniyle her bir organizasyon için uygulama kodunu değiştirmeye gerek olmadan dinamik bir şekilde uyarlanması zorunludur.

Risk tahmin yöntemi, risk analizi sürecinde önemli bir yere sahiptir. Farklı zafiyet ve tehditlere sahip risk ile ilişkilendirilen farklı varlıkların sayısı ve sınıflandırılması risk analizi sürecinde elde edilmektedir. ISO/IEC 17799 (ISO 27001)'a uyum sağlamaktadır (Melo ve Gondim, 2012: 243). Büyük organizasyonların kullanımına uygundur (ENISA, 2006).

2.3.2. COBRA

COBRA, Danışma, Nesnel ve Çift Fonksiyonlu Risk Analizi anlamına gelmektedir (The Security Risk Analysis Directory). Birleşik Krallık'ta bir sistem güvenliği şirketi tarafından 1990'lı yıllarda geliştirilmiştir. COBRA yöntemiyle tüm tehdit ve zafiyetlerin önemliliği değerlendirilir ve uygun çözümler üretilir. İş birimi için tanımlanan riskleri potansiyel etkilerle otomatik olarak ilişkilendirir. Belirli bir alan veya konu, herhangi bir etki ilişkisi olmadan bağımsız bir şekilde incelenebilmektedir. ISO 17799 (ISO 27001)'a uyum sağlamaktadır (ENISA, 2006).

2.3.3. CORAS

Kritik Güvenlik Sistemlerinin Risk Değerlendirmesi (CORAS) yöntemi 2003 yılında birkaç Avrupa şirketi tarafından oluşturulmuştur. CORAS metodolojisi terminoloji, kütüphane, metotlar ve yazılım araçları olmak üzere dört ana unsurdan oluşmaktadır. Terminoloji; güvenlik, risk analizi ve dokümantasyon üzerine tanımlamaların yapılmasıdır. Kütüphane; varlıkların, depolama durumlarının ve sistemlerin sınıflandırmasından oluşur. Metotlar; risk analizi prosedürlerinde kullanılan süreçleri ve dilleri içerir. Yazılım araçları; metotların uygulanması için gerekli olan araçlardır. Risk analizinde birleşik modelleme dili (UML) modelleme kullanılmaktadır. Geçmişe dayalı risk değerlendirmesi depolama ile yapılabilmektedir (Melo ve Gondim, 2012: 241-242).

2.3.4. EBIOS

EBIOS, Merkezi Bilgi Sistemleri Güvenlik Bölümü tarafından Fransa'da geliştirilmiştir. Kullanıcıların tüm risk analizi ve yönetimini aşamalı olarak üretmesini sağlamaktadır. Çalışma sonuçlarının kayıt altına alınmasıyla birlikte özet belgelerin üretilmesini sağlar. ISO 13335, ISO 15408 ve ISO 17799 ile uyum göstermektedir.

EBIOS; bağlamsal çalışma, güvenlik ihtiyaçlarının ifadesi, riskin belirlenmesi, güvenlik hedefleri ve güvenlik gereksinimlerinden oluşmaktadır. Bağlamsal çalışma; hedeflenen sistem, genel bilgilerin vb. tanımlanmasıdır. Güvenlik ihtiyaçlarının ifade edilmesi; risk tahmini ve risk kriterlerinin tanımlanmasıdır. Riskin belirlenmesi; tehdit kaynaklarının ve zafiyetlerin belirlenmesi, tehditlerin kayıt altına alınmasıdır. Güvenlik hedeflerinin belirlenmesi ve güvenlik gereksinimlerinin belirlenmesi diğer bileşenleridir (Ebios).

2.3.5. MEHARI

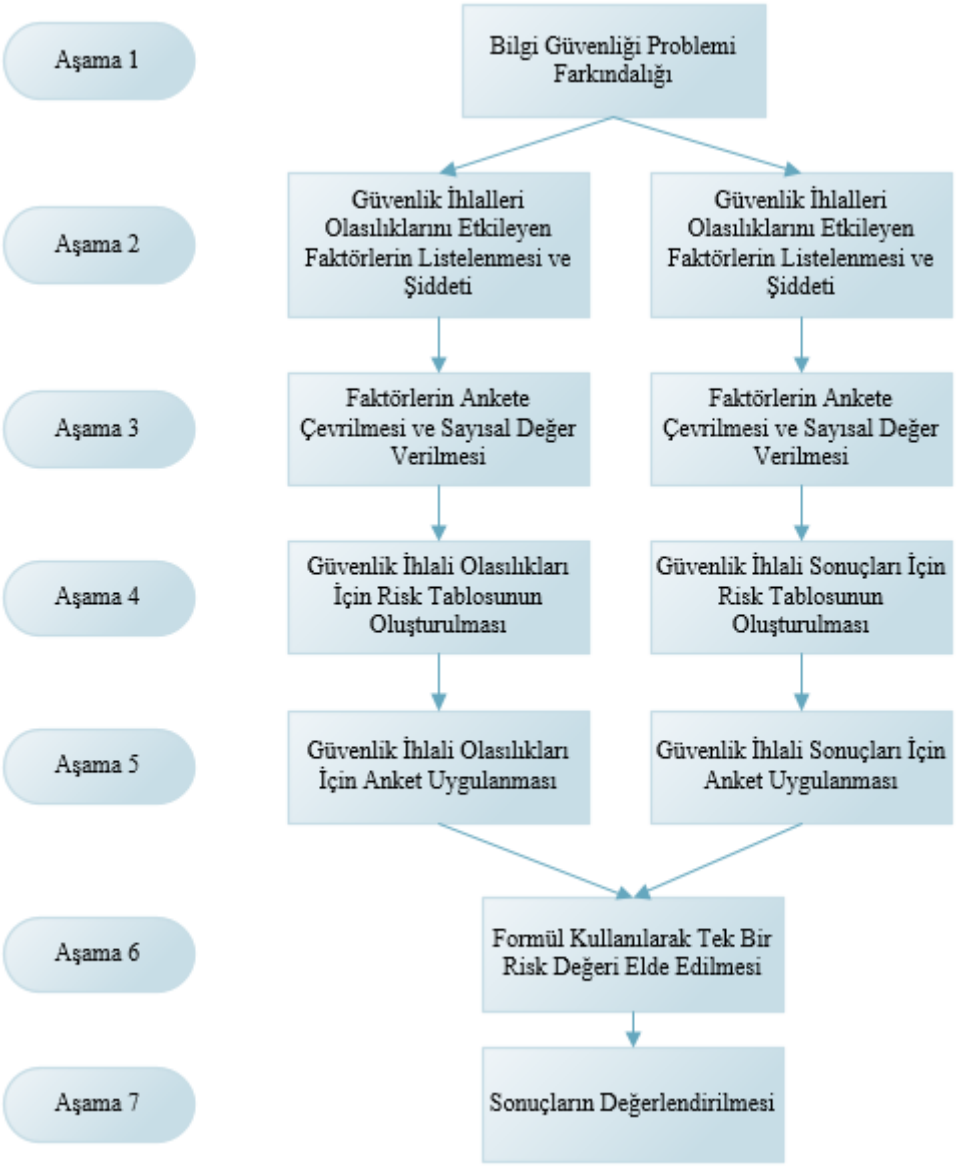
Uyumlaştırılmış Risk Analizi Yöntemi (MEHARI), Fransa kaynaklı Fransa Bilgi Güvenliği Kulübü (CLUSIF) tarafından 1996 yılında geliştirilmiştir. MEHARI, ISO 27001 ve 27005 ile uyumludur.

MEHARI yapısında; bağlamın kurulması, pay analizleri ve varlıkların sınıflandırılması, risk tanımlama, risk analizi, risk değerlendirme aşamaları bulunmaktadır. Bağlamın kurulmasında; tüm organizasyonu veya organizasyon içindeki bir bölümü kapsam ve sınırlar belirlenerek ele alınır. Pay analizleri ve varlıkların sınıflandırılmasında; işlevsizliğin sonuçları düşünülerek varlıklara hizmetler, veriler, düzenlemelere uyumlu bir şekilde değer verilir. Risk tanımlamada; gizlilik, bütünlük, erişilebilirlik dikkate alınarak varlık sınıflandırması yapılır ve varlık değeri belirlenir. Risk analizinde, varlıklar ve çeşitli tehditler için risk senaryoları oluşturulur. Risk değerlendirme; risk ölçümü, riske tepki, risk kabulü, risk iletişimi olmak üzere dört aşamada gerçekleşmektedir (Mehari).

2.3.6. ISRAM

Bilgi Güvenliği Risk Analizi Yöntemi (ISRAM) günümüz güvenlik ihtiyaçlarını karşılamak için kurulmuş olan bir yazılım ile desteklenen nicel bir risk analizi yöntemidir.

Şekil 2.12'de ISRAM için akış diyagramı verilmektedir (Karabacak ve Soğukpınar, 2005).



Şekil 2.12. ISRAM akış diyagramı (Karabacak ve Soğukpınar, 2005)

Şekil 2.12'de görüldüğü üzere bilgi güvenliği probleminin fark edilmesiyle başlayan süreç güvenlik ihlalleri olasılıklarını etkileyen faktörlerin belirlenmesi ve ağırlığının ölçülmesi ve faktörlerin ankete çevrilerek sayısal değerler verilmesi, güvenlik ihlali olasılıkları ve sonuçları için iki farklı risk tablosunun oluşturulması ve bunlar için anket uygulanması, iki sonucun birleştiği bir formül ile risk değerinin bulunması ve sonuçların değerlendirilmesi aşamalarından oluşmaktadır.

2.3.7. OCTAVE

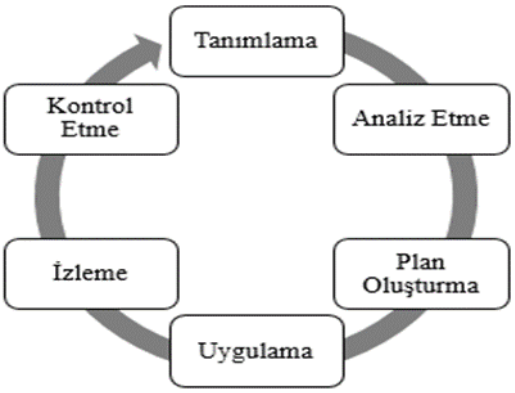
Operasyonel Kritik Tehdit, Varlık ve Zafiyet Değerlendirmesi (OCTAVE), 2003 yılında ISO 27002 örnek alınarak Carnegie Mellon Üniversitesi tarafından geliştirilmiştir (Melo ve Gondim, 2012, 240-242). OCTAVE için risk değerlendirme aşamaları Çizelge 2.13'te gösterilmiştir (Ritchie, 2013).

Çizelge 2.13. OCTAVE risk değerlendirme aşamaları (Ritchie, 2013)

Aşama	Maddeler
1	Risk değerlendirme kriterinin oluşturulması
2	Bilgi varlıkları envanteri profilinin geliştirilmesi
3	Bilgi varlıklarını içeren envanterin oluşturulması
4	İlgili alanların belirlenmesi
5	Tehdit senaryolarının belirlenmesi
6	Risklerin belirlenmesi
7	Risk analizinin yapılması
8	Risk azaltma yaklaşımlarının seçilmesi

Çizelge 2.13'te görüldüğü üzere kriterin oluşturulmasıyla başlayan süreç, varlık envanterinin, senaryoların geliştirilmesi, risk analizi ve risk azaltma yaklaşımlarının uygulanmasıyla sonlanır.

OCTAVE, örgütsel, teknolojik ve stratejik olmak üzere üç ana unsurdan oluşmaktadır. Örgütsel; risk yönetimi ekibi oluşturulur ve organizasyon çapında bilgi varlıkları listesi çıkartılır. Her bir varlık için tehdit ve zafiyetleri içeren risk profili çıkartılarak BT altyapısının alınacak olan kontrol ve önlemler olarak tanımlanmasını sağlar. Teknolojik; örgütsel alandaki bilgiler kullanılarak güvenlik ihlali olduğunda hangi varlıkların kurum için daha fazla öneme sahip olduğu önceden tanımlanmış kriterler ile ölçülerek belirlenir ve sonra her bir kritik varlık için zafiyetleri raporlanır. Stratejik; kritik varlıklardaki riski azaltmak için ISO 27001'e uyumlu güvenlik politikaları ve stratejileri geliştirilerek gerekli önlemler ve güvenlik kontrolleri oluşturulur. Şekil 2.13'te OCTAVE döngüsü verilmiştir (Melo ve Gondim, 2012: 240-242).



Şekil 2.13. OCTAVE döngüsü (Melo ve Gondim, 2012: 240-242)

Şekil 2.13'te görüldüğü üzere OCTAVE metodolojisi, sürekli değişen ve gelişen BT altyapısı, iş süreçleri ve güvenlik gereksinimleri nedeniyle yaşayan bir döngüdür belirli periyotlarda gerekli güncellemelerin yapılması gerekmektedir.

2.3.8. TIRM

Toplam Bilgi Risk Yönetimi (TIRM) süreci; bağlamın kurulması, risk değerlendirmesi ve riske tepki olmak üzere üç bölümden oluşmaktadır (Borek, Parlikad, Webb ve Woodall, 2013: 61-155).

Bağlamın kurulması

- TIRM süreciyle ilgili hedeflerin, kapsam ve sorumlulukların belirlenmesi: Organizasyon içinde risk yönetimine ilişkin motivasyonun bulunması, iş süreçleriyle ilgili hedeflerin belirlenmesi, risk yönetimi sürecinin kapsamının belirlenmesi, organizasyon içindeki sorumlulukların belirlenmesi, risk yönetimi sürecinin diğer iş birimleriyle olan bağlamının belirlenmesi oluşturur.
- Dış çevrenin kurulumu: Sosyal ve kültürel çevrenin araştırılması, düzenlemelerin ve yasaların araştırılması, finansal durumun araştırılması, teknolojik ve ekonomik ilerlemelerin araştırılması, doğal afetler yönünden çevrenin araştırılmasıdır.
- Organizasyonun analizi: Organizasyon modelinin belirlenmesi, iş süreçlerinin belirlenmesi, organizasyonel yapının ve kültürün belirlenmesidir.
- İş hedeflerinin, ölçüm ve risk kriterlerinin belirlenmesi: İş hedeflerinin belirlenmesi (operasyonel verimlilik, müşteri tatmini), ölçüm birimlerinin ve iş hedeflerine olan etkilerinin belirlenmesi, risk kriterlerinin (yüksek, orta, düşük) belirlenmesidir.

- Bilgi ortamının farkındalığı: BT sistemlerinin ve veri tabanının değerlendirilmesi, benzer bilgi yönetimi süreçlerinin değerlendirilmesi, bilgi yönetimi ve kalite ile ilgili araştırma yapılmasıdır.

Risk değerlendirmesi

- Her bir iş sürecindeki görevlerin analizi: İş süreçlerindeki tüm görev ve sorumlulukların tanımlanması, her bir görevin tanımlanması, görev sürelerinin belirlenmesidir.
- Her görev için gerekli olan bilgilerin incelenmesi: Görev için gerekli olan varlıkların belirlenmesi ve açıklanmasıdır.
- Görevler yerine getirilirken bilgi kalitesiyle ilgili problemlerin tanımlanması: İş için gerekli olan veri kalitesi ve bilgi varlıklarının değerlendirilmesi, bilginin kalitesiyle ilgili problemlerin tanımlanması, problemlerin gerçekleşme olasılığının tahmin edilmesidir.
- Bilgi kalitesiyle ilgili problemlerin sonuçlarının tanımlanması, her bir sonucun açıklanmasıdır.
- İş hedeflerini etkileyen her bir sonucun tanımlanması, sonuçların tanımlanması ve iş amaçlarına olan etkisinin açıklanması,
- Var olan risk kontrollerinin incelenmesi,
- Her bir sonucun etki ve olasılığının tahmin edilmesi,
- Sonuçların doğrulanması,
- Bilgi risklerinin derecelendirilmesi ve değerlendirilmesi: Her bir problem için toplam risk hesabının yapılması, risk kriterlerini kullanarak risklerin değerlendirilmesi ve derecelendirilmesidir.

Risk tedavisi

- Bilgi kalitesiyle ilgili problemlerin nedenlerinin analizi; problemlerin nedenlerinin ve problem derecelerinin belirlenmesidir.
- Tedavi seçeneklerinin tanımlanması,
- Tedavi seçeneklerinin maliyet, fayda ve risk yönünden tahmini; maliyet, fayda ve risk yönünden risk tedavi seçeneklerinin tahmin edilmesi ve her bir risk tedavi seçeneği için uygulamanın yapılmasıdır.

- Tedavinin seçilmesi ve değerlendirilmesi,
- Paydaşlar ile sonuçların paylaşılması,
- Risk tedavi planlarının geliştirilmesi, uygulanması ve verimliliğinin doğrulanmasıdır.

2.4. Risk Yönetimi Yazılımları ve Karşılaştırmaları

Risk değerlendirmesi için geliştirilen yazılımlar mevcut olmakla birlikte bu yazılımların kullanımı zorunluluk taşımamaktadır. Yazılımların etkili olabilmesi için kurum yapısına uygun olması gerekmektedir. Yazılımların kullanılması veya kullanılmaması fark etmeksizin risk değerlendirme zaman alan bir uygulamadır (Calder ve Watkins, 2003: 98). Risk yönetimi için yöntemlerin ve yaklaşımların kullandığı yazılımlar olarak; Callio, GStool, Isamm, Proteus, Ra2 ve RiskWatch incelenmiştir. Organizasyonun yapısına uygun olan yazılım seçilebilir.

2.4.1. Callio

Callio Technologies tarafından 2001 yılında Kanada'da geliştirilmiştir. Kullanıcının veri tabanı desteğiyle BGYS sürecinin uygulamasına ve dokümantasyonuna izin veren web tabanlı bir araçtır. ISO 17799 (ISO 27001) ile uyumlu olarak çalışmaktadır (ENISA, 2006).

2.4.2. GStool

GStool, Bilgi Güvenliği Federal Ofisi (BSI) tarafından 1998 yılında Almanya'da, BT Temel Koruma Kılavuzu'nun kullanıcılarını desteklemek için geliştirilmiştir. Kullanıcılara, gerekli bilgiler toplandıktan sonra analizlerin ve verilerin yer aldığı kapsamlı bir raporlama sunmaktadır (ENISA, 2006).

2.4.3. Isamm

Isamm, Telindus tarafından 2002 yılında Belçika'da geliştirilmiştir. Güvenlik yatırımı geri dönüşlerini dikkate alarak ideal risk iyileştirme planının hesaplamasını yapmaktadır. Isamm risk değerlendirmeleri, danışmanlık hizmetleri ve rehber değerlendirmeler olarak önerilmektedir. ISO 17799 (ISO 27001) ile uyumluluk göstermektedir (ENISA, 2006).

2.4.4. Proteus

Proteus, Infogov tarafından 1999 yılında Birleşik Krallık'ta geliştirilmiştir. ISO 17799 (ISO 27001) ve BGYS kurulumu ile uyumludur. Proteus tamamlayıcı ve yapısal bir çerçeve sağlar ve Proteus ile BGYS'deki zayıflıklar belirlenerek boşluk analizi yapılabilmektedir (ENISA, 2006).

2.4.5. Ra2

ISO 17799 ve ISO 27001 standartlarına uyumlu bir yazılım aracıdır. AEXIS tarafından 2000 yılında Almanya'da geliştirilmiştir. Süreçlerdeki her bir aşama için sonuçların raporlanmasına olanak sağlamaktadır. Art of Risk'in bilgi toplama aracıyla risk değerlendirme sürecindeki bilgilerin toplanması sağlanmaktadır (ENISA, 2006).

2.4.6. RiskWatch

RiskWatch ve ISO 17799, RiskWatch şirketinin bilgi güvenliği risk yönetimi konusundaki çözümleridir. RiskWatch Amerika'da geliştirilmiştir. Risk analizi ve zafiyet değerlendirmesi için otomasyon sağlamaktadır. NIST 800-26 standartlarıyla da uyumluluk göstermektedir (ENISA, 2006).

2.4.7. Uygulama yazılımlarının karşılaştırması

Risk yönetiminde kullanılan belli başlı yazılımlar ile ilgili 2009 yılında yapılan bir araştırmada; uygulama türü olarak BGYS ve risk yönetimi ele alınmıştır. Yazılımların yaklaşım, yöntem, risk değerlendirme yaklaşımı, yazılım platformu, veri tabanı, nicel/nitel analiz, araştırma kaynakları gibi yönlerden karşılaştırması Çizelge 2.14'te verilmektedir (Şahinaslan, Kandemir ve Kantürk, 2010). Her iki analizden yararlanan yazılımlarda bulunmaktadır. Organizasyon kendi gereksinimine uygun gördüğü yazılımı seçmelidir.

Çizelge 2.14. Risk yazılımları karşılaştırması (Şahinaslan ve diğerleri, 2010)

Kriter-Nitelik		Art of Risk	Asset Track	Callio	COBRA	CRAMM	EBIOS	GRC	GSTOOL	ISAMM	ISMART	ISMS RAT	OCTAVE	PROTEUS	Real ISMS	RiskWatch	Secure Aware
Uygulama Türü	BGYS	+	+	+							+	+			+		+
	Risk Yönetimi				+	+	+	+	+	+			+	+		+	
Standart Yaklaşımı	BS 7799			+		+											
	ISO 17799	+		+	+		+				+	+				+	+
	ISO 27001	+	+	+		+		+		+	+	+		+	+		+
	ISO 13335-						+										
	BS 25999							+						+			
	SOX							+						+		+	
	COBIT							+						+	+	+	
	ITIL							+									
	HIPAA					+											
	Risk IT							+									
	PCI DSS							+		+				+	+		
	NIST 800-26													+		+	
	Basel II									+							
	GLBA					+											
Kendi Metodolojisi	Diğer (*)				+	+	+		*				+				*
Risk Değerlendirme Yaklaşımı	Nitel Analiz	+	+	+	+	+	+	+	+		+	+	+	+	+		+
	Nicel Analiz					+				+				+	+	+	
Yazılım Platformu	Php		+														
	XML						+										
	Java						+	+			+						
	Ulaşılamadı	+		+	+	+			+	+		+	+	+	+	+	+
Veri Tabanı	SQL Server			+					+						+		
	MS Access	+										+	+				
	My SQL			+										+			
	ORACLE							+							+		
	Ulaşılamadı		+		+	+	+			+	+					+	+
Araştırma Kaynağı	Demo	+	+	+				+			+	+			+		+
	Internet	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Çizelge 2.14'te görüldüğü üzere bankalardaki bilgi teknolojileri için ISO 27001 ve COBIT ön planda olarak incelendiğinde COBIT için; GRC, Proteus, Real ISMS ve RiskWatch kullanılmaktadır. ISO 27001 için; Art of Risk, Asset Track, Callio Secura, CRAMM, GRC, ISAMM, ISMS RAT, Proteus, Real ISMS ve Secura Aware kullanılabilmektedir.

Risk değerlendirme yaklaşım çeşidi olarak daha çok nitel analiz seçilmiştir. Her iki analizden yararlanan yazılımlarda bulunmaktadır.

3. BİLGİ TEKNOLOJİLERİNDE RİSK YÖNETİMİ VE RİSK ANALİZİ

Güvenlik sistemlerinin oluşturulması, donanım ve yazılım satın alarak kurmanın çok ötesindedir. Tüm kurumu kapsayan bir güvenlik politikası oluşturma ile başlayan süreç; doğrulama, yetkilendirme ve erişim kontrolü ile devam eder. Güvenlik politikası; güvenlikle ilgili her türlü süreç tanımlanır ve görev ayrımı yapılır. Doğrulama, kullanıcının belirttiği kişi olup olmadığının kontrol edilmesidir. Yetkilendirme, kullanıcının ne kadarlık bir veri kullanımına kullanım yetkisi olacağının belirlenmesidir. Erişim kontrolü, kullanıcının erişim haklarının belirlenmesidir (Tutar, 2010: 138). Risk yönetiminin yapılabilmesi için gizlilik, bütünlük, erişilebilirlik kavramlarını dikkate alarak güvenlik ve risk politikaları oluşturulmalıdır.

3.1. Risk Yönetiminin Gerekliliği

Risk yönetimi ve yönetim birbirine çok yakın kavramlardır. Yönetim, organizasyonu yönlendiren ve faaliyetlerin kontrolünü sağlamakla görevliyken; risk yönetimi ise; organizasyonun yönlendirilmesini ve faaliyetlerin kontrolünün risk baz alınarak sağlanmasıdır (Lark, 2015).

Günümüz şartlarında sektörel olarak geri kalmamak için güvenlik ve risk kontrolleri en önemli öncelik olmalıdır. Güvenlik; politikaların, prosedürlerin ve teknik ölçümlerin, bilgi sistemlerindeki yetkisiz erişim, yetkisiz değişiklik, hırsızlık veya fiziksel zararı önlemek için kullanılmasıdır. Kontrol ise metotlar, politikalar ve organizasyonel prosedürlerin; varlıkların, kayıtların doğruluğunu, güvenirliliğini ve yönetim standartlarına olan uyumunu sağlamaktadır (K. Laudon ve J. Laudon, 2014: 325).

Dünyada 2001 yılında gerçekleşen Enron skandalı, Türkiye'de ise 2003 yılında Türkiye İmar Bankası'nın çifte kayıt olayı neticesinde bilgi teknolojilerine ait risk kontrolünün gerekliliği ortaya çıkmıştır. Riskler tanımlanır; fakat risk denetimi yapılmazsa sistemin güvenirliliğinden ve verimliliğinden emin olunamaz (Özbilgin, 2003). 2001 yılında Code Red Worm virüsü ilk 14 saatte 359 bin adet sistemde zarara yol açmışken bundan iki sene sonraki Sequel Slammer virüsü, ilk 10 dakikada 75 bin sisteme zarar vermiştir. Şu ana kadar İnternet web serverlerinin en az %85'i bir kere saldırıyla karşılaşmıştır. Bu durum

sadece ekonomik zararı telafi etmek için değil ülkeler arası çapta bilgi güvenliğine karşı bilincin geliştirilmesi gerekliliğini önemli kılmaktadır (Özenç, 2007).

Organizasyon, güvenlik ve bilgi sistemlerinin kontrolünü sağlarken hangi varlıkların korunması gerektiği ve hangi varlıkların zafiyetlere maruz kalabileceğini belirtmelidir. Varlıkları korumak için risk değerlendirme yöntemiyle en verimli kontroller belirlenmelidir. Bilgi varlıklarının değeri, zafiyetlerin derecesi, problemlerin olma sıklığı ve potansiyel zararlar belirlenmelidir (K. Laudon ve J. Laudon, 2014: 341).

Organizasyon için stratejik bir karar olan yeni donanım ve yazılım yapılanmasında doğru tercih yapılmazsa sonuç almak gecikebilmekte veya gerileme gibi operasyonel riskler ile karşılaşılabilmektedir, tercih doğru ise kurum başarısı artacaktır. Projelerde ise; projenin zamanından önce bitirilmesi ya da yetişmemesi, bütçenin yeterli olup olmaması gibi risklerle karşılaşılmaktadır (Airmic, Alarm ve Irm, 2010). Örneğin; riskin gerçekleşme durumunda 500 TL kayıp olacak bir durumu önlemek için yıllık 10 000 TL'lik bir harcama maliyet açısından uygun değildir; fakat riskin gerçekleşme durumunda 5 000 TL bir kayıp için 2 000 TL'lik bir harcama yapılacaksa verimlilik söz konusu olmaktadır.

Risk yönetimi, güvenlik gereksinimlerini belirlerken ve uygularken fayda/maliyet açısından uygunluğunu dikkate alır. Riskleri azaltmak veya yok etmek için alınan her bir önlem belirli bir maliyet gerektirir ve kurumların kaynakları sınırlıdır. Kurumlar, kendileri için gerekli olan önlemleri alırken bu önlemleri almadıkları zamanki riskleri ve maliyeti de dikkate almaları gerekmektedir. İş ve bilgi teknolojileri ile ilgili stratejik kararlar alırken risk yönetiminin önemi büyüktür.

Risk yönetiminin başarılı olabilmesi için; üst yönetimin sorumluluğu alması, risk kontrollerinin geliştirilmesinde ve tehditlerin belirlenmesinde risk yönetimi ekibinin yeterli beceri ve tecrübeye sahip olması, bilgi varlıkları tehditlerini yönetirken risk ekibinin ve iş birimlerinin ortak çalışması, risk değerlendirmenin ve raporlamanın düzenli periyotlar içinde yapılması ve ihtiyaç duyulduğunda toplantıların düzenlenmesi gerekmektedir (Peltier, 2005: 298).

3.2. Risk Yönetimi Politikası Oluşturma

Bilgi güvenliği sadece kurumda bilgi işlem birimini değil tüm kurumu kapsayacak şekilde ele alınmalıdır. Gittikçe artan bilgi hırsızlıkları ve yetkisiz erişimlerle ilgili sorunların üstesinden gelebilmek için güvenlik politikalarının oluşturulması, dokümantasyonun sağlanması ve paydaşlara aktarılması ve bu doğrultuda risk yönetimi politikalarının da oluşturulması gerekmektedir (Ersoy, 2012: 11).

Risk ve bilgi güvenliği politikaları yılda en az bir kere güncellenmeli veya iş sürecinde, risk hesaplanmasında kullanılacak kriterlerde ve risklerde herhangi bir değişikliğe ihtiyaç olduğunda güncellemelerin daha kısa periyotlar halinde yapılması gerekmektedir (Calder ve Watkins, 2008: 70).

Bilgi güvenliği politikası içeriğinde; politikanın yazılışındaki sebeplerin ve risklerin belirtildiği, politika amacının ve kapsamının belirlendiği, politikanın açıklaması, politikanın uygulaması ve yaptırımları, tanımlamalar, düzeltme geçmişi gibi bölümler yer almalıdır (Kalman, 2002).

Risk yönetimi politikasının içeriğinde, risk yönetimi ve iç kontrol hedefleri ve stratejisi, roller, sorumluluklar ve yükümlülükler, dokümantasyon yapılacak belgeler ile ilgili bilgiler, risk kültürünün ve farkındalığını sağlayıcı bilgiler, risk belirleme ve sınıflandırma, risk seviye tanımlamaları, riske tepki bilgileri, risk izleme yöntemi, risk yönetimi için kaynak tahsisi bilgileri ve yıllık bazda risk öncelikleri gibi bilgiler yer almalıdır (Airmic, Alarm, ve Irm, 2010).

3.3. Risk Yönetimi Tanımlamaları

Verilerin paylaşımının yaygınlaşması sebebiyle bilginin göndericiden alıcıya kadar gizlilik içinde, bozulmadan, imha edilmeden, değiştirilmeden, yetkisiz kişilerin eline geçmeden ve bütünlüğü sağlanarak istenilen zamanda ulaşılabilecek şekilde iletilmesi bilgi güvenliği için ana kriterdir (Erol ve diğerleri, 2015).

Donn Parker bilgi güvenliğine aitlik, doğruluk, yararlılık olmak üzere 2002 yılında üç kriter daha eklemiştir (Raggad, 2010: 24-25).

- Gizlilik: Bilginin yetkisiz kişilerin kullanımına açık olmamasının garanti altına alınmasıdır. Sistemlere, yetkisiz veya yetkisiz erişim ile kasten girilmesiyle gizlilik kavramı ihlal edilmektedir. Hackerlerin yetkisiz erişimle ticari sırları öğrenmesi vb. (Kouns ve Minoli, 2010).
- Bütünlük: Bilginin içeriğinin değiştirilmeden, bozulmadan korunmasıdır. Sistemin veya verinin yetkisiz bir şekilde değiştirilmesi veya bozulmasıyla bütünlük kavramı ihlal edilmektedir. Virüslerin kaynak kodu değiştirmesi sonucunda hackerlara yetkisiz erişim verilmesi vb.
- Erişilebilirlik (kullanılabilirlik): Bilginin istenilen zamanda erişilebilir olmasıdır. Yetkili kullanıcının sisteme veya veriye zamanında erişiminin olmaması durumunda erişilebilirlik kavramı ihlal edilmektedir. DOS saldırıları vb. (Kouns ve Minoli, 2010).
- Aitlik: Bilgi kontrolünün ve sahipliğinin sağlanmasıdır (Raggad, 2010).
- Doğruluk: İletimin kaynağının doğru olması ve iletilen dokümanların kaynağının geçerli olmasıdır (Raggad, 2010).
- Yararlılık: Bilginin fayda sağlamasıdır. Örneğin; bilinmeyen bir dildeki mesajın faydasız olması gibi (Raggad, 2010).

3.3.1. Varlık envanterinin oluşturulması ve örnekler

Varlık envanteri; donanım, yazılım, bilgi, alt yapı, personel, süreç vb. bileşenlerden oluşan envanterdir. Varlıklar çok fazla ise varlıklar için ayrı birer tablo oluşturulması gerekir. Donanımsal ve yazılımsal varlıklar için model, seri numarası, lisans bilgisi, yama bilgisi gibi donanıma ve yazılıma özel bilgiler envanterin değerini artıracaktır. Çizelge 3.1'de varlık envanteri örneği yer almaktadır. (Koç F. , 2008).

Varlık değeri hesaplanmasında; gizlilik, bütünlük, kullanılabilirlik değerlerinin kurum tercihine uygun olarak toplamı veya çarpımıyla o varlığa ait varlık değeri bulunmaktadır.

Çizelge 3.1. Varlık envanteri örneği (1) (Koç F. , 2008)

No	Varlık Grubu	Varlık	Varlık Kategorisi	Varlık Sahibi	Adedi	Sahip/Sorumlu	Bulunduğu Yer	Gizlilik	Bütünlük	Erişilebilirlik	Varlık Değeri	Açıklamalar

Çizelge 3.1'de görüldüğü üzere varlık envanteri içeriğinde yazılım veya donanım için üzerinde çalıştığı servisler, varlık grubu (süreç bazlı varlık ya da fiziksel varlık olması), varlık kategorisi, varlığın bulunduğu yer, yedek bilgileri, lisans bilgileri, aitlik, gizlilik, bütünlük, erişilebilirlik gibi değerleri yer almalıdır. Varlık envanteri kalitesi personelin o varlık ile ilgili bilgisi düzeyinde gerçekleşmektedir. Varlık envanterinin kullanışlı olabilmesi için periyodik olarak güncellenmesi gerekmektedir.

Çizelge 3.1'den farklı olarak iş süreçlerinin de yer aldığı teknoloji envanteri örneği Çizelge 3.2'de verilmektedir (Kamu İç Denetim Koordinasyon Kurulu, 2014).

Çizelge 3.2. Örnek varlık envanteri (2) (Kamu İç Denetim Koordinasyon Kurulu, 2014)

Uygulamanın İsmi	Uygulama Açıklaması	Ana İş Süreci	Bilgi Sistemleri Donanımı	İşletim Sistemi ve Versiyonu	Veri tabanı ve Versiyonu	Uygulamanın Kaynağı	Uzaktan Erişim	Açıklamalar	Sistem Sahibi	Unvanı	Bölümü	Telefon	E-posta

Çizelge 3.2'de görüldüğü üzere envanterde uzaktan erişim, uygulama ve veri tabanı ile ilgili bilgiler, sahip/sorumlu bilgileri yer almaktadır.

Fiziksel ve süreç bazlı varlıkları kapsayacak ve risk analizinde kullanılabilecek nitelikte olan detay bilgileri de içeren örnek varlık envanteri Çizelge 3.3'te verilmiştir (Ersoy, 2012).

Çizelge 3.3. Varlık envanteri örneği (3) (Ersoy, 2012)

Özellik	**Açıklama**
Varlık Adı	Veri tabanı sunucusu
Açıklama	X projesi kapsamında 1, 2 uygulamalarının bilgileri saklanmaktadır. Donanımın çalışmaması durumunda X projesini kullanan birimler etkilenmektedir
Konum	Sistem odasında bulunmaktadır
Üzerinde Çalışan Servisler/Donanımlar/Yazılımlar	İşletim sistemi: Y Uygulama: 1 ve 2 uygulamaları ve muhasebe uygulamaları
Yedeğinin Olup/Olmaması	Yedeği bulunmamaktadır
IP Adresi	5.1.2.a
Erişim Bilgileri	Sistem sorumluları tarafından erişim sağlanmaktadır
Sorumlu Personel	Bilgi İşlem Dairesi Başkanı
Yetkili Personel	Sistem Sorumluları
İşletim Sistemi ve Sürümü	Üzerinde çalışan işletim sistemi UNIX Versiyon X.0.2
Kritiklik	Yüksek(5)
Gizlilik	Çok Gizli(5)
Varlık Değeri	25(Kritiklik*Gizlilik)
Maddi Değeri	20 000 TL
Hizmet Verdiği Grup	Bütün kurum personeli

Çizelge 3.3'te görüldüğü üzere varlık envanteri üzerinde çalışan donanım/yazılım, erişim bilgisi, maddi değeri, hizmet verdiği grup ile ilgili bilgilerle detaylandırılmıştır. Bu şekilde bir envanter kullanılması risk analizi yapılırken varlığa ait maliyet hesaplamasının yapılmasına da olanak sağlayacaktır.

Fiziksel ve süreç tabanlı varlıklar belirlenirken ve hesaplaması yapılırken Çizelge 3.4'teki gibi bir anketten faydalanılabilir. Anketler belirli periyotlar halinde iş ve süreç sahiplerince yapılarak yeni varlıkların kaydı ve mevcut varlıklarda meydana gelen değişikliğin izlenmesi yönünden katkı sağlayacaktır (Sağıroğlu, Ersoy ve Alkan, 2007).

Çizelge 3.4. Envanter soruları (Sağıroğlu ve diğerleri, 2007)

Anket Soruları	Cevaplar
Varlık üzerinden kullanılan bilgilerin gizlilik derecesi ne kadardır?	a) Çok Gizli(5) b) Gizli(3) c) Açıklanabilir(1)
Varlığa zarar gelmesi durumunda iş kesilmeleri ne derecede etkilemektedir?	a) Hiç kesinti olmamalı (5) b) Maksimum 24 saat (3) c) 1 günden fazla (1)
Süreçte görevi çalışanın konuya hâkimiyet derecesi nedir?	a) Düşük (5) b) Orta (3) c) Yüksek (1)
Süreçteki personelin yedeği bulunmakta mıdır?	a) Yoktur (5) b) Vardır (1)
Süreç kurum için ne kadar önemlidir?	a) Çok önemli (5) b) Orta (3) c) Önemsiz (1)
Yedekleme yapılmakta mıdır?	a) Hayır (5) b) Evet (1)
Bilginin erişilebilirlik düzeyi nedir?	a) Tüm herkes erişebilir (5) b) Yetkili kişilerce erişilebilir (1)

Çizelge 3.4'te görüldüğü üzere varlığa ait gizlilik derecesi, varlığın iş sürekliliği yönünden önemi, süreç sahiplerinin konuya hakimliği, yedeklilik durumu gibi varlığın niteliği bakımından önemli bilgiler elde edilebilmektedir**.**

3.3.2. Tehdit kategorisi ve tehditler

İller Bankası (İLBANK) BT için tehditleri; çevresel, insan kaynaklı ve teknik olarak kaynağına göre üç gruba ayırmıştır (İLBANK, 2017). Çevresel tehditler; sel, yıldırım, deprem, fırtına, yangın, kemirgen böcekler vb. olarak tanımlanabilir. İnsan kaynaklı tehditler; programcı/sistemci hatası/ihmali, yetkililerin olmaması, hırsızlık, bombalama/sabotaj/patlama, hacker saldırısı vb. olarak örneklenebilir. Teknik tehditler; elektriksel sorunlar, donanım arızaları, yazılım hataları/eksiklikleri, network hataları vb. olarak örneklenebilir.

İç ve dış kaynaklı tehditler olarak ayrıldığında ise: Dış kaynaklı tehditler: Politik ve düzenleyici tehditler; hükümet politikasının değişmesi, yeni mevzuat ve idari düzenlemelerdeki değişiklikler vb. Çevresel/doğal tehditler; yangın, sel ve deprem vb. Ekonomik tehditler; rekabetçi gizli anlaşmalar, parasal dalgalanmalar ve ekonomik krizler vb. Teknolojik tehditler; hackerlık ve sızdırmalar, telekomünikasyon hataları vb. İç kaynaklı tehditler: Stratejik tehditler; yanlış yönlenme, yapısal uyumsuzluk, personel uyumsuzluğu,

yetersiz sermaye ve ürün/hizmet tasarımı vb. Operasyonel tehditler; hedefleri zaman, maliyet ve kalite olarak yetersiz kalması, hassas bilgilere yetkisiz erişim, kazalar ve korunmasız iş koşulları, yönetmelik ihlalleri, bilgi sistemleri hataları, personel dolandırıcılığı vb. (Slay ve Koronios, 2006: 14).

3.3.3. Zafiyet kategorisi ve zafiyetler

Bilgi teknolojilerine ait zafiyetler ve kategorileri Çizelge 3.5'te verilmiştir (Eskiyörük, 2007). Zafiyet kategorisi olarak altyapı ve çevre, donanım, yazılım, haberleşme, dokümantasyon ve insan olarak altı gruba ayrılmıştır.

Çizelge 3.5. Zafiyet kategorileri ve zafiyetler (Eskiyörük, 2007)

Altyapı ve Çevre
Binada yeterli düzeyde fiziksel güvenliğin bulunmaması (kartlı geçiş, alarm, yangın söndürme sistemi)
Bina ve odalara girişte yetersiz fiziksel kontrol (kasten zarar verme)
Deprem bölgesinde bulunan yapılar
Herkesin eriştiği kablosuz ağlar (bilginin açığa çıkması, yetkisiz erişim)
Donanım
Değişim yönetimi eksikliği (kullanıcı hataları)
Periyodik bakım eksikliği (bakım hataları)
Periyodik yenilemenin yapılmaması (donanımların bozulması nedeniyle erişimin durması)
Voltaj değişikliği, ısı, nem ve toza duyarlılık (güç dalgalanmaları, erişim güçlükleri)
Yazılım
Erişim izinlerinin hatalı verilmesi (yetkisiz erişim)
İzinsiz yazılım yüklenmesi (zararlı yazılımlar, yasal gerekliliklere uyum)
Kayıt yönetimi yetersizliği (yetkisiz erişim)
Kimlik tanımlama, doğrulama eksiklikleri (yetkisiz erişim, başkalarının kimliğine bürünme)
Saklama ortamlarının uygun şekilde silinmemesi, imha edilmemesi (verinin ortaya çıkması, yetkisiz erişim)
Şifre yönetimi eksikliği (yetkisiz erişim, başkalarının kimliğine bürünme)
Yama yönetimi yetersizliği (yetkisiz erişim, hassas bilginin açığa çıkması)
Yazılım gereksinimlerinin hatalı veya eksik belirlenmesi (yazılım hataları)
Yazılımların yeterince test edilmemesi (yetkisiz erişim, güvenlik açıklıkları, yazılımların yetkisiz kullanımı)
Haberleşme
Ağ yönetimi eksikliği (trafiğin aşırı yüklenmesi)
Hat üzerinden şifrelerin açık olması (yetkisiz erişim)
Korunmayan haberleşme hatları (haberleşmenin dinlenmesi)
Telefon hattıyla kurum ağına erişim (yetkisiz erişim)
Dokümantasyon
Dokümanların güvenli ortamda saklanmaması (hırsızlık)
Dokümanların imha edilmemesi (hırsızlık, hassas bilginin açığa çıkması)
Dokümanların kontrolsüz bir şekilde çoğaltılması (hırsızlık)
Personel
Donanım veya yazılımın yanlış kullanımı (personel hataları)
Eğitim eksikliği (personel hataları)
Güvenlik farkındalığı noksanlığı (kullanıcı hataları)
İletişim ve mesajlaşma ortamların kullanımı için politika eksikliği (yetkisiz erişim)
İşe alımda yetersiz özgeçmiş incelemesi (kasten zarar verme)

Çizelge 3.5'te belirtildiği üzere altyapı ve çevre de oluşabilecek açıklıklar özellikle fiziki güvenliğin yetersizliği nedeniyle oluşmaktadır. Donanımda, özellikle bakım eksikliğinden kaynaklanan zafiyetler almaktadır. Yazılımda, yetkisiz erişim; haberleşmede, ağ yönetimi eksikliği; dokümantasyonda, dokümantasyon imhası ve saklaması; personelde, eğitim eksikliği ve kasten zarar verme neticesinde zafiyetler oluşmaktadır.

3.3.4. Olasılıkların belirlenmesi

Olasılık değeri üçlü skalada tahmin, olma sıklığı ve gösterge olarak Çizelge 3.6'da gösterilmektedir (Grünendahl ve Will, 2006: 103).

Çizelge 3.6. Üçlü olasılık skalası (Grünendahl ve Will, 2006: 103)

Olasılık		
Tahmin	**Açıklama**	**Göstergeler**
Yüksek	Her yıl olma şansının %25'ten fazla olması	Zaman periyodu (10 yıl) içinde böyle bir olay birkaç kere meydana gelmiştir
Orta	10 yıl içinde meydana gelebilir veya her yıl olma şansının %25'ten düşük olması	Zaman periyodu (10 yıl) içinde böyle bir olay meydana gelmiştir
Düşük	10 yıl içinde meydana gelme olasılığı çok düşüktür olma şansı %2'den düşük olması	Şimdiye kadar böyle bir olay meydana gelmemiştir

Çizelge 3.6'da belirtildiği üzere geçmişte meydana gelen veya gelmeyen durumların sıklığına yönelik tahmin edilmektedir. Orta seviyesindeki tahmin için 10 yıl içinde olayın meydana gelmiş olması ve bu doğrultuda 10 yıl içinde meydana gelmesi ihtimal dahilinde; fakat her yıl meydana gelme olasılığının %25'ten düşük olması gerekmektedir.

Olasılık değeri yedili skalada en küçük değer olan ihmal edilebilir ile en yüksek değer olan aşırıya kadar Çizelge 3.7'de gösterilmektedir (Calder ve Watkins, 2008: 93).

Çizelge 3.7. Yedili olasılık skalası (Calder ve Watkins, 2008: 93)

İhmal Edilebilir	Her beş yılda bir defadan az olması
Çok Düşük	Yılda bir defadan daha az ama beş yılda bir defadan fazla olabilir
Düşük	Yılda bir defadan fazla olabilir ama altı ayda bir defadan az
Orta	Her altı ayda bir defadan fazla olabilir ama ayda bir defadan az
Yüksek	Ayda bir kereden fazla olabilir ama haftada bir defadan az
Çok Yüksek	Haftada bir kereden fazla olabilir ama günde bir defadan az
Aşırı	Günde en az bir kere

Çizelge 3.7'de gösterildiği üzere yedili skala çok detaylıdır, büyük organizasyonlar için veya bilgi teknolojileri kritikliğinin önemli olduğu şirketlerde kullanılması avantaj sağlayacaktır. Orta seviyesindeki bir risk için her altı ayda birden fazla kez olması; fakat ayda bir defadan az olması durumudur.

3.3.5. Risklerin belirlenmesi

BT faaliyetlerinin yürütülmesi sırasında zafiyetlerden dolayı maruz kalınabilecek tehditler BT varlıkları bazında tanımlanır. Varlık envanterinden ve kritiklik oluşturabilecek süreçlerden varlıklar belirlenir ve yazılım, donanım, insan, veri tabanı, altyapı ve tesisat, sunucular vb. olarak varlıklar kategorilere ayrılır. Risklerin belirlenmesinde Kendi-Kendini Değerlendirme Yöntemi uygulanır. Yöntemde, Risk Komiteleri, ilgili BT Müdürleri ve etkilenen süreçlere ilişkin iş birimleri, yürütülen faaliyetlere ilişkin risklerin değerlendirilmesini sağlamaktadır (İLBANK, 2015). Kurum yapısına göre BT risk yönetimi, üst yönetim, farklı birimlerin yöneticileri ve iç kontrol gibi iş birimlerinin katkısıyla oluşur.

Risk yöneticisinin ana görevleri; risklerin tanımlanması analiz ve raporlanması için metodoloji belirlemek, risk uygulamalarında kullanılacak olan zorunlu değişiklikler, ana sözleşmeler ve yeni program faaliyetlerinin oluşturulmasına yardım etmek, iç ve dış personel kaynaklarının tamamlayıcı bir risk kontrol eğitim programından geçmelerini koordine etmek, yöneticiler ve üst yönetim kullanımına sunmak için risk yönetimi politika, prosedür ve rehber hazırlamaktır. Üst yönetim; iç kontrolün sağlanması adına uygun politikalar ve sistemin fonksiyonelliğini ölçmek için kontroller geliştirmelidir. Kurumun içinde olduğu risk boyutunu, hangi risklerin kabul edilebilir olduğunu, risk yönetimi için ayrılacak olan kaynakları belirlemek ana görevleridir (Grünendahl ve Will, 2006: 80-83).

Risklerin işlenmesi; karşılaşılan risklerin ilk defa tanımlanması, yeni oluşan risklerin risk kütüğüne işlenmesi veya önceden artık risk olarak kabul edilen risklerin yeni durumda gerçek bir risk oluşturmasıyla birlikte risk kütüğünün sürekli güncellenmesiyle oluşan risk işleme uygulamasıdır. Risklerin belirlenme şekillerinden mülakatlar ve atölye çalışmaları; özellikle kilit personel olarak seçilmesi gerekli olan kurum içinden veya dışından personel ile yapılan periyodik değerlendirmelerdir. Odak grubu çalışmaları; beyin fırtınası şeklinde yapılan en az beş en fazla dokuz kişi ile hem mülakattaki bilgilerin gözden geçirilmesini hem de yeni fikirler ortaya atılmasını sağlamaktadır. Vaka envanteri; eş değerdeki

kurumlarda oluşan vakaların listesinden faydalanmaktır. Dâhili analiz; iş birimlerinin kendi içinde yaptığı toplantılardan çıkan sonuçlardır. Geçmiş veriler; eskide karşılaşılmış olan vakaların neden ve kökenlerinin araştırılmasıyla oluşmaktadır. İşlem akış analizi; süreç bazlı olarak girdiler, işlem ve çıktı olarak detaylandırılmasıdır. Uyarıcı gösterge; niceliksel veya niteliksel bir değeri eşik nokta kabul ederek aşıldığında işlem yapılmasını gerektirecek göstergelerdir (Derici, Tüysüz ve Sarı, 2007: 156-157).

Bilgi teknolojilerinde risk oluşturabilecek alanlara örnek olarak (Bağcı, 2007):

- BT yönetimi ve stratejisi ile ilgili riskler: BT stratejileri taktik plan ve iş stratejileriyle uyumlu olmaması ve iyi yönetilememesi sonucunda ortaya çıkan risklerdir.
- BT mimarisi riskleri: BT altyapısının yetersiz olması neticesinde meydana gelebilecek zafiyet ve tehditlere açık olmasına neden olacak risklerdir.
- Beceri ve teknolojik iyileştirme riskleri: Organizasyonun kendi sektörü içinde avantaj kazanmasını ve işlerini daha hızlı bir şekilde yapmasına olanak sağlayacak teknolojiden geri kalınması gibi risklerdir.
- Uyumluluk riskleri: Düzenlemelere ve mevzuatlara uyumsuz olma riskleridir.
- İş sürekliliği ile ilgili riskler: Organizasyonun işini idame ettirebilmesi için gerekli olan kaynaklarını kullanamaması riskleridir.
- Kaynak yönetimi riskleri: Organizasyonun kaynak planlamasını iyi şekilde yönetememesi riskleridir.
- Tedarikçi yönetim riskleri: Organizasyonun üçüncü taraflar ile uygun ilişki kuramaması riskleridir.
- Proje yönetimi riski: BT organizasyonunun proje yönetimi konusunda yetersizliği sonucunda oluşabilecek risklerdir.
- Değişiklik yönetimi riski: Organizasyon içindeki sistem, donanım, yazılım vb. alanlarda değişikliklerin iyi yönetilememesi neticesinde ortaya çıkabilecek risklerdir.
- Bilgi güvenliği riskleri: Bilgi güvenliği sürecinin alınacak kontroller ile tehdit ve zafiyetlere karşı iyi yönetilememesi sonucunda ortaya çıkabilecek risklerdir.

BT riskleri, BT faaliyetlerini etkileyen ya da BT faaliyetlerinden etkilenen, doğal afetler, düzenlemelerdeki değişiklikler, üretim ve hizmet kalitesini etkileyen iç süreçler, organizasyon performansı, yasal kontroller gibi alanları kapsar. Symantec riski güvenlik,

kullanılabilirlik, performans ve uyum olmak üzere dört sınıfa ayırmakta ve BT risklerini değer ve zafiyet olarak Çizelge 3.8'de tanımlamaktadır (Symantec, 2008).

Çizelge 3.8. BT risk etmenleri (Symantec, 2008)

BT Risk: Değer ve Zafiyetler		
BT Risk Elementleri	**Uzlaşılmış Ana Değerler**	**Risk Kökeni**
Güvenlik	Güven, itibar	Dış saldırı, zararlı kod, fiziksel yıkım, yetkisiz erişim, çalışan iş tatminsizliği
Uyum	Yasal, finansal ve operasyonel bütünlük	Değişen ya da yanlış anlaşılan düzenlemeler, BT politikalarının yetersizliği, yetersiz denetim kapasitesi
Performans	Verimlilik ve üretkenlik	Zayıf sistem mimarisi, ağ sıkışıklığı, verimsiz kod, yetersiz kapasite, verimsiz süreç tasarımı
Kullanılabilirlik	Finansal ve tedarik zinciri bütünlüğü, ticari sorumluluk	Ağ hataları, yetersiz değişiklik yönetimi, veri merkezi hataları, bölgesel afetler

Çizelge 3.8'de görüldüğü üzere Symantec BT risk elementlerini, uzlaşılmış ana değerleri ve bu değerleri etkileyebilecek risk kökenini ifade etmiştir. Uyum incelendiğinde; uzlaşılmış ana değerin mevzuat/finans/operasyonel bütünlük olduğunda, oluşabilecek risk kökenini bilgi teknolojileri politikalarının yetersizliği ve yanlış anlaşılan düzenlemeler oluşturur.

3.3.6. Risk değerlendirme ve risk değerlendirme yöntemleri

Risk değerlendirme yöntemleri niteliksel ve niceliksel olmak üzere ikiye ayrılır. Her iki yönteminde üstün olduğu noktalar bulunmaktadır. Organizasyonun yapısına göre uygun yöntem seçilmelidir. Niteliksel risk değerlendirmenin üstünlük sağladığı noktalar; riskleri önceliklendirerek yüksek önceliği olan risklere karşı hızlı önlemler alınmasını sağlaması, parasal değer hesaplamasının olmaması ve esnek raporlama imkânlarına sahip olmasıdır. Sayısal olarak derecelendirme yapmaması ve bunun sonucunda fayda/maliyet analizinin etkin yapılamaması ise dezavantajıdır. Niceliksel risk değerlendirme yönteminin avantajı ise; sayısal hesaplamalar yapıldığı için riski verimli yönetmek adına fayda/maliyet analizinin yapılmasına olanak sağlamasıdır. Hesaplamaların karışık olması ve hesaplama yapılabilmesi için verinin kaliteli olması gerektiği için risk değerlendirme öncesindeki faaliyetler hem zaman almakta hem de nitelikli personel gerektirmesi dezavantajıdır (Peltier, 2005: 77-80).

Aynı tehdit ve zafiyete sahip iki farklı organizasyonun risk skorları, farklı süreç ve yapı barındırdıkları için farklı olabilmektedir.

Varlık sınıflandırması: Nicel ve/veya nitel tahmin yöntemiyle değerler atanarak varlık değeri belirlenir. Nicel tahminde risk seviyeleri uygun rakamsal ifadeler (1-2-3) ile belirlenirken, nitel tahmin de risk seviyeleri (düşük-orta-yüksek) gibi veya her iki yöntem birlikte tanımlanarak uygulanabilir. Sayısal olarak değer verilmesi kolay olan varlıklarda nicel değerlendirme rahatlıkla uygulanabilirken organizasyonun itibari, ticari değeri gibi soyut varlıklarda nitel tahmin kullanılması gerekmektedir. Derecelendirme seviyesi, organizasyonun güvenliğe olan ihtiyacı düzeyinde belirlenir. Güvenlik ihtiyacı fazla olan organizasyon için 5-7 derecelendirme seviyesi uygunken, güvenlik ihtiyacı düşük olan bir organizasyon için 3-4 derecelendirme seviyesi kullanımı uygun olmaktadır (Koç F. , 2008). Nicel ve nitel değerlendirme örnekleri Çizelge 3.9 ve Çizelge 3.10'da gösterilmektedir.

Çizelge 3.9. Nicel yaklaşım (Sağıroğlu ve diğerleri, 2007)

	Çok Az Zarar (1)	**Önemsiz Zarar (2)**	**Orta Zarar (3)**	**Ciddi Zarar (4)**	**Çok Ciddi Zarar (5)**
Çok Düşük Olasılık(1)	1	2	3	4	5
Düşük Olasılık(2)	2	4	6	8	10
Orta Olasılık(3)	3	6	9	12	15
Yüksek Olasılık(4)	4	8	12	16	20
Çok Yüksek Olasılık(5)	5	10	15	20	25

Çizelge 3.9'da görüldüğü üzere beşli skala kullanılmıştır ve 1-3: Çok Düşük, 4-6: Düşük, 8-10: Orta, 12-16: Yüksek, 20-25: Çok Yüksek olarak derecelenmiştir. Risk=Olasılık*Tehdidin Etkisi. Yüksek olasılık ve orta zarar olduğunda 12 sonucu çıkmaktadır. Orta seviyede tehdidin olma olasılığı bulunmaktadır.

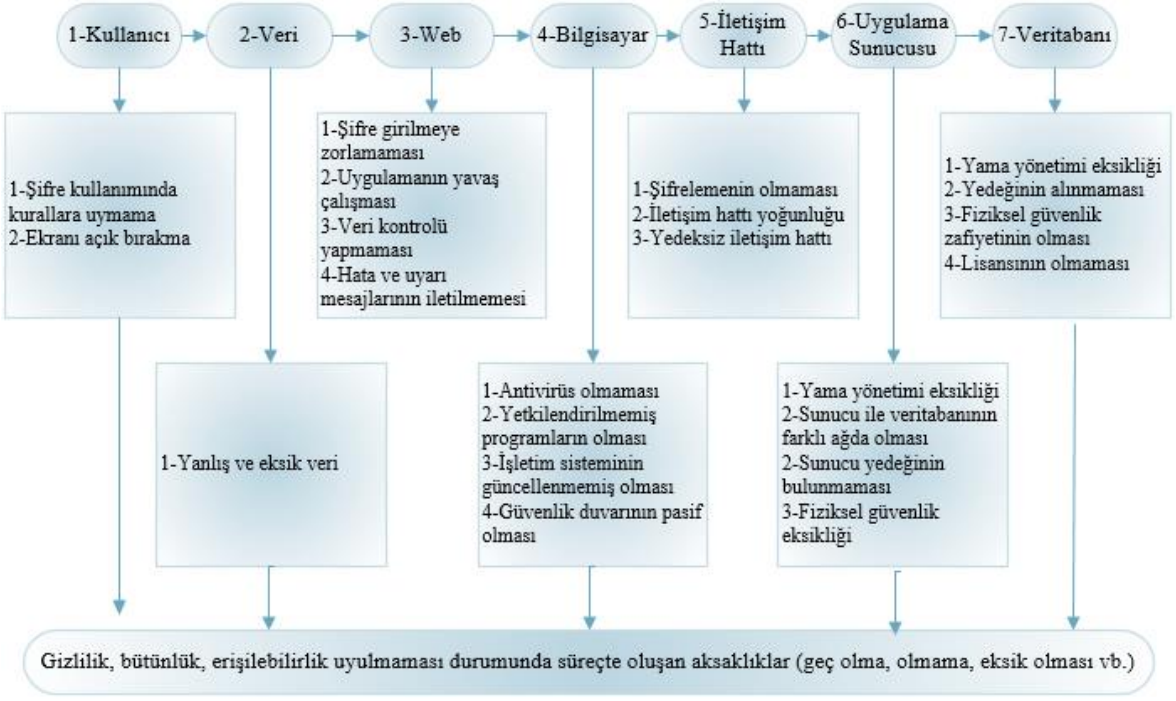
Nitel olarak tehdidin olma olasılığı Çizelge 3.10'da verilmiştir. Nitel yaklaşımda beşli skala kullanılmıştır. A= çok az, B= az, C= orta, D= ciddi, E= çok ciddi düzeyinde kullanılmıştır. Risk=Olasılık*Tehdidin Etkisi.

Çizelge 3.10. Nitel yaklaşım (Sağıroğlu ve diğerleri, 2007)

	Çok Az Zarar(A)	Önemsiz Zarar(B)	Orta Zarar(C)	Ciddi Zarar(D)	Çok Ciddi Zarar(E)
Çok Az Olasılık(A)	Çok Düşük	Çok Düşük	Düşük	Düşük	Orta
Az Olasılık(B)	Çok Düşük	Düşük	Düşük	Orta	Orta
Orta Olasılık(C)	Düşük	Düşük	Orta	Yüksek	Yüksek
Yüksek Olasılık(D)	Düşük	Orta	Yüksek	Yüksek	Çok Yüksek
Çok Yüksek Olasılık(E)	Orta	Yüksek	Yüksek	Çok Yüksek	Çok Yüksek

Çizelge 3.10'da belirtildiği üzere yüksek olasılık ile ciddi zarar durumunda tehdidin meydana gelme olasılığı da yüksek olmaktadır.

Bileşen tabanlı risk analizi yaklaşımı; donanım, yazılım, bilgi ve ağ gibi varlıkların risk analizi yapılır. Örneğin; sistem odası, sunucular, veri tabanı vb. Süreç tabanlı risk analizi: Bilgi işleme dair süreçlerin içinde gelişen risk analizidir. Örneğin; bir yazılım projesinin yapımı, sistem odası girişleri vb. Şekil 3.1'de süreç tabanlı analiz örneği verilmiştir (Ersoy, 2012).



Şekil 3.1. Süreç tabanlı analiz örneği (Karabacak ve Özkan, 2010; Ersoy, 2012: 68-69)

Şekil 3.1'de kullanıcının veri girişi süreç akışı olarak incelenmiştir. Kullanıcı evrakta bulunan veriyi web kullanarak sayısallaştırır, veri iletişim hattından sonra uygulama sunucusuna gelmekte sonra veri tabanına veri yazılmaktadır. Kullanıcı, veri, web, bilgisayar, iletişim hattı, uygulama sunucusu ve veri tabanının her biri birer varlıktır. Her bir varlık için tehditler ve zafiyetler belirlenir. Tehditler ve zafiyetler süreçte oluşabilecek olan gecikme, eksiklik gibi risklere sebep olmaktadır (Karabacak ve Özkan, 2010; Ersoy, 2012: 68-69).

3.3.7. Riske tepki

Risk yönetimi planları genellikle risk azaltma, risk önleme, risk transfer etme ve risk kabullenme olarak dört amaca sahiptir (Raggad, 2010).

Risk azaltma: Riskin azaltılarak kabul edilebilir seviyelere çekilmesinin sağlanmasıdır. Zafiyetlerden gelebilecek risklere karşı öncesinde ve sonrasında alınabilecek kontrol kriterlerinin iş sürekliliği ve olağanüstü durum planı ve felaket kurtarma planlarında yer almasıyla risklere ve etkilerine karşı hazırlıklı olmayı gerektirir. Risk azaltma kapasitesi, atakların belirlenme ve zamanında tepki verme süresine bağlıdır.

Risk önleme: Zafiyet kaynaklı olan artık riskleri azaltmak veya tamamen yok etmek için güvenlik kontrollerinin uygulanması faaliyetlerinden oluşan risk kontrol stratejisidir. Güvenlik politikaları yönetimi, mevcut ve gelecekteki tehditlerin yönetimi ve uygun güvenlik kontrollerinin benimsenmesiyle risk önleme faaliyetleri başarıya ulaşmaktadır.

Risk transfer etme: Riski farklı varlık, süreç ve kuruluşlara devrederek yapılan bir kontrol yaklaşımıdır. İş fonksiyonlarının yeniden gözden geçirilmesi, dış kaynak kullanımı, sigorta yaptırmak veya dış kaynak kullanımında risk transferini içeren anlaşmalar yaparak riskin olumsuz etkisi azaltılmakta veya yok edilmektedir.

Risk kabulü: Riskin sonuçlarının değerlendirilip hiçbir kontrol kriteri konulmamasıdır. Yöntem, güvenlik kontrolleri yatırımları fizibilite, fayda/maliyet analizleriyle örtüşmediğinde veya risk çok düşük seviyelerde olduğunda kullanılmaktadır. Saldırıların sonuçları, olasılıklar, zafiyetlerin seviyesi ve risklerin bilindiği durumlarda kullanılmaktadır.

Kurumun bilgi güvenliği politikalarına ve risk kabul kriterlerine uyumlu, içinde riskler, kontrol kriterleri ve sorumluluklarının tanımlandığı formel bir risk değerlendirme dokümantasyonu yapılması gerekmektedir (Calder ve Watkins, 2008).

Riske tepkiyi gerçekleştirmek için kontrollerin uygulanması gerekmektedir. Aşağıda kontrol türleri ve örnekleri verilmektedir. BT risk kontrolü önleyici, algılayıcı ve düzeltici kontroller uygulanarak sağlanmaktadır. Örnek olarak yangın olayı ele alındığında; önleyici kontrol olarak, yanmaz eşyalar ile odaları tasarlamak veya önceden yangın ile ilgili prosedürler belirleyerek yangın durumuna karşı önlemler almaktır. Algılayıcı kontrol olarak, duman ve sıcaklık dedektörlerinin olmasıyla yangına en erken şekilde müdahaleye imkân tanınmasını sağlamaktır. Düzeltici kontrol olarak, yangın söndürme sistemlerinin bulunmasıyla en az zararla yangından kurtulmak mümkün olmaktadır. Oluşan zararları geri dönüşüm planlarıyla destekleyerek yangın için donanımların değiştirilmesi ve yedekleme sistemlerinin yeniden yüklenmesi gibi kontroller alınır (Slay ve Koronios, 2006: 20-62).

Önleyici kontroller

Teknik, yönetimsel ve operasyonel olmak üzere üçe ayrılmaktadır. Teknik kontroller; güvenlik duvarı ve sanal özel ağ, anti virüs programları ve şifreleme ile içten ve dıştan gelebilecek saldırılara karşı koruma sağlamaktadır.

Önleyici teknik kontroller; kimlik doğrulama (dijital sertifika, şifreleme ile bilginin gerçek doğru kişiye iletimi), yetkilendirme (veri üzerinde değişiklik yapma yetkisine sahip olunması), erişim kontrolü (verinin bütünlüğünün ve gizliliğinin sağlanmasına yönelik yazılımsal ve donanımsal olarak alınan kontroller), red olmama (göndericinin alıcıyı ve mesajının alındığını bilmesi durumu), işlem gizliliği (işlem yaparken kullanılan kredi kartı vb. bilgilerin gizliliğinin sağlanması) olmak üzere beş ilkeye sahiptir. Yönetimsel kontroller; güvenliğe yönelik politika, prosedür ve rehberlerin hazırlanarak uygulanabilirliğinin sağlandığı kontrollerdir. Örnek olarak görev ayrımının uygun yapılması veya güvenliğe yönelik eğitim programlarının düzenlenmesi gibi kontrolleri içermektedir. Operasyonel kontroller; varlıkları hırsızlık, yangın, sıcaklık gibi tehditlerden korumak için güvenlik personeli bulundurma, ziyaretçi protokollerinin olması gibi önleyici kontrollerden oluşmaktadır.

Algılayıcı kontroller

Teknik, yönetimsel ve operasyonel olmak üzere üçe ayrılmaktadır. Teknik kontroller; duman, sıcaklık, nem gibi durumları algılayan alarm, uyarı ve saldırı tespit sistemlerinin kurulduğu kontrollerdir. Yönetimsel kontroller; sürekli risk değerlendirmesini içermektedir. Örneğin yeni alınacak personel geçmişinin risk açısından değerlendirilmesi gibi. Operasyonel kontroller; güvenlik ihlallerini algılayabilecek video kayıtları gibi kontrol sağlayıcılardan oluşmaktadır.

Düzeltici kontroller

Teknik, yönetimsel ve operasyonel olmak üzere üçe ayrılmaktadır. Teknik kontroller; yedekleme sisteminin bulunması, denetim izinin tutularak kök nedene inilerek gerekli düzeltici faaliyetlerin yapılmasını sağlamaktadır. Aynı zamanda denetim iziyle birlikte olayların tekrarlanması önlenebileceği için bu tür kontroller önleyici kontrol olarak adlandırılabilmektedir. Yönetimsel kontroller; olay sonrasında finansal kaynak sağlanması ve fiziksel altyapının iyileştirilmesine yönelik olan kontrollerden oluşmaktadır. Operasyonel kontroller; erişimin durduğu veya altyapının zarar gördüğü durumlarda farklı bir lokasyonda acil durum merkezinin kurularak yedeklemenin yapılması ve işlemlerin oradan devam etmesinin sağlanması gibi kontrollerden oluşmaktadır (Slay ve Koronios, 2006: 20-62).

Maliyet açısından etkin olabilmesi için kontrolün uygulanması ve bakım maliyetleri kontrolün olmaması durumundaki olumsuz etkisinden daha fazla olmamalıdır. Tüm risklere karşı önlem almak olanaksızdır o yüzden etkin risk yönetimi için etkin maliyet yönetimi yapılmalıdır (Calder ve Watkins, 2008: 86).

Sayıştay tarafından bilgi sistemleri faaliyetlerinin sürekliliğinin sağlanması adına yapı, prosedür ve yöntemlere yönelik kontroller aşağıda incelenmiştir (Sayıştay, 2013):

Yönetim kontrolleri

Bilgi sistemlerinin organizasyon hedeflerine uyumlu bir şekilde çalışmasını sağlayıcı kontrolleri oluşturmasıdır. Strateji oluşturma, güvenlik politikaları, organizasyon, varlık envanteri ve yönetimi, personel ve eğitim politikaları, düzenlemelere uygunluk alt bölümlerinden oluşmaktadır.

Stratejik planlama riskleri: Hedeflere uygun olarak kurumsal ihtiyaçların karşılanmaması, önceliklerin doğru tanımlanamaması ve yanlış kaynak tahsisi, tehlikelerin ve etkilerinin belirlenememesi, bütünsel yaklaşımla risklerin etkin yönetilememesi, üst yönetimin önemli kararlarda etkin olmaması, BT bütçe kontrolünün yetersizliği gibi riskler bulunmaktadır. Stratejik planlama temel kontrolleri olarak; yazılı bir strateji ve uygulama planlarının bulunması, stratejik planlamanın yürütülebilmesi için yönlendirme kurulunun bulunması, periyodik olarak risk değerlendirmelerinin yapılması gerekmektedir.

Güvenlik politikaları riskleri: Güvenlik olaylarına uygun ve tam zamanında tepki verilmemesi, güvenlik farkındalığının olmaması, tehditlerin zamanında fark edilememesi, güvenlik politikalarının güncel olmaması gibi riskler bulunmaktadır. Güvenlik politikaları temel kontrolleri olarak; yazılı, üst yönetimce onaylı, tüm personelle paylaşılmış, amaç, kapsam ve sorumlulukların belirlendiği belirli aralıklarla güncellenen güvenlik politikalarının oluşturulması gerekmektedir.

Organizasyon riskleri: Sorumluluk paylaşımının etkin yapılamaması, organizasyonun karşılaşabileceği tehlikelerin belirlenememesi ve risklerinin yönetilememesi, prosedür, politika ve süreçlere uyumsuzluk, çalışan iş tatmininin sağlanamaması, mükerrer işlemlerin yapılması, personel istihdamının yetersizliği gibi riskler bulunmaktadır. Organizasyon için temel kontroller olarak; organizasyon yapısının güçlendirilmesi, bilgi güvenliği faaliyetlerinde koordinasyonun, görev ve sorumlulukların belirlenmesi, bağımsız denetimlerin yapılması, tedarikçiler ve diğer kurumlarla bilgi güvenliği anlaşması yapılması gerekmektedir.

Varlık yönetimi riskleri: Varlıklar üzerindeki maliyet, getiri ve risklerine karşı kontrolün, denetim izinin kaybedilmesi, lisanssız yazılımların oluşturabileceği zararlar, imhada yapılacak hatalar neticesinde veri kaybı, varlık üzerindeki sorumlulukların tanımlanmaması, varlık yatırımının verimsizliği, üst yönetim desteğinin sağlanamaması gibi riskler bulunmaktadır. Varlık yönetimi temel kontrolleri olarak; varlık envanterinin yapılması, varlık kullanımındaki kuralların belirlenmesi, varlık imhasına ait belirli prosedürlerin oluşturulması, veri sınıflandırılmasının yapılması, iş ve işlemlerin belgelendirilmesi gerekmektedir.

Personel ve eğitim politikaları riskleri; gerekli bilgi ve tecrübeden yoksun personel alımı, personelin kurum politikalarına aykırı hareket etmesi, güvenlik farkındalığının oluşmaması sonucunda personel kaynaklı meydana gelebilecek güvenlik olayları ve zararları, kilit personelin olmaması, personel kariyer gelişiminin ilerletilememesi, eğitim politikalarının yetersizliği, işten ayrılan personelin sistemlere yetkisiz erişimi gibi riskler bulunmaktadır. Personel ve eğitim politikaları temel kontrolleri olarak; rol ve sorumlulukların güvenlik politikalarına uygun olarak belirlenmesi, kritik bölgelerde çalışan personel seçimine önem verilmesi, çalışanlarla bilgi güvenliği politikalarının yer aldığı sözleşmenin yapılması, çalışanlara sürekli bilgi güvenliğiyle ilgili eğitimlerin verilmesi, işten ayrılan personelin kullanımında olan varlıkların teslim edilmesi ve erişim yetkilerinin kaldırılması gerekmektedir.

Uygunluk riskleri; yasalara ve düzenlemelere uyumsuzluk sonucunda maddi zararların ortaya çıkması, itibar kaybına yol açması, suç teşkil edebilecek fiillerin ortaya çıkması, mevzuatın takip edilmemesi gibi riskler bulunmaktadır. Uygunluk temel kontrolleri olarak; bilgi sistemleriyle ilgili düzenlemelerin gereklerine uyulması, bilgi güvenliğine yönelik düzenlemelerin sürekli güncellenmesi, mevzuata uygunluğun denetlenmesi ve raporlanması gerekmektedir.

Fiziksel ve çevresel kontroller

Fiziksel ve çevresel riskler; erişim yetkisi olmayan kişilere karşı fiziksel engeller konulması, yangın ve elektrik vb. çevresel tehlikelere karşı önlemler alınmasıdır. Fiziksel ve çevresel riskler neticesinde; bilgi sistemlerinin çalışanlar tarafından verilebilecek zararlara açık hale gelmesi, kritik bilgilere yetkisiz erişimin açık hale gelmesi, varlıkların çalınması veya bozulması, yangın, sel gibi nedenlerden dolayı sistemin çalışamaz hale gelmesi, yetkisiz kişilerce fiziksel müdahaleye maruz kalmasıdır. Fiziksel ve çevresel temel kontrolleri olarak; yetkisiz fiziksel erişime ve çevresel tehlikelere karşı prosedürlerin oluşturulması, ana bilgi sistemlerinin bulunduğu alanlara yetkisiz fiziksel erişimin engellenmesi, yangın, sel, elektrik, nem, sıcaklık için gerekli uyarı sistemleri ve önlemlerin kurulması gerekmektedir.

Ağ yönetimi ve güvenliği kontrolleri

Ağ sistemlerini oluşturan bütün varlıkların korunmasına, yetkisiz erişimlerin önlenmesine yönelik politikalardır. Ağ yönetimi ve güvenliği riskleri; verilerin bozulması ve kötüye kullanılması, ağ anahtarlarının yetkisiz kişilerce kullanılması, ağ bağlantısı ve sunucuların yeterli seviyede korunmaması neticesinde sistemin işlememesi, ağ tasarımının yetersizliği nedeniyle ağ performansında azalmanın meydana gelmesi, virüs gibi yazılımların sistemde açıklıklara sebep olması, yasal mevzuatın ihlal edilmesi, yazılımların gereklilikleri karşılayamaması vb. riskler bulunmaktadır.

Ağ yönetimi ve güvenliği temel kontrolleri olarak; güvenlik politikası içeriğinde ağ ve internet kullanımının yer alması, çalışanların şifre, e-posta gibi konularda bilinçlendirilmesi, mantıksal erişim kontrolleri politikalarının oluşturulması ve uyumunun sağlanması, ağ olaylarının izlenmesi, yazılım güncellemeleri ve yamaların periyodik olarak yapılması, anti virüs sistemlerinin kurulması ve etkin şekilde yönetilmesi, belirli durumlarda kriptolamanın yapılması, özel hatların kullanılması gerekmektedir.

Mantıksal erişim kontrolleri

Bilgi sistemlerine yetkisiz mantıksal erişimin engellenmesine yönelik uygulamalardır. Mantıksal erişim politikaları riskleri; erişim yetkisi karmaşıklığı, kullanıcıların yetersiz bilgilenmesi, yetersiz şifre kurallarının sisteme ve uygulamalara yetkisiz erişime sebep olması, yetersiz veya aşırı yetkilendirme, ayrıcalıklı kullanıcıların denetlenememesi, şifrelerin ele geçirilmesi, erişim politikalarına uyumsuzluk, yetkisiz erişim girişimlerinin belirlenememesi gibi risklerdir. Mantıksal erişim politikaları temel kontrolleri olarak; mantıksal erişim politikasının bulunması, erişim yönetimiyle ilgili düzenlemelerin yapılması, sistem ve uygulamalara erişimin kayıt altında tutulması, yetkisiz erişimlerin raporlanması gerekmektedir.

İşletim sistemi erişim riskleri: Sistem kaynaklarına ve uygulamalarına yetkisiz erişime yol açması, kullanıcı hesaplarına yetkisiz erişim ve kullanma, yardımcı programların kullanımının kısıtlanmaması sonucunda erişime açık hale gelmesi gibi risklerdir. İşletim sistemi erişimi temel kontrolleri olarak; oturum açma uygulamaları politikalarının oluşturulması, sistem yapılandırmasında kullanılan yardımcı programların kontrolünün

sağlanması, sisteme giriş sonrasında kullanılmayan sistemlerin otomatik kapanması, sisteme bağlı kalma süre kısıtının bulunması gerekmektedir.

Uygulama programlarına erişim riskleri: Uygulama programlarındaki bilgilerin güvenilirliğinin azalması, verilerin ve programların yetkisiz değiştirilmesi ve çalınması, hatalı işlemlerin yapılması gibi risklerdir. Uygulama programlarına erişim temel kontrolleri olarak; uygulama programlarına erişimin politikalar doğrultusunda yapılması, ana dosyalara erişimin kısıtlanması gerekmektedir.

İşletim kontrolleri

Bilgi sistemleri faaliyetlerinin süreklilik ve güvenlik sağlanacak şekilde işletilmesidir. İşletim sistemi ve bilgisayar işlemleri riskleri; gereksinim dışı sistem temini, yetkisiz erişim, işlem verimliliğinin azalması, ortam araçlarının bozulması, çalınması ve erişilememesi, pasif hesapların silinememesi, programların ve verilerin bozulması, çalınması, olay ve problem yönetimi prosedürlerindeki eksiklikler nedeniyle aksamaların oluşması gibi risklerdir. İşletim sistemi ve bilgisayar işlemleri temel kontrolleri olarak; işletim sistemi seçimi ve kurulumuna yönelik prosedürlerin geliştirilmesi ve uygulanması, konsollara erişimin yetkili kişilerce yapılması, yama prosedürünün oluşturulması, sistem performansını artırıcı konfigürasyonların yapılması, kapasite ve performans değerlendirmelerinin yapılması, acil durumlar için personel sorumluluğunun atanması, kasetler, manyetik diskler gibi araçların korunma ve saklanma prosedürlerinin oluşturulması, olayların takibi ve çözümü için kayıtların tutulması, yardım masasının kurulması gerekmektedir.

Veri tabanı güvenlik riskleri: Kullanıcı kimliklerinin karışması ve çalınması, veri tabanı zafiyeti neticesinde yetkisiz erişim, kullanılmayan hesapların silinmemesi, verilerin bozulması, yok olması ve çalınması, veri tabanı uygulamalarının güvenilirliğinin zayıf olması neticesinde işlem ve raporlamalardaki aksaklıklar gibi risklerdir. Veri tabanı güvenliği temel kontrolleri olarak; veri tabanına yönelik prosedürlerin oluşturulması, uygulama ve veri tabanı arasında uyumluluğun sağlanması, veri tabanı güncellemelerinin yapılması, veri tabanı performansının izlenmesi ve parametrelerin değerlendirilmesi, yedekleme ve geri yükleme prosedürlerinin oluşturulması gerekmektedir.

Sistem geliştirme ve değişim yönetimi kontrolleri

Sistem geliştirme riskleri: Sistem geliştirmenin yetersizliği, prosedürlerin standartlarla uyumsuz olması, sistem geliştirme ekibinin yeterli nitelikte olmaması, kaynak sorunlarının ortaya çıkması, fizibilite çalışmasında analiz eksikliği, seçilen sistemin etki değerlendirmesinde hataların yapılması gibi risklerdir. Sistem geliştirme temel kontrolleri olarak; sistem geliştirmesine yönelik prosedürlerin oluşturulması, yeterli nitelik ve tecrübeye sahip proje ekibinin kurulması, fayda/maliyet analizi yapılarak kaynak sağlanması, projelerin izleme ve değerlendirmesinin yapılması, geliştirilmekte olan sistemin risk değerlendirmesinin yapılması, projeye ilişkin fizibilite çalışmalarının yapılması, sistem gelişimindeki sözleşmelerin bütün ayrıntıları içermesi ve düzenlemelere uygun olması gerekmektedir.

Değişim yönetimi riskleri (kurulum ve kabul): Sistem kurulumu tasarım dokümanının yeterli detayda olmaması, kodlamanın ve modül testlerinin yetersizliği, kullanıcı kabul testinin yetersizliği, uygulamalar sonucunda oluşan verinin organizasyon gereksinimlerini karşılayamaması gibi risklerdir. Değişim yönetimi temel kontrolleri olarak; sistem kurulumuna yönelik prosedürlerin tasarım belgesiyle uyumlu olması, kodlama işlemlerinin yanı sıra testlerininde yeterli düzeyde yapılması, kullanıcı kabul testlerinin yapılması, uygulamaya alma prosedürlerinin oluşturulması, sistem başarısını ölçecek kriterlerin belirlenmesi ve izlenmesi gerekmektedir.

Acil durum ve iş sürekliliği planlaması kontrolleri

Acil durum sebebiyle bilgi sistemlerinin işleyişinin geçici veya sürekli bir şekilde aksaması durumunda yapılacak işlemlerdir. Acil durum ve iş sürekliliği planlaması riskleri; felaketlere maruz kalınma olasılığının yükselmesi, kaybın ve zararın artması, felaket sonrası belirlenen sürede faaliyetlerin başlatılamaması, tedarikçilere ve yasal kişilere karşı sorumlulukların sağlanamaması, felaket sonrası iletişimin, bilgi işleme kapasitesinin, insan kaynağının ve kritik varlıkların kaybedilmesi vb. risklerdir. Acil durum ve iş sürekliliği planlaması temel kontrolleri olarak; tahmin edilebilen veya tahmin edilemeyen iç ve dış kaynaklı acil durumlara yönelik yönetim prosedürlerinin oluşturulması, iş aksamalarına sebep olabilecek ve organizasyonu olumsuz etkileyebilecek olaylara karşı risk değerlendirmesinin yapılması, risk değerlendirmesi neticesinde fayda/maliyet düşünülerek

gerekli önlemlerin alınması, acil durum ve iş sürekliliği planlamasının yapılması, güncellenmesi ve tatbikatların yapılması, yedeklemelerin günlük, haftalık veya aylık olarak alınması ve kurum dışında güvenlik önlemleri bulunan bir yerde saklanması gerekmektedir.

Bulgular risk yönünden derecelendirildikten sonra denetlenen kuruma önleyici faaliyet almaları için bilgilendirme yapılmaktadır. Sayıştay'ın BT risk yönetimi alanında denetimi neticesinde çok yüksek, yüksek, orta ve düşük olarak değerlendirme matrisi oluşturulmaktadır. Çok yüksek risk seviyesinde; telafisi çok zor olacak kritik kontrol zayıflıkları bulunmaktadır ve hızlı bir şekilde önlem alınması gerekmektedir. Yüksek risk düzeyinde; önemli kontrol zayıflıkları bulunmakla birlikte uygun bir süre içinde önlem alınması gerekmektedir. Orta risk düzeyinde; kontrol zayıflıkları vardır; fakat önlem almada hızlı davranılmasına gerek yoktur. Düşük risk düzeyinde ise; riskler kabul edilebilecek düzeydedir (Sayıştay, 2013).

4. BİLGİ TEKNOLOJİLERİ RİSK YÖNETİMİ ÖRNEK UYGULAMASI

BT risk yönetimi temel olarak; risklerin belirlenmesi, değerlendirilmesi, risk kabulü seviyesine kadar gelmesi için aksiyon alınması ve takibinin sağlanması aşamalarından oluşmaktadır. Organizasyon içinden ve/veya dışından iş süreçleri ile ilgili çalışanların bir araya gelerek risk yönetimi sürecinin başından sonuna kadar tasarlayıp uygulanmaya başlanması ve en son takibinin gerçekleşmesini de içeren bir çerçeve oluşturması gerekmektedir (Bağcı, 2007).

Örnek uygulama olarak COBIT 5 çerçevesinde yapılan risk çalışması, tehdit değeri ve süreklilik değeri içeren risk çalışması ve tehdit, zafiyet, olasılık değerlerini ayrı şekilde işleyen risk çalışması yer almaktadır.

4.1. COBIT 5 Çerçevesinde Risk Yönetimi Uygulaması

2017 yılında yapılan bir çalışmada COBIT 5 risk yönetimi uygulanmıştır. Çalışma; verilerin toplanması, verilerin analizi ve risk analizi bölümlerinden oluşmaktadır (Astuti, Muqtadiroh, Darmaningrat ve Putri, 2017; ISACA, 2013)

4.1.1. Verilerin toplanması

Görüşme, anket, durum ve doküman incelemesi neticesinde veriler toplanarak, ideal durum ve ideal durumdaki faaliyetlerin ne olması gerektiği Çizelge 4.1'de belirtilmiştir. Faaliyetler uygulanıyorsa evet, uygulanmıyorsa hayır olarak nitelendirilmiştir. U=uygulama, E=evet, H=hayır anlamına gelmektedir.

Çizelge 4.1. Verilerin toplanması (Astuti ve diğerleri, 2017; ISACA, 2013)

No	Faaliyetler	U	Notlar
1	Kullanıcıları bilgilendirmek ve trend analizi yapmak için olay ve hizmet talebi sınıflandırmasını ve önceliklendirme şemalarının ve sorun kaydı kriterlerinin tanımlanması	E	Kullanıcılar e-posta, telefon veya e-bilet sistemi aracılığıyla bir olay bildirir veya bir hizmet talep eder. Servis masası, gelen olay ve talep dağılımlarını kategorize eder, dağıtım ve yükseltme süreçlerini basitleştirir. Hizmet masası olayın aciliyetine göre olaya öncelik vermeli ve talep etmelidir
2	Etkin ve etkili çözümlemeyi sağlamak için bilinen hataların olay modellerinin tanımlanması	E	Hizmet masası birimi, doğru çözümü belirlemelerine yardımcı olmak için olay modelini tanımlamıştır.
3	Özellikle büyük olaylar ve güvenlik olayları için olay yükseltme kurallarının ve prosedürlerinin tanımlanması	H	Hizmet masası birimi, olay yükseltme kurallarını ve prosedürlerini uygulamamıştır.
4	Olay tanımlaması ve bilgi kaynaklarının ve kullanımlarının talep edilmesi	E	Hizmet masası birimi, kullanıcı bakış açısıyla iletişim ve bilgi toplama yoluyla tanımlanan bilgi kaynaklarına ve kullanımlarına sahiptir.

Çizelge 4.1'de görüldüğü üzere faaliyetlerin uygulanma/uygulanmama durumlarına yönelik notlar alınmıştır. Olay modellemesi tanımlaması faaliyete uygun olarak yapılmaktadır; fakat büyük olaylar için yükseltme prosedürlerinin uygulanmadığı not edilmiştir. Veriler toplandıktan sonra belirlenen riskler Çizelge 4.2'de gösterilmiştir.

Çizelge 4.2. Risk belirleme süreci sonuçları (Astuti ve diğerleri, 2017; ISACA, 2013)

No	Faaliyet	Potansiyel Risk	Notlar	Nedenleri
1	Özellikle büyük olaylar ve güvenlik olayları için olay yükseltme kurallarının ve prosedürlerinin tanımlanması	Olay ve hizmet talebi için kategorizasyon sistemi veya önceliklendirme sistemi oluşturma hataları	Hizmet masasının kategorizasyonda veya önceliklendirmede hata yapması ve bu sistemlerin eksik kalması	Hizmet masasının, BT servislerinde önceliklendirme veya kategorizasyon sistemi oluşturmak için yeterli bilgiye sahip olmaması
2	Etkin ve etkili çözümlemeyi sağlamak için bilinen hataların olay modellerinin tanımlanması	E-bilet sistemine erişim hatası	E-bilet sisteminin kullanıcılar tarafından hataları veya hataların neden olduğu olayları bildirmek ve BT hizmetleri talep etmek için kullanılamaması	Sistem hatası

Çizelge 4.2'de görüldüğü üzere tüm faaliyetler eklendikten sonra her bir faaliyet için potansiyel riskler, risk ile ilgili notlar ve riske ait nedenler tanımlanmaktadır. Büyük olaylar için potansiyel risk; kategorizasyon veya önceliklendirme sistemi oluşturma hatasıdır. Potansiyel riskin nedeni; hizmet masasının bu konudaki yetersiz bilgisi nedeniyle hata yapabilmesi ve sistemde eksiklik meydana gelebilmesi durumudur.

Olay modellemesi faaliyetinde potansiyel risk e-bilet erişiminde meydana gelebilecek erişim hatalarıdır. Kullanıcılar, hataları ve hataların neden olduğu olayları bildirmeyi sistem hatası nedeniyle talep edememektedir.

4.1.2. Verilerin analiz edilmesi

Riskler belirlendikten sonra risk türleri, risk kategorileri ve risk faktörleri belirlenir. COBIT 5, risk türlerini üçe ayırmıştır.

BT fayda/değer gerçekleştirme riski (1); iş süreçlerinin verimliliğini artırmak için teknoloji kullanımı fırsatı (kaçırılmış) ya da yeni iş girişimleri için gerçekleştirici olarak kullanılan risk türüdür.

BT program ve proje dağıtımı riski (2); BT'nin yeni veya geliştirilmiş iş çözümlerine, program ve proje kullanarak katkısı ile ilgili risk türüdür.

BT operasyon ve hizmet sunumu riski (3); BT hizmetlerinin operasyonel kararlılık, kullanılabilirliği ve kurum değerinin azalması ile ilgilidir.

Risk türü belirlenirken risk ile türü arasında yüksek ilgi varsa (Y), düşük ilgi varsa (D), hiç ilgi yoksa boş bırakılmıştır. Risk kategorisi COBIT 5 içinde belirlenen kategorilerden seçilmiştir. İç ve dış risk faktörleri veri analizinde kullanılmıştır. Risk türü tanımlaması, risk türleri, kategorileri ve faktörleri Çizelge 4.3'te gösterilmiştir.

Çizelge 4.3. Veri analizi sonuçları (Astuti ve diğerleri, 2017; ISACA, 2013)

No	Risk	Risk Türü			Kategorisi	Risk Faktörleri	
		1	2	3		İç	Dış
1	Kullanıcı veri girişi hatası	D	D	Y	Personel çalışması (insan hatası ve kötü niyet)	BT nin Karmaşıklığı-kullanıcının BT'yi kullanma zorunluğu İşletme Modeli-kullanıcıların olay raporlama modeline alışkın olmamaları	Teknoloji durumu ve gelişimi-gelişen teknolojinin BT hizmetleri taleplerinde karmaşıklığa yol açması
2	E- bilet sistemine erişim hatası	D	D	Y	Yazılım	BT'nin Karmaşıklığı- e-bilet siteminin karmaşık ve hatalara sahip olması Risk yönetimi felsefesi-organizasyonun hata kaynaklı sistem hatalarını önlemek için bir strateji oluşturmaması	Teknoloji durumu ve gelişimi teknolojik gelişmelerin e-bilet sisteminde periyodik bakım gerektirmesi Yetkisiz kişilerce yapılan sistem saldırı tehdidi

Çizelge 4.3'te belirtildiği üzere e-bilet sistemine erişim hatası riskinde risk türü seçilmiş, risk kategorisi yazılım ve iç risk faktörü e-bilet sisteminin karmaşık hatalara sahip olması ve çözümlenmesi için strateji oluşturmamasıdır. Dış risk faktörü olarak, teknolojik gelişimin bakım ihtiyaçlarını ortaya çıkarması ve erişim yetkisi olmayan kişilerce yapılan sistem saldırı tehdididir. Kullanıcı veri girişi hatasında da benzer iç ve dış risk faktörü bulunmaktadır.

4.1.3. Risk analizi sonuçları

Pozitif ve negatif olmak üzere iki tür BT risk senaryosu oluşturulmaktadır. Pozitif senaryoda tanımlanan riskler meydana gelmez ve süreçlerin işleyişi sorunsuz bir şekilde devam eder. Negatif risk senaryosunda ise riskler meydana gelir ve iş süreçlerinde bozulmalar oluşur. Çizelge 4.4'te tanımlanan riskler için pozitif ve negatif senaryolar geliştirilmiştir.

Çizelge 4.4. Risk analizi sonuçları (Astuti ve diğerleri, 2017; ISACA, 2013)

No	Risk	Pozitif Senaryolar	Negatif Senaryolar
1	Olay ve hizmet talebi için kategorizasyon sistemi veya önceliklendirme sistemi oluşturma hataları	Olay uygun bir şekilde ele alınır ve belirlenen kategoriye göre problem yükseltilir	Veriler uygun değilse, olay ve hizmet talebi işlemleri engellenmekte veya tamamlanması uzun sürmektedir
2	Kullanıcı veri girişi hatası	Kullanıcıların olay raporu veya hizmet talebini doğru ve tam bir şekilde doldurmasıyla olay tespiti ve yönetimi sorunsuz bir şekilde gerçekleşir	Kullanıcıların yanlış veya ilgisi olmayan veriler girmesiyle olay tespiti ve yönetimi zaman almaktadır
3	E- bilet sistemine erişim hatası	Kullanıcılar olay raporu ve hizmet talebi oluştururken e-bilet kullanabilmekte ve hizmet masası kullanıcılardan raporları alabilmektedir	Raporlama sistemi kullanılamamakta ve hizmet masası raporlama durum takibini yapamamaktadır

Çizelge 4.4'te belirtildiği üzere e-bilet erişim hatası riski için pozitif senaryo; olay raporlaması ve hizmet talebinin yapılabilmesidir. Negatif senaryo ise; raporlamanın ve hizmet masasının raporlama durum takibinin yapılamamasıdır.

Risk değerlendirmesi, riskin meydana gelme sıklığı ve şiddeti hesaplamasını gerektirmektedir. Çizelge 4.5'te risk önceliklendirmesinde kullanılmak üzere risk sıklığı sayısal değer ve olma olasılığı verilerek gösterilmiştir. Sıklık değeri olarak en yüksek 5 seçilmiştir. S= sıklık anlamına gelmektedir.

Çizelge 4.5. Risk sıklığı değeri (Astuti ve diğerleri, 2017; ISACA, 2013)

Sıklık Değeri	Sıklık	Açıklama
1	$S \leq 0{,}2$	Çok Düşük (Olma olasılığı çok düşüktür) Yılda 0.2 kere olabilir
2	$0{,}2 < S \leq 1$	Düşük (Bazı durumlarda meydana gelmektedir) Yılda 0.2 – 1 kere meydana gelebilir
3	$1 < S \leq 10$	Orta (Bazen meydana gelmektedir) Yılda 1 – 10 kere meydana gelebilir
4	$10 < S \leq 110$	Yüksek (Meydana gelmeye yatkındır) Yılda 10 – 110 kere meydana gelebilir
5	$110 < S$	Çok Yüksek (Sürekli meydana gelmektedir) Yılda 110'dan fazla meydana gelebilir

Çizelge 4.5'te görüldüğü üzere yüksek seviyesindeki risk sıklığında 4 değeri için yılda 10 ile 110 (dâhil) arasında meydana gelmesi gerekmektedir.

COBIT 5 riskin şiddetini; verimlilik değeri, tepki maliyeti, rekabet avantajı, kanun yönü olmak üzere dörde ayırmıştır. Verimlilik değeri, hizmet masası personelinin bir yıl içinde sebep olduğu finansal kaybı ölçmektedir. Tepki maliyeti, riskin önlenmesi için gereken parayı göstermektedir. Rekabet avantajı değeri, risk sonucunda kullanıcı tatminindeki azalmayı göstermektedir. Kanun yönü, organizasyonun yasalara göre ne kadar ceza ödeyeceğini ölçmektedir. Risk şiddeti bu dört değerin ortalamasından oluşmaktadır. (V= Verimlilik, M= Maliyet). Örnek Risk değerlendirme sonucu Çizelge 4.6'da verilmiştir.

Çizelge 4.6. Risk değerlendirmesi (Astuti ve diğerleri, 2017; ISACA, 2013)

Şiddet Değeri	Verimlilik Değeri	Tepki Maliyeti	Rekabet Avantajı	Kanun Yönü
1	V ≤ %1	V ≤ M 1 milyon	V ≤ 1	< M 1 milyon
2	%1 < V ≤ %3	M 1 milyon < V ≤ M 10 milyon	1 < V ≤ 1,5	< M 10 milyon
3	%3 < V ≤ %5	M 10 milyon < V ≤ M 100 milyon	1,5 < V ≤ 2	< M 100 milyon
4	%5 < V ≤ %10	M 100 milyon < V ≤ M 500 milyon	2 < V ≤ 2,5	< M 500 milyon
5	%10 < V	M 500 milyon < V	2,5 < V	> M 500 milyon

Çizelge 4.6'da görüldüğü üzere şiddet değerinin 3 olması için verimlilik değerinin %3 ile %5 (dâhil) arasında olması, tepki maliyetinin, 10 milyon ile 100 milyon (dâhil) arasında olması, rekabet avantajı için 1,5 ile 2 (dâhil) arasında olması ve kanun yönünün 100 milyondan düşük olması gerekmektedir.

Risk hesaplaması sonucunda ilgili risk kategorisine ve sürecine uygun olarak gerekli görülen risklerde COBIT 5'in sürecinde önerdiği risk azaltma planı uygulanmaktadır. Risk değerlendirme sonucuna uygun olan risk azaltma planı uygulanmalıdır. Risk değerlendirme sonucunda şiddet ortalaması ve risk seviyesi Çizelge 4.7'de gösterilmektedir.

Çizelge 4.7. Risk değerlendirme sonucu (Astuti ve diğerleri, 2017; ISACA, 2013)

Risk No	Risk	Sıklık	Şiddet Ortalaması	Risk Seviyesi
ABC01	Virüs Saldırısı	3	2	Orta

Çizelge 4.7'de görüldüğü üzere risk değerlendirme sonucunda ABC01 risk numarasına sahip olan riskin sıklığı, 3; şiddet ortalaması, 2; risk seviyesi orta olarak belirtilmiştir. Sonuca uygun olan riske tepki planı gerçekleştirilir ve risk azaltması uygulanır.

4.2. Risk Yönetimi Örnek Uygulaması (1)

Risk yönetimi hesaplamaları için oluşturulan tüm taslaklar ve hesaplama yöntemleri ve anlatımlar dört farklı kaynaktan yararlanılarak ortaya çıkarılmıştır (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007).

4.2.1. Varlıkların belirlenmesi

Varlıkların belirlenmesi süreci görüşme, anket, toplantı gibi yollar ile bilgi işlem ve kritik iş birimlerinin bir araya gelmesiyle başlamaktadır. Riskin belirlenmesi için süreç bazlı varlıklar ve fiziksel varlıklar belirlenmelidir. Çizelge 4.8 ve Çizelge 4.9'da varlık envanteri düzenlenmiştir.

Çizelge 4.8. Fiziksel envanter (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

Varlık Numarası	1	2
Varlık Kodu	A10	Ö11
Varlık Adı	Klima	Çalışma Odası
Varlık Kategorisi	Altyapı ve Tesisat	Özel Alanlar
Varlığın Sahibi	Bilgi İşlem	Bilgi İşlem
Varlığın Kullanıcısı	İlgili Personel	İlgili Personel
Varlığın Yeri	Bilgi İşlem Binası	Bilgi İşlem Binası
Gizlilik Değeri (G)	3	2
Bütünlük Değeri (B)	3	3
Erişilebilirlik Değeri (E)	2	2
Toplam Değer (G+B+E)	8	7
Maddi Değeri	20 000	5 000
Açıklama		

Çizelge 4.8'de görüldüğü üzere fiziksel envanterde varlıkla ilgili genel bilgiler, sahipliği, bulunduğu yer, varlık değeri ve varlığa zarar gelmesi durumundaki maddi değeri belirtilmektedir.

Çizelge 4.9. Süreç tabanlı envanter (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

Süreç Adı	İşten Ayrılma Süreci	İşten Ayrılma Süreci
Süreç No	SRC1-1	SRC1-2
Süreç	İşten ayrılacak personel yazı ile talepte bulunur ve işten ayrılmadan önce zimmetinde bulunan demirbaşları teslim eder	İşten ayrılan personelin tüm hesapları insan kaynaklarının yazısıyla pasif hale getirilir
Süreç Sahibi	Bilgi İşlem/İnsan Kaynakları	Bilgi İşlem/İnsan Kaynakları
Süreç Sorumlusu	Kurum	Kurum
Bulunduğu Yer	Genel Müdürlük	Genel Müdürlük
Bilgiyi İşleyen Yazılımlar	ORACLE	ORACLE
Bilgiyi İşleyen Donanımlar	Masaüstü Bilgisayar	Masaüstü Bilgisayar
Bilgiye Erişim Yetkisi Olan Kişiler	İlgili Kişiler	İlgili Kişiler
Gizlilik Değeri	2	4
Bütünlük Değeri	2	3
Erişilebilirlik Değeri	2	3
Toplam Değer	6	10
Açıklama		

Çizelge 4.9'da görüldüğü üzere süreç bazlı envanterde süreçle ilgili genel bilgiler, sürecin sahipliği/sorumlusu, bulunduğu yer, erişim yetkisi bilgisi, varlık değeri yer almaktadır.

Varlık envanterinde yer almakta olan gizlilik, bütünlük ve erişilebilirlik için değer tablosundan Çizelge 4.10'dan yararlanılır.

4.2.2. Risklerin sayısallaştırılması ve ölçülmesi

Her bir bilgi varlığına, gizlilik, bütünlük ve erişilebilirlik açısından çok düşük, düşük, orta, yüksek ve çok yüksek olmak üzere değer verilir. Çizelge 4.10'da varlığın gizlilik, bütünlük, erişilebilirlik için değer ve değer kriterleri verilmiştir.

Çizelge 4.10. Gizlilik, erişilebilirlik, bütünlük değerleri (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	1	2	3	4	5
Gizlilik	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu etkilemez.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
Bütünlük	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkilemez.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
Erişilebilirlik	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu etkilemez.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki orta vadede telafi edilebilir	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.

Çizelge 4.10'da belirtildiği üzere değer kriteri varlığa zarar gelmesi durumunda varlığa ait zararın derecesini ve telafi edilebilirliğini içermektedir. Varlığın gizlilik seviyesinin 4 olması için varlığa zarar geldiğinde önemli bilgiler ortaya çıkar ve organizasyon zararı orta vadede telafi edebilir.

Varlık değerleri hesaplaması için gizlilik, bütünlük, erişilebilirlik değerleri toplanmaktadır. Çizelge 4.11'de varlık değeri hesaplaması yapılmıştır.

Çizelge 4.11. Varlık değeri hesaplaması (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

Gizlilik	Bütünlük	Erişilebilirlik	Varlık Değeri
Yüksek	Çok Yüksek	Çok Yüksek	4+5+5=14
Yüksek	Düşük	Yüksek	4+2+4=10

Çizelge 4.11'de görüldüğü gibi gizlilik, bütünlük, erişilebilirlik değerleri sırasıyla; 4,5,5 olarak verilmiş ve varlık değeri ise 14 olmuştur.

4.2.3. Süreklilik değerleri (SD)

Risk grubu; finansal zarar (TL), performans kaybı (saat), itibar kaybı (yer), uyumsuzluk (yer ve ceza) maddelerinden oluşmaktadır. Etki seviyesine uygun olan kriter seçilerek süreklilik değeri belirlenmektedir. Çizelge 4.12'de süreklilik değer tablosu örneği verilmiştir.

Çizelge 4.12. Süreklilik değeri tablosu (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

Süreklilik Değeri					
Etki Türü		**Finansal Zarar**	**Performans Kaybı**	**İtibar Kaybı**	**Uyumsuzluk**
Etki Seviyesi		**TL**	**Saat**	**Yer**	**Yer/Ceza**
Çok Yüksek	**5**	> 40 000	> 8	Tüm Medyada	Sözleşme ve yasalara uyumsuzluk sebebiyle aşırı maddi kayıp ve ceza
Yüksek	**4**	18 001 - 40 000	5-8	Bazı haberlerde	Sözleşme ve yasalara uyumsuzluk sebebiyle maddi kayıp ve ceza
Orta	**3**	10 001 - 18 000	3-5	Sektör çapında uygunsuz tanıtım	Sözleşme ve yasalara uyumsuzluk sebebiyle düşük seviyede maddi kayıp ve ceza
Düşük	**2**	4.001-10.000	3	Bir kaç müşteriye olumsuz tanıtım	Sözleşme ve yasalara uyumsuzluk sebebiyle uyarı
Çok Düşük	**1**	< 4 000	< 1	İhmal edilebilir	İhmal edilebilir

Çizelge 4.12'de görüldüğü üzere etki seviyesinin 3 olması durumunda; finansal değer 10 000-18 000 (dâhil) arasında yer alır, performans kaybı 3-5 saattir, sektör çapında itibar kaybı gerçekleşir, uyumsuzluk olarak düşük seviyede maddi ceza ve kayıp yaşanır.

4.2.4. Olasılık değerleri (OD)

Organizasyonun belirleyeceği zaman dilimine uygun olan yıl, ay, gün şeklinde gerçekleşme sıklığı değer verilerek belirlenir. Tehdidin meydana gelme olasılığı Çizelge 4.13'te gösterilmiştir.

Çizelge 4.13. Olasılık değeri (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

Olasılık Değeri	
Değer	**Açıklama**
1	10 yılda bir (Risk durumunun gerçekleşmesi söz konusu değil, istisnai durum İmkânsız ya da 10 yıl ve üzeri sıklıkta)
2	5 yılda bir (Risk, 1-5 yıl içinde bir kez oluşabilir Risk durumu ancak çok özel koşullar altında söz konusu olabilir)
3	Yılda bir (Risk, 1 yıl içinde en az bir kez oluşabilir, ortam gerçekleşmesi için uygun)
4	3 ayda bir (Risk, 3 ay içinde en az bir kez oluşabilir, ortam gerçekleşmesi için son derece uygun)
5	Ayda bir (Risk, 1 ay içinde en az bir kez oluşabilir, ortam gerçekleşmesi için son derece uygun çok kolay uygulanabilir)

Çizelge 4.13'te görüldüğü üzere olasılık değerinin 3 olması için; riskin en az yılda bir kez oluşması ve riskin meydana gelebileceği ortamın bulunması gerekir.

4.2.5. Aksiyon öncesi risk değeri

Aksiyon öncesi risk değeri hesaplaması; Risk değeri=Varlık değeri*Süreklilik değeri*Tehdit olasılığı değeri, şeklinde yapılır. Çizelge 4.14'te aksiyon öncesi risk hesaplaması yapılmıştır.

Çizelge 4.14. Aksiyon öncesi risk değeri hesaplaması (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

Varlık Değeri	**Süreklilik Değeri**	**Tehdit Olasılığı**	**Risk Değeri**
9	Düşük=2	Orta=3	9*2*3=54
5	Yüksek=4	Yüksek=4	5*4*4=80

Çizelge 4.14'te gösterildiği üzere varlık değeri 9 olan bir varlığın, süreklilik değerinin 2, tehdit olasılığının 3 olması durumunda risk değeri 54 olarak hesaplanmıştır.

4.2.6. Aksiyon sonrası risk değeri

Alınan aksiyonlar ve uygulanan kontroller belirtilerek aksiyon sonrası süreklilik değeri, olasılık değeri ve kalan risk durumu hesaplanır. Aksiyon sonrası yeni belirlenen süreklilik ve olasılık değeri risk değerini değiştirmektedir. Yeni oluşan risk değeri, kalan riski vermektedir. Çizelge 4.15'te aksiyon sonrası risk değeri hesaplaması gösterilmektedir.

Çizelge 4.15. Aksiyon sonrası risk değeri (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

Varlık Değeri	Süreklilik Değeri	Tehdit Olasılığı	Risk Değeri	Aksiyon Sonrası (SD)	Aksiyon Sonrası (OD)	Risk Değeri	Kalan Risk
9	Düşük=2	Orta=3	9*2*3=54	2	2	9*2*2=36	36
5	Yüksek=4	Yüksek=4	5*4*4=80	3	2	5*3*2=30	30

Çizelge 4.15'te görüldüğü üzere aksiyon sonrası risk hesaplamasında; varlık değeri 9, süreklilik değeri 2, tehdit olasılığı 3, risk değeri 54 olduğunda aksiyon alındıktan sonra süreklilik değeri değişmemiştir; fakat tehdit olasılığı azaldığı için yeni ve kalan risk değeri 36 olmuştur.

4.2.7. Risk limitlerinin tanımlanması

Kabul edilebilir risk eşiği hesaplanırken orta seviye varlık değerinin toplamının, orta seviye süreklilik değeri ve tehdit olasılığı ile çarpıldığında (9*3*3=81) kabul edilebilir veya kontrol konulabilir risk seviyesi bu değer ve aşağısı olacaktır. Yüksek olduğunda kontrol alınması zorunlu veya yönetim kararına bağlı olarak kontrol alınacaktır. Örnekte en yüksek risk değeri (15*5*5=225) olmaktadır.

4.2.8. Risklerin yanıtlanması

Risk limitleri belirlendikten sonra risk iştahına uygun olarak riskler değerlendirilir. Düşük düzeydeki riskler için kontrol alınabilir ancak zorunluluk yoktur. Kabul edilebilir düzeyin üzerindeki riskler için risk azaltma, risk önleme, risk transfer etme vb. önlemler alınır. Çizelge 4.16'da ölçüm parametresi, risk seviyesi ve risk iştahı verilmiştir.

Çizelge 4.16. Ölçüm parametresi, risk seviyesi ve risk iştahı (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

Ölçüm Parametresi	Risk Seviyesi	Risk İştahı
Risk ≤ 81	Düşük	Kabul Edilebilir
81 < Risk ≤ 225	Orta/Yüksek	Zorunlu Önlem

Çizelge 4.16'da görüldüğü üzere; risk parametresine göre 81 ve altındaki riskler için risk seviyesi düşük kabul edilir, 81 üstü riskler için risk seviyesi organizasyonun değerlendirmesine uygun olarak orta veya yüksek olarak nitelendirilir. Çıkan risk iştahı durumuna uygun olan aksiyonlar alınır.

4.2.9. Risklerin izlenmesi, analizi ve denetimi

Risk izleme ve değerlendirme çalışmaları yılda en az bir kez değişen kritik iş süreçleri, yeni eklenen bilgi varlıkları, değişen iş koşulları, tehditler, zafiyetler, olasılıklar vb. değerlendirilerek yapılmalıdır. YGG toplantılarında risk yönetimi ele alınmalıdır. Fiziksel ve süreç bazlı varlıklar için risk kataloğu hazırlanmalıdır. Risk kataloğu içeriğinde; varlığın risk kontrolü uygulanmadan önceki durumu ve risk kararı sonrası toplam değeri belirtilmelidir. Çizelge 4.17 ve Çizelge 4.18'de fiziksel ve süreç bazlı varlıklara ait risk kataloğu verilmiştir.

Çizelge 4.17. Fiziksel risk kataloğu (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

No	Ö11
Varlık	Çalışma Odası
Varlık Değeri	7
Zafiyet	Binada yeterli fiziksel güvenliğin bulunmaması
Tehdit	Çevresel tehdit
Risk	Finansal Zarar
Risk Sahibi	Sorumlu Personel
Mevcut Kontroller	Binaya giriş çıkışlarda kartlı sistemin bulunması
İlave Kontrol Öncesi Süreklilik Değeri	3
İlave Kontrol Öncesi Tehdit Olasılığı	3
İlave Kontrol Öncesi Toplam Değer	(7*3*3) 63
Risk Kararı	Kontrol (azaltma)
İlave Kontrol	Özel güvenlik alınmalı
İlave Kontrol Sonrası Süreklilik Değeri	2
İlave Kontrol Sonrası Tehdit Olasılığı	3
İlave Kontrol Sonrası Toplam Değer	(7*2*3)= 42

Çizelge 4.17'de görüldüğü üzere fiziksel varlık ile ilgili değerler, varlık sahipliği, mevcut kontroller, kontrol sonrası risk değeri, risk kararı ve ilave kontroller sonrası toplam değeri içeren risk kataloğu tanımlanır. Çalışma odası örneği için; varlık değeri 7, çevresel tehdit kaynaklı, sorumlu personeli tanımlı, mevcut kontrolü kartlı girişin bulunması, ilave kontrol öncesi risk değeri 63, risk kararı olarak; özel güvenlik alınarak risk azaltımı uygulanması neticesinde kontrol sonrası değeri 42'dir.

Fiziksel risk kataloğundan farklı olmak üzere ilgili varlıklarda fiziksel ve süreç bazlı varlıkları içeren süreç bazlı risk kataloğu Çizelge 4.18'de gösterilmiştir.

Çizelge 4.18. Süreç bazlı risk kataloğu (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

No	SRC1-2
Süreç	İşten Ayrılma Süreci
Süreç Değeri	10
Zafiyet	İnsan kaynaklarının talepte bulunmaması
Tehdit	İnsan kaynaklı (yetkililerin olmaması)
Risk	Bilgilerin dışarı çıkarılması
Risk Sahibi	Kurum
Mevcut Kontroller	Yeni personel alımı yapılması
İlave Kontrol Öncesi Süreklilik Değeri	3
İlave Kontrol Öncesi Tehdit Olasılığı	3
İlave Kontrol Öncesi Toplam Değer	(10*3*3) 90
Risk Kararı	Kontrol (azaltma)
İlave Kontrol	Eğitimlerin yapılması
İlave Kontrol Sonrası Süreklilik Değeri	1
İlave Kontrol Sonrası Tehdit Olasılığı	2
İlave Kontrol Sonrası Toplam Değer	(10*1*2) 20
İlgili Varlıklar	(İ10), (Ö11)

Çizelge 4.18'de görüldüğü üzere süreç bazlı risk kataloğunda süreç ile ilgili değerler, süreç sahipliği, mevcut kontroller, kontrol sonrası risk değeri, risk kararı ve ilave kontroller sonrası toplam değeri içeren risk kataloğu tanımlanır. İşten ayrılma süreci örneği için; süreç değeri 10, insan kaynaklı tehdit, sorumlu personeli tanımlı, mevcut kontrolü personel alınması, ilave kontrol öncesi değeri 90, risk kararı olarak; eğitim alınarak risk azaltımı uygulanması neticesinde kontrol sonrası değeri 20 olmuştur. İlgili varlıkları tanımlanan varlık numarasına göre belirtilmiştir.

4.3. Risk Yönetimi Uygulaması (2)

Risk yönetimi hesaplamaları için oluşturulan tüm taslaklar ve hesaplama yöntemleri ve anlatımlar dört farklı kaynaktan yararlanılarak ortaya çıkarılmıştır (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007).

Varlıkların belirlenmesi: Görüşme, anket, toplantı vb. yollar ile bilgi işlem ve kritik iş birimlerinin bir araya gelmesiyle fiziksel ve süreç bazlı varlıklar belirlenmektedir. (Bkz. Çizelge 4.8), (Bkz. Çizelge 4.9).

Varlık envanterinde yer almakta olan gizlilik, bütünlük ve erişilebilirlik için değer tablosundan yararlanılır. (Bkz. Çizelge 4.10).

Risklerin sayısallaştırılması ve ölçülmesi: Her bir bilgi varlığına, gizlilik, bütünlük ve erişilebilirlik açısından çok düşük, düşük, orta, yüksek ve çok yüksek olmak üzere değer verilir. (Bkz. Çizelge 4.10), (Bkz. Çizelge 4.11).

4.3.1. Tehditlerin belirlenmesi

Zafiyetlerin yol açabileceği tehditler ve tehdit kategorisi belirlenir. Her bir tehdidin olasılığı ve etkileyeceği kriterler belirlenir. Tehditlerin derecesi; çok düşük, düşük, orta, yüksek ve çok yüksek olmak üzere belirlenir. Çizelge 4.19'da tehdit değer tablosu gösterilmiştir.

Çizelge 4.19. Tehdit değeri (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

Tehdit Değeri	
Çok Düşük (1)	Tehdidin etkisi yoktur
Düşük (2)	Tehdidin iş üzerinde az bir etkisi olur.
Orta (3)	Tehdidin etkisi küçük olmasına rağmen, hasarın yok edilmesi ve önlem için harcamalar olabilir
Yüksek (4)	İtibar kaybına ve önemli harcamalara neden olabilir
Çok Yüksek (5)	Zarar derecesi oldukça büyüktür veya sistemde büyük ölçüde yeniden yapılandırmaya gerek vardır

Çizelge 4.19'da belirtildiği üzere yüksek seviyesindeki tehdit değerinin olması için itibar kaybı ve önemli harcamalara neden olması gerekmektedir.

4.3.2. Zafiyet değerleri

Her bir varlık için olası zafiyetler, zafiyetin kategorisi ve zafiyetin derecesi (etkisi); çok düşük, düşük, orta, yüksek ve çok yüksek olmak üzere belirlenir. Zafiyet değer tablosu Çizelge 4.20'de gösterilmiştir.

Çizelge 4.20. Zafiyet değeri (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

Zafiyet Değeri	
Çok Düşük (1)	Tehdidin kullanacağı zayıflık yoktur.
Düşük (2)	Tehdidin kullanacağı zayıflığı çok azdır.
Orta (3)	Tehdidin kullanacağı zayıflık az düzeydedir.
Yüksek (4)	Tehdidin kullanacağı zayıflık bulunmaktadır.
Çok Yüksek (5)	Tehdidin kullanacağı zayıflık değeri yüksektir.

Çizelge 4.20'de gösterildiği üzere zafiyet değerinin çok yüksek olması için tehdidin kullanacağı zayıflık değerinin yüksek olması gerekmektedir.

Risk olasılık değeri için (Bkz. Çizelge 4.13).

4.3.3. Aksiyon öncesi risk değeri

Aksiyon öncesi risk değeri hesaplanır. Etki Değeri*Olasılık değeri, Risk Değerini vermektedir. Yani Risk=Varlık Değeri*Tehdit Değeri*Zafiyet Değeri*Olasılık olarak hesaplanmaktadır. Aksiyon öncesi risk değeri Çizelge 4.21'de gösterilmektedir.

Çizelge 4.21. Aksiyon öncesi risk değeri (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

Varlık Değeri	Tehdit Derecesi	Zafiyet Derecesi	Olasılık	Risk Değeri
9	Düşük=2	Orta=3	4	9*2*3*4=216
5	Yüksek=4	Yüksek=4	5	5*4*4*5=400

Çizelge 4.20'de belirtildiği üzere varlık değeri 9, tehdit derecesi 2, zafiyet derecesi 3, olasılığı 4 olan varlığın risk değeri 216 olarak hesaplanmıştır.

4.3.4. Aksiyon sonrası risk değeri

Alınan aksiyonlar ve uygulanan kontroller belirtilerek aksiyon sonrası olasılık değeri ve kalan risk durumu hesaplanır. Aksiyon alınmışsa olasılık değerinin düşeceği düşünülür. Aksiyon sonrası risk değeri Çizelge 4.22'de gösterilmiştir.

Çizelge 4.22. Aksiyon sonrası risk değeri (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

Varlık Değeri	Tehdit Derecesi	Zafiyet Derecesi	Olasılık	Risk Değeri	Aksiyon Sonrası Olasılık	Risk Değeri	Kalan Risk
9	Düşük=2	Orta=3	4	9*2*3*4=216	2	9*2*3*2=108	108
5	Yüksek=4	Yüksek=4	5	5*4*4*5=400	1	5*4*4*1=80	80

Çizelge 4.22'de aksiyon sonrası risk değeri hesaplamasında; varlık değeri 9, tehdit derecesi 2, zafiyet derecesi 3, olasılık derecesi 4, risk değeri 216 olarak bulunan varlığın aksiyon alındıktan sonraki olasılığı azalmış ve yeni/kalan risk değeri 108 olmuştur.

Her bir varlık için kalan riskler arasındaki en büyük değer o varlık için genel risk durumunu belirtmektedir.

4.3.5. Risk limitlerinin tanımlanması

Kabul edilebilir risk eşiği hesaplanırken en yüksek varlık değeri (15), düşük tehdit veya zafiyet seviyesi değeri (1) Yüksek tehdit veya zafiyet seviyesi değeri (5) ve olasılığı 5 yılda bir alınırsa değeri (2) dir. Kabul edilebilir risk değeri 15*1*5*2=150 ve aşağı bir değer olacaktır.

Risk değeri 150 den büyük olan ve en yüksek varlık değeri (15), orta seviye tehdit veya zafiyet seviyesi değeri (3) , orta seviye tehdit veya zafiyet seviyesi değeri (3) ve olasılığı 5 yılda bir alınırsa değeri (2) olmaktadır. Orta seviye risk değer sınırı 15*3*3*2=270 arasındaki riskler çok sıkı şekilde takip edilmeli ve risk değerinin 150 ve altı bir değere indirilmesi için aksiyonlar alınmalıdır.

Risk değeri 270 üstü riskler kabul edilemez olarak değerlendirilmeli ve kabul edilebilir seviyeye veya en azından 270 ve altı bir değere indirmek için kritikliğine göre önceliklendirmeler yapılarak kontroller devreye alınmalıdır.

4.3.6. Risklerin yanıtlanması

Risk limitlerinin belirlenmesinin ardından, risk iştahına uygun olarak riskler değerlendirilir ve ilgili aksiyonlar alınır. Ölçüm parametresinin büyüklüğüne uygun olarak risk seviyesi ve risk iştahı belirlenmektedir. Ölçüm parametresi, risk seviyesi ve risk iştahı Çizelge 4.23'te gösterilmektedir.

Çizelge 4.23. Ölçüm parametresi, risk seviyesi ve risk iştahı (Koç F. , 2008; İLBANK, 2015; Ersoy, 2012; Eskiyörük, 2007)

Ölçüm Parametresi	Risk Seviyesi	Risk İştahı
Risk ≤ 150	Düşük	Kabul edilebilir
150 < Risk ≤ 270	Orta	İhtiyatlılık gerektiren
Risk >270	Yüksek	Tehlikeli

Çizelge 4.23'te belirtildiği üzere ölçüm parametresinde 150 ve aşağısında kalan risk seviyesi düşük ve kabul edilebilir olarak nitelendirilirken, risk seviyesi 270 üstü riskler için risk seviyesi yüksek ve kontrol alınması gerekli görülür.

4.4. Bilgi Teknolojileri Risk Yönetimi Alanında Yapılmış Olan Çalışmalar

Bandyopadhyay ve grubu bilgi teknolojileri ile bütünleşmiş bir risk çerçevesi geliştirilmesi çalışması yapmıştır. Geliştirilen çerçeve; riskin tanımlanması, riskin analizi, risk azaltmak için alınan önlemler ve riskin izlenmesi aşamalarından oluşmaktadır. Aşamalardan herhangi birini öne çıkarmak yerine tüm aşamaları sırasıyla uygulayarak BT risk yönetiminin tümüne etki edecek şekilde bir çerçeve geliştirilmiştir. Yöntemin yöneticilere, organizasyonun genel risk yönetimi durumu hakkında kapsamlı bir şekilde bilgi verilmesine olanak sağlayacak bir sistem olduğunu vurgulamışlardır (Bandyopadhyay, P. Mykytyn ve K. Mykytyn, 1999).

2005 yılında yapılan bir çalışmada geleneksel risk analizi yöntemlerinin bilgi güvenliğini sağlamada yetersiz olduğu vurgulanmış ve alternatif yaklaşımın somut

varlıkların yanı sıra soyut varlıkları da içine alan bütünsel bir risk yönetimi yaklaşımını sağlaması amaçlanmıştır. Risk yönetiminin verimli bir şekilde yapılabilmesi için risk analizinde finansal, yasal dayanak ve politikalar gibi faktörlerin dikkate alınarak yapılması gerektiğini belirtmişlerdir. Risk analizi (tanımlama, tahmin, değerlendirme) ve risk yönetimi aşamalarından oluşmaktadır. Bilgi güvenliği gereklilikleri, her bir organizasyonun sahip olduğu benzersiz özelliklere dayalı olarak bilgi kaynaklarının etkin bir şekilde korunması için gereken güvenlik miktarı ve spesifikasyonları ile belirlenmiştir. Bilgi güvenliği gereksinimlerinin, yalnızca maddi varlıklara ilişkin riskleri değil, aynı zamanda bilgi veya maddi olmayan varlıklara yönelik riskleri de analiz etmesini önermiştir (Gerber ve Solms, 2005).

2008 yılında yapılan bir çalışmada bilgi güvenliği yatırımlarının belirlenmesiyle ilgili çıkabilecek problemlerin analizi açıklanmıştır. Analiz sonucunda standart bir yaklaşımın geliştirilmesiyle sorunlara çözüm olunabileceğinden bahsedilmiştir. Yaklaşım içeriği; bilgi varlıklarının tanımlanmasını sağlayan bir yöntemin geliştirilmesi ile başlamaktadır. Varlıkların tanımlanmasıyla organizasyonun niçin ve neyi korunması gerektiğinin anlaşılması sağlanmaktadır. Sunucular, ağ altyapısı, gibi somut varlıkların değerinin maddi olarak ölçülebildiği için kolay; veri, itibar, fikri mülkiyet gibi soyut varlıkların değerinin belirlenmesinin maddi olarak ölçülemediği için zor olduğu belirtilmektedir. Varlıkların; kritik, orta ve düşük olmak üzere üç grupta sınıflandırılabileceği ve kritik olarak; fikri mülkiyet, orta olarak; işletme içi bilgiler ve düşük olarak; erişilebilir web sayfaları vb. gösterilmiştir.

İkinci olarak tehdit analizi yapılır ve organizasyonun iş süreçlerinde karşı karşıya kalacağı tehditler hakkında bilgi sağlanmaktadır. Tehditleri insan kaynaklı ve doğal afetler olarak ayırmış olmakla birlikte insan kaynaklı tehditler kötü niyetli olarak ve kötü niyet aranmadan olarak ayrılmıştır. Yaklaşım, devam eden işleri etkileyebilecek bilginin korunması gerekliliğinin anlaşılmasını sağlamaktadır. Zafiyet analizi ile tehdidin nerede ve nasıl oluşabileceği gösterilmektedir. Zafiyetlerin; güvenlik prosedürlerinde, teknik kontrollerde, fiziksel kontrollerde ve diğer kontrollerde bulunduğu tehdide açık hale getirmesinden bahsedilmiştir. Zafiyetlerin en çok teknik konulardan kaynaklandığı bilinse de asıl açıklığa sebep olanların insan faktörü olduğu belirtilmiştir. İnsan faktörlü açıklıklar olarak; şifre paylaşımı, güvenlik politikalarının ihmal edilmesi gibi örnekler verilmiştir.

Tanımlanmış zafiyet ve riski azaltan ilgili kontrollerin birleşimi ile tehdidin oluşma ihtimali tahmin edilebilmektedir.

Risk değerlendirmesi için yaklaşımlar üzerinde durulmuştur. Risk değerlendirme yöntemleri olarak; OCTAVE, FRAP, FAA, CRAMM ve INFOSEC örnekleri verilmiştir. Risk azaltıcı stratejilere örnek verilmiştir. Risk tanımlandıktan sonra, riskleri azaltmak için güvenlik yatırımlarını değerlendirecek finansal ölçümler uygulanabilmektedir. Güvenlik olaylarıyla ilişkili finansal riski belirlemek için hiçbir standart model bulunmadığından maliyetin hesaplanmasına yönelik yöntemler olarak birkaç yöntemin kullanılmasının gerekliliğinden bahsedilmiştir. Finansal yönden hesaplama olarak iç verimlilik oranının (İVO), net bugünkü değer (NBD) ve yatırım getirisi (ROI) formülleri kullanılmıştır. Kullanılan yöntemlerden bazıları donanım, yazılım ve servis maliyetlerini içerirken, bazıları dolaylı yük giderleri de dâhil olmak üzere iç maliyetleri ve verimlilik üzerindeki uzun vadeli etkileri de içermektedir. Yöntemlerin ayrı ayrı kullanımı uygun bir çözüm oluşturmadığı için yöntemlerden kombinasyon oluşturularak kullanılması gerekliliği önerilmiştir (Bojanc ve Blazic, 2008).

2011 yılında yapılan bir çalışmada BGYS çerçevesi ele alınmıştır. Çerçeve, kapsam ve kriterlerin bulunduğu yapısal bölüm, süreç ve araçların bulunduğu prosedürel bölüm olarak ayrılmıştır. Kapsam kısmı; strateji, teknoloji, organizasyon, insan ve çevre olarak ayrılmıştır. BGYS ile ilgili geniş kapsamlı konularda kullanılabileceği belirtilmiştir. Kriter kısmı; gereksinimler, standartlar, maliyet, karşılaştırmalı değerlendirmeler olarak ayrılmıştır. ISO bilgi güvenliği kontrolleri ve önceden belirlenen karşılaştırmalı kriterleri de içeren bir yönetim kriteri kullanımını sağlamaktadır. Araçlar kısmı; toplanan bilgiler, matematiksel modeller, geçmiş çalışmalar olarak ayrılmıştır. Süreçler kısmı; tanımlama, ölçme, analiz etme, geliştirme ve kontrol olarak ayrılmıştır. BGYS yöntemlerinin çeşitli süreçlerini birleştirilmiş ve yaygın şekilde kabul gören bir süreç içinde barındırmasına izin verdiği belirtilmiştir. BGYS yöntemlerinde olduğu üzere, sürecin çeşitli aşamalarının etkili bir şekilde gerçekleştirilmesi için destek araçlarının kullanımı da önerilmektedir (Saleh ve Alfantookh, 2011).

2011 yılında BT altyapısı ve hizmet yönetimi için rasyonel uygulamaları kullanmaları için organizasyonların mevcut ihtiyaçları üzerine araştırma yapılmıştır. ITIL ve Proje Yönetimi Bilgi Tabanı (PMBOK) gibi bilgi teknolojileri yönetimi için kullanılan en

iyi uygulamalar açıklanmıştır. Standartlara, yönergelere ve en iyi uygulamalara rağmen risk yönetimi prosedürlerinin uygulamada doğaçlama olarak yapıldığı belirtilmiştir. Otomasyon, standardizasyon ve bilginin tekrar kullanımının olmaması, risk yönetimini verimsiz yapan ve hatta çevreye zarar veren nedenler olduğu belirtilmiş ve iş akışı tabanlı bir risk yönetimi çerçevesi oluşturulmuştur. Risk olaylarının olasılıklarını ve etki faktörlerini değerlendirmek için geçmiş iş akışları kayıtlarından bilgi toplanması gerekmektedir. Veri toplama prosedürü yalnızca insan tecrübesine dayanarak yapıldığında çok zaman ve kaynak harcanmakta ve sonuçlar yanlış kararlara yol açabilmektedir.

Çerçeve risk bilgilerinin etkileşimli ve kapsamlı raporlarda düzenlenmesine olanak sağlamaktadır. Yöneticilere, tehditlerin hızlı bir şekilde belirlenmesi ve risk azaltma çabalarının etkili bir şekilde yönetilmesini sağlayan, farklı seviyelerde otomatik olarak değerlendirilen risklere karşı genel bir bakış açısı sağlamaktadır. Bilgi teknolojileri değişiklik yönetimi ve bilgi teknolojileri proje yönetimi olmak üzere iki farklı senaryoda belirtilen olay incelemeleri, çerçevenin en az iki farklı ortama uygulanabileceğini ve belirli ihtiyaçları daha iyi yansıtacak şekilde özelleştirilebileceğini göstermiştir. Sonuçların, önerilen çerçevenin jenerik olduğunu ve daha geniş bir çevrede uygulanabileceği belirtilmiştir. Her bir modül kendi içinde bağımsız olarak hesaplama yapmaktadır. Çerçeve olasılık ve etki tahminleri için veri toplama gibi belirli prosedürleri otomatikleştirerek risk yönetimine fayda sağlamaktadır.

Vaka analizlerinden yola çıkarak riskleri temsil eden olayların sınıflandırılması önerilmiştir. Sınıflandırma yapılırken yönetici görüşlerini yansıtan olayların birlikte gruplandırılmasının faydalı olduğu ve böylelikle risk değerlendirmesi sonuçlarının daha anlamlı olduğuna değinilmiştir. İş akışları arasındaki benzerliği hesaplamak için bir strateji ortaya atılarak, yeni tasarlanmış iş akışlarının analizinin otomatik değerlendirilerek bilginin yeniden kullanılması sağlanmıştır. Analiz edilen çevrenin farklarını dikkate alan olayların olasılıklarını ve etkilerini hesaplamak için farklı algoritmalar sunulmuştur. Kapsamlı ve etkileşimli risk raporları sağlamayı hedefleyen risk bilgilerini kategorize etme ve özetleme stratejileri önerilmiştir. Gelecekteki araştırmalarda çerçevenin genişletilerek olay yönetimi veya portföy yönetimi gibi diğer senaryolara da uygulanabileceği belirtilmiştir. Makale rastgele oluşturulan iş akışı yürütme kayıtları ve taklit BT ortamları üzerinde yapılmıştır. Gerçek veriler kullanılarak yapılacak olan çalışmanın ve raporların değerlendirilebileceğini tavsiye etmektedirler (Wickboldt ve diğerleri, 2011).

2011 yılında Bursa'da küçük ve orta ölçekli şirketlerde kurumsal bilgi güvenliği yönetimini etkileyen faktörler araştırılmıştır. Araştırmada kullanılan faktörler; güvenlik politikaları, organizasyon çapında güvenlik, varlık sınıflandırması ve varlık kontrolü, personel, fiziksel ve çevresel güvenlik, iletişim ve operasyon yönetimi, sistem geliştirme ve bakım, erişim kontrolü, iş sürekliliği yönetimidir. Araştırmanın sonucunda bir takım genel sonuçlar elde edilmiştir. Türkiye'de güvenlik politikalarının standartlara bağlı kalmaksızın şirketler tarafından bilgi güvenliği konusundaki sınırlı bilgilerine dayanarak oluşturulduğu belirtilmiştir. Durumun düzeltilmesi için, bilgi güvenliğinin uygulanmasında ülkeler arası kabul görmüş ve test edilmiş standartların takip edilmesi gerektiği belirtilmiştir.

Bilgi Güvenliği Yönetim Sistemlerinin oluşturulması, uygulanması ve belgelenmesinin gerekliliğinden bahsedilmiştir. BGYS uygulanırken, üst yönetimin desteğinin sağlanması ve personelin bu standartlara bağlı olarak oluşturulan politikalara uymasının bilgi güvenliğinin sağlanmasında etkili olacağı belirtilmiştir. BGYS'nin tüm gerekliliklerini (güvenlik uzmanı, teknik personel, danışmanlık hizmeti) sağladıktan sonra ülkeler arası geçerliliği olan bir sertifikanın alınması gerekliliğinden bahsedilmiştir. Bilgi güvenliğini sağlamada penetrasyon testlerinin öneminden ve periyodik olarak yapılması gerekliliğinden bahsedilmiştir. Güvenlik politikası, iletişim ve operasyon yönetimi geliştirildiğinde; personel, fiziksel ve çevresel güvenlik parametrelerinin de gelişeceği belirtilmiştir. Türk şirketlerinin farklı ülkelerdeki muadil şirketlere oranla BT güvenliğine fazla önem vermediği belirtilmiştir (Yıldırım, Akalp, Aytaç ve Bayram, 2011).

2013 yılında yapılan bir çalışmada bilgi sistemleri güvenliği yönetimi başarı faktörleri incelenmiştir. Başarı faktörlerinin, güvenlik yönetimi uygulamaları, organizasyon yapısı, çevresel etkiler ve kültür olmak üzere dörde ayrıldığı belirtilmiştir. Güvenlik yönetimi uygulamalarının içinde; informel kontrol (üst yönetim desteği), formel kontrol (yönetim) ve teknik bileşenler yer almaktadır. Organizasyon yapısında; iş gereksinimleri, iş hedefleri, güvenlik gereksinimleri, organizasyon büyüklüğü ve endüstri türü yer almaktadır. Çevresel etkilerde; devlet uygulamaları, kullanıcının katılımı ve endüstri etkisi yer almaktadır. Kültürde; farkındalık, motivasyon, odaklılık, inançlar yer almaktadır. Başarı faktörlerinin bir organizasyon içindeki iş süreçleri ve insan kontrolü arasındaki dengeyi sağladığı belirtilmiştir. Yapılan incelemede organizasyonel yapının bilgi sistemleri güvenlik yönetimi uygulamalarını nasıl tespit ettiği gösterilmektedir. Organizasyon yapısı bilgi sistemleri güvenlik yönetiminin uygulanmasını gerçekleştirmektedir. Kültürün, bir

işletmenin bilgi sistemleri güvenlik yönetimi uygulaması başarısının şekillenmesine yardımcı olacağı belirtilmiştir (Norman ve Yasin, 2013).

Ankara'daki devlet üniversitelerinin BT risk yönetimi başarısını etkileyen dışsal faktörler (kurumsal, insan, çevresel, teknolojik) ile ilgili yapılan araştırmada kurumsal faktörlerde; üst yönetim desteği, BT bütçesi ve bilgi güvenliği politikaları risk yönetimi başarısının sağlanmasında ön plandadır. İnsan faktöründe; BT personeli yetkinliği, BT personeli deneyimi ve eğitim ön plandadır. Çevresel faktörlerde; standartlara uyum, yasalara uyum ve doğal tehditler ön plandadır. Teknolojik faktörlerde; yazılım güvenliği, kritik altyapı analizi ve donanım güvenliği ön plandadır. BT risk yönetimi başarısı göstergelerinde ise; hizmet sürekliliği ve kullanıcı memnuniyeti ön plandadır (Ateş ve Güneş, 2016).

SONUÇ VE ÖNERİLER

Bilgi toplumu çağında yaşamamız neticesiyle kurumsal veya bireysel olarak sürekli bilgi teknolojileri riskleriyle karşılaşmaktayız. Teknolojinin sürekli değişim göstermesiyle meydana gelebilecek risk çeşitliliğinde de artış olmaktadır. Toplum yaşamında bilgi teknolojilerinden tamamen kaçınmak olanaksız olduğu için mevcut olan risklere veya gelecekte oluşabilecek olan risklere karşı önlemlerin alınması gerekmektedir. Risk yönetimi ve yönetim çok yakın anlamlıdır. Yönetim, organizasyonu yönlendirmeyi ve faaliyet kontrolü sağlarken; risk yönetimi, organizasyonu yönlendirirken ve faaliyet kontrolü sağlarken riski temel alır (Lark, 2015). Tüm organizasyonlarda risk yönetimi gerekliliği bulunsa da özellikle bankacılık gibi parasal ve itibari kaybın yaşanabileceği alanlarda bilgi teknolojileri risk yönetimi daha çok önem taşımaktadır.

Bu tez çalışmasında bilgi, bilgi güvenliği ve özellikle risk kavramı üzerinde durulmuştur. Çalışmada; risk yönetimi için oluşturulan mevzuatlar, standartlar, yaklaşımlar, yöntemler ve yazılımlardan bahsedilmiş, risk yönetimi uygulamasına yönelik risk yönetimi sürecindeki adımlar aşamalı şekilde izlenerek, örnek olay olarak risk hesaplaması yapılmış ve risk yönetimi konusunda daha önce yapılan çalışmalara değinilmiştir. Çalışmada; bilgi teknolojilerinde risk yönetimi konusunda farkındalık oluşturmak, risklerin belirlenmesi ve değerlendirilmesi süreçleriyle ilgili bilgiler vermek amaçlanmıştır. Çalışmada elde edilen bilgiler doğrultusunda sonuçlar ve öneriler aşağıda ifade edilmiştir:

Bilgi teknolojilerine yapılan yatırımlar yıldan yıla artmaktadır. Bilgi teknolojilerine yapılan yatırımların yanında yatırımların sürdürülebilir olması önem taşımaktadır. Risklerin meydana gelmesinin en büyük kaynağı insan olduğu için sürdürülebilirliğin sağlanması için teknolojiyle birlikte insana da yatırım yapılması gerekmektedir.

Mevzuatta belirtildiği üzere risk ölçümü, uygulaması ve takibinin yapılması için süreçler ve prosedürler oluşturularak risk yönetimine sistematik bir şekilde yaklaşılması gerekmektedir. Mevzuatta, yılda en az bir kez sızma testinin ve risk değerlendirmesinin yapılması zorunlu kılınmıştır.

Kurumun yapısına ve ihtiyaçlarına uygun bilgi güvenliği yönetim sistemi kurulmalıdır. Sistem içinde PUKÖ döngüsü uygulanarak bilgi güvenliği yönetimi süreci

dinamikleştirilmelidir. Bilgi güvenliği risklerine karşı kontroller ancak sürekli güncellemenin yapılmasıyla geliştirilebilir.

COSO çerçevesinden faydalanarak kurum içinde risk yönetiminin geliştirilmesine yönelik kültürün oluşturulmasıyla uygun kontrol ortamı kurularak değer artırımı sağlanabilir.

İlke, çerçeve ve süreçten oluşan ISO 31000'de risk yönetimi sürecinin tüm aşamalarında iç ve dış paydaşlar ile sürekli iletişim içinde olunmalıdır. Risk yönetiminin etkili olmasını sağlamada izleme ve gözden geçirmenin her bir risk süreci aşamasında yapılması gerekmektedir.

Standartlara bağlı olarak şekillenen risk yönetimi planı uygulanmalı ve sürekli gelişimi sağlanmalıdır. Riskler, sadece bilgi işlem süreçlerinde değil tüm iş birimlerini kritik seviyede etkileyebilecek süreçleri kapsayacak şekilde belirlenmelidir.

Varlık envanteri oluştururken sadece fiziksel değil risklerin etkisinin tam anlamıyla belirlenmesi için süreç bazlı envanterin de oluşturulması gerekmektedir. Risk yönetimi hesaplamaları önceden her bir varlık baz alınarak hesaplanırken bu durum hem zaman alıcı hem de çıkan sonuçlar, süreçler ile etkileşim içinde olmadığı için tam anlamıyla risk değerini ifade etmemektedir. Mevcut çalışmalar özellikle süreç bazlı risk yönetimine odaklandığı için sürecin içinde etkisi olan varlıkların da hesabının yapılmasıyla daha etkili sonuçlar alabilmeyi sağlamaktadır. Süreç bazlı risk değerlendirmesinin geliştirilmesiyle süreç içinde değer kazanan varlıklarında dikkate alınmasıyla daha doğru sonuçlar alınmakta ve riske uygun aksiyonlar geliştirilmektedir.

Bilgi güvenliği ve risk yönetimi konusunda üst yönetim desteği sağlanmalı ve gerektiğinde kurallara uymama durumunda yükümlülükler getirilmelidir. Uluslararası mevcut olan uygulamalar sürekli olarak takip edilmeli ve risk yönetiminde bu uygulamalardan faydalanılmalıdır. Riskleri verimli bir şekilde yönetmek için fayda/maliyet analizinin doğru ve etkin yapılması gerekmektedir. Kullanılan koruma sistemlerinin iyi olması riskleri tamamen önlemeye yetmeyebilir veya kurum yatırımlarının gereksiz yere harcanmasına sebep olabilmektedir.

Bilgi teknolojileri denetimini süreçler üzerinden sağlayan COBIT riskin maliyetini de dikkate alan bir risk yönetim süreci geliştirmiştir. Risk hesaplamasında da yer verildiği üzere risk yönetiminin içeriğine senaryolar eklenmiştir. Riskin meydana geleceği en kötü durum ve riskin meydana gelmemesi durumundaki senaryolar ile risk yönetimine yeni bir bakış açısı getirilmiştir.

Bilgi teknolojileri risk yönetiminde öne çıkan iki yaklaşım karşılaştırıldığında kapsam olarak COBIT'in daha detaylı ve sadece bilgi işlemi değil bütünleşik yaklaşım ile tüm kurumu risk yönünden ele almasıyla BGYS'den daha geniş kapsamlı olduğu açıktır. COBIT 5, BT yönetişiminin sağlanmasına yönelik olarak ISO 31000, ISO 27001, COSO ve ITIL gibi kurumsal ve BT temelli standartlardan yararlanarak yeni bir çerçeve geliştirmiştir.

Risk yönetimi yaklaşımı seçilirken kurumun ihtiyaç ve imkânına uygun olmasına dikkat edilmelidir. Risk yönetimiyle ilgili yapılan çalışmalarda geleneksel risk analizi yöntemlerinin bilgi güvenliğini sağlamada yetersiz olduğu ve alternatif yaklaşım olarak soyut olan itibar vb. kavramların da dikkate alındığı bir risk analizi modelinin faydalı olacağı belirtilmiştir. Maliyet açısından verimlilik düşünüldüğünde sadece tek bir hesaplamaya bağlı kalmayıp farklı hesaplama yöntemleriyle karşılaştırılan sonuçların değerlendirilmesi daha doğru sonuçlar çıkarmaya yardımcı olacaktır (Bojanc ve Blazic, 2008).

Risk değerlendirme işlemi süreç alan bir uygulamadır. Yazılımların kullanılması zorunluluk taşımamakla birlikte organizasyon yapısına uygun yazılım seçilebilir (Calder ve Watkins, 2003).

Riskleri; stratejik planlama, güvenlik politikası, organizasyon, varlık, personel, uygunluk, ağ yönetimi, fiziki güvenlik, erişim güvenliği, veri tabanı, sistem, süreklilik, değişiklik ve acil durum riskleri şeklinde kategoriler oluşturarak riskler karşısında düzenleyici, önleyici ve algılayıcı kontroller uygulanmalıdır.

Bankacılıkta COBIT bazlı risk denetimi yapılmaktadır. Riskler tanımlandıktan sonra sistemin güvenilirliğinin ve verimliliğinin sağlanması için risk denetimi yapılmalıdır.

Bilgi teknolojileri bütçesinin yönetimi için yatırım planlamasına önem verilmelidir. Risk önceliğini de dikkate alan bir planlama yapılmasıyla fayda/maliyet etkinliği

sağlanabilir. Bilgi güvenliğini sağlamada ve riskleri yönetmede diğer kurum ve kuruluşlarla ortak hareket ederek teknolojik altyapının geliştirilmesine katkı sağlanmalıdır.

Risk yönetiminin başarılı olması için; üst yönetim sorumluluğu almalı, riske karşı kontrollerin geliştirilmesinde ve tehditlerin belirlenmesinde risk yönetimi ekibi yeterli seviyede bilgi ve tecrübeye sahip olmalı, bilgi varlıkları risklerini yönetirken risk ekibi ve iş birimleri beraber çalışmalı, risk değerlendirme ve raporlama faaliyetleri düzenli periyotlar halinde yapılmalı ve ihtiyaç duyulduğunda toplantıların düzenlenmesi gerekmektedir (Peltier, 2005).

Organizasyonun, bilgi güvenliği politikalarına ve risk kabul kriterlerine uyum gösteren risklerin, kontrol kriterlerinin ve sorumlulukların tanımlandığı formel bir risk değerlendirme dokümantasyonu yapması gerekmektedir. Maliyet açısından etkin olabilmesi için kontrolün uygulama ve bakım maliyetlerinin, kontrolün olmaması durumundaki olumsuz etkisinden daha fazla olmaması gerekmektedir. Tüm risklere karşı önlem almak olanaksızdır o yüzden etkin risk yönetimi için etkin maliyet yönetimi yapılmalıdır (Calder ve Watkins, 2008).

Bilgi teknolojileri risk yönetimi alanında Türkiye genelinde kapsamlı bir çalışma yapılamamıştır. Birkaç konferans bildirisi ve makale dışında risk yönetimi ve hesaplaması olarak yeterli bir kaynağa rastlanmamıştır. Türkiye'de yapılan çalışmalar bilgi güvenliği ve risklerinin belirlenmesi ve hesaplanmasından öte henüz bilgi güvenliği farkındalığının yerleşmediğini göstermektedir. Bilgi güvenliği farkındalığının yerleşmesiyle birlikte mevcut veya oluşabilecek riskler belirlenebilecek ve uygun kontroller yardımıyla risklerin olumsuz etkileri bertaraf edilecektir.

Bu çalışma, İller Bankası Anonim Şirketi'nde bilgi teknolojilerine ait risklerin yönetimini sağlamada yardımcı bir kaynak niteliğindedir. Bilgi sistemleri denetiminde kullanılan COBIT ve ISO 27001 ile uyumlu olarak hazırlanmıştır. Gelecek çalışmalarda bütün yaklaşım, metodoloji ve yazılımların daha detaylandırıldığı bir inceleme yapılarak kurum yapısına uygun, kendi bilgi teknolojileri risk standartlarının oluşturulduğu bir çerçeve geliştirilebilir.

KAYNAKLAR

Acar, Ş. B. (2013). *Risk Yönetimi ve Kontrol Faaliyetleri.* Van: Maliye Bakanlığı.

Airmic, Alarm, and Irm. (2010). A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000. Airmic, Alarm, IRM.

Akay, İ. G. (2014). *Bilgi Güvenliği Yönetim Sistemleri: Bilgi Güvenliği Uygulama Mülakatları,* Yüksek Lisans Tezi, Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü, Bilecik.

Aktaş, F. Ö., ve Soğukpınar, İ. (2010). Bilgi Güvenliğinde Uygun Risk Analizi ve Yönetimi Yönteminin Seçimi İçin Bir Yaklaşım. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 3*(1), 39-46.

Astuti, H. M., Muqtadiroh, F. A., Darmaningrat, E. W., and Putri, C. U. (2017). Risk Assessment of Information Technology Processes Based on COBIT 5 Framework: A Case Study of ITS Service Desk. *Procedia Computer Science, 124*, 569-576.

Ateş, V., ve Güneş, B. (2016). Üniversitelerde Bilişim Teknolojileri Risk Yönetimi Başarısını Etkileyen Faktörler Üzerine Nitel Bir Araştırma: Ankara İli Örneği. *Bilgi Dünyası, 17*(1), 39-56.

Bağcı, B. (2007). Bilgi Teknolojileri Risk Yönetimine Genel Bakış. İstanbul: Deloitte.

Bahtit, H., and Regragui, B. (2013). Risk Management for ISO 27005 Decision Support. *International Journal of Innovative Research in Science, Engineering and Technology, 2*(3), 530-538.

Bandyopadhyay, K., Mykytyn, P. P., and Mykytyn, K. (1999). A Framework for Integrated Risk Management in Information Technology. *Management Decision, 37*(5), 437-444.

Bojanc, R., and Blazic, B. J. (2008). An Economic Modelling Approach to Information Security Risk Management. *International Journal of Management, 28*, 413-422.

Borek, A., Parlikad, A. K., Webb, J., and Woodall, P. (2013). *Total Information Risk Management: Maximizing the Value of Data and Information Assets.* San Francisco: Morgan Kaufmann, 61-155.

Brand, K., and Boonen, H. (2007). *IT Governance Based On COBIT 4.1- A Management Guide.* Van Haren Publishing, 21-36, 80.

Broad, J. (2013). *Risk Management Framework: A Lab-Based Approach to Securing Information Systems.* Waltham: Syngress, an imprint of Elsevier, 24.

Calder, A., and Watkins, S. (2003). *IT Governance : A manager's Guide to Data Security and BS 7799/ISO 17799.* Londan and Sterling, 98.

Calder, A., and Watkins, S. (2008). *IT Governance A Manager's Guide to Data Security and ISO 27001/ISO 27002*. United States: Kogan Page Limited, 64, 70, 86, 93.

Canbek, G., ve Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi, 9*(3), 165-174.

Cantürk, S. (2013). Bilgi Teknolojileri Yönetişimi İçin Yeni Bir Adım: COBIT 5. *KPMG Gündem*. KPMG.

COSO. (2017). Enterprise Risk Management Integrating with Strategy and Performance Executive Summary. COSO.

Derici, O., Tüysüz, Z., ve Sarı, A. (2007). Kurumsal Risk Yönetimi ve Sayıştay Uygulaması. *Sayıştay Dergisi*(65), 151-172.

ENISA. (2006). Risk Management: Implementation Principles and Inventories for Risk Management/Risk Assessment Methods and Tools. ENISA.

Erol, S. E., Ceyhan, E. B., ve Sağıroğlu, Ş. (2015). Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme. *8. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 144-151). Ankara: Bilgi Güvenliği Derneği.

Ersoy, E. V. (2012). *ISO/IEC 27001 Bilgi Güvenliği Standardı Tanımlar ve Örnek Uygulamalar*. Ankara: ODTÜ Yayıncılık, 8-20, 68-69.

Ertürk, H. (2010). Bankacılık Sektörünün Karşılaştığı Riskler ve Risk Yönetimi. *Denetişim*, 62-70.

Eskiyörük, D. (2007). *BGYS-Risk Yönetim Süreci Kılavuzu.* Kocaeli: TÜBİTAK.

Evrin, V., ve Demirer, M. (2011). Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği. *IV. Ağ ve Bilgi Güvenliği Sempozyumu Bildiriler Kitabı* (s. 25-33). Ankara: TMMOB Elektrik Mühendisleri Odası Ankara Şubesi.

FAIR. (2010). *FAIR-ISO/IEC 27005 Cookbook.* United Kingdom: The Open Group.

Gerber, M., and Solms, R. V. (2005). Management of Risk in the Information Age. *Computers & Security, 24*, 16-30.

Grünendahl, R.-T., and Will, P. H. (2006). *Beyond Compliance: 10 Practical Actions on Regulation, Risk and IT Management.* Weisbaden: Vieweg, 80-83, 87-100, 103.

Güneş, F., Kızıldeniz, S., Selçuk, S., Suna, B., ve Coşkun, S. (2013). Bilgi Teknolojileri Denetimi ve COBIT'in Sektörel Uygulanabilirliği. *XV. Akademik Bilişim Konferansı Bildirileri.* Antalya: İnternet Teknolojileri Derneği.

ISACA. (2007). *COBIT 4.1*. United States of America: IT Governance Instıtute.

ISACA. (2009). The Risk IT Framework Excerpt. USA: ISACA.

ISACA. (2010). The Business Case Guide: Using VAL IT 2.0. USA: ISACA.

ISACA. (2012). COBIT 5 Enabling Processes. USA: ISACA.

ISACA. (2013). COBIT 5 for Risk. USA: ISACA.

ISO. (2009). ISO 31000-Risk Management-Principles and Guidelines. Switzerland: ISO.

ISO. (2011). ISO/IEC 27005: 2011. Switzerland.

ISO. (2011). ISO/IEC 27005: Information Technology-Security Techniques-Information Security Risk Management. Switzerland: ISO.

IT Governance Institute. (2007). *IT Control Objectives for Basel II-The Importance of Governance and Risk Management for Compliance.* ISACA.

İLBANK. (2015). Risk Yönetimi Prosedürü. Ankara: İller Bankası Anonim Şirketi.

İLBANK. (2017). BT Risk Yönetimi Politikası. Ankara: İller Bankası Anonim Şirketi.

İnternet: Bankacılık Kanunu (2005). Bankacılık Kanunu Hakkında. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.resmigazete.gov.tr%2Feskiler%2F2005%2F11%2F20051101M1-1.htm&date=2018-03-01, Son Erişim Tarihi: 01.03.2018

İnternet: BDDK. (2007). Bankalarda Bilgi Sistemleri Yönetimi Tebliği Hakkında. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.resmigazete.gov.tr%2Feskiler%2F2007%2F09%2F20070914-1.htm&date=2018-03-01, Son Erişim Tarihi: 01.03.2018

İnternet: Bilgi Sistemleri Yönetimi Tebliği. (2018). Sermaye Piyasası Kurulu. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.resmigazete.gov.tr%2Feskiler%2F2018%2F01%2F20180105-9.htm&date=2018-03-01, Son Erişim Tarihi: 01.03.2018

İnternet: Ebios. European Union Agency for Network and Information Security. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.enisa.europa.eu%2Ftopics%2Fthreat-risk-management%2Frisk-management%2Fcurrent-risk%2Frisk-management-inventory%2Frm-ra-tools%2Ft_ebios.html+&date=2018-02-15, Son Erişim Tarihi: 15.02.2018.

Internet: Mehari. European Union Agency for Network and Information Security. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.enisa.europa.eu%2Ftopics%2Fthreat-risk-management%2Frisk-management%2Fcurrent-risk%2Frisk-management-inventory%2Frm-ra-methods%2Fm_mehari.html&date=2018-02-15, Son Erişim Tarihi: 15.02.2018

İnternet: The Security Risk Analysis Directory. Introduction to Cobra. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.security-risk-analysis.com%2Fintrocob.htm&date=2018-02-15, Son Erişim Tarihi: 15.02.2018

İnternet: Türkiye Elektrik İletişim A.Ş.' ye Siber Saldırı. Enerji Enstitüsü. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fenerjienstitusu.com%2F2014%2F11%2F15%2Fteias-turkiye-elektrik-enerji-iletim-siber-saldiri-hack%2F&date=2018-02-15, Son Erişim Tarihi: 15.02.2018

İnternet: Türk Standardı 17799. Türk Standardları Enstitüsü. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fintweb.tse.org.tr%2FStandard%2FStandard%2FStandard.aspx%3F081118051115108051104119110104055047105102120088111043113104073098109078043074104065084049079057&date=2018-03-01, Son Erişim Tarihi: 01.03.2018.

İnternet: Türk Standardı 27001. Türk Standardları Enstitüsü. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fintweb.tse.org.tr%2FStandard%2FStandard%2FStandard.aspx%3F081118051115108051104119110104055047105102120088111043113104073084111119114114118066111103110052&date=2018-03-01, Son Erişim Tarihi: 01.03.2018.

İnternet: Türk Standardı 27005. Türk Standardları Enstitüsü. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fintweb.tse.org.tr%2FStandard%2FStandard%2FStandard.aspx%3F081118051115108051104119110104055047105102120088111043113104073089049080057120080122097053070075&date=2018-02-15, Son Erişim Tarihi:15.02.2018.

Kalman, S. (2002). *Web Security Field Guide.* Cisco Press.

Kalkınma Bakanlığı. (2015). *2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı.* Ankara: Kalkınma Bakanlığı.

Kalkınma Bakanlığı. (2017). *Kamu Bilgi ve İletişim Teknolojileri Yatırımları.* Kalkınma Bakanlığı.

Kamu İç Denetim Koordinasyon Kurulu. (2014). Kamu Bilgi Teknolojileri Denetimi Rehberi. Ankara: İç Denetim Koordinasyon Kurulu, 276.

Karabacak, B., ve Özkan, D. (2010). Bilgi Güvenliği Yönetim Sistemi için Süreç Tabanlı Risk Analizi. *3.Ağ ve Bilgi Güvenliği Ulusal Sempozyumu Bildirileri.* Ankara.

Karabacak, B., and Soğukpınar, İ. (2005). ISRAM: Information Security Risk Analysis Method. *Computer & Security, 24*(2), 147-159.

Koç, F. (2008). BGYS-Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu. TÜBİTAK-UEKAE.

Koç, F. Ö., ve Uzay, Ş. (2015). Risk Raporlaması: Gelişmiş Ülke Uygulamalarından Çıkarılacak Dersler. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*(45), 205-230.

Koç, S., ve Çelik, A. (2015). Kurumsal Risk Yönetimi: Türkiye'de Bankacılık Sektöründe Bir Uygulama. *Cumhuriyet Üniversitesi İdari Bilimler Dergisi, 16*(2), 311-334.

Kouns, J., and Minoli, D. (2010). *Information Technology Risk Management in Enterprise Environments.* Hoboken, New Jersey: Wiley, 35.

Kuyumcuoğlu, M., ve Başoğlu, A. N. (2008). Bilişim Sistemlerinde Risk Yönetimi Benimseme Modeli. *Yönetim*, 143-164.

Lark, J. (2015). ISO 31000 Risk Management-A Practical Guide for SME's. Switzerland: ISO.

Laudon, K. C., and Laudon, J. P. (2014). *Management Information Systems.* England: Pearson Education, 325, 341.

Melo, L., and Gondim, P. (2012). Risk Assessment and Real Time Vulnerability Identification in IT Environments. In T.-S. Chou, and T.-S. Chou (Eds.), *Information Assurance and Security Technologies for Risk Assessment and Threat Management.* USA: Information Science Reference, 240-243.

Norman, A. A., and Yasin, N. M. (2013). Information Systems Security Management (ISSM) Success Factor: Retrospection from the Scholars. *African Journal of Business Management, 7*(27), 2646-2656.

OECD. (2015). Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. Paris: OECD Publishing.

Özbilgin, İ. G. (2003). Bilgi Teknolojileri Denetimi ve Uluslararası Standartlar. *Sayıştay Dergisi*(49), 123-128.

Özenç, K. (2007). Bilgi ve İletişim Teknolojilerinde Kişisel ve Kurumsal Bilgi Güvenliğinin Sağlanması. *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı*, (s. 183-190). Ankara.

Öztürk, C., Tekerek, M., ve Yılmaz, A. S. (2016). Bilgi Güvenliği Endüstrisinin Ülkelere Göre Karşılaştırması. *9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*, (s. 235-243). Ankara.

Pelnekar, C. (2011). Planning for Implementation ISO 27001. *Isaca Journal, 4*.

Peltier, T. R. (2005). *Information Security Risk Analysis.* Boca Raton: Auerbach Publications, 77-80, 298.

Polat, N. (2007). Yönetim Bilgi Sistemi ve Sayıştayda Yürütülen Çalışmalar. *Sayıştay Dergisi*(65), 187-198.

Raggad, B. G. (2010). *Information Security Management.* Boca Raton: Taylor ve Francis, 11, 24-25.

Ritchie, S. (2013). Security Risk Management. ISACA.

Ross, R. (2004). *NIST Special Publication 800-53: Recommendation Security Controls for Federal Information Systems.* USA: National Institute of Standards and Technology.

Sağıroğlu, Ş., Ersoy, E., ve Alkan, M. (2007). Bilgi Güvenliğinin Kurumsal Bazda Uygulanması. *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı*, (s. 200-207). Ankara.

Saleh, M. S., and Alfantookh, A. (2011). A New Comprehensive Framework for Enterprise Information Security Risk Management. *Applied Computing and Informatics, 9*, 107-118.

Sayıştay. (2013). Bilişim Sistemleri Denetimi Rehberi. Ankara: Sayıştay.

Slay, J., and Koronios, A. (2006). *Information Technology Security & Risk Management.* Milton: John Wiley & Sons Australia, 14, 20-62.

Stoneburner, G., Goguen, A., and Feringa, A. (2002). NIST SP 800-30 Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology. Gaithersburg: NIST-National Institute of Standards and Technology.

Symantec. (2008). *IT Risk Management Report 2: Myths and Realities.* Symantec.

Şahinaslan, E., Kandemir, R., ve Kantürk, A. (2010). Bilgi Güvenliği Risk Yönetimi Metodolojileri ve Uygulamaları Üzerine İnceleme. *3.Ağ ve Bilgi Güvenliği Ulusal Sempozyumu Bildirileri.* Ankara.

Şen, Ş., ve Yerlikaya, T. (2013). ISO 27001 Kurumsal Bilgi Güvenliği Standardı. *XV. Akademik Bilişim Konferansı Bildirileri* (s. 719-723). Antalya: İnternet Teknolojileri Derneği.

Tarantino, A. (2006). *Manager's Guide to Compliance: Sarbanes-Oxley, COSO, ERM, COBIT, IFRS, BASEL II, OMB A-123, ASX 10, OECD Principles, Turnbull Guidance, Best Practices, and Case Studies.* Hoboken, New Jersey: John Wiley & Sons.

TBD. (2016). *TBD Bilişim 2016 Değerlendirme Raporu.* TBD Bilişim Derneği.

Teker, D. L. (2006). *Bankalarda Operasyonel Risk Yönetimi.* İstanbul: Literatür Yayıncılık, 11, 29-38.

TSE. (2016). TS EN ISO 9001:2015 Kalite Yönetim Sistemi Eğitimi. Türk Standardları Enstitüsü.

Tutar, H. (2010). *Yönetim Bilgi Sistemi.* Ankara: Seçkin Yayıncılık, 31, 45, 51-55, 138, 145.

Türk Dil Kurumu. (2011). *Büyük Türkçe Sözlük.* Türk Dil Kurumu Yayınları.

Uzunay, V. (2007). *COBIT (Control Objectives for Information and Related Technology).* Ankara.

Varlı, A. T. (2007). Bankacılıkta Bilgi Sistemleri Yönetimi ve Denetimi. İstanbul.

Vorster, A., and Labuschagne, L. (2005). A Framework for Comparing Different Information Security Risk Analysis Methodologies. *SAICSIT'05 Proceedings of the 2005 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries,* (s. 95-103). South Africa.

Wickboldt, J. A., Bianchin, L. A., Lunardi, R. C., Granville, L. Z., Gaspary, L. P., and Bartolini, C. (2011). A Framework for Assesment Based on Analysis of Historical Information of Workflow Execution in IT Systems. *Computer Networks, 55*, 2954-2975.

Workman, M., Phelps, D. C., and Gathegi, J. N. (2013). *Information Security For Managers.* Burlington: Jones and Bartlett Learning, 84-85.

Yıldırım, E. Y., Akalp, G., Aytaç, S., and Bayram, N. (2011). Factors Influencing Information Security Management in Small-and Medium-Sized Enterprises: A Case Study from Turkey. *International Journal of Information Management, 31*, 360-365.

Yıldız, Ö. R. (2007). Bilişim Sistemleri Denetimi ve Sayıştay. *Sayıştay Dergisi*(65), 173-185.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : ATAR, Merve

Doğum yılı ve yeri : 1990 Afyonkarahisar

Telefon (İş) : 0 (312) 508 72 45

e-mail : mervea@ilbank.gov.tr

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Lisans	Orta Doğu Teknik Üniversitesi (İşletme)	2013
Lise	Afyon Milli Piyango Anadolu Lisesi	2008

İş Deneyimi

Yıl	**Yer**	**Görev**
2014 – Halen	İller Bankası A.Ş.	Uzman Yardımcısı

Yabancı Dil

İngilizce

Hobiler

Akvaryum, Sudoku


İLBANK
TÜRKİYE'NİN YAPICI GÜCÜ