T.C.
GAZİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

BANKACILIKTA OPERASYONEL RİSK VE TÜRKİYE'DE TEKNOLOJİ RİSKİ YÖNETİMİ ÜZERİNE UYGULAMA

ŞEFİK BAYCAN

İŞLETME ANABİLİM DALI
İŞLETME BİLİM DALI

OCAK 2015


GAZİ ÜNİVERSİTESİ
Gazi
1926

BANKACILIKTA OPERASYONEL RİSK VE TÜRKİYE'DE TEKNOLOJİ RİSKİ YÖNETİMİ ÜZERİNE UYGULAMA

Şefik BAYCAN

YÜKSEK LİSANS TEZİ
İŞLETME ANABİLİM DALI
İŞLETME BİLİM DALI

GAZİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

OCAK 2015

Şefik BAYCAN tarafından hazırlanan "Bankacılıkta Operasyonel Risk ve Türkiye'de Teknoloji Riski Yönetimi Üzerine Uygulama" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ / ~~OY ÇOKLUĞU~~ ile Gazi Üniversitesi İşletme Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Prof. Dr. Metin KAMİL ERCAN
İşletme Anabilim Dalı, Gazi Üniversitesi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum .....

Başkan : Prof. Dr. Mehmet ARSLAN
Bankacılık Anabilim Dalı, Gazi Üniversitesi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum .....

Üye : Prof. Dr. Kürşat YALÇINER
İşletme Anabilim Dalı, Gazi Üniversitesi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum .....

Tez Savunma Tarihi: 29/01/2015

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....
Prof. Dr. Hikmet KAVRUK
Sosyal Bilimler Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Sosyal Bilimler Enstitüsü Tez 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.

Şefik BAYCAN

29.01.2015

BANKACILIKTA OPERASYONEL RİSK VE TÜRKİYE'DE TEKNOLOJİ RİSKİ YÖNETİMİ ÜZERİNE UYGULAMA

Yüksek Lisans Tezi

Şefik BAYCAN

GAZİ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

Ocak 2015

ÖZET

Bu çalışmada bankacılık sektöründe operasyonel risk çeşitlerinden son yıllarda önemi oldukça artan bilgi teknolojileri riskinin ne olduğu, risk yönetiminin nasıl yapıldığı ve bu risklerin yönetilmesi için Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından bankalara zorunlu tutulan COBIT 4.1 (Control Objectives for Information and related Technology) standartı genel hatlarıyla ele alınmıştır. Bu kapsamda çalışmanın uygulama kısmında ise Türkiye'de faaliyet gösteren bir bankanın bilgi teknolojileri risk yönetimi süreçlerinin neler olduğu ve bu risklerin yönetiminin nasıl gerçekleştirildiği, bilgi sistemlerinin karmaşıklığı dikkate alındığında temel bir düzeyde anlatılmaya çalışılmıştır.

Bilim Kodu : 1153
Anahtar Kelimeler : Risk, Risk Yönetimi, Bankacılıkta Risk Yönetimi, Bilgi Teknolojileri riski, Teknoloji riski, COBIT
Sayfa Adedi : 83
Tez Danışmanı : Prof. Dr. Metin Kamil ERCAN

OPERATIONAL RISK IN BANKING AND A CASE STUDY ON THE TECHNOLOGY RISK MANAGEMENT IN TURKEY

(M.Sc. Thesis)

Şefik BAYCAN

GAZİ UNIVERSITY

INSTITUTE OF SOCIAL SCIENCES

October 2015

ABSTRACT

In this study, risk of information technology, which is one of the operational risks and has recently gained considerable attention is examined. In this context, the risk of information technology and how to conduct the risk management is analyzed. Spesifically, principles and procedures of COBIT 4.1 (Control Objectives for Information and related Technology) which is obligated to banks by Banking Regulation and Supervision Agency (BRSA) are explained in general.
In this framework, as a case study, a bank operating in Turkey is basically examined with regard to the processes of IT risk management considering the complexity of information technology systems.

Science Code : 1153
Key Words : Risk, Risk Management, Risk Management in Banking, Information Technology Risk, Technology Risk, COBIT
Number of Pages : 83
Adviser : Prof. Dr. Metin Kamil ERCAN

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
ATM	Automatic Teller Machine
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BT	Bilgi Teknolojileri
COBIT	Control Objectives for Information and related Technology
Debit Kart	Banka Kartı
ISACA	Information Systems Audit and Control Association
POS	Point of Sale
RTO	Recovery Time Object

1. GİRİŞ

Küreselleşen dünyanın finansal piyasalarında ve bilgi teknolojilerindeki (BT) gelişmeler bankaların karşılaştığı risk türlerinde artışlara neden olmuş ve risk kavramının daha fazla dikkatle ele alınması gerektiğini göstermiştir.

Bu çalışmanın ana amacı son yıllarda önemi giderek artan bilgi teknolojilerinin maruz kaldığı risklerin bankalarda öneminin anlaşılması ve bankaların maruz kaldıkları operasyonel risk çeşitlerinden olan bilgi teknolojileri risklerini yönetebilmek için uluslararası kabul görmüş bilgi teknolojileri risk yönetimi "Control Objectives for Information and related Technology" (COBIT) 4.1 standartının öneminin anlaşılarak etkin ve etkili bir bilgi teknolojileri risk yönetiminin gerekliliğini ortaya koymaktır.

Çalışmamızın ilk bölümüne risk kavramına giriş yapılarak başlanılmış olup risk ve risk yönetimi kavramları anlatılarak bankacılık sektöründe bu kavramların önemine değinilmiştir. Ayrıca, finansal piyasaların baş aktörleri olan bankaları etkileyebilecek risklerin neler olduğu detaylı bir şekilde irdelenmiştir.

İkinci bölümde bankaların maruz kaldığı risk çeşitlerinden birisi olan operasyonel riskler, personel, süreç, teknoloji ve dışsal riskler olarak gruplandırılarak teknoloji risklerinin neler olduğu ve bu riskleri yönetmek için dünyada kabul görmüş standartlardan bahsedilmiştir.

Üçüncü bölümde Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından faaliyetlerinde bilgi teknolojilerini kullanıyor olmalarından dolayı kaynaklanan risklerin yönetilmesi ve gerekli önlemleri alma zorunluluğu bulunan bankaların bu amacına ulaşılabilmesini sağlayan uluslararası kabul görmüş COBIT 4.1 standartının ne olduğu, usul ve esasları genel hatlarıyla anlatılmıştır.

Çalışmamızın son bölümünde ise Türkiye'de bankacılık sektöründe faaliyette bulunan büyük ölçekli bir bankanın bilgi teknoloji risklerinin belirlenip değerlendirilerek takip edildiği sürecin aşamalarının önemli bir kısmının teknik hesaplamalarına girilmiş olup bankadan edinilen verilerin kısıtlı olması ve bu büyüklükteki bir finans kurumunun bilgi sistemlerinin karmaşıklığı göz önüne alındığında anlaşılabilecek basit bir düzeyde uygulaması yapılmıştır.

2. BANKACILIK SEKTÖRÜNDE RİSKLERİN TANIMLANMASI VE RİSK TÜRLERİ

2.1. Risk Kavramı

Günlük hayatta risk kavramı oldukça sık kullanılmasına rağmen, riskin tanımını yapmak bir hayli zordur. Risk, farklı şekillerde tanımlanabilir. Bunlardan bazıları şunlardır: Risk, bir olayın ya da olaylar setinin ortaya çıkma olasılığıdır. Risk, gerek belirsizlik gerekse belirsizliğin sonuçları olarak tanımlanabilir. Genel anlamda risk, belirli bir zaman aralığında, hedeflenen bir sonuca ulaşmada, kayba ya da zarara uğrama olasılığıdır ya da bir olayın beklenenden farklı olarak gerçekleşebilme olanağıdır. Olabilecek sonuçların sayısının artması ile risk meydana gelir. Riskin mevcut olması demek bir olayın sonucunun tam olarak tahmin edilemeyeceği demektir. Risk, gelecekte oluşabilecek potansiyel sorunlara, tehdit ve tehlikelere işaret eder. Risk genellikle tam ve net olarak bilinemez ya da öngörülemez, belirsizdir. Belirsizliğin sonuç üzerinde olumsuz etkileri vardır. Riskin subjektif ve objektif tarafları olduğunu savunanlar ve bu yargıya karşı çıkanlar olmasına rağmen, genel olarak riskin objektif ve ölçülebilen bir faktör olduğu söylenebilir. Risk, objektif ve ölçülebilen bir faktör olduğu sürece yönetilebilir bir olgudur.[1]

Riskin temel bileşenleri, oluşma olasılığı ve oluşması durumunda sonucu ne ölçüde etkileyeceğidir. Ancak riski, yalnızca olumsuz etkileri olan bir kavram olduğunu düşünmek büyük bir yanlış olur. Riske kazanç elde etme fırsatı olarak bakılmalı, fırsata dönüştürülmesi için sistematik bir çaba gösterilmelidir.[2]

[1] Hacısüleymanoğlu, E. (2010). *Bilgi Teknolojileri Yönetişimi Yöntemleri ve COBIT ile Ulusal bir Bankada Uygulaması*, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.
[2] Hacısüleymanoğlu, *a.g.m.*, s. 88.

Çizelge 2.1. Belirsizlik Skalası

Belirsizlik Seviyeleri	Özellikler	Örnekler
Seviye 0 Belirsizlik Yok (Kesinlik)	Sonuçlar tam olarak tahmin edilebilir.	Fizik Yasaları, Doğa Bilimleri
Seviye 1 Objektif Belirsizlik	Sonuçlar tanımlanmış ve olasılıklar bilinmektedir.	Şans oyunları (Zar, İskambil vb.)
Seviye 2 Subjektif Belirsizlik	Sonuçlar tanımlanmış ve olasılıklar bilinmemektedir.	Yangın, Trafik kazaları, Birçok yatırım kararı vb.
Seviye 3 Sonsuz (Mutlak) Belirsizlik	Sonuçlar tam olarak tanımlanmamış ve olasılıklar bilinmemektedir.	Uzay keşifleri, Genetik araştırmalar vb.

2.1.1. Belirsizlik kavramı

Belirsizlik, meydana gelecek sonuçların belirlenememesi ve bilinememesi olarak tanımlanabilir. Belirsizlik subjektif bir kavramdır, kişiye ve duruma göre değişir ve bu yüzden de kesin olarak ölçülemez. Bu nedenledir ki iki firma için de aynı riske sahip bir pazarda firmalar yeni ürünler üretmek için yatırım yapmayı düşünürken, bu firmaların sadece birisi yatırım kararı alabilir. Her iki firma için de risk aynı iken, yalnızca birinin yatırım kararı alması, belirsizliğin subjektifliğini gösterir.[3]

Belirsizlik yoksa kesinlik (belirlilik) vardır ve dolayısıyla meydana gelecek sonuçlarla ilgili şüphe yoktur. Geleceği öngörebilme yeteneği, öngörülmek istenilen olay ile ilgili bilgiye bağlıdır. Belirsizlik de sahip olunan bilgiye göre sınıflara ayrılabilir.[4]

2.1.2. Risk belirleme süreci

Riski tanımak ve ölçmek mevcut durumu değiştirmediği gibi, yatırımın sonucunu da bilinir hale getirmez. Ayrıca bir yatırımın riski hesaplandıktan sonra yatırımın başarısız olabilme riski ortadan kalkmaz. Fakat kurumlar riski tanıyıp ve bildiklerinde yatırım konusunda daha bilinçli kararlar verebilecektir. Riski, mevcut durumu bulanık hale getirip yöneticileri yanlış kararlar vermeye sürükleyen bir tuzak olarak kabul edersek, ancak risk belirlenerek ve hesaplanarak bu belirsizlik

[3] Hacısüleymanoğlu, *a.g.m.*, s. 88.
[4] Hacısüleymanoğlu, *a.g.m.*, s. 89.

ortadan kaldırılabilir.[5] Risk ve belirsizlikle karşı karşıya kalındığında öncelikle yapılması gereken riskin belirlenmesidir. Riskin belirlenebilmesi için aşağıda belirtilen sırada bir yaklaşım izlenebilir.[6]

2.1.2.1. Riskin tanımlanması

İlk aşamada riskli olduğu düşünülen önemli değişkenlerin gizli etki ve kimliği konusunda belirsizlik azaltılmaya çalışılmalıdır. Belirsizliğin azaltılmasına ve sorunun çözülmesinde yardımcı olabilecek bilginin işlevi daha iyi belirlenmelidir. Önemli değişkenler ve onların belirsiz etkisini ortaya koymak için geleceğe yönelik planlama araçları kullanılabilir. Örneğin, gelecekteki işletme fırsatlarını tanımak için en iyi, en olası ve en kötü biçimde geleceğe ilişkin senaryolar geliştirilir ve bu senaryolara ilişkin çeşitli olaylar tanımlanır. Bu tür araçlar ve yöntemler, önemli değişkenlerin ve onların belirsiz etkilerinin yönetimce kavranmasını kolaylaştırabilir.[7]

2.1.2.2. Riskin ölçülmesi

Tek bir projenin ya da yatırımın riski ile toplam riskin ya da portföy riski birbirinden farklıdır. Bu nedenle riskin ölçülmesinin bir amacı da projelerin ya da yatırımların tek başlarına hangi risk sınıfına gireceğini belirlemek ve ona göre karar almaktır. Bu aşamada olaylara ilişkin öznel olasılık dağılımları belirlenir. Bu dağılımlar, projenin ya da yatırımın riskini belirlemeye çalışan çözüm yöntemi olan risk simülasyonunun girdileridir. Kurulan model çözülerek ilgi duyulan değişkene/değişkenlere ilişkin olasılık dağılımı/dağılımları elde edilir. Bu çalışma, kurumu sadece projenin ya da yatırımın riskinin yüksek, orta ya da düşük olup olmadığı konusunda aydınlatır; projenin üstlenilmesinin ya da yatırımın yapılmasının iyi ya da kötü olacağı konusunda hiçbir şey getirmez. Bu konudaki yargı, firmanın toplam riski ve diğer stratejik etmenlere dayanır.[8]

---

[5] Hacısüleymanoğlu, *a.g.m.*, s. 89.
[6] Hacısüleymanoğlu, *a.g.m.*, s. 88.
[7] Hacısüleymanoğlu, *a.g.m.*, s. 89.
[8] Hacısüleymanoğlu, *a.g.m.*, s. 90.

2.1.2.3. Riskin değerlendirilmesi

Yatırımın değeri yargılanırken yalnızca yukarıdaki belirtilen düşünce biçimi yeterli olmaz, ayrıca soyut ve ölçülemeyen etkenler de göz önüne alınmalıdır. Ayrıca, hesaplamalarda kullanılan tüm varsayımların net şimdiki değere olan duyarlılığı da test edilmelidir. Bu aşamadan sonra yatırımın benimsenmesi söz konusu olabilir. Kurumun yatırımı benimserken soyut etmenlere karşı olası tutumu genellikle daha fazla önem kazanır. Bu etmenler, rekabete ilişkin ve örgütsel veya toplumsal niteliği olan stratejik etmenlerdir.[9]

2.1.2.4. Riskin yargılanması

Yönetimin kararı firmanın toplam riski konusunda bir yargıyı içermelidir. Bu nedenle bir projenin ya da yatırımın toplam riske ya da portföy riskine etkisi göz önüne alınmalıdır. Firmanın amacı sermayedarlarının servetini arttırmaksa yönetimin, getirisi (verimi) sermaye piyasasında beklenen getiriyi aşan projelere yatırım yapması gerekir. Sermaye piyasasında getiri, risk primlerini içerir. Yüksek riskli yatırımlar, sermaye piyasasındaki fırsatlara bağlı olarak yüksek getiri sağlamalıdır. Bu nedenle benzer yatırımlar, tabi olduğu riske göre sınıflandırılmalı ve bu risk sınıfına giren projeler için riske göre ayarlanmış uygun iskonto (verim) oranları çıkarılmalıdır. Yönetim, böylece riske göre ayarlanmış oranlar kullanarak yatırımın, firmanın pazar değerine olası net etkisini kestiren net şimdiki değer rakamlarını belirleyebilir. Yönetim, bu yolla firma değerinin artacağını bekleyebilir. Çünkü bu yaklaşım, tek bir yatırımla firmanın portföy riski arasındaki ilişkileri göz önüne almaktadır.[10]

Bu sürecin çıktısı, firmanın pazar değerine yatırımın olası etkisini gösteren yatırımın net şimdiki değer rakamıdır. Bu aşamada kurum yatırım konusunda değerleme yapmalı ve sonuç olarak kabul ya da ret konusunda bir karara ulaşmalıdır.[11]

---

[9] Hacısüleymanoğlu, *a.g.m.*, s. 90.
[10] Atan, M. (2002). *Risk Yönetimi ve Türk Bankacılık Sektöründe Bir Uygulama*, Doktora Tezi, Gazi Üniversitesi Sosyal Bilimleri Enstitüsü, Ankara.
[11] Hacısüleymanoğlu, *a.g.m.*, s. 90.

2.1.3. Risk yönetimi

Risk Yönetimi, proaktif ve hızlı kararlar ve faaliyetler ile sürekli olarak risklerin belirlendiği, hangi risklerin öncelikle çözümlenmesi gerektiğinin değerlendirildiği, risklerle başa çıkmak için stratejiler ve planların geliştirilerek uygulandığı bir sistematiktir. Başka bir deyişle, risk yönetimi belirsizlikleri ve belirsizliğin yaratacağı olumsuz etkileri daha kabul edilebilir düzeye indirgemeyi hedefleyen bir disiplindir. Risklerin probleme ya da tehlikeye dönüşmeden belirlenmesi ve en aza indirgenmesi faaliyetlerinin planlanması ve yürütülmesini kapsar. Farkında olmasalar da ekonominin içinde yer alan bütün aktörler, özellikle de finansal kuruluşlar aslında risk yönetimine odaklanmışlardır. Ancak, sadece son on-yirmi yıldır bu amaçla yürütülen faaliyetler "risk yönetimi" diye adlandırılmış ve bütünlükçü bir yaklaşımla "sistem" haline getirilmiştir. Bu sistemin geliştirilmesine yönelik çabalar, piyasaların (ülkelerin) gelişmişlik düzeylerine göre farklı boyutlarda fakat hemen aynı hızla devam etmektedir. Günümüzün modern işletme teorisinin ulaştığı en kapsamlı çözümlerden bir tanesi risk yönetimidir. Çünkü risk yönetimi getiri, sermaye ve riski ilişkilendiren; bunların arasında optimum dengeyi kuran bir yaklaşım, bir yönetim tekniği, bir yönetim anlayışıdır. Risk yönetimi tüm işletmeler için önemli bir iştir. Ancak risk yönetimi bankalar için özel bir öneme sahiptir. Çünkü bankacılık sektöründe ortaya çıkabilecek olan yeni bir risk, sadece o sektörü değil, ekonomik sistemin tamamını peşinden sürükleyebilmektedir.[12]

Risk yönetiminin en temel amacı, firmalara taşıdıkları risklerle uyumlu sermaye tahsisi sağlamak ve riske göre düzeltilmiş sermaye getirisini en üst düzeye çıkartarak yaratılan katma değeri artırmaktır. Risk yönetiminin bir diğer önemli hedefi ise, karar verme mekanizmaları için riskleri görünür ve ölçülebilir hale getirmek, subjektifliği azaltmak ve firmaların yapacakları yatırımın sonuçlarını görerek hareket etmelerini sağlamaktır.[13]

Son yıllarda finans piyasalarında ortaya çıkan krizlerin çoğunda etkin bir risk yönetimi bulunmayışının neden olarak gösterilmesi daha karmaşık risk yönetimi tekniklerine olan ihtiyacı artırmıştır. Geleceğin belirsizliklerle dolu olmasından dolayı geleceğe yönelen her kararda risk unsuru hesaba katılmalıdır. Günümüzde

[12] Çolak, Ö. F. (2001). *Finansal Piyasalar ve Para Politikası*. Ankara: Nobel Yayın Dağıtım, 17.
[13] Hacısüleymanoğlu, *a.g.m.*, s. 91.

kuruluşları en çok zorlayan ekonomik konulardan biri de finansal riskin etkin yönetimidir. Son zamanlarda dünyada yaşanan krizler, global bazda otoritelerin, yatırım bankalarının ve şirket müdürlerinin risk yönetimi kavramını yöneticinin birincil ihtiyatlılık sorumluluklarından biri olarak görmelerine sebep olmuştur.[14] Genellikle finansal risklerin şirket bilançoları ve gelir tablolarında kendilerini anlaşılması güç ve lineer olmayan bir şekilde göstermeleri, dikkatleri piyasa değerlerindeki dalgalanmaların istatistiksel anlamda ölçülmesinde yoğunlaştırmıştır. Çoğu güncel risk yönetimi sistemleri ve protokollerinin altında yatan, riskin istatistiksel elde edilmiş değer hesaplamalarıdır.[15]

2.2. Bankacılıkta Risk ve Yönetimi

Bir banka için risk, kazançlardaki dalgalanma olarak tanımlanabilir. Kazançlardaki dalgalanmalar olası kayıplar için potansiyel yaratırken, kayıpların gerçekleşmesi durumunda finanse edilmesi gerekmektedir. Sermaye ayrılması, potansiyel kayıpları ortadan kaldırmak için banka bilançolarında kesintiye neden olurken kazançlarında büyük dalgalanmalar gerçekleşen bankaların aciz duruma düşmelerini engellemektedir.[16]

Bankalar mevduat kabul ederek topladıkları fonları kredilere, menkul kıymet yatırımlarına ve diğer finansal varlıklara iletimini sağlayan finansal kurumlardır. Fon aktarım sistemi bütünsel olarak ele alındığında bu süreç boyunca para arzının katlanarak büyüdüğü görülür. Bankanın mevduat bulundurma gibi yükümlüklerinin genelde bir değere sabitlenmesi ve istenilmesi halinde ödenmesinin zorunlu olması, bankanın krediler ve yatırım yapılan menkuller gibi varlıklarının ise değişken değerli olması ve istenildiği zaman geri çağrılamaması nedeniyle bankaya güvenini kaybeden mevduat sahipleri tarafından ani fon çıkışı olması durumunda bankalar zor duruma düşebilecektir. Böyle bir durumda güvenilir kurumların da olumsuz etkilenmesi ve bütün finansal sistemin zarara uğraması

[14] Mandacı, P. E. (2003). Türk Bankacılık Sektörünün Taşıdığı Riskler ve Finansal Kriz Aşmada Kullanılan Risk Ölçüm Teknikleri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 5(1), 67-84.
[15] Hacısüleymanoğlu, *a.g.m.*, s. 92.
[16] Atay, M. B. (2010). *Operasyonel Risk Yönetimi ve Türk Bankacılık Sektöründe Bir Uygulama, Yüksek Lisans Tezi*, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

olasılığı günümüzde bankacılık sektörünün denetlenmesi gereğinin temel nedeni olarak görülmektedir.[17]

Bankacılık sektöründe 1970'li yılların ortalarından itibaren yaşanan dalgalanmalar ve ardından gelen krizler ile ortaya çıkan zararlar risk ve risk yönetimi kavramının finans piyasaları açısından büyük önem taşıdığını ortaya koymuştur.[18]

Bankaların ödemeler sistemindeki yeri ve finansal kaynakların dağıtımındaki rolü bir takım kamu düzenlemelerinin yapılmasını gerektirmektedir. Tek bir bankanın bile ödeme sıkıntısına düşmesi durumunda ortaya çıkabilecek sosyal maliyetler finansal sistemin istikrarına etki etmektedir. Bunun sonucunda bankaların çok yüksek seviyede risk almalarını önlemek ve temerrüt riski olasılıklarını azaltmak amacıyla faaliyetlerine bir takım idari kısıtlar getirilmektedir. Bu yaklaşım bankaları bulunduracakları varlık miktarına doğrudan bir sınırlama getirirken riskli faaliyetlerini gerçekleştirmelerine herhangi bir engel yaratmamaktadır. Yatırımların çeşitliliğine getirilen idari sınırlandırmalar bankaları daha riskli olmasına rağmen daha yüksek getirili yatırımlara yönelmesini teşvik etmektedir. Yüksek seviyede risk alındığı durumlarda bankaları koruyan ana araç olarak bankaların tercih ettikleri risk/getiri yapısını seçmede serbestçe hareket edebilecekleri iyi geliştirilmiş bir teşvik mekanizmasının oluşturulmasının, asgari sermaye ayrılmasını öngören yapısal denetimlerden daha etkili olacağına inanılmaktadır. 1988 yılında yayımlanan Basel Uzlaşısının (Basel I) temel amacı bu anlayışın uluslararası seviyede uygulanmasını sağlamaktır.[19]

Risklerle karşılaşıldığında sezgi yoluyla ortaya çıkan tepki, risklerden kurtulmada başarı sağlayamaz. Risklerin önceden saptanması, bunların gerçekleşmesi hususunda kayıp ve zararların tahmin edilmesi, potansiyel fırsatların öngörülmesi ve bunlara karşı nasıl bir tepki verileceğinin belirlenmesi ile risklere karşı başarı sağlanmanın gerekliliğidir. Bankalarda yanlış tahmine dayalı kararlar, bankaların

[17] Rodriquez, L. J. (2003). Banking Stability and The Basel Capital Standards. *Cato Institute*, 23(1),115-126.
[18] Teker D. L. (2006). *Bankalarda Operasyonel Risk Yönetimi - Örnek Banka Uygulamalı* (1.Basım), İstanbul: Literatür Yayıncılık, 3.
[19] Cannata, F. and Quagliariello, M. (2009). *The Role of Basel II in the Subprime Financial Crisis: Guilty or Not Guilty?*. Carefin Working Paper, Milan: Universita Bocconi, 4.

karlılığı ve likiditesi için risk oluşturmaktadır. Mevcut bu risklere karşı uygulanan politikalar risk yönetimi olarak adlandırılabilir.[20]

Risk Yönetimi hangi risklerin önemli olduğunun belirlendiği ve bu risklerin önlenmesi için strateji ve planların geliştirildiği aktif bir süreçtir. Bu açıklamadan hareketle en basit şekilde risk yönetiminde riskler tanımlanır ve önleyici tedbirler alınır. Riskin büyüklüğü sayısallaştırılarak kabul edilebilir risk düzeyi belirlenir. Risk yönetimi potansiyel risklerin sistematik olarak değerlendirilerek, olası zararların etkisini azaltıcı yönde verilere dayalı karar vermeyi sağlayan bir disiplindir.[21]

Basel Komitesinin 1988 tarihli Sermaye Uzlaşısında piyasa ve kredi riski için gözetim altında bulunan bütün bankalara uygulanabilecek belirli sermaye yükümlülükleri oluşturulmuştur. Finansal istikrarın korunmasında Basel I ilkelerinin sadece kredi riskini dikkate alması, tarafların kredibilitesinin ölçümünde risk duyarlılığının yetersiz olması, risk yönetimi sistemlerinin geliştirilip güçlendirilmesinde bankaların yeterince teşvik edilmemesi gibi sebeplerle geliştirilmesine ihtiyaç duyulmuştur. Bu sebepler finansal yenilikler vesilesiyle düzenleyici kurallar oluşturulması için belirli fırsatlar sunmuştur. Basel II çalışması, daha güncel ve gelişen finansal piyasalarla daha uyumlu bir düzenleme oluşturarak bankacılık risklerinin kapsamını genişletmek ve bu sorunları gidermek amacıyla hazırlanmıştır. Mevcut görüşler çerçevesinde hazırlanan çalışma ile bankaların kendi içsel yönetim metotlarını vurgulayan daha özel bir yaklaşım sunulmuş ve risk sermayesi hesaplaması için çeşitli yaklaşımlar önerilmiştir. Yeni Uzlaşının ana amacı bankacılık sisteminde istikrarın sağlanması, sermaye ve riskler arasında daha güçlü bir bağ oluşturulmasıdır. Basel II Uzlaşısının getirdiği ana yeniliklerden birisi de risklerin daha kapsamlı bir biçimde ele alınmasını sağlayacak üç temel dayanağı olan bir yapının oluşturulmasıdır. Bunlar sermaye yeterliliğinin belirlenmesi, risk yönetimi sistemleri ve sermaye yeterliliğinin denetimi ve bir bankanın risk yönetimini piyasa değerindeki değişimler yoluyla ödüllendirecek veya cezalandıracak risk bilgisinin kamuoyuna açıklanmasıdır. Denetim ve piyasa disiplini olarak iki ek dayanağın yanı sıra yeni Basel Sermaye Uzlaşısı ilk defa bir bankanın maruz kaldığı operasyonel risklerin tahminini ve

[20] Şahin, S. (2011). *Bankacılıkta Risk Yönetimi ve Operasyonel Risk*, Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimleri Enstitüsü, İstanbul.
[21] Babuşçu, Ş. (2005). *Basel II Düzenlemeleri Çerçevesinde Bankalarda Risk Yönetimi* (1.Basım). Ankara: Akademi Consulting & Training, 4.

ölçümünü öngörmüş ve bu risk türü için düzenleyici sermaye gereksinimi hesaplanmasını önermiştir.[22]

Basel bankacılık denetim komitesinin risk yönetiminden beklentisi, bankaların sermayeleriyle orantılı risk almasını sağlamak ve işlerin olumsuz gitmesi durumunda ortaya çıkacak zararın sermaye ile karşılanabilmesini bugünden sağlamaktır.[23] Diğer bir ifade ile beklenmedik durumlarda ortaya çıkacak zararların, öz kaynaklarla karşılanamayıp, yabancı kaynaklara sirayet etmesini önlemek için bugünden önlem alınmasını sağlamaktır. Bu ise bankalarda çok iyi bir risk yönetimi sistemlerinin kurulması ve devamlılığının sağlanması ile mümkün olabilir.[24]

Güçlü risk yönetimi sadece analitik modellerin geliştirilmesi ile olmaz, üst yönetimin bu konuyu benimsemesi şarttır. Banka üst yönetimi tespit edilen risklere göre önlemler almadığı takdirde, risk yönetimi kesinlikle başarıya ulaşamaz. Risk analiz ve ölçümlerini sadece denetleyicilere, düzenleyicilere raporlama amacıyla yapan bankalarda güçlü bir risk yönetimi olduğu kesinlikle söylenemez.[25]

Bankalar güçlü risk yönetimi sayesinde bir yandan risklerini kontrol ederek olası kayıplarını azaltırken, diğer yandan da risklere ayarlı karlılık analizi ışığında daha karlı alanlarda büyüyerek hissedara değer katarlar. Güçlü risk yönetimi olan bankalar karşı karşıya kaldıkları riskleri detaylı olarak inceler, olası krizlerde kayıplarını daha önceden belirler, bu kayıpları minimize etmek için önceden önlemlerini alırlar.[26]

Riskler karlılık üzerindeki etkilerine göre tanımlanırlar. Bu doğrultuda risk yönetimi, belirsizlik ve karlılık üzerinde durmak zorundadır.[27] Dolayısıyla bankacılıkta risk ve getiri birlikte düşünülmeli ve birlikte yönetilmelidir.

---

[22] Wahler, B. (2005). *Process-Managing Operational Risk Developing a Concept for Adapting Process Management to the Needs of Operational Risk in the Basel II - Framework*. Hochschule für Bankwirtschaft and John Hopkins University Paul H.Nitze School of Advanced Internetional Studies, 16.

[23] Altıntaş, M.A. (2011). *Bankacılıkta Risk Yönetimi ve Sermaye Yeterliliği - 5411 Sayılı Bankacılık Kanunu, Basel I ve Basel II Düzenlemeleri Çerçevesinde.* Ankara: Turhan Kitap Evi, 3.

[24] Şahin, (2011). *a.g.m.,* s. 7.

[25] Köylüoğlu, H.U. (2001). Risk Yönetimi! Zaman Geçirmeden Neden? Nasıl?. *Active Bankacılık ve Finans Dergisi*, (17), 1.

[26] Şahin, (2011). *a.g.m.,* s. 6.

[27] Alkin E., Savaş A.T. (2002). *A Modern Approach to Risk Management in Financial Intermediaries.* İstanbul: Filiz Kitabevi, 92.

2.2.1. Risk yönetimi süreci

Bankacılıkta etkin ve verimli bir risk yönetimi süreci, beraberinde başarılı bir risk yönetimini de getirmektedir. Risk yönetimi süreci temelde şu aşamalardan oluşmaktadır:

- Risklerin belirlenmesi
- Risklerin ölçülmesi
- Risklerin izlenmesi
- Risklerin kontrol edilmesi
- Risklerin raporlanması

Bankaların yönetim kurulu, riskin belirlenmesi, ölçümü, izlenmesi, kontrol edilmesi ve raporlanması evrelerinden oluşan risk yönetimi sürecinin yönlendirilmesi ve izlenmesini teminen kendisine bağlı alt komite niteliğinde, risk yönetiminden sorumlu bir risk komitesinin üyelerini belirler.[28]

Risk yönetimi süreci, risklerin tanımlanması ve özelliklerinin belirlenmesiyle başlar. Her bankanın faaliyet alanına göre bu riskler de farklılık gösterir. Tanımlanan risklere ilişkin politika ve usullerin de bu aşamada tespiti gerekir. Risklerin tanımlanmasından sonra risklerin sayısallaştırılması ise risklerin ölçülmesi aşamasıdır. Bu aşamada bankaların maruz kaldığı riskler belli ölçüm ve kıstaslara göre sayısal ya da analitik biçimde ifade edilmesi amaçlanmaktadır.[29]

Bankaların maruz kaldıkları risklerin belirli periyotlarda analiz edilmesi, risklerin izlenmesi aşamasını oluşturmaktadır. Bu süreçte elde edilen veriler derlenir, bilgiye dönüştürülür ve bu bilgiler analiz edilir. Yapılan analiz neticesinde belirlenen ve ölçülen risklere karşı, eğer gerekiyorsa koruyucu tedbirlerin devreye sokulması veya riski üstlenme kararırın verilmesi, riski kontrol etme sürecini oluşturmaktadır.[30] Kısacası bu aşamada yönetilecek risklere uygun politika ya da politika demetleri oluşturulur.

Politika ve uygulamaların başarısının sürekli takip ve değerlendirmeye tabi tutulması, risk yönetimi sürecinin son aşaması olan risklerin raporlanması

[28] Türkiye Bankalar Birliği Çalışma Grubu. (2006). Risk Yönetimi Prensipleri. *Bankacılar Dergisi*, 57, 15.
[29] Şahin, (2011). *a.g.m.*, s. 7.
[30] Altıntaş, (2011). *a.g.m.*, s. 4.

aşamasını oluşturmaktadır. Bu aşama, risk yönetiminde var olan bütün süreçlerin içerdiği faaliyetlerin kontrol edilmesi ve değerlendirilmesi amacıyla gerekli raporların yapıldığı bir süreci içermektedir.[31]

Risk yönetimi sürecinin banka iç denetim faaliyetleri ile de denetlenmesi gerekmektedir. Risk yönetimi sürecinin bütünlüğü, doğruluğu ve tutarlılığı, bu süreçten bağımsız iç denetim birimlerince denetim ve kontrol altında tutulmalıdır.[32]

2.2.2. Risk yönetiminin amacı ve önemi

Risk yönetiminin amacı, bankaların risk almasını önlemek değildir. Tam tersine bankacılık risk almaya dayalı bir faaliyet olduğundan, risk almaktan kaçarak bankacılık faaliyetlerini yürütmek söz konusu değildir. Bankacılıkta risk yönetiminin iki temel hedefi vardır.[33]

- Bankaların finansal performansını iyileştirmek,
- Bankaların kabulü mümkün olmayan ölçüde büyük zararlarla karşılaşmasını önlemektir.

Bankalarda, her ticari işletmede olduğu gibi temel amaç, eğer özel bir faaliyet söz konusu değilse, nihai olarak karı maksimize ederek, hissedarlarca yatırılan sermayeye en iyi getiriyi sağlayabilmektir. Bu ise ancak yüksek finansal performansla mümkündür. Dolayısıyla bankacılıkta risk yönetimini, bankaların kurulup faaliyete geçirilmesindeki temel amaçtan soyutlamak imkansızdır.[34]

Risk yönetimi sistemlerinin organizasyonu, tüm faaliyet ve finansal sonuçlardan nihai olarak sorumlu olan yönetim kurulu tarafından, bankanın yapısı ve faaliyetlerinin karmaşıklığıyla uyumlu şekilde belirlenmelidir. Banka yönetim kurullarının, bankanın günlük işlerinden ziyade hedefler ve hedeflere dönük stratejileri izleme odaklı, faaliyetlerin bunlarla uyumunu denetleyen ve bu doğrultuda politika belirleyen bir rolü bulunmaktadır. Risk yönetiminin banka

[31] Şahin, (2011). *a.g.m.*, s. 8.
[32] Şahin, (2011). *a.g.m.*, s. 8.
[33] Best P. (1999). *Implementing Value At Risk*. Chichester: John Wiley & Sons, 2.
[34] Şahin, (2011). *a.g.m.*, s. 9.

içindeki organizasyonu, icradan bağımsız, doğrudan yönetim kuruluna bağlı olacak şekilde yapılandırılmalıdır.[35]

Yönetim kurulu, risk yönetimi fonksiyonuna gerekli uygulama desteğini sağlamalı, risk yönetimi uygulamalarının içerdiği kavram ve tekniklere mümkün olduğunca yakınlaşmalı ve risk yönetimi faaliyetlerinin amaç ve kapsamı konusunda bilgi sahibi olmalıdır.[36]

Bankalarda, diğer işletmelerde de olduğu gibi yapılan ya da yapılmayan her türlü faaliyetin riski bulunmaktadır. Riskin var olması ise, onun yönetilmesini gerektirmektedir. Risklerin tanımlanması ve ölçülmesi, risk gerçekleşmeden alınacak tedbirler, bankalara olası tehlikelere karşı hazırlıklı olma yeteneği kazandırır. Bankaların bu riskleri yönetmesindeki amaç, piyasaların yaşadığı olağanüstü durumlarda bankanın karşılaşabileceği zararları önceden ölçebilmek ve olağanüstü durumlara hazırlıklı olmaktır.[37]

Risk yönetimi fonksiyonunun etkinliği ve işlevselliği, bankaların yönetim kalitesinin önemli göstergelerinden biri olarak algılanmalıdır. Bunun için bankanın stratejik ve yönetsel süreçlerinde risk yönetimine yer verilmesi gerekir. Risk yönetimi hedeflerinin banka örgütüne yayılması ve banka içinde risk kültürünün yerleştirilmesi zorunludur. Etkili bir risk yönetimi için banka çalışanlarının risk yönetimi bilgi ve deneyimine sahip olması kaçınılmazdır.[38]

2.3. Bankacılık Sektörü Riskleri

1970'li yıllar ile mali ve reel kesimde yaşanan gelişmeler, tüm dünyada bankaların karşı karşıya kaldıkları risklere yenilerini eklerken, riskin boyutunun belirlenmesi için yapılan çalışmalar zaman içerisinde giderek daha da karmaşıklaşmıştır.[39]

Ülkemizde risk yönetimi olgusu ilk olarak 1999 Uluslararası Para Fonu (IMF) niyet mektubunda gündeme gelmiş ve BDDK'nın kurulması ile birlikte Türk bankacılık sistemi risk yönetimi düzenlemeleri ile tanışmıştır. 2000 yılından bu yana Türk

[35] Şahin, (2011). *a.g.m.,* s. 9.
[36] Candan H., Özün A. (2009). *Bankalarda Risk Yönetimi ve Basel II* (2. Baskı). İstanbul: Türkiye İş Bankası Kültür Yayınları, 16.
[37] Babuşçu, (2005). *a.g.m.,* s. 16.
[38] Şahin, (2011). *a.g.m.,* s. 10.
[39] Şahin, (2011). *a.g.m.,* s. 10.

bankacılık sistemi risk yönetimi yapılanmasını tamamlamış ve risklerin ölçümü konusunda takip eden olmanın avantajını kullanarak büyük ilerlemeler kaydetmiştir.[40]

Genel olarak bakıldığında bankaların faaliyetleri nedeniyle maruz kaldıkları riskleri, Kredi riski, Piyasa riski ve Operasyonel risk olarak üç ana kategoride toplamak mümkündür. Kredi riski, bankanın alacaklarını zamanında ve tam olarak tahsil edememe durumu olarak değerlendirilebilir. Piyasa riski, bankaların finansal varlık portföylerinin değerini etkileyen risklerdir. Bu risk grubu içerisinde, faiz oranı riski, döviz kuru riski ve likidite riski yer almaktadır. Operasyonel risk ise piyasa ve kredi riski dışında kalan riskleri kapsamaktadır.[41]

2.3.1. Kredi riski

Kredi riski, kredi müşterisinin yapılan sözleşme gereklerine uymayarak yükümlülüğünü kısmen veya tamamen zamanında yerine getirememesinden dolayı bankanın maruz kalabileceği zarar olasılığını ifade etmektedir.[42]

Bankalar tarafından verilen krediler, kredi riskinin en önemli unsuru olmakla birlikte özellikle son yıllarda artan bankalar arası para piyasaları işlemleri, döviz işlemleri, garanti ve kefaletler, türev piyasa işlemleri ve bono yatırımları gibi işlemler, bankaların karşı karşıya kaldıkları diğer önemli kredi riski kaynaklarıdır. Kredi riski, yaşanan iflaslar çerçevesinde ele alındığında, sermaye piyasalarının en temel riski olduğu görülmektedir. Banka tarafından kullandırılan fonların fiyatının en önemli belirleyici unsuru kredi riskidir. Banka bilançolarının çok önemli bir kısmının bu risk unsuruyla karşı karşıya olması nedeniyle, kredi riski yönetimi bankalar açısından çok büyük önem taşımaktadır.[43]

Kredi riski yönetimi, bankanın kredi riskini kabul edilebilir düzeylerde tutarak, risk ayarlı getirisinin en yükseğe çıkarılmasını amaçlamaktır. Bu çerçevede etkin risk yönetimi, kredi riski ile ilgili uygun ortamın oluşturulması, kredilendirilme sürecinin

[40] Akan N. B. (2007). Piyasa Risk Ölçümü. *Bankacılar Dergisi,* 61, 59.
[41] Teker, (2006). *a.g.m.*, s. 3.
[42] Bankaların İç Sistemleri Hakkında Yönetmelik. Madde 3.
[43] Şahin, (2011). *a.g.m.*, s. 11.

etkin bir şekilde sürdürülmesi, doğru bir kredi risk ölçümünün yanı sıra kredi riskinin kontrolünün sağlanması işlevlerini içermelidir.[44]

Kredi risk yönetiminin vazgeçilmez unsurları, kredi riskinin tanımlanmasına yönelik politikaların oluşturulması, kontrol edilmesi, ölçülmesi, izlenmesi ve raporlanmasıdır. Bankaların uygulamış olduğu politikalar kredi faaliyetlerinin çerçevesini belirlemelidir.[45]

2.3.2. Piyasa riski

Piyasa riski, bankanın genel piyasa riski, kur riski, spesifik risk, emtia riski, takas riski nedenleriyle maruz kalabileceği zarar olasılığını ifade etmektedir.[46]

Piyasa riski en genel tanımıyla, herhangi bir finansal kuruluşun, bilanço içi ve bilanço dışı hesaplarında tuttuğu pozisyonlarında, piyasalardaki dalgalanmalar neticesinde oluşan faiz, kur ve hisse senedi fiyat değişimlerine bağlı olarak ortaya çıkan faiz oranı riski, kur riski ve hisse senedi pozisyon riski gibi riskler nedeni ile zarar etme ihtimalini ifade etmektedir. Piyasa riskinin ölçümünde alım-satım portföyünün riski dikkate alınır. Kısacası, piyasa riski varlıkların alım-satım, pozisyon, taşıma, faiz oranı, döviz piyasası veya mal piyasasında fiyat değişikliğine uğramasıdır.[47]

Piyasa riski, makroekonomik dengesizlik, siyasal istikrarsızlık ve benzeri nedenlerle meydana gelebilecek, piyasa fiyatlarında yüksek dalgalanmalar ile sonuçlanacak beklenmedik olay riski olarak değil; kur ve faiz gibi piyasa fiyatlarındaki volatilitenin taşınan pozisyonların ekonomik değeri üzerinde yaratacağı günlük etki olarak değerlendirilir.[48]

Faiz oranı ve hisse senedi risklerinin spesifik ve genel piyasa riski olmak üzere iki bileşeni vardır. Spesifik risk karşılığında sermaye yükümlülüğü konulmasının amacı, bankaları esas itibarıyla genel piyasa hareketlerinden ziyade, menkul kıymeti çıkaranın niteliğine ilişkin olarak ortaya çıkabilecek risklere karşı

---

[44] Basel Committee On Banking Supervision Report. (2000). *Principles For The Management Of Credit Risk*, 1.
[45] Şahin, (2011). *a.g.m.*, s. 13.
[46] Bankaların Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik. Madde 3.
[47] Candan, (2009). *a.g.m.*, s. 45.
[48] Numanoğlu, M. (2009). *Operasyonel risk yönetimi ve ölçümünde son gelişmeler*. TBB Eğitim ve Tanıtım Grubu Semineri, İstanbul, 6.

korumaktır. Spesifik riskler bu nedenle hiçbir şekilde netleştirmeye tabi değildir. Kur riskine ilişkin hesaplamalar her bir döviz cinsi için yapılmakta ve dövizlerin birbirleri ile netleştirilmesine imkan tanınmaktadır.[49]

2.3.2.1. Faiz oranı riski

Bankaların aldıkları kaynağa ödedikleri faizle, verilen kredilerden aldıkları faiz oranı arasındaki fark genel olarak bankanın karını oluşturmaktadır. Bankalar genelde bu işlemleri sabit faiz oranı üzerinden yapmaktadır. Faiz oranları işlemlerin yapılması anında belirlenmekte ve işlem sonuçlanana kadar değiştirilmemektedir. Bu durumlarda kredinin vadesi gelmeden banka piyasa faiz oranlarında bir yükselme olması durumunda kısa vadeli kaynaklarını yenilerken, yeni faiz oranını değiştiremeyecektir. Faiz oranlarındaki bu hareketlenmelere karşı banka önlem almadığı için karı azalacak veya zarar edecektir.[50]

Bankaların aktiflerinin ortalama vadesi genellikle pasiflerinin ortalama vadesinden daha uzun olmaktadır. Bu nedenle bankalar piyasa faiz oranlarındaki değişmeler sonucunda faiz oranı riski ile karşı karşıya kalmaktadırlar.[51]

Diğer bir ifade ile faiz riski bir bankanın bugünkü ve gelecekteki gelirlerinin ve sermayesinin olumsuz faiz oranı değişmelerine maruz kalmasıdır. Faiz oranlarındaki dalgalanmalar banka gelirlerine, net faiz gelirlerinin ve diğer faize duyarlı gelir ve giderlerinin değişmesi şeklinde etki ederken, bu dalgalanmaların sermaye üzerindeki etkisi bankanın nakit akımlarının zamanlamasının ve gelecekteki nakit akımlarının net bugünkü değerinin (NBD) değişmesiyle ortaya çıkmaktadır. Bu riski kabul etmek bankacılık açısından doğal bir durumdur ve bankanın karlılığı ve kar payı açısından önemli bir kaynak oluşturabilmektedir. Bununla birlikte aşırı düzeyde bir faiz riski bankanın, gelirini, sermayesini, likiditesini ve ödeme kapasitesini tehdit edebilir.[52]

---

[49] Bankacılık Düzenleme ve Denetleme Kurumu. (2002). Piyasa Riskinin Dahil Edildiği Yeni Sermaye Yeterliliği Rasyosunun Standart Metoda Göre Hesaplanmasına İlişkin Örnek. Risk ve Gözetim Teknikleri Araştırma Dairesi, 2.
[50] Şahin, (2011). *a.g.m.,* s. 15.
[51] Babuşçu, (2005). *a.g.m.,* s. 63.
[52] Yalçınkaya J., Ekinci A. (2007). Bankalarda Faiz Oranı Riskinin Ölçülmesi, *Eskişehir Osman Gazi Üniversitesi Sosyal Bilimler Dergisi,* 8(1), 21.

2.3.2.2. Döviz kuru riski

Bankaların kur riski, döviz varlıkları ve yükümlülükleri, döviz cinsinden cayılmaz nitelikteki gayri nakdi yükümlülükleri, gayri nakdi kredilere ilişkin alacakları, vadeli döviz işlemleri, takas işlemleri gibi kur riski içeren türev sözleşmeleri üzerinden hesaplanır. Bankaların altın pozisyonları da kur riski kapsamında değerlendirilir. Kur riskindeki temel varsayım aynı döviz cinsinden varlık ve yükümlülüklerin eşitliği durumunda kur riskinin olmayacağı, varlık ya da yükümlülüklerin birinin diğerinden fazla olması durumunda kur riskine yol açacağı yönündedir.[53]

Döviz kuru riski bankaları doğrudan ve dolaylı olmak üzere iki yoldan etkilemektedir. Döviz kurunun bankalar üzerindeki doğrudan etkisi, döviz kuru değişikliklerinin yabancı para cinsinden aktif ve pasif kalemler ile bilanço dışı işlemleri üzerindeki etkisinden kaynaklanmaktadır. Böylece bankanın nakit akışları değişmektedir. Diğer yandan, döviz kuru değişiklikleri, banka müşterilerinin, rakiplerinin ve fon sağlayan nakit akışlarını etkileyerek bankayı dolaylı biçimde de etkileyebilmektedir.[54]

2.3.2.3. Likitide riski

Likidite riski bankanın pozisyonlarını uygun bir fiyatta, yeterli tutarlarda ve hızlı olarak kapatamaması durumunda ortaya çıkan zarar ihtimali riskini ifade eder.[55]

Likidite bankanın hem aktifinde hem de pasifinde meydana gelen nakit ihtiyaçlarını karşılayabilme gücünün diğer bir ifade ile yükümlülüklerini tam olarak karşılama ve gereksinim duyduğu kaynakları zamanında temin edebilme kapasitesinin bir göstergesi olarak ortaya çıkmaktadır.[56]

Bankalar için özellikle likidite riski önemli bir risk olması nedeni ile bazı sınırların aşılması bankaların iflasını bile gündeme getirebilmektedir. Böyle bir noktaya gelinmesi ise diğer risklerin de gündeme gelmiş olmasına neden olacaktır. Likidite sıkıntısı yaşayan bankaların her zaman için piyasadan fon girdisi sağlama imkanı

---

[53] Candan, (2009). *a.g.m.*, s. 55.
[54] Kandır S. Y., Erişmiş A. (2010). Banka Hisse Senetlerinin Döviz Kuru Riskine Açıklığının İncelenmesi: İMKB Üzerine Bir Uygulama. *İMKB Dergisi*, 12(46), 50.
[55] Şahin, (2011). *a.g.m.*, s. 20.
[56] Şahin, (2011). *a.g.m.*, s. 20.

mevcut olabilir. Fakat bu durum piyasanın likiditesine, işlem hacmine, faiz oranları seviyesine ve fon talebini karşılayabilecek kuruluş bulunmasına bağlıdır[57]

2.3.3. Operasyonel risk

Operasyonel risk genel olarak kredi ve piyasa riski dışında kalan tüm riskler olarak ifade edilmektedir. Basel komitesi operasyonel riski uygun olmayan ya da işlenmeyen iç süreçler, insanlar, teknoloji (sistem) ya da dış etkenler nedeniyle ortaya çıkabilecek zarara uğrama riski olarak tanımlamıştır. Son yıllarda finansal piyasalarda yaşanan krizler dolayısıyla operasyonel riskin önemi ve gerçekleşmesi durumunda finansal kuruma vereceği zararın büyüklüğü daha açıkça anlaşılmaya başlanmıştır. Basel komitesi, Haziran 2004'te yayımladığı Basel II düzenlemesi ile birlikte 2007 yılından itibaren öncelikle Gelişmiş 10 ülkede (G-10) başlamak üzere bankaların operasyonel risklerini ölçerek gerekli sermaye karşılığını ayırmalarını öngörmüş ve bu amaçla bankalarda operasyonel risklerin ölçümü üzerine çeşitli modeller önermiştir.[58]

Operasyonel risk Basel komitesince, "Yetersiz ve başarısız içsel süreçlerden, personel ve teknolojiden (sistemlerden) ya da dışsal olaylardan kaynaklanan, doğrudan veya dolaylı zarar riskidir" şeklinde tanımlanmaktadır.[59]

Basel I uzlaşısı sermaye hesaplamasında, dikkate alınan tek risk türü kredi riski iken Basel II düzenlemesinde operasyonel risk türüne de yer verilmiştir.

[57] Altıntaş, (2011). *a.g.m.,* s. 112.
[58] Teker, (2006). *a.g.m.,* s. 1.
[59] Basel Committee on Banking Supervision. (2001). *Operasyonel Risk*. Consultative Document, 2.

3. BANKACILIKTA OPERASYONEL RİSK ÇEŞİTLERİNDEN TEKNOLOJİ RİSKİ

Operasyonel risk bankaların karşılaştıkları en eski risk türüdür. Yeni kurulan bir banka kredi işlemleri veya piyasa pozisyonuyla ilgili karar vermeden önce operasyonel risklere maruz kalır. Son yıllarda bankalar açısından operasyonel riskin öneminin artması, özellikle uluslararası finansal piyasalarda kullanılmakta olan ürünler, yöntemler ve teknolojinin oldukça karmaşık bir düzeye ulaşmasından kaynaklanmaktadır. Son 20 yıldaki teknolojik atılımlar, finansal piyasaların ve finans mühendisliğinin gelişiminde önemli bir rol oynamıştır. Bu durum özellikle türev ürünleri ve diğer finansal yeniliklerin oluşumunu mümkün kılmıştır. Böylece bankaların risk profilini değerlendirme ve aktif olarak yönetme (örneğin hedging-finansal risklere karşı korunma ve aktif-pasif yönetimi) konusundaki yetenekleri gelişmiş ve bu da risk yönetimi sürecini (riskleri belirleme, ölçme, izleme, kontrol etme ve raporlama) çok yönlü ve karmaşık hale getirmiştir. İşlemlerin karmaşıklığıyla beraber tamamlanma hızı ve verilere olan ihtiyaç artmıştır. Bu gelişmelere paralel olarak finansal kurumların teknolojik sistemlere ve kilit personele bağımlılığı daha da belirginleşmiştir.[60]

Bu gelişmeler doğrultusunda denetim otoritelerinin operasyonel riske yönelik ilgileri artmış ve operasyonel risk yönetimi kredi ve piyasa riski dışında ayrı bir disiplin olarak görülmeye başlanmıştır. Bu gelişmenin önemli bir diğer nedeni de, son yıllarda çok sayıda bankanın operasyonel riskin neden olduğu büyük boyutlu zararlara maruz kalmalarıdır.[61]

3.1. Operasyonel Riskin Tanımı ve Türleri

Operasyonel riskin tanımı üzerinde kesin bir birlik olmamakla birlikte, son yıllarda genel kabul görmüş dolaylı ve doğrudan tanımlama türlerinden söz etmek mümkündür. Dolaylı tanıma göre operasyonel risk, “Kredi veya piyasa riskleri altında sınıflandırılamayan diğer tüm risklerdir”.[62] Sade bir şekilde formüle edilen bu tanım, başlangıçta geniş çapta kabul görmüş ve denetim otoriteleri tarafından

[60] Boyacıoğlu M. A.(2002). Operasyonel Risk ve Yönetimi. *Bankacılar Dergisi*, (43), 51.
[61] Boyacıoğlu, (2002). *a.g.m.*, s. 51.
[62] Boyacıoğlu, (2002). *a.g.m.*, s. 51.

da kullanılmıştır. Fakat son yıllarda bu tanımın pratik ve teorik düzeyde tatmin edici olmadığı ortaya çıkmıştır. Daha sonra geliştirilen tanıma göre ise operasyonel risk, "Yetersiz ve başarısız içsel süreçlerden, personel ve teknolojiden (sistemlerden) ya da dışsal olaylardan kaynaklanan, doğrudan veya dolaylı zarar riskidir".[63]

Ülkemizde de BDDK'nın 8 Şubat 2001 tarih 24312 Sayılı Resmi Gazete'de yayımlanan "Bankaların İç Denetim ve Risk Yönetimi Hakkında Yönetmelik"te operasyonel risk, "Banka içi kontrollerdeki aksamalar sonucu hata ve usulsüzlüklerin gözden kaçmasından, banka yönetimi ve personeli tarafından zaman ve koşullara uygun hareket edilmemesinden, banka yönetimindeki hatalardan, bilgi teknolojisi sistemlerindeki hata ve aksamalar ile deprem, yangın, sel gibi felaketlerden kaynaklanabilecek kayıplara ya da zarara uğrama ihtimali" olarak tanımlanmaktadır.

Operasyonel riskler, personel (insan) riski, teknoloji riskleri, organizasyon (süreç) riski ve dışsal risklerden oluşmaktadır.

3.1.1. Personel (insan) riski

Banka yönetiminin ve personelin yetersizliğinden, ihmalinden, görevlerini unutmalarından ya da kötüye kullanmalarından veya kasıtlı olarak suç sayılan eylemleri gerçekleştirmelerinden kaynaklanan risklerdir. Örneğin banka yönetiminin limitleri aşarak ve yeterli güvence almadan kredi açması, gerekli incelemeleri yapmadan başka teşebbüslere iştirak etmesi, teknolojik yenilikleri bankaya adapte edememesi, değişime ayak uyduramaması, ürün ve hizmet tanıtımındaki yetersizlik ve belirsizliğin yanı sıra personelin yolsuzluk, hırsızlık ve sahtekarlık yapması, emirleri dikkate almaması veya kurallara aykırı olarak yerine getirmesi, bilerek işi engellemesi, kötü niyetli davranması gibi hususlar personel riski kapsamında değerlendirilebilir. Bu riske neden olan faktörler içerisinde ise personelin bilgi ve tecrübe yetersizliği, motivasyon eksikliği, aşırı iş yükü,

[63] Basel Committee on Banking Supervision. (2001). Operasyonel Risk. Consultative Document, 2.

personelin düzensiz yer değişimi, iş yerinin elverişsizliği ya da düzeninin iyi kurulmamış olması gibi konular sayılabilir.[64]

3.1.2. Organizasyon (süreç) riski

Banka örgüt yapısı ve işleyişiyle ilgili sorunlardan doğan risklerdir. Örneğin, örgüt içerisindeki kademeler arasındaki bilgi akışının yetersizliği, yetki sınırlarının kesin olmaması, yapı işleyiş değişikliklerinden doğan belirsizlikler bu gruba girmektedir.[65]

Banka faaliyetlerinin işleyişi ile ilgili süreçleri tamamlayıcı fonksiyona sahip iç kontrollere ilişkin prosedürlerin olmamasından, mevcut prosedürlerin hatalı tasarlanmasından ya da yanlış şekilde uygulanmasından kaynaklanan bir risk türüdür. Banka içi birimler arasında bilgi akışındaki yetersizlikler, yetkililerin sınırlarının açık olarak belirlenmemesi, etkin kontrol mekanizmalarının olmamasının yanında karşılaşılan risklerin tam olarak saptanamaması gibi hususlar bu gruba dahil olan risklere yol açan faktörlerdendir.[66]

3.1.3. Dışsal riskler

Banka dışındaki üçüncü kişiler ile ilgili sahtekarlık olayları, hukuki düzenlemelerdeki değişiklik ve boşluklar, deprem, yangın, sel gibi felaketler, terörist faaliyetler vb. olaylar sonucunda bankanın maruz kalacağı risklerdir.

3.1.4. Teknoloji (bilgi teknolojileri) riski

Kullanıldıkça tükenmeyen bir kaynak olan bilgi, günümüzde mal ve hizmet üretim süreçlerinde önemli bir girdi haline gelmiştir. Bilginin öneminin artması ile birlikte, elde edilmesi ve üretim süreçlerinde kullanılacak hale dönüştürülmesi ihtiyacı doğmuştur. Bu ihtiyaca cevap vermek amacı ile süren çalışmalar, bilgi teknolojilerini geliştirmiştir. Bilgiyi toplama, işleme ve dağıtma görevini üstlenen teknolojiler, bilgi teknolojileri olarak adlandırılmaktadır. Bilgi teknolojileri günümüzde, sosyal yaşamın ayrılmaz bir parçası olmuştur. Söz konusu

[64] Boyacıoğlu, (2002). *a.g.m.*, s. 52.
[65] Boyacıoğlu, (2002). 52.
[66] Şahin, (2011). *a.g.m.*, s. 33.

teknolojilerin dünya genelinde uygulama alanı hızla artmaktadır, dolayısıyla bu gelişimin dışında kalma şansı bulunmamaktadır. Güvenilir bilgi teknolojileri, çok fazla birbirine bağlanmış sistem ve fonksiyonel bilgi teknolojileri işleyişine ihtiyaç duyulması nedeniyle, toplumlar ve ekonomiler için önem arz etmektedir. [67]

Günümüzde teknolojinin gelişimi için bilgi teknolojileri lokomotif rol üstlenmektedir. Bilgi teknolojilerindeki hızlı değişim, teknoloji geçişlerini bir tercih olmaktan çıkarıp zorunluluk haline getirmiş bulunmaktadır.[68]

Teknoloji, geleneksel yapıda olmayan pek çok riski bünyesinde barındırmaktadır. Teknoloji riskleri yazılım, donanım ve telekomünikasyon sistemlerinin kullanımından ya da bu sistemlere olan güvenden oluşan zarar, kayıp, düzensizlik ya da hatalarla ilişkili risklerdir. Bu riskler aynı zamanda sistem göçmeleri, işleme hataları, yazılım kusurları, işletim yanlışları, donanım arızaları, kapasite yetersizlikleri, ağ kırılganlıkları, kontrol süreçlerindeki zayıflıklar, güvenlik eksiklikleri, kötü niyetli ataklar, saldırı (hacking) olayları, dolandırıcılık eylemleri ve yetersiz yeniden elde etme kapasiteleri ile birlikte de düşünülmelidir.[69]

Günümüzde bireysel ya da kurumsal her türlü gelişme internet ve bilgi teknolojileri sistemlerine daha da fazla bağlı hale gelmektedir. Bunun sonucu olarak sistemler üzerindeki riskler daha fazla fark edilmekte ve önemli olarak görülmektedir. Bilgi teknolojileri kaynaklı oluşacak riskler sistemde tıkanmaya, sistemin durmasına ve hatta bozulmasına neden olabilmektedir. Bilgi sistemleri üzerindeki güvenlik açıkları ya da hatalar ciddi iş krizlerine ve itibar kayıplarına yol açmaktadır. Bu sebeple pek çok düzenleyici kuruluş yeni uyum zorunlulukları getirmektedir. [70]

Bilgi teknolojileri riskleri kurumdaki tüm risklerin bir parçası olarak belirlenmeli, ölçülmeli ve yönetilmelidir. Bilgi her kuruluş için kritiktir ve çoğunluğu bilgi teknolojileri sistemlerinde oluşturulur, işlenir, iletilir ve saklanır. Bunun sonucu

---

[67] Rumelili, Ö. M. (2006). *Ödeme Sistemlerinde Bilgi Teknolojileri Riskleri,* Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimleri Enstitüsü, Ankara.
[68] Rumelili, (2006). *a.g.m.*, s. 78.
[69] Rumelili, (2006). *a.g.m.*, s. 79.
[70] İnternet: Bağcı, B. (2010). Bilgi Teknolojileri Risk Yönetimine Genel Bakış. Deloitte. 1. Web: http://www.denetimnet.net/Pages/bilgiteknolojileririskyonetimi.aspx adresinden 8 Ocak 2014'de alınmıştır.

olarak, bilgi teknolojileri riskleri sadece bilgi teknolojileri birimlerinin sorumluluğunda değil, aynı zamanda tüm kurumun sorumluluğundadır.[71]

3.2. Teknoloji (Bilgi Teknolojileri) Riski Yönetimi

Risk yönetimi, risk belirlemek, değerlendirmek ve riski kabul edilebilir bir seviyeye indirmek için aksiyon alma sürecidir. Bilgi teknolojileri risk yönetimini, her biri farklı öneme sahip ancak birbirini etkileyen ve destekleyen beş temel fonksiyonla yerine getirmek mümkündür.

- Risk Belirleme
- Risk Analizi
- Risk Değerlendirme
- Riske Müdahale Etme
- Risk Yönetimini İzleme

Bilgi teknolojileri risk yönetimi süreci, servisler ile iş birimleri arasında iletişim kurmalı, organizasyona uygun, yapısal ve tekrar edilebilir, uluslararası en iyi uygulamalara yatkın ve bu konuda denetim sahibi iç ve dış birimlerce kontrol edilebilir olmalıdır.[72]

BDDK tarafından yayımlanan “Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik” uyarınca bankalara COBIT’te yer alan usul ve esaslar uygulanmalıdır. Bu kapsamda COBIT’in önemli konu başlıklarından olan “Bilgi Sistemleri Riskinin Değerlendirilmesi ve Yönetimi” kontrol hedefinin de bankalarda uygulanması beklenmektedir. COBIT, bir bilgi teknolojileri (bilgi sistemleri) yönetişim çerçevesi olarak, bilgi sistemleri ile ilişkili risklerin yönetilmesi için referans oluşturmaktadır. COBIT kontrol güvencesi dahilinde bilgi sistemleri risklerinin değerlendirilmesi ve yönetilmesi için gerekli kontroller açıklanmıştır.[73]

---

[71] İnternet: Bağcı, B. (2010). Bilgi Teknolojileri Risk Yönetimine Genel Bakış. Deloitte. 1. Web: http://www.denetimnet.net/Pages/bilgiteknolojileririskyonetimi.aspx adresinden 8 Ocak 2014’de alınmıştır.

[72] İnternet: Bağcı, B. (2010). Bilgi Teknolojileri Risk Yönetimine Genel Bakış. Deloitte. 4. Web: http://www.denetimnet.net/Pages/bilgiteknolojileririskyonetimi.aspx adresinden 8 Ocak 2014’de alınmıştır.

[73] Bağcı, (2010). *a.g.m.*, s. 1.

COBIT'in risk yönetimi kapsamı içerisinde incelediği hususlar, risk yönetimi çerçevesinin oluşturulması, risk kapsamının kurulması, olay belirleme, risk değerlendirme, risk yanıtlama ve risk aksiyon planlarının yürütülmesi ve izlenmesidir. Bilgi teknolojileri risklerinin değerlendirilmesi ve yönetilmesi için bir risk yönetim çerçevesi oluşturulmalı ve sürdürülmelidir. Risk yönetimi çerçevesi, genel ve üzerinde anlaşılmış bilgi teknolojileri risk seviyelerini, risk karşılama stratejilerini ve artakalan riskleri (residual risk) içermelidir. Organizasyonun hedefleri üzerinde herhangi bir potansiyel etkinin oluşturacağı beklenmedik olaylar önceden belirlenir, analiz edilir ve değerlendirilir. Artakalan riskleri kabul edilebilir bir seviyeye ulaştırmak için risk karşılama stratejileri uygulanır. Değerlendirmenin sonuçları, paydaşların risklere kabul edilebilir seviyeden tolerans göstermeleri için anlaşılabilir ve finansal terimlerle izah edilebilir olmalıdır. BDDK tarafından yayımlanan "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ Taslağı"nın 5. maddesinde yer aldığı üzere bankalar, bankacılık faaliyetlerinde bilgi teknolojilerini kullanıyor olmasından kaynaklanan riskleri tanımlamalı, analiz etmeli, izlemeli ve yönetmek üzere gerekli önlemleri almalıdır. Bilgi sistemlerine ilişkin risklerin yönetilmesi, kurumsal bilgi sistemleri yönetiminin önemli bir bileşeni olarak ele alınmalıdır. Bankaların, risk yönetimlerini ve politikalarını, bilgi teknolojilerinin kullanımına bağlı olarak gözden geçirmesi ve bilgi sistemleri kullanımından kaynaklanan risklerin yönetimini içerecek şekilde yenilemesi gerekmektedir. Bilgi teknolojilerinden kaynaklanan riskler bilinen bankacılık risk sınıfları arasına yeni bir risk sınıfı eklememektedir. Bilgi teknolojilerinin yönetimi ve izlenmesine yönelik çalışmalardan edinilen veriler bankanın risk yönetimi çerçevesinin bir parçası haline gelmeli ve bilgi teknolojilerinden kaynaklanan riskleri de içeren bütünleşik bir risk yönetimi yaklaşımı uygulanmalıdır. Bankaların, kendi risk profiline, kurumun operasyonel yapısına, yönetim kültürüne ve ilgili diğer yasal yükümlülüklerle belirtilen çerçeveye uygun olarak risk yönetiminin oluşturulması ve bilgi teknolojileri risklerini de bu kapsamda değerlendirmeye alması gereklidir. Belirlenecek sıklıkta veya bilgi sistemlerindeki önemli değişikliklerden önce risk analizleri tekrarlanmalı ve analizlere ilişkin yazılı politikalar belirlenmelidir. [74]

[74] İnternet: Bağcı, B. (2010). Bilgi Teknolojileri Risk Yönetimine Genel Bakış. Deloitte. 2. Web: http://www.denetimnet.net/Pages/bilgiteknolojileririskyonetimi.aspx adresinden 8 Ocak 2014'de alınmıştır.

3.3. Bilgi Teknolojileri Riskini Yönetmek İçin Geliştirilen Standartlar

Bilgi teknolojileri yönetiminin etkinliği, teknolojik gelişmelere paralel olarak giderek daha fazla önem kazanmakta ve bu durum da kurumların bilgi teknolojilerine yönelik sektördeki en iyi uygulamaları kullanmayı istemelerine sebep olmaktadır. Bu çerçevede, kurumların BT'ye dönük yatırım kararlarını yeniden şekillendiren birçok neden vardır.[75]

Öncelikle, kurumlar bilgi teknolojilerine yapmış oldukları yatırımlar dolayısıyla daha fazla değer elde etmek istemektedirler ve BT'ye ayrılan kaynaklar kurum bütçelerinde geçmiş dönemlere kıyasla daha fazla pay almaktadır. Ayrıca, kamuya açıklanan mali tabloların gerçeği yansıttığına dönük olarak BT kontrollerinin tesis edilmesi ve gizlilik ilkelerine uyulması konusunda gerçekleştirilmiş olan yasal düzenlemeler kurumların BT yatırımlarının niceliğine ve niteliğine dönük bakış açılarını etkilemiştir.[76]

Kurumların kendi geliştirdikleri bazı hizmet ve ürünleri maliyet etkinliği açısından değerlendirip dış tedarikçilerden temin etmeleri, BT yönetimine ilişkin sektördeki en iyi uygulamaları örnek almaları konusundaki yaklaşımlar BT risk yönetimini etkileyen unsurlar olarak göze çarpmaktadır. Kurumsal iş ortamının globalleşme eğilimleri, değişen iş yapma şekilleri ve müşteri/paydaş beklentileri, BT'ye kurumların operasyonel işleyişinde merkezi ve kritik bir rol yükleyerek BT risk yönetimini kurumlar için oldukça önemli hale getirmiştir.[77]

Çünkü kurumsal strateji ve hedeflerin gerçekleştirilmesinde etkin işleyen bir BT yönetimi merkezi bir rol oynadığı gibi, BT faaliyetlerinin etkin bir şekilde yönetilmesinde "en iyi uygulama örnekleri" ve uluslararası kabul görmüş standartların uygulanması da önemli bir unsurdur. Diğer taraftan, kurumda çalışan her bir personelin; politikalar, iç kontroller ve tanımlanmış prosedürler sayesinde ne şekilde hareket etmesi gerektiğine dönük yönetim tarafından oluşturulmuş çerçevelerden haberdar olması ve bu normlar bağlamında operasyonel faaliyetleri

[75] Aykın, H. (2009). Bankalarda Operasyonel Risk Yönetimi ve Bir Endeks Önerisi: Oryos Endeksi, Doktora Lisans Tezi, Kadir Has Üniversitesi Sosyal Bilimleri Enstitüsü, İstanbul, 75.
[76] Aykın, (2009). *a.g.m.,* s. 76.
[77] Aykın, (2009). *a.g.m.,* s. 76.

yürütüyor olması, “en iyi uygulama örneklerinin” kurumsal BT risk yönetimi isleyişinde uygulanıyor olmasıyla kurumsal verimlilik artacak, daha az operasyonel hata gerçekleşecek, düzenleyiciler ve birlikte iş yapılan tarafların kuruma karşı sahip oldukları güven duygusu artacaktır.[78]

Dolayısıyla, tutarlı ve istikrarlı bir bilgi teknolojileri risk yönetimi politikasının oluşturulabilmesi için öncelikle sağlam, tutarlı ve programlı bir projeksiyona sahip olunması, kurumsal ve operasyonel risklerin doğru belirlenmesi, bazı risklerin daha az önemli olduğu yaklaşımından uzak durulması, risk yönetimini belirlerken tüm sistemlerin entegre olarak düşünülmesi, stratejik kontrollerin etkili ve doğru düzenlenmesi, risklerin ve kontrollerin tüm personele zamanında aktarılması gereklidir. En önemli husus, BT risk yönetimi oluşturulmasının üst yönetimce öncelikli olarak kabul görmesidir. BT risk yönetimi süreci sürekli devam eden, kendini yenileyen ve belli bir son noktası olmayan bir süreç olarak algılanmalıdır. Zira teknoloji geliştikçe, kurumun faaliyetleri değiştikçe ve büyüdükçe yeni risklerin ortaya çıkma durumları da kaçınılmazdır.[79]

Kurumlar için BT risk yönetiminin çok önemli bir husus haline gelmesine bağlı olarak bu konuda kapsamlı ve etkin işleyen süreç ve altyapı oluşturmak kurumların en önde gelen hedeflerinden biri olmuştur. Çünkü, BT risk yönetimi bir taraftan kurumsal verimliliği artırmaya dönük ön koşulları sağlayıp kurumun bazı noktalarda rekabetçi bir üstünlük oluşturabilmesi için kuruma fırsatlar sunarken, diğer taraftan ise lokal ölçüde de olsa operasyonel faaliyetlerin ve bilgi sistemlerinin belirli bir süre kesintiye uğraması bile kurumlar için oldukça yüksek maddi ve itibari kayıplara sebebiyet verebilecektir.[80]

BT risk yönetiminin özellikle finansal sektörde faaliyet gösteren kurumlar için yaşamsal derecedeki önemi, bu alanda da COBIT, ITIL, ISO/IEC 27001, ISO/IEC 27002, BS 15000, BS, 7799, ISO/IEC 17799 gibi uluslararası bazı standartların ve en iyi uygulama örneklerinin oluşmasına sebebiyet vermiştir.[81]

BT risk yönetimine ilişkin olarak geliştirilmiş olan çeşitli standartların ilki İngiltere tarafından geliştirilmiştir. İngiltere hükümeti, BT’ye dönük en iyi uygulama

[78] Aykın, (2009). *a.g.m.*, s. 76.
[79] Aykın, (2009). *a.g.m.*, s. 76.
[80] Aykın, (2009). *a.g.m.*, s. 77.
[81] Aykın, (2009). *a.g.m.*, s. 77.

örneklerinin BT risk yönetiminde kullanılması gerektiğini çok uzun zaman önce fark etmiş ve bu doğrultuda da BT risk yönetimine dönük en iyi uygulama örneklerini yıllar içinde geliştirmiştir. İngiltere tarafından yaklaşık 20 yıl önce geliştirilmiş olan ITIL (Information Technology Infrastructure Library) uluslararası kabul görmüş standartların ilkidir. ITIL, sektörde faaliyet gösteren uzmanlardan ve sektörel danışmanlardan faydalanılarak oluşturulmuş olan ve BT hizmet yönetimine ilişkin olarak en iyi uygulama örneklerini dokümante eden bir standartlar setidir. BS 15000 ise yaklaşım olarak ITIL ile paralel olan bir hizmet yönetimi standardıdır. BT Güvenlik Uygulama Rehberi (IT Security Code of Practice) olarak oluşturulmuştur.[82]

BS 7799-2 standardı ilk olarak 1999 yılında BSI (British Standarts Institution) tarafından bilgi güvenlik yönetimi sistemi için sertifikasyon vermek amacıyla hazırlanmış bir kılavuz iken, 2002 yılında revizyona uğramış ve 2005 yılında da ISO/IEC 27001:2005 (BS 7799-2:2005) adıyla uluslararası bir standarda dönüşmüştür. ISO/IEC 27001:2005, bilgi güvenliği yönetimi sisteminin kurulması, uygulanması, izlenmesi, sürdürülmesi ve geliştirilmesi için gerekli adımları ortaya koyan süreçsel yaklaşımın çerçevesini çizmektedir. ISO/IEC 27002:2005 standardı kapsamlı bir karşı önlem havuzudur. Özetle önlemler ISO 27002 standardında, önlemlerin nasıl yaşatılacağı ise ISO 27001 standardında açıklanmaktadır.[83]

COBIT metodolojisi diğer BT risk yönetimi standartlarına kıyasla uzmanlık alanı BT olmayan yöneticilere ve denetçilere de hitap edebilmektedir. Çünkü, denetçiler, yöneticiler ve BT birimlerinde çalışanlar arasında oluşan iletişim kopukluğundan kaynaklanan sorunlara karşı COBIT sürece dahil olan tüm tarafların kolaylıkla anlayabileceği şekilde jenerik BT risk yönetimi süreçleri üzerine tesis edilen bir BT kontrol çerçevesi olarak geliştirilmiştir.[84]

Bir sonraki bölümde bilgi teknolojileri kapsamında geliştirilmiş operasyonel riskin sistem tarafını ilgilendiren bilgi güvenliğinin sağlanmasına yönelik önlemleri sıralayan ve BDDK'nın bankalar için getirdiği bir düzenleme olan COBIT metodolojisi detaylı bir şekilde açıklanacaktır.

---

[82] Aykın, (2009). *a.g.m.,* s. 77.
[83] Bayoğlu B.(2008). Bilgi Güvenliği Yönetim Sistemi Uygulama ve Denetleme Semineri Notları. Takasbank, Tubitak Uekae: Ulusal Elektronik ve Kriptoloji Arastırma Enstitüsü, 73.
[84] Aykın, (2009). *a.g.m.,* s. 77.

4. TEKNOLOJİ RİSKLERİNİN YÖNETİMİ İÇİN COBIT STANDARTI

COBIT, “Control Objectives for Information and related Technology” kelimelerinden üretilmiş türkçe karşılığı bilgi ve ilgili teknolojiler için kontrol hedefleri anlamına gelen bir kısaltmadır. Bu bölümde COBIT 4.1 standartının ne olduğu, usul ve esasları genel hatlarıyla anlatılmaya çalışılmıştır.

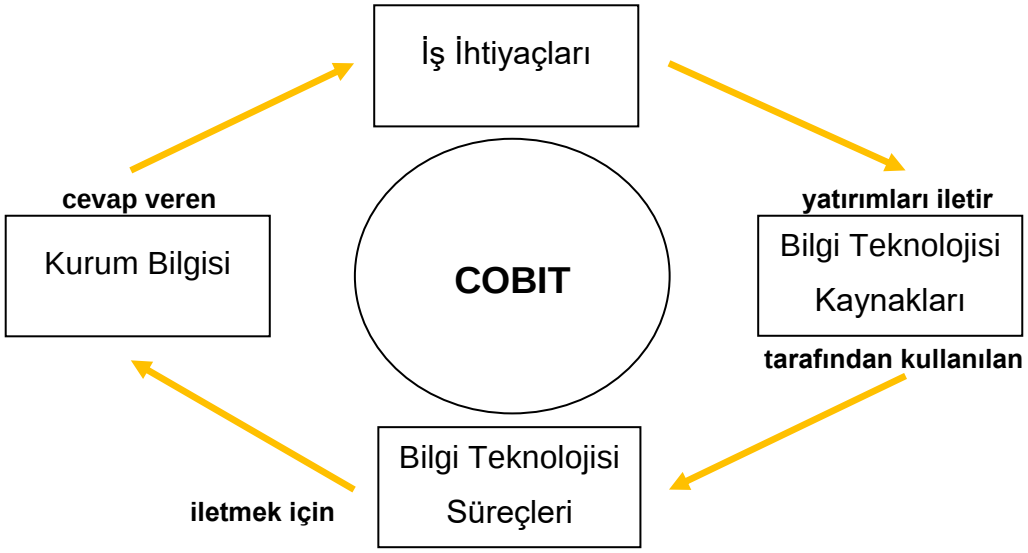
COBIT, en genel anlamıyla kurumların operasyonel işleyiş süreçlerinde oluşturulan ve dış kaynaklardan alınan verilerin hızlı, sürekli ve güvenli bir ortamda sağlanabilmesi için bilgi sistemlerine ve iletişim teknolojilerinin kullanılmasından kaynaklanan risklerin tespit edilmesi, yönetimi ve kontrolünün etkin ve verimli olarak yapılmasını temin etmek için oluşturulmuş olan bir kontrol hedefler çerçevesidir.[85] COBIT, kurumların BT risklerini nasıl yöneteceklerine ve bağlı oldukları BT yapısını nasıl daha güvenli hale getirebileceklerine dönük sorulara sistematik bir yaklaşım sergileyerek ve aynı zamanda üst yönetimin ihtiyaçlarına da yanıt verecek şekilde oluşturulmuş olan bir yöntemdir. COBIT ayrıca, kurumda BT risk yönetimine ilişkin olarak gerekli kontrollerin tesis edildiğini, uluslararası düzenlemelerle uyumun sağlandığını gösteren bir çerçeve sunarak kontrol hedefleri, teknik gereksinimler, ticari riskler ve performans ölçümleri arasındaki ilişkiyi sağlar.[86]

COBIT, üst yönetimin bilgi teknolojileriyle ilgili olarak kurumun operasyonel işleyişi içerisinde karşılaştıkları fırsatları ve riskleri anlamalarına ve yönetmelerine yardımcı olmak amacını taşıyan, Information Systems Audit and Control Association (ISACA) tarafından ilk defa 1996 yılında geliştirilmiş olan bir kontrol çerçevesidir. COBIT, ISACA bünyesindeki, BT Yönetişim Enstitüsü (ITGI: IT Governance Institute) tarafından geliştirilen, desteklenen ve sürekli güncellenen bilgi teknolojilerine yönelik kontrol çerçevesini içeren bağımsız bir açık standartlar setidir.[87]

Bir şirkette teknolojinin kullanımından ve BT yönetişimi ile kontrol geliştirmekten türeyen faydayı en üst düzeye çıkarmaya yardım etmesi için yöneticilere, denetçilere ve BT kullanıcılarına genel olarak kabul görmüş ölçüler, göstergeler,

[85] Artinyan, E. N.(2007). COBIT Çerçevesi. *Active Dergisi*, (54), 1.
[86] Aykın, (2009). *a.g.m.*, s. 79.
[87] Aykın, (2009). *a.g.m.*, s. 78.

süreçler ve en iyi uygulamalar sağlar. COBIT'in vizyonu, bilişim teknolojileri yönetişim (IT governance) modeli olmaktır. COBIT sadece bir denetim aracı değil, aynı zamanda bir yönetişim aracı olma amacını da taşır. Bu nedenle yönetimden bilişim teknolojileri personeline kadar kurum içi ve dışında, kurumun varlığı ve sağlıklı faaliyet göstermesi konularında risk üstlenen çeşitli taraflara fayda sağlama amacını da yerine getirmeyi hedeflemektedir.[88]



Şekil 4.1. Temel COBIT İlkesi

COBIT aşağıdakileri sağlayacak bir çerçeve sağlayarak bilgi teknolojileri yönetimini destekler:

- Bilgi teknolojileri ile iş tarafı bağlantılıdır.
- Bilgi teknolojileri iş tarafına kolaylık sağlar ve yararları maksimize eder.
- Bilgi teknolojileri kaynakları sorumlu bir şekilde kullanılır.
- Bilgi teknolojileri riskleri uygun bir şekilde yönetilir.

COBIT'in iş odaklı bir yaklaşım olması, kurumun hedefleriyle bilgi teknolojilerinin hedeflerini uyumlu hale getirmesini ve sorumlulukları da BT ve BT dışı süreç sahiplerine verilmesini sağlar. Dolayısıyla COBIT, kaynakların en verimli şekilde kullanılmasını ve risklerin en etkin bir şekilde yönetilmesini sağlayan bir çerçeve sunarak BT risk yönetimini oluşturur.

[88] Hacısüleymanoğlu, *a.g.m.*, s. 16.

“Teknoloji risklerini nasıl yöneteceğiz ve bağlı bulundukları sistemsel yapıyı daha güvenli hale nasıl getireceğiz?” sorularının yanıtları, sadece BT yöneticileri değil, teknoloji yoğun çalışan ve iş süreçlerine teknolojiyi entegre etmiş tüm kurum yöneticileri için önem taşımaktadır. COBIT, bu ve bunun gibi sorulara sistematik bir yaklaşım sergileyerek ve yönetsel ihtiyaçlara da yanıt verecek şekilde oluşturulmuş bir yöntemdir.

COBIT, bir kurumda BT risklerinin etkin bir şekilde yönetilmesine ilişkin olarak daha fazla ne yapılması gerektiğini açıklarken nasıl yönetilmesi gerektiği üzerinde fazla durmaz.[89] COBIT, sadece kullanıcılar ve denetçiler tarafından kullanılması için değil, aynı zamanda ve daha da önemlisi iş süreci sahipleri için kapsamlı bir kontrol listesi olarak da tasarlanmış ve geliştirilmiştir.[90]

COBIT yapısı, bilgi teknolojisi aktivitelerini izlemek ve yönetmek için kurum içerisindeki herkese referans işlem modeli ve ortak bir dil sağlar. Bilgi teknolojisine dahil olan şirketin bütün bölümleri için oluşturulan operasyonel model ve ortak dil, başarılı yönetime giden en önemli ve ilk adımlardan biridir. Aynı zamanda bilgi teknolojisi performansının ölçülmesi ve izlenmesi, hizmet sağlayıcılar ile iletişim kurulması, en iyi yönetim uygulamalarının bütünleştirilmesi için bir yapı sağlar. Süreç modeli, mali sorumluluk ve hesap verilebilirlik tanımlamalarını sağlayarak süreç sahipliğini destekler.

COBIT’te tanımlanan bilgi teknolojisi kaynakları aşağıdaki gibi ifade edilebilir:

- **Uygulamalar**, bilgiyi işleyen manuel prosedürler ve otomatikleştirilmiş kullanıcı sistemleridir.

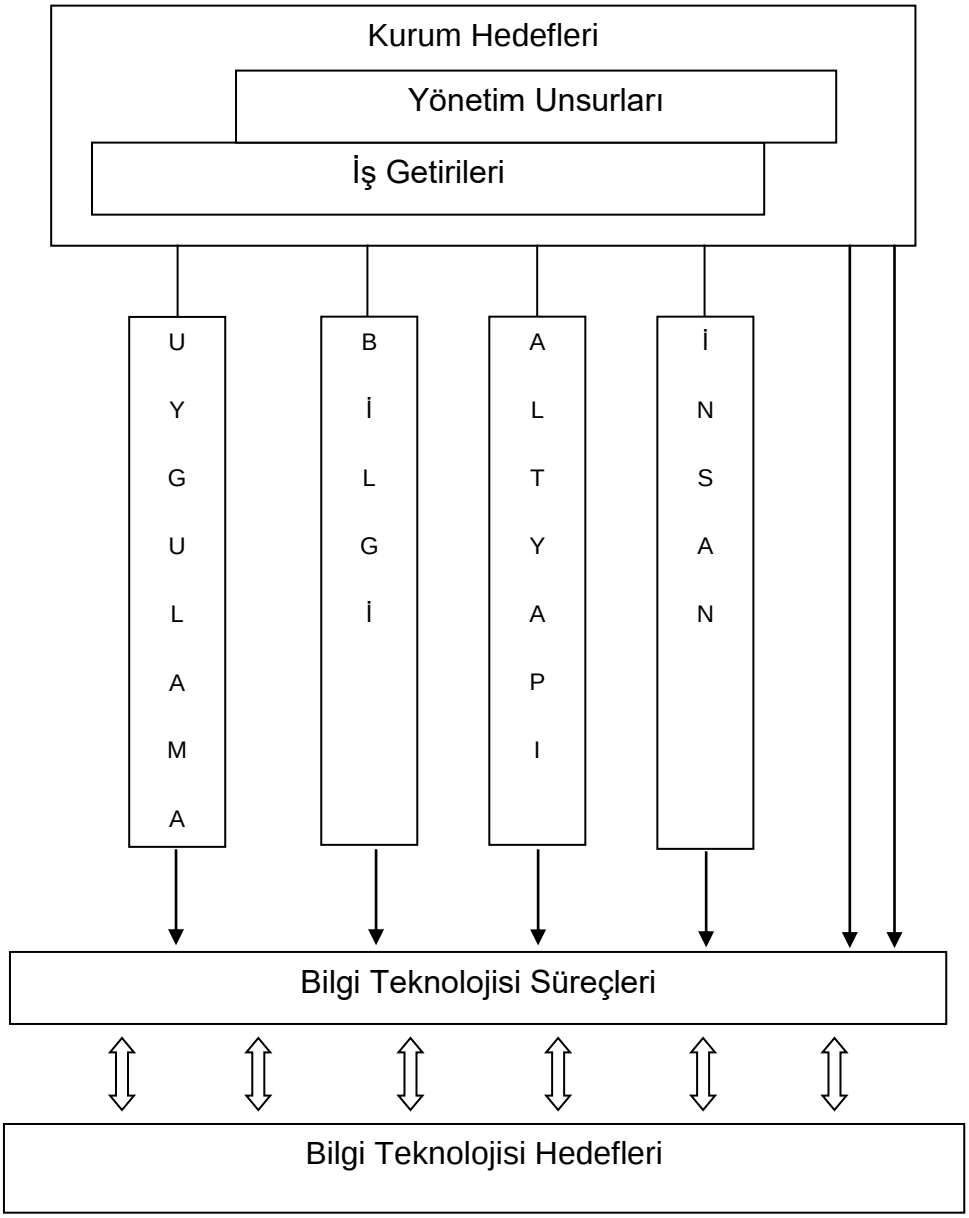
- **Bilgi**, bütün şekilleriyle, şirket tarafından kullanılan ve her ne şekilde olursa olsun bilgi sistemleri tarafından ortaya koyulan girdi, işlem ve çıktıdan oluşan veridir.

- **Altyapı**, uygulamaların çalıştırılmasını sağlayan teknoloji ve olanaklardır. (Donanım, işletim sistemleri, veri tabanı yönetim sistemleri, ağ bağlantıları, çoklu ortam ve bunlara ev sahipliği yapan destekleyen çevre vb.)

---

[89] Aykın, (2009). *a.g.m.*, s. 79.
[90] Global Technology Audit Guide(2008). Bilgi Teknolojisi Kontrolleri. Uluslararası İç Denetim Ensititüsü, 99.

- **İnsanlar**, planlama yapmak, organize etmek, edinmek, uygulamak, iletmek, desteklemek, izlemek ve bilgi sistemleri ve hizmetlerini değerlendirmek için gerekli olan personeldir. Bunlar, dışarıdan alınan ya da gerektiğinde sözleşme yapılan personel olabilir.



Şekil 4.2. Bilgi Teknolojisi Hedeflerini İletmek için Bilgi Teknolojileri Kaynaklarının Yönetilmesi

COBIT denetleme ihtiyaçları, teknik konular, işletme riskleriyle ilgili eksiklikler arasında yöneticilere rehber ilkeler sağlayan ve ortakların bu denetim düzeyinde iletişim kurmalarına izin veren bir yapıdır. COBIT kurumlar arasında bilgi teknolojileri denetimi için iyi uygulamaların ve açık politikaların gelişimini temin

eder. COBIT sürekli olarak güncellenir ve diğer standartlar ve ilkeler ile harmonize edilir.

COBIT'in bilgi teknolojileri üzerinde yönetim çerçevesi olarak uygulanmasının faydaları şunları içerir:

- İş odağına dayanan daha iyi bir sıralama
- Bilgi teknolojilerinin ne yaptığına dair yönetime anlaşılabilir bir izlenim
- Süreç yönlendirmesine dayanan açık sahiplik ve sorumluluklar
- Üçüncü şahıslar ve düzenleyiciler ile genel kabul edilebilirlik
- Ortaklar arasında ortak bir dile dayanan paylaşılan anlayış

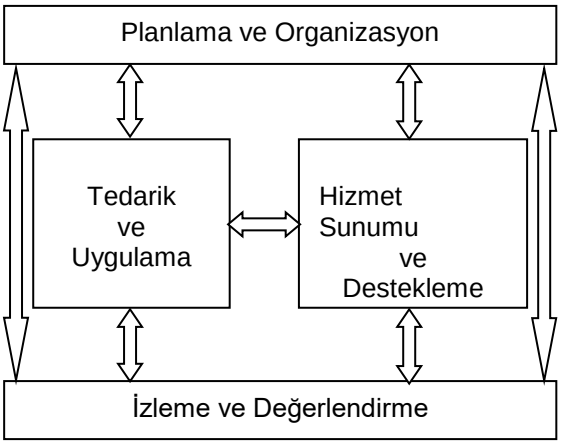
Böylece COBIT, bilgi teknolojilerinin başarılı uygulamaları için bir bütünleştirici, bilgi teknolojileri ile bağlantılı yararların ve risklerin yönetilmesi ve anlaşılmasına yardım eden bilgi teknolojileri yönetimi için kapsayıcı bir yapı olmuştur. COBIT'in süreç yapısı ve üst seviye iş eksenli yaklaşımı, bilgi teknolojilerinin baştan sona izlenmesini ve bilgi teknolojileri hakkında karar verilmesini sağlar.

COBIT'in şu ana kadar dört ana sürümü yayımlanmıştır.

- 1996, birinci sürüm yayımlandı.
- 1998, ikinci sürüm yayımlandı.
- 2000, üçüncü sürüm yayımlandı.
- 2005, dördüncü sürüm yayımlandı.
- 2007, güncel sürümü 4.1 yayımlandı.
- 2015, beşinci sürümü yayımlanması planlanıyor.

2007 yılının mayıs ayında, şu anda kullanılan 4.1 sürümü yayımlanmıştır. COBIT'in herhangi bir kurumda yer alabilecek tüm teknoloji süreçlerini kapsayan yapısı dahilinde, gruplanmış 4 alan (domains) içerisinde toplam 34 süreç ve 318 detaylı kontrol hedefi (detailed control objectives) yer almaktadır.

1) Planlama ve Organize Etme (PO: Plan and Organize)
2) Tedarik ve Uygulama (AI: Acquire and Implement)
3) Hizmet Sunumu ve Destekleme (DS: Deliver and Support)
4) İzleme ve Değerlendirme (ME: Monitor and Evaluate)



Şekil 4.3. COBIT'in Birbirleriyle İlgili Olan 4 Etki Alanı

Bu bölümün alt başlıklarında COBIT 4.1'in dört alanı içerisindeki süreçleri ve kontrol kontrol hedefleri anlatılmıştır.

4.1. Planlama ve Organize Etme (PO)

Bu alan, strateji ve taktikleri kapsar, bilgi teknolojisinin şirket hedeflerine ulaşmasında en iyi katkıyı sağlayan yolun tanımı ile ilgilenir. Organizasyon, teknolojik altyapıyla birlikte uygun bir hedefe yönlendirilmelidir.

Bu alan aşağıdaki yönetim sorularına hitap eder:

- Bilgi teknolojisi stratejisi ve şirket stratejisi örtüşüyor mu?
- Kurum, kaynaklarını ideal şekilde kullanıyor mu?
- Organizasyondaki herkes bilgi teknolojisi hedeflerini anlıyor mu?
- Bilgi teknolojisi riskleri anlaşılıyor ve yönetiliyor mu?
- Bilgi teknolojisi sitemlerinin kalitesi şirket ihtiyaçları için uygun mu?

Planlama ve organize etme (PO) alanı aşağıda sıralanan 10 adet süreçten oluşmaktadır.

PO1: Stratejik BT Planı Tanımlama

PO2: Bilgi Mimarisini Tanımlama

PO3: Teknolojik Yönelimi Belirleme

PO4: BT Süreçlerini, Organizasyonunu ve İlişkilerini Tanımlanması

PO5: BT Yatırımlarının Yönetimi

PO6: Yönetim Hedeflerinin ve Yönelimlerinin İletimi

PO7: BT İnsan Kaynaklarının Yönetimi

PO8: Kalite Yönetimi

PO9: BT Risklerinin Belirlenmesi ve Yönetimi

PO10: Proje Yönetimi

4.1.1. Stratejik BT planı tanımlama (PO1)

BT stratejik planlama, tüm BT kaynaklarını iş stratejisi ve öncelikleriyle birlikte yönetme ve yönlendirme için gereklidir. BT işlevi ve iş paydaşları, hizmet portföyü ve projeden en uygun değeri sağlamakla sorumludurlar. Stratejik plan, iş paydaşlarının BT fırsatlarına ve kısıtlamalarına yaklaşımını, mevcut performansı değerlendirmeyi, kapasite ve insan kaynakları gerekliliklerini saptama ve gerekli yatırım seviyesini belirleme anlayışını geliştirir. Kurumun stratejisi ve öncelikleri portföye yansıtılmalı, hem BT hem de iş tarafı tarafından anlaşılarak kabul edilmiş amaç ve görevlerin açıkça ifade edildiği BT taktik planı ile uygulamaya konulmalıdır.

Stratejik BT planı tanımlama (PO1) süreci aşağıda sıralanan 6 adet detaylı kontrol hedefinden oluşmaktadır.

- BT değer yönetimi (PO1.1)
- İş - BT birlikteliği (PO1.2)
- Mevcut kapasitenin ve performansın değerlendirilmesi (PO1.3)
- Stratejik BT planı (PO1.4)
- BT taktik planları (PO1.5)
- BT portföy yönetimi (PO1.6)

4.1.2. Bilgi mimarisini tanımlama (PO2)

Bilgi sistemleri işlevi kurumun bilgi modelini oluşturur. Kurumun bilgi modeli düzenli olarak güncellenir ve kullanımının optimize edilmesi için uygun sistemleri kullanır. Bilgi mimarisinin oluşturulması, organizasyonun veri sözdizimi (sentaks) kuralları, veri sınıflandırma şemaları, veri sözlüğünün geliştirilmesi gibi aşamaları kapsar. Bu süreç, yönetimin karar alma mekanizmasının kalitesini ve güvenilir bilginin elde edilmesini garanti altına alarak geliştirir ve bilgi sistemleri kaynaklarının uygun bir şekilde iş stratejileri ile eşleşmesini sağlar. Bu BT süreci,

aynı zamanda, bilginin güvenliği ve bütünlüğü için olan sorumluluğu artırmak, varlıklar ve uygulamalar arasındaki bilgi paylaşımının kontrolü ve etkinliğini geliştirmek için gereklidir.

Bilgi mimarisini tanımlama (PO2) süreci aşağıda sıralanan 4 adet detaylı kontrol hedefinden oluşmaktadır.

- Kurumsal bilgi mimarisi modeli (PO2.1)
- Kurumsal veri sözlüğü ve sentaks (söz dizimi) kuralları (PO2.2)
- Veri sınıflandırma şeması (PO2.3)
- Bütünlük yönetimi (PO2.4)

4.1.3. Teknolojik yönelimi belirleme (PO3)

Bilgi teknolojileri işlevi, iş birimlerine destek olmak için teknolojinin yönünü belirler. Bu süreç, teknolojik bir alt yapı planının oluşturulmasını, ürünler ve hizmetler açısından teknolojinin sunabilecekleriyle ilgili beklentileri belirleyecek ve yönetecek bir komisyonun oluşturulmasını gerektirir. Bu durum, bilgi sistemleri yatırımlarına, personel kadrosu oluşturulmasına ve rekabetçi ortamdaki değişikliklere güncel cevaplar verilebilmesini sağlar.

Teknolojik yönelimi belirleme (PO3) süreci aşağıda sıralanan 5 adet detaylı kontrol hedefinden oluşmaktadır.

- Teknolojik yönelimi planlama (PO3.1)
- Teknolojik altyapıyı planlama (PO3.2)
- Gelecek eğilimlerinin ve düzenlemelerin izlenmesi (PO3.3)
- Teknoloji standartları (PO3.4)
- BT mimarisi kurulu (PO3.5)

4.1.4. BT süreçlerinin, organizasyonunun ve ilişkilerinin tanımlanması (PO4)

Bir BT organizasyonu, personel, rol ile sorumluluklar ve denetim için gereksinimler dikkate alınarak tanımlanır. Bütün BT organizasyonu, kalite güvencesi, risk yönetimi, bilgi güvenliği, veri ve sistem sahipliği ile görevler ayrılığı için süreç, politika ve prosedürlerle belirlenmiştir.

BT süreçlerinin, organizasyonunun ve ilişkilerinin tanımlanması (PO4) süreci aşağıda sıralanan 15 adet detaylı kontrol hedefinden oluşmaktadır.

- BT sürecinin çerçevesi (PO4.1)
- BT strateji komitesi (PO4.2)
- BT yönlendirme komitesi (PO4.3)
- BT işlevinin organizasyondaki yeri (PO4.4)
- BT organizasyonel yapısı (PO4.5)
- Sorumluluk ve rollerin belirlenmesi (PO4.6)
- BT kalite güvencesi sağlama sorumluluğu (PO4.7)
- Risk, güvenlik ve uygunluk sorumlulukları (PO4.8)
- Sistem ve veri sahipliği (PO4.9)
- Gözetim (PO4.10)
- Görevler ayrılığı (PO4.11)
- BT ekibi oluşturma (PO4.12)
- Kilit BT personeli (PO4.13)
- Sözleşmeli personelle ilgili politika ve prosedürler (PO4.14)
- Diğer bölümlerle ilişkiler (PO4.15)

4.1.5. BT yatırımlarının yönetimi (PO5)

BT eksenli yatırım programlarını yönetmek için bir çerçeve belirlenmeli ve bunun devamı sağlanmalıdır. Bu çerçeve, önceliklendirme kriterlerini ve bütçe oluşturma sürecini kapsamalıdır. Bu süreç, BT ve iş tarafındakiler arasındaki ortaklığı güçlendirmeli, BT kaynaklarının etkili ve verimli kullanımını sağlamalı ve toplam sahip olma maliyetini düşürmelidir.

BT yatırımlarının yönetimi (PO5) süreci aşağıda sıralanan 5 adet detaylı kontrol hedefinden oluşmaktadır.

- Finansal yönetim çerçevesi (PO5.1)
- BT bütçesinde önceliklendirme (PO5.2)
- BT bütçesi (PO5.3)
- Maliyet yönetimi (PO5.4)
- Fayda yönetimi (PO5.5)

4.1.6. Yönetim hedeflerinin ve yönelimlerinin iletimi (PO6)

Yönetim, kurumsal bir bilgi teknolojileri kontrol çerçevesi geliştirip politikaları tanımlamalı ve kurumun hedeflerinnin açıkça belirtildiği bir iletişim programı uygulamaya konulmalıdır.

Yönetim hedeflerinin ve yönelimlerinin iletimi (PO6) süreci aşağıda sıralanan 5 adet detaylı kontrol hedefinden oluşmaktadır.

- BT politikaları ve kontrol ortamı (PO6.1)
- Kurumsal BT riskleri ve kontrol çerçevesi (PO6.2)
- Kurumsal BT riskleri ve kontrol çerçevesi (PO6.3)
- Politika, standart ve prosedürlerin açıklanması (PO6.4)
- BT hedeflerinin ve yönelimlerinin anlatılması (PO6.5)

4.1.7. BT insan kaynaklarının yönetimi (PO7)

BT hizmetlerinin oluşturulması ve sunulması için yeterli bir işgücü ve bunun sürekliliği sağlanmalıdır. Bu süreç, işe alım, eğitim, performans değerlendirmesi, görevde yükselme, işe son verme gibi alt süreçlerden oluşur. BT insan kaynakları yönetimi süreci son derece önemli bir süreçtir çünkü insanlar en önemli BT varlıklarıdır.

BT insan kaynaklarının yönetimi (PO7) süreci aşağıda sıralanan 8 adet detaylı kontrol hedefinden oluşmaktadır.

- Personel alımı ve muhafazası (PO7.1)
- Personel yeteneklerinin gelişimi (PO7.2)
- Rollerin personele dağıtılması (PO7.3)
- Personel eğitimi (PO7.4)
- Kişilere bağımlılığının azaltılması (PO7.5)
- Personel uygunluk prosedürleri (PO7.6)
- Çalışanın iş performansının değerlendirilmesi (PO7.7)
- İş değiştirme ve sonlandırma (PO7.8)

4.1.8. Kalite yönetimi (PO8)

Standartlar içeren bir kalite yönetimi sistemi geliştirilir ve bunun devamı sağlanır. Kalite Yönetimi, BT'nin iş tarafına katkı sağlaması ve sürekli iyileştirme çalışmaları için önemlidir.

Kalite yönetimi (PO8) süreci aşağıda sıralanan 6 adet detaylı kontrol hedefinden oluşmaktadır.

- Kalite yönetimi sistemi (PO8.1)
- BT standartları ve kalite uygulamaları (PO8.2)
- Geliştirme ve temin standartları (PO8.3)
- Müşteri odaklılık (PO8.4)
- Sürekli iyileştirme (PO8.5)
- Kalite ölçümü, izlemesi ve gözden geçirilmesi (PO8.6)

4.1.9. BT risklerinin değerlendirilmesi ve yönetimi (PO9)

Bir risk yönetimi çerçevesi belirlenip bunun sürdürülmesi sağlanır. Bu çerçeve, kurumun kabul ettiği, azaltmayı hedeflediği ve kalıcı olduğunu düşünerek üstlendiği risklerin neler olduğunu gösterir.

BT risklerinin değerlendirilmesi ve yönetimi (PO9) süreci aşağıda sıralanan 6 adet detaylı kontrol hedefinden oluşmaktadır.

- BT risk yönetimi çerçevesi (PO9.1)
- Risk içeriğinin oluşturulması (PO9.2)
- Olay tanımlama (PO9.3)
- Risk değerlendirme (PO9.4)
- Risk cevaplama (PO9.5)
- Risk eylem planının bakımı ve izlenmesi (PO9.6)

4.1.10. Proje yönetimi (PO10)

Bütün BT projelerinin yönetimi için bir proje yönetimi çerçevesi belirlenir. Çerçeve, bütün projelerin önceliklendirilmesini ve işbirliği içinde hareket etmesini sağlar. Bu

çerçeve, bir ana plan dahilinde, kaynakların belirlenmesi, başarı tanımı, kullanıcı onayları, kalite güvencesi, proje risk yönetimi, test planları gibi sistematik bir yapıyı içerir.

Proje yönetimi (PO10) süreci aşağıda sıralanan 14 adet detaylı kontrol hedefinden oluşmaktadır.

- Program yönetimi çerçevesi (PO10.1)
- Proje yönetimi çerçevesi (PO10.2)
- Proje yönetimi yaklaşımı (PO10.3)
- Paydaşların onayı (PO10.4)
- Proje kapsamı belirleme (PO10.5)
- Proje safhalarını başlatma (PO10.6)
- Bütünleşik proje planı (PO10.7)
- Projenin kaynakları (PO10.8)
- Proje risk yönetimi (PO10.9)
- Proje kalite planı (PO10.10)
- Proje değişiklik kontrolü (PO10.11)
- Güvence işlemleri için proje planlama (PO10.12)
- Proje performansının ölçülmesi, raporlanması ve izlenmesi (PO10.13)
- Proje kapanışı (PO10.14)

4.2. Tedarik ve Uygulama (AI)

Bilgi teknolojileri stratejisini gerçekleştirebilmek için bilgi teknolojilerinin tanımlanmasına, geliştirilmesine ve edinilmesine ihtiyaç vardır. Ayrıca varolan sistemlerin korunması ve değiştirilmesi konuları da bu alana dahildir.

Bu alan aşağıdaki yönetim sorularına hitap eder:

• Yeni projelerin, iş ihtiyaçlarını karşılayacak çözümler ortaya koyma olasılığı var mıdır?
• Yeni projelerin bütçe dahilinde zamanında ortaya konulma olasılığı var mıdır?
• Yeni sistemler uygulandığında uygun şekilde işleyecek mi?
• Güncel iş uygulamalarını başarısızlığa uğratmadan yeni değişimler yapılabilecek mi?

Tedarik ve uygulama (AI) alanı aşağıda sıralanan 7 adet süreçten oluşur.

AI1: Rutin Çözümlerin Tanımlanması
AI2: Uygulama Yazılımlarının Temini ve Bakımı
AI3: Teknoloji Altyapısının Temini ve Bakımı
AI4: İşletim ve kullanıma İzin Verme
AI5: BT Kaynaklarının Temini
AI6: Değişiklik Yönetimi
AI7: Çözüm ve Değişikliklerin Kurulması ve Kabul Edilmesi

4.2.1. Rutin çözümlerin tanımlanması (AI1)

İş gereksinimlerinin etkili ve yeterli bir yaklaşımla karşılanmasını sağlamak için, satın alma öncesinde satın alınmak istenen işleve olan ihtiyacın analiz edilmesi gereklidir. Bu süreç, ihtiyaçların tanımının yapılmasını, alternatif kaynakların araştırılmasını, ihtiyacın teknolojik ve ekonomik olarak uygulanabilirliğini, risk analizi ve maliyet - fayda analizlerinin gerçekleştirilmesini sağlar.

Rutin çözümlerin tanımlanması (AI1) süreci aşağıda sıralanan 4 adet detaylı kontrol hedefinden oluşmaktadır.

- İş fonksiyonlarının tanımlanması, bakımı ve teknik gereksinimler (AI1.1)
- Risk analiz raporu (AI1.2)
- Verimlilik öğretisi ve alternatif yolların formüle edilmesi (AI1.3)
- İhtiyaçlar, fizibilite kararı ve onayı (AI1.4)

4.2.2. Uygulama yazılımlarının temini ve bakımı (AI2)

Uygulamalar iş gereksinimleri ile uyumlu şekilde yapılır. Bu süreç, uygulamaların tasarımını, uygulama kontrolleri ile güvenlik gereksinimlerinin uygun olarak sürece katılımını ve standartlarla uyumlu geliştirme ve konfigürasyonu kapsar.

Uygulama yazılımlarının temini ve bakımı (AI2) süreci aşağıda sıralanan 10 adet detaylı kontrol hedefinden oluşmaktadır.

- Üst düzey tasarım (AI2.1)
- Detaylı tasarım (AI2.2)

- Uygulama kontrolü ve denetlenebilirlik (AI2.3)
- Uygulama güvenliği ve kullanılabilirlik (AI2.4)
- Sağlanan uygulamanın konfigürasyonu ve kurulumu (AI2.5)
- Mevcut sistemde ana güncellemeler (AI2.6)
- Uygulama yazılımı geliştirme (AI2.7)
- Yazılım kalite güvencesi (AI2.8)
- Uygulama gereksinim yönetimi (AI2.9)
- Uygulama yazılımının bakımı(AI2.10)

4.2.3. Teknoloji altyapısının temini ve bakımı (AI3)

Organizasyonlar, teknolojik altyapının tedariki, uygulanması ve güncellenmesi için süreçlere sahiptirler. Bu süreçler, teknoloji stratejileri ile geliştirme ve test ortamlarıyla örtüşecek şekilde, altyapının tedariki, bakımı ve korunması için planlı bir yaklaşım gerektirir. Bu durum da, kurum uygulamaları için sürekli bir teknolojik destek ihtiyacını doğurur.

Teknoloji altyapısının temini ve bakımı (AI3) süreci aşağıda sıralanan 4 adet detaylı kontrol hedefinden oluşmaktadır.

- Teknolojik altyapı tedarik planı (AI3.1)
- Altyapı kaynak korunması ve kullanılabilirliği (AI3.2)
- Altyapı bakımı (AI3.3)
- Fizibilite test ortamı (AI3.4)

4.2.4. İş ve kullanımın etkin kılınması (AI4)

Organizasyonun tüm kaynaklarının iş gereksinimlerini karşılayacak şekilde verimlilik esasına göre kullanılması amaçlanmalıdır. Bu süreç, iş tarafı ve BT için sistematik hale gelmiş dokümantasyonu gerektirir ve altyapının doğru kullanımıyla işletilmesi için alıştırmalar sağlar.

Teknoloji altyapısının temini ve bakımı (AI4) süreci aşağıda sıralanan 4 adet detaylı kontrol hedefinden oluşmaktadır.

- Operasyonel çözümler için planlama (AI4.1)
- Kurum yönetimine bilgi aktarımı (AI4.2)

- Son kullanıcılara bilgi aktarımı (AI4.3)
- Operasyon ve destek personeline bilgi aktarımı (AI4.4)

4.2.5. BT kaynaklarının sağlanması (AI5)

Bilgi teknolojileri sistemlerinin sürekliliği için insan, donanım, yazılım ve hizmetler dahil tüm BT kaynaklarının sağlanmasına ihtiyaç duyulur. Bu durum, tedarik prosedürlerinin yazılmasını, tedarikçi seçiminin yapılmasını, yazılı kontrat düzenlenmelerinin tanımlanması ve uygulanması gibi süreçlerin yapılmasını gerektirir.

BT kaynaklarının sağlanması (AI5) süreci aşağıda sıralanan 4 adet detaylı kontrol hedefinden oluşmaktadır.

- Tedarikçi kontrolü (AI5.1)
- Tedarikçi kontrat yönetimi (AI5.2)
- Tedarikçi seçimi (AI5.3)
- BT kaynaklarının tedarik edilmesi (AI5.4)

4.2.6. Değişiklik yönetimi (AI6)

Bilgi teknolojileri sistemlerinde üretim ortamı içerisinde, altyapı ve uygulamalar ile ilgili tüm değişiklikler, kontrol edilebilir şekilde resmi olarak yönetilir. Değişiklikler, prosedürlere, süreçlere, sistem ve hizmet parametrelerine yapılanlar dahil olmak üzere kayıt altına alınır, değerlendirilir ve uygulamadan önce yetkilendirilerek uygulama sonucunda planlanmış çıktılara karşı değerlendirilir. Bu sürecin doğru işletilmesi, üretim ortamının bütünlüğünü olumsuz yönde etkileyen riskleri azaltmayı garanti eder.

Değişiklik yönetimi (AI6) süreci aşağıda sıralanan 5 adet detaylı kontrol hedefinden oluşmaktadır.

- Değişiklik yönetimi standartları ve prosedürleri (AI6.1)
- Etki değerlendirmesi, önceliklendirme ve yetkilendirme (AI6.2)
- Acil değişiklikler (AI6.3)
- Değişikliklerin takip edilmesi ve raporlanması (AI6.4)
- Değişikliklerin sonlanması ve dokümantasyonu (AI6.5)

4.2.7. Çözüm ve değişikliklerin kurulması ve kabul edilmesi (AI7)

Bilgi teknolojileri sistemlerinde geliştirme çalışmaları tamamlandıktan sonra yeni sistemlerin production (üretim) ortamına atılarak operasyonel hale getirilmesi gerekir. Bu süreç, geliştirme çalışmalarının ilişkili test verileriyle tahsis edilen ortamlarda tam olarak test edilmesini, üretim ve yayılma talimatlarının tanımlanması gibi gereklilikleri içerir. Bu sürecin doğru işletilmesi, operasyonel sistemlerin üzerinde anlaşılmış beklentilerle çıktıların uyumlu olmasını garanti eder.

Çözüm ve değişikliklerin kurulması ve kabul edilmesi (AI7) süreci aşağıda sıralanan 9 adet detaylı kontrol hedefinden oluşmaktadır.

- Eğitim (AI7.1)
- Test planı (AI7.2)
- Uygulama planı (AI7.3)
- Test ortamı (AI7.4)
- Sistem ve veri dönüşümü (AI7.5)
- Değişikliklerin test edilmesi (AI7.6)
- Son kabul testi (AI7.7)
- Üretim teşviki (AI7.8)
- Ön uygulama değerlendirmesi (AI7.9)

4.3. Hizmet Sunumu ve Destek (DS)

BT'nin teslimat durumlarına odaklanır. Bu alan, hizmet sunumu, güvenlik ve devamlılığın yönetimi, kullanıcılar için servis desteği ve veri yönetimini içeren gerekli hizmetlerin ortaya konulmasıyla ilgilenir. Uygulamaların BT sistemi içinde yürütülmesi ve sonuçlarıyla olduğu kadar, BT sistemlerinin etkili işletilmesine olanak sağlayan destek süreçlerini de kapsar.

Bu alan aşağıdaki yönetim sorularına hitap eder:

• Bilgi teknolojisi hizmetleri iş öncelikleri ile uyumlu ortaya konulabilir mi?
• Bilgi teknolojisi harcamaları optimize edilebilir mi?
• İş gücü, bilgi teknolojisi sistemlerini verimli ve güvenli bir şekilde kullanabilir mi?

• Bilgi güvenliği için hali hazırda yeterli gizlilik, bütünlük ve elverişlilik var mı?

Hizmet sunumu ve destek (DS) alanı aşağıda sıralanan 13 adet süreçten oluşur.

DS1: Hizmet Seviyelerinin Belirlenmesi ve Yönetimi
DS2: Üçüncü Parti Hizmet Yönetimi
DS3: Performans ve Kapasite Yönetimi
DS4: Sürekli Hizmetin Sağlanması
DS5: Sistem Güvenliğinin Sağlanması
DS6: Maliyetlerin Belirlenmesi ve Bütçelenmesi
DS7: Kullanıcı Eğitimi
DS8: Kullanıcılara Yardım ve Danışmanlık
DS9: Konfigürasyon Yönetimi
DS10: Problem Yönetimi
DS11: Veri Yönetimi
DS12: Fiziksel Ortam Yönetimi
DS13: Operasyonların YönetimiBelirleme ve Yönetimi

4.3.1. Hizmet seviyelerinin belirlenmesi ve yönetimi (DS1)

Bilgi teknolojileri ile iş tarafı arasındaki iletişim, dokümante edilmiş hizmet seviyeleriyle sağlanır. Bu süreç, hizmet seviyelerinin izlenmesi, hizmet seviyelerinin başarısının raporlanması gibi alt süreçleri kapsar.
Hizmet seviyelerinin belirlenmesi ve yönetimi (DS1) süreci aşağıda sıralanan 6 adet detaylı kontrol hedefinden oluşmaktadır.

- Hizmet düzeyi yönetimi çerçevesi (DS1.1)
- Hizmetlerin tanımı (DS1.2)
- Hizmet seviyesi anlaşmaları (DS1.3)
- Operasyonel seviyedeki anlaşmalar (DS1.4)
- Hizmet düzeyi işlemlerinin raporlanması ve izlenmesi (DS1.5)
- Hizmet düzeyi anlaşmaları ve kontratlarının gözden geçirilmesi (DS1.6)

4.3.2. Üçüncü parti hizmet yönetimi (DS2)

Üçüncü parti (sağlayıcılar, üreticiler ve iş ortakları) tarafından sağlanan hizmetlerin iş gereksinimlerine uyduğundan emin olmak için etkin bir üçüncü parti yönetim süreci gereklidir. Bu süreç, üçüncü parti anlaşmalarındaki rollerin, sorumlulukların ve beklentilerin açıkça belirlenmesiyle gerçekleştirilir. Üçüncü parti hizmetlerin etkinlik ve uygunluk bakımından izlenmesi ve değerlendirilmesi gerekir. Üçüncü parti hizmetlerin etkin yönetimi, gerektiği gibi çalışmayan sağlayıcılar tarafından kaynaklanan riski minimize eder.

Üçüncü parti hizmet yönetimi (DS2) süreci aşağıda sıralanan 4 adet detaylı kontrol hedefinden oluşmaktadır.

- Tüm tedarikçi ilişkilerinin belirlenmesi (DS2.1)
- Tedarikçi ilişkileri yönetimi (DS2.2)
- Tedarikçiler risk yönetimi (DS2.3)
- Tedarikçi performans izlemesi (DS2.4)

4.3.3. Performans ve kapasite yönetimi (DS3)

BT kaynaklarının performans ve kapasitelerinin yönetilmesi ihtiyacı, varolan performans ve kapasitelerinin periyodik olarak değerlendirilmesi sürecini gerektirir. Bu süreç, iş yükü, depolama ve acil durum gereksinimlerini temel alan gelecek ihtiyaçları öngörmeyi de kapsar.

Performans ve kapasite yönetimi (DS3) süreci aşağıda sıralanan 5 adet detaylı kontrol hedefinden oluşmaktadır.

- Performans ve kapasite planlaması (DS3.1)
- Mevcut performans ve kapasite (DS3.2)
- Beklenen performans ve kapasite (DS3.3)
- BT kaynaklarının kullanılabilirliği (DS3.4)
- İzleme ve raporlama (DS3.5)

4.3.4. Sürekli hizmetin sağlanması (DS4)

Sürekli bilgi teknolojisi hizmetlerinin sağlanması ihtiyacı, periyodik devamlılık eğitimi, alan dışı yedek bellek kullanımı, bilgi teknolojisi devamlılık planlarının test edilmesi, korunması ve geliştirilmesini gerektirir. Etkili devamlı bir hizmet süreci, kilit iş fonksiyonlarında ve işlemlerinde temel bilgi teknolojisi hizmetinin kesilmesinin etkisini ve olasılığını azaltır.

Sürekli hizmetin sağlanması (DS4) süreci aşağıda sıralanan 10 adet detaylı kontrol hedefinden oluşmaktadır.

- Bilgi teknolojisi devamlılık yapısı (DS4.1)
- Bilgi teknolojisi devamlılık planları (DS4.2)
- Kritik bilgi teknolojisi kaynakları (DS4.3)
- Bilgi teknolojisi devamlılık planının korunması (DS4.4)
- Bilgi teknolojisi devamlılık planının test edilmesi (DS4.5)
- Bilgi teknolojisi devamlılık planı eğitimi (DS4.6)
- Bilgi teknolojisi devamlılık planının dağıtımı (DS4.7)
- Bilgi teknolojisi hizmetlerinin onarımı ve devam etmesi (DS4.8)
- Yerleşke dışı yedekleme (DS4.9)
- Devam etme sonrasında gözden geçirme (DS4.10)

4.3.5. Sistem güvenliğinin sağlanması (DS5)

Bilginin bütünlüğünü ve niteliklerini koruma ihtiyacı bir güvenlik yönetimi sürecini gerektirir. Bu süreç, bilgi teknolojisi güvenlik rollerini ve sorumluluklarını, politikalarını, standartlarını ve prosedürlerini oluşturmayı ve korumayı içerir. Etkili güvenlik yönetimi, şirketin güvenlik açıkları ve olaylar üzerindeki etkisini azaltmak için bütün bilgi teknolojisi varlıklarını korur.

Sistem güvenliğinin sağlanması (DS5) süreci aşağıda sıralanan 11 adet detaylı kontrol hedefinden oluşmaktadır.

- Bilgi teknolojisi güvenliğinin yönetimi (DS5.1)
- Bilgi teknolojisi güvenlik planı (DS5.2)
- Kimlik yönetimi (DS5.3)
- Kullanıcı hesap yönetimi (DS5.4)

- Güvenlik testi, güvenliğin gözaltında tutulması ve izlenmesi (DS5.5)
- Güvenlik olay tanımı (DS5.6)
- Güvenlik teknolojisinin korunması (DS5.7)
- Şifreleme ile ilgili anahtar yönetimi (DS5.8)
- Kötü niyetli yazılımın önlenmesi, tespiti ve düzeltilmesi (DS5.9)
- Ağ güvenliği (DS5.10)
- Hassas verinin değişimi (DS5.11)

4.3.6. Maliyetlerin hesaplanması ve paylaştırılması (DS6)

Bilgi teknolojisi maliyetlerinin kuruma adil ve eşit bir sistemle tahsis edilmesi ihtiyacı, bilgi teknolojisi maliyetlerinin eksiksiz değerlendirilmesini ve adil bir dağıtım üzerinde iş tarafındaki kullanıcıların anlaşmasını gerektirir. Adil bir paylaşım sistemi, şirketin bilgi teknolojisi hizmetlerinin kullanımını göz önüne alarak daha bilgili kararlar vermesini sağlar.

Maliyetlerin hesaplanması ve paylaştırılması (DS6) süreci aşağıda sıralanan 4 adet detaylı kontrol hedefinden oluşmaktadır.

- Hizmetlerin tanımı (DS6.1)
- BT muhasebesi (DS6.2)
- Maliyet modelleme ve maliyetlendirme (DS6.3)
- Maliyet modelinin bakımı (DS6.4)

4.3.7. Kullanıcı eğitimleri (DS7)

BT sistemlerindeki tüm kullanıcıların etkili eğitimi için BT bünyesindeki her kullanıcı grubunun eğitim ihtiyaçlarını tespit etmek gerekir. Tespit edilen ihtiyaçlara ek olarak bu süreç, etkili bir eğitim ve sonuçları ölçmek için strateji tanımlamayı ve bu stratejiyi uygulamayı içerir. Etkili bir eğitim programı, kullanıcı hatalarını azaltarak, verimliliği artırarak, kullanıcı güvenlik önlemleri gibi önemli kilit kontrollerle uyumu artırarak teknolojinin etkili kullanımını artırır.

Kullanıcı eğitimleri (DS7) süreci aşağıda sıralanan 3 adet detaylı kontrol hedefinden oluşmaktadır.

- Eğitim ihtiyaçlarının tanımlanması (DS7.1)
- Eğitimin sağlanması (DS7.2)
- Alınan eğitimin değerlendirilmesi (DS7.3)

4.3.8. Olay ve servis masası yönetimi (DS8)

Bilgi teknolojileri, kullanıcı soru ve problemlerine uygun ve etkili cevap, iyi düzenlenmiş ve iyi yönetilmiş hizmet yardımı ve danışmanlık yönetimi sürecini gerektirir. Kullanıcı sorularının hızlı çözümü sayesinde kurumda verimlilik artışı gerçekleşir. Buna ek olarak, şirket etkili raporlama sayesinde temel nedenlere (zayıf kullanıcı eğitimi, yetkin olmayan personel vb.) erişebilir.

Olay ve servis masası yönetimi (DS8) süreci aşağıda sıralanan 5 adet detaylı kontrol hedefinden oluşmaktadır.

- Servis masası (DS8.1)
- Müşteri sorunlarının kaydedilmesi (DS8.2)
- Olayın ilgiliye yönlendirilmesi (DS8.3)
- Olaya son verme (DS8.4)
- Raporlama ve trend analizi (DS8.5)

4.3.9. Konfigürasyon yönetimi (DS9)

Yazılım ve donanım konfigürasyonlarının bütünlüğünün sağlanması, eksiksiz ve hatasız bir konfigürasyon havuzu oluşturulmasını ve bunun sürdürülmesini gerektirir. Bu süreç, temel konfigürasyon bilgisinin toplanmasını, ana hatların belirlenmesini, konfigürasyon bilgisinin doğrulanmasını ve denetlenmesini ve gerektiğinde konfigürasyon havuzunun güncellenmesini içerir. Etkili konfigürasyon yönetimi, daha büyük sistemlere sahip olmayı, üretim sorunlarını azaltmayı ve sorunları daha hızlı bir şekilde çözmeyi olanaklı kılar.

Konfigürasyon yönetimi (DS9) süreci aşağıda sıralanan 3 adet detaylı kontrol hedefinden oluşmaktadır.

- Konfigürasyon havuzu (DS9.1)
- Konfigürasyon unsurlarının tanımlanması ve bakımı (DS9.2)
- Konfigürasyon bütünlüğünün gözden geçirilmesi (DS9.3)

4.3.10. Problem yönetimi (DS10)

Etkili problem yönetimi, problemlerin belirlenmesi ve sınıflandırılmasını, kök - neden analizini ve problemlerin çözümünü gerektirir. Ayrıca, problem yönetimi süreci, gelişim için tavsiyelerin formule edilmesini, problem kayıtlarının bakımını ve düzeltici eylemlerin durumlarının gözden geçirilmesini içerir. Etkili bir problem yönetimi süreci işletim sisteminin kullanılırlığını maksimize eder, hizmet seviyesini yükseltir, maliyetleri azaltır ve müşteri rahatlığını ve memnuniyetini arttırır.

Problem yönetimi (DS10) süreci aşağıda sıralanan 4 adet detaylı kontrol hedefinden oluşmaktadır.

- Problemlerin belirlenmesi ve sınıflandırılması (DS10.1)
- Problem izleme ve çözümleme (DS10.2)
- Problemi sona erdirme (DS10.3)
- Konfigürasyon, olay ve problem yönetimi ile entegrasyon (DS10.4)

4.3.11. Veri yönetimi (DS11)

Etkin veri yönetimi, veri gereksinimlerini belirlemeyi gerektirir. Veri yönetimi süreci, medya kütüphanesi, verinin yedeklenmesi, verinin kurtarılması ve medyanın düzgün şekilde imhası gibi işlemleri yönetmek için etkin prosedürlerin oluşturulmasını içerir. Etkin veri yönetimi, kurum verilerinin kaliteli, güncel ve kullanılabilir olmasını sağlar.

Problem yönetimi (DS10) süreci aşağıda sıralanan 6 adet detaylı kontrol hedefinden oluşmaktadır.

- Veri yönetimi için iş gereksinimleri (DS11.1)
- Depolama ve tutma düzenlemeleri (DS11.2)
- Medya kütüphanesi yönetimi sistemi (DS11.3)
- İmha işlemleri (DS11.4)
- Yedekleme ve kurtarma (DS11.5)
- Veri yönetimi için güvenlik gereksinimleri (DS11.6)

4.3.12. Fiziksel ortam yönetimi (DS12)

Fiziksel ortamın yönetimi süreci, fiziksel alan gerekliliklerinin tanımlanması, uygun araç gereçlerin seçimi, çevresel faktörlerin izlenmesi ve fiziksel erişimin yönetimi için etkin işlevlerin tasarımı aşamalarını içerir. Fiziksel çevrenin etkin yönetimi, bilgisayar donanımı ve personele gelen hasardan kaynaklı kurum zararlarını azaltır.

Fiziksel ortam yönetimi (DS12) süreci aşağıda sıralanan 5 adet detaylı kontrol hedefinden oluşmaktadır.

- Yer seçimi ve planı (DS12.1)
- Fiziksel güvenlik kriterleri (DS12.2)
- Fiziksel erişim (DS12.3)
- Çevresel etkenlere karşı koruma (DS12.4)
- Fiziksel araçların yönetimi (DS12.5)

4.3.13. Operasyonların yönetimi (DS13)

Verilerin tam ve eksiksiz olarak işlenmesi, veri işleme prosedürlerinin etkin yönetimini ve donanımların özverili şekilde bakımını gerektirir. Bu süreç, planlanan işlemlerin etkin yönetimi, hassas çıktıların korunması, altyapı performansının izlenmesi ve donanımın önleyici bakımının sağlanması için gereken operasyonel politika ve prosedürlerin tanımlanmasını içerir. Etkin operasyonel yönetim, veri bütünlüğünün sağlanmasına, iş süreçlerindeki gecikmelerin ve BT maliyetlerinin azalmasına yardımcı olur.

Operasyonların yönetimi (DS13) süreci aşağıda sıralanan 5 adet detaylı kontrol hedefinden oluşmaktadır.

- Operasyonel prosedürler ve talimatlar (DS13.1)
- İş planlaması (DS13.2)
- BT altyapısının izlenmesi (DS13.3)
- Hassas belgeler ve çıkış aygıtları (DS13.4)
- Donanım için önleyici bakımlar (DS13.5)

4.4. İzleme ve değerlendirme (ME)

Kurum ihtiyaçlarının tayin edilmesiyle ilgili kurum stratejilerinin belirlenmesi ve mevcut BT sisteminin tasarlanırken niyetlenildiği ihtiyaçları karşılayıp karşılamadığı ile ilgilenir. Bilgi teknolojisi işlemleri kalitelerinin zaman içerisinde düzenli bir şekilde değerlendirilmeye ihtiyacı vardır. İzleme ve değerlendirme alanı performans yönetimi, iç kontrolün izlenmesi, mevzuat uyumu ve yönetimle ilgilenir.

Bu alan aşağıdaki yönetim sorularına hitap eder:

• Problemleri çok geç olmadan tespit edebilmek için bilgi teknolojisinin performansı değerlendiriliyor mu?
• Yönetim, iç kontrolün etkili ve verimli olmasını sağlayabiliyor mu?
• Bilgi teknolojisi performansı, geçmişteki şirket hedefleri ile ilişkilendirilebilir mi?
• Bilgi güvenliği için hali hazırda yeterli gizlilik, bütünlük ve elverişlilik var mı?

İzleme ve değerlendirme (ME) alanı aşağıda sıralanan 4 adet süreçten oluşur.

ME1: Süreç İzleme
ME2: İç Kontrol Değerlendirme Yeterliliği
ME3: Bağımsız Güvence Elde Edilmesi
ME4: Bağımsız Denetimin Sağlanması

4.4.1. Bilgi teknolojileri performansını izleme ve değerlendirme (ME1)

Etkili bir BT performans yönetimi için gözlem süreci gerekmektedir. Bu süreç, uygun performans göstergelerinin tanımını, performansın sistematik ve zamanında raporlanmasını ve ihlallere karşı acil tedbir alınmasını içermektedir. Gözlem, doğru şeylerin yapıldığından ve yapılan bu şeylerin talimat ve politikalara uygun olduğundan emin olunabilmesi için gerekmektedir.

Bilgi teknolojileri performansını izleme ve değerlendirme (ME1) süreci aşağıda sıralanan 6 adet detaylı kontrol hedefinden oluşmaktadır.

- İzleme yaklaşımı (ME1.1)
- İzlenecek verinin tanımlanması ve toplanması (ME1.2)
- İzleme metodu (ME1.3)

- Performans değerlendirmesi (ME1.4)
- Üst yönetime raporlama (ME1.5)
- İyileştirici faaliyetler (ME1.6)

4.4.2. İç denetimin izlenmesi ve değerlendirilmesi (ME2)

BT için etkili bir iç denetim programının kurulması, iyi tanımlanmış bir gözlem sürecini gerektirmektedir. Bu süreç, kontrol beklentilerinin izlenmesi ve raporlanmasını, öz değerlendirmelerin sonuçlarını ve üçüncü kişi gözlemlerini içermektedir. İç denetim izlemesinin en temel faydası, etkili ve verimli işlemler ile uygulanabilir yasalara ve düzenlemelere uyum konusunda güvence sağlamaktır.

İç denetimin izlenmesi ve değerlendirilmesi (ME2) süreci aşağıda sıralanan 7 adet detaylı kontrol hedefinden oluşmaktadır.

- İç denetim çerçevesinin izlenmesi (ME2.1)
- Denetim revizyonu (ME2.2)
- Kural dışı durumların denetlenmesi (ME2.3)
- Denetimin öz değerlendirmesi (ME2.4)
- İç denetimin güvence altına alınması (ME2.5)
- Üçüncü kişilerden (dışarıdan) sağlanan iç denetim (ME2.6)
- Çözüm eylemleri (ME2.7)

4.4.3. Dış gereksinimlere uyumluluğun sağlanması (ME3)

Yasa, yönetmelik ve sözleşme gereklilikleriyle uyumun sağlanması için etkin bir gözetim süreci gerekmektedir. Bu süreç, uyumluluğun gereksinimlerinin tespit edilmesi, çözümün değerlendirilmesi ve optimizasyonu, gereksinimlerin yerine getirildiğine dair güvence sağlanması ve bilgi teknolojileri uyumluluk raporunun işletmenin geri kalan kısmıyla entegrasyonu aşamalarını içermektedir.

Dış gereksinimlere uyumluluğun sağlanması (ME3) süreci aşağıda sıralanan 5 adet detaylı kontrol hedefinden oluşmaktadır.

- Hukuki, düzenleyici ya da anlaşmalara dayanan dış zorunlulukların tanımlanması (ME3.1)

- Dış gereksinimlere verilen cevabın optimize edilmesi (ME3.2)
- Dış gereksinimlerle uyumluluğun değerlendirilmesi (ME3.3)
- Uyumluluğun olumlu biçimde sağlanması (ME3.4)
- Tümleşik raporlama (ME3.5)

4.4.4. BT yönetiminin sağlanması (ME4)

Etkili bir yönetim çerçevesinin kurulması, kurumsal yapıların, süreçlerin, liderliklerin, rollerin ve sorumlulukların tanımlanmasını ve BT yatırımlarının işletmenin hedef ve stratejileriyle uyumunu içermektedir.

Dış gereksinimlere uyumluluğun sağlanması (ME3) süreci aşağıda sıralanan 7 adet detaylı kontrol hedefinden oluşmaktadır.

- BT yönetimi çerçevesinin oluşturulması (ME4.1)
- Stratejik düzenleme (ME4.2)
- Değer yaratma (ME4.3)
- Kaynak yönetimi (ME4.4)
- Risk yönetimi (ME4.5)
- Performans ölçümü (ME4.6)
- Bağımsız denetim (ME4.7)

5. TÜRKİYE'DEKİ BİR BANKADA TEKNOLOJİ RİSKİ YÖNETİMİ ÜZERİNE UYGULAMA

Bu bölümde Türkiye'de bankacılık sektöründe faaliyette bulunan büyük ölçekli bir bankanın COBIT standartlarına uygun bir şekilde teknoloji riski yönetimi süreci kapsamında risklerinin belirlenip, değerlendirilerek takip edildiği sürecin aşamalarının önemli bir kısmının nasıl oluşturulduğu basit bir uygulama üzerinde gösterilecektir.

Bankadan elde edilebilen verilerin kısıtlı olması ve bu büyüklükteki bir finans kurumunun bilgi sistemlerinin karmaşıklığı göz önüne alındığında bilgi teknolojileri risk yönetimi süreci temel anlamda incelenecektir.

5.1. Bankanın Teknoloji Riski Yönetimi Süreci

Çalışmamızı gerçekleştirdiğimiz bankanın teknoloji riski yönetimi süreci aşağıdaki aşamalardan oluşmaktadır.

- Sürecin amacının ve kapsamının belirlenmesi
- Sürecin sahibinin belirlenmesi
- Sürecin sorumlularının belirlenmesi
- Sürecin akışının belirlenmesi
- Teknoloji varlık risk analizlerinin yapılması ve değerlendirilmesi
- Risk işleme yönteminin seçilmesi
- Riskin takip edilmesi

5.1.1. Sürecin amacı ve kapsamı

Banka'da bilgi teknolojileri sistemleriyle servis ve süreçlerin risk analizlerini gerçekleştirmek ve maliyet etkin risk engelleme kontrollerinin gerçekleştirilmesini sağlamak amaçlanmaktadır.

Teknoloji riski yönetimi süreci bilgi teknolojileri sistemleri süreçlerini kapsamaktadır. Bu kapsam dahilinde,

- Bilgi teknolojileri ile ilgili risk yönetimi metodolojisi, sınırları, risklerden kaçınma ve kalan risklerin hesaplanma yöntemleri tanımlanır.
- Planlanmamış, beklenmeyen olayların iş hedefleri üzerinde yarattığı potansiyel etkileri tanımlanır, analiz edilir ve değerlendirilir.
- Risk azaltma stratejileri ile kalan riskler minimize edilerek kabul edilebilir sınırlar içinde kalması sağlanır.
- Değerlendirme sonuçlarının tüm paydaşlar ile paylaşılıp kabul edilebilir olması sağlanır.

5.1.2. Süreç sahibi

Sürecin hazırlanmasından ve düzenlenmesinden bankanın bilgi güvenlik birimi sorumludur. Fakat sonrasındaki tüm aşamalarda bankanın her çalışanı sürecin bir parçasıdır.

5.1.3. Süreç sorumluları

Süreçte tanımlanan işlerin gerçekleştirilmesinden bilgi güvenlik birimi koordinasyonunda bankanın ilgili tüm birimleri sorumludur. Teknoloji varlıklarıyla ilgili risklerin analiz edilmesi ve işlenmesinden bankanın bilgi sistemleri birimindeki riskin teknik sahipleri sorumludur.

5.1.4. Süreç akışı

Bilgi teknolojilerinde risk yönetimi operasyonel risk kapsamında ele alınmaktadır. Bankanın operasyonel risk çerçevesi ile aynı doğrultuda bir teknoloji varlık risk envanteri oluşturulması gerekmektedir.

Bankada teknoloji varlık risk envanteri aşağıdaki sıraya göre hazırlanmaktadır.

• Her bir risk için riskin hem teknik sahibi hem de iş sahibi belirlenir. Risk sahipleri risk analizlerinde değerlerin atanmasından, mevcut kontrollerin ve risk gerçekleşmesi durumunda alınacak aksiyon bilgileri gibi bilgilerin girilmesi ve güncel tutulmasından sorumludur.

• Teknoloji risklerinin bankada tutarlı bir şekilde analiz ve değerlendirilmesi için risk hesaplama araçları olan teknoloji riski olabilirlik skalası, teknoloji riski etki skalası ile teknoloji risk skorları ve seviye tabloları kullanılmaktadır.

Teknoloji riski olabilirlik skalası

Risklerin oluşma olasılığına uygun bir değer atanması için kullanılır.

Çizelge 5.1. Teknoloji Riski Olabilirlik Skalası

Teknoloji Riski Olabilirlik Skalası	
Seviye	**Ters etki yaratacak olayın meydana gelme sıklığı**
1	Her 10 yılda (veya daha fazla sürede) bir
2	Her 5 yılda bir
3	Yılda bir
4	Yılda bir ile ayda bir arasında
5	Aylık
6	Haftalık
7	Günlük veya daha fazla

Teknoloji riski etki skalası

Risklerin gerçekleşmesi durumunda etkisine uygun bir değer atanması için kullanılır. Risk etkileri beş ana başlıkta ele alınarak risk skoru hesaplaması yapılır. Risk etkileri sırasıyla finansal, itibar, erişilebilirlik, yasal gereksinimler ve müşterilere olan etkileri şeklinde sıralanırlar. Bu başlıklar için puanlama yapılır. Risk skoru hesaplamasında, risk için belirlenmiş etki değerlerinden en yüksek etki derecesi (o senaryonun genel etki seviyesini göstermektedir) dikkate alınır.

Çizelge 5.2. Teknoloji Riski Etki Skalası

Teknoloji Risk Etki Skalası					
Seviye	**Finansal**	**Erişebilirlik**	**İtibar**	**Müşteriler**	**Yasal**
1	Etki < 2.500 €	Müşteri üzerinde etkisi görülmeyen iş hizmeti kesintisi veya banka iç kullanıcısı üzerinde etkisi görülmeyen iş hizmeti kesintisi	Bazı gizli bilgilerin yalnızca üst / kıdemli yönetim kadrosu tarafından bilinmesi	Diğer organizasyonlara şikayet edilmeden birkaç müşterinin / müşteri kitlesinin kaybı veya şikayet edilmeden birkaç üst düzey yetkilinin memnuniyetsizliği	Harici etkisi olmayan belirli düzenlemelere ara sıra uyumsuzluk
2	2.500 € < Etki < 25.000 €	Müşteri üzerinde etkisi görülmeyen iş hizmeti kesintisi veya banka iç kullanıcısı üzerinde etkisi görülmeyen iş hizmeti kesintisi	Bazı gizli bilgilerin yalnızca yönetim kadrosu tarafından bilinmesi	Diğer organizasyonlara şikayet edilerek birkaç müşterinin / müşteri kitlesinin kaybı veya şikayet edilerek birkaç üst düzey yetkili kitlesinin memnuniyetsizliği	Harici etkisi olan belirli düzenlemelere ara sıra uyumsuzluk
3	25.000 € < Etki < 100.000 €	Müşteri için sunulan minör servislerde görünen iş kesintileri veya banka iç kullanıcısı için sunulan minör servislerde görünen iş kesintileri	Bazı gizli bilgilerin banka personeli tarafından bilinmesi	Sınırlı sayıda toplu pazar müşterisinin kaybı veya sınırlı sayıda belli banka iç kullanıcısının memnuniyetsizliği	Mevzuat ile ilgili uyumsuzluk ancak durum kolaylıkla düzeltilebilir.
4	100.000 € < Etki < 250.000 €	Belirli bir RTO (recovery time object) içinde tekrar müşteriye sunulan kısmi hizmet kesintisi veya belirli bir RTO içinde tekrar banka iç kullanıcısına sunulan kısmi hizmet kesintisi	Bazı gizli bilgilerin banka ve direkt olarak bağlantılı partiler (diğer bankalar, uluslararası organizasyonlar, düzenleyiciler vb.) tarafından bilinmesi	Yüksek meblağlı hesap kaybı	Belirli bir yasa / mevzuat ile ilgili uyumsuzluk nedeniyle para cezası
5	250.000 € < Etki < 1.000.000 €	Belirli bir RTO içinde tekrar müşteriye sunulan genel hizmet kesintisi veya belirli bir RTO içinde tekrar banka iç kullanıcısına sunulan genel hizmet kesintisi	Yargıya intikal	Önemli bir miktardaki toplu pazar müşterilerinin kaybı veya sınırlı sayıda yüksek meblağlı hesap kaybı	Belirli bir yasa/mevzuat ile ilgili uyumsuzluk nedeni ile yasal bir soruşturmanın başlatılması ve para cezası
6	1.000.000 € < Etki < 5.000.000 €	Belirli bir RTO içinde tekrar müşteriye sunulamayan kısmi hizmet kesintisi veya belirli bir RTO içinde tekrar banka iç kullanıcısına sunulamayan kısmi hizmet kesintisi	Basında yayınlanmış bir makale (sektörel yayınlar, genel basın, TV vb.)	Önemli Müşteri kaybı veya üst yönetime intikal etmeyen tüm banka kullanıcılarının memnuniyetsizliği	Bankacılık faaliyetlerinin engellenmesine ilişkin hüküm ve cezalar (şube açılmasının engellenmesi, borsada işlem yapma yetkisinin kaldırılması vb.)
7	Etki > 5.000.000 €	Belirli bir RTO içinde tekrar müşteriye sunulamayan genel hizmet kesintisi veya belirli bir RTO içinde tekrar banka iç kullanıcısına sunulamayan genel hizmet kesintisi	Medyadaki sürekli yorumlarla birlikte halkın / hissedarların / basının fikrini değiştirmenin imkansızlığı.	Komple bir segmentin / sektörün kaybedilmesi veya üst yönetime intikal eden tüm banka iç kullanıcılarının memnuniyetsizliği	Bankacılık lisansını kaybetme riski

Teknoloji risk skorları ve seviyeleri

Olabilirlik ve etki değerleri dikkate alınarak tespit edilen risk skoruna göre risklerin ne şekilde ele alınması gerektiğini belirlemek için kullanılır.

Çizelge 5.3. Teknoloji Risk Skorları ve Seviyeleri

Teknoloji Risk Skorları ve Seviyeleri	
Risk skor	**Seviye**
2	Düşük
3	Düşük
4	Düşük
5	Düşük
6	Düşük
7	Düşük
8	Orta
9	Orta
10	Orta
11	Orta
12	Yüksek
13	Yüksek
14	Yüksek

Teknoloji riski seviye hesaplama yönteminde risk skoru hesaplanırken en yüksek etki seviyesi değeri ile kontrol öncesi olabilirlik seviyesi değeri toplanır ve doğal risk seviyesi tespit edilir. Riskle ilgili en yüksek etki seviyesi ile varlık için mevcut kontroller dikkate alınarak tespit edilmiş olan kontrol sonrası olabilirlik değeri toplanarak hesaplanan sonuç genel kontrol düzeyi (GKD) olarak ifade edilir, diğer bir ifade ile kalan risktir.

• Varlıklar üzerinde bu risklerin oluşma olasılığı ve etkilerini azaltacak mevcut kontroller tanımlanır. Risk olabilirlik seviyesi, teknoloji riski olabilirlik skalası dikkate alınarak kontrol öncesi ve kontrol sonrası olmak üzere her bir risk için belirlenir.

5.1.5. Risk işleme yönteminin seçilmesi ve riskin takip edilmesi

Mevcut risklerin, varlıklar üzerindeki risk seviyelerinin kabul edilebilir risk seviyesine indirilmesi veya riskin tamamen ortadan kaldırılması amacıyla yapılacak çalışmalarda aşağıdaki hususlar dikkate alınmalıdır.

- Teknoloji varlık risk analizi ve değerlendirmesi sonrasında kurum gereksinimleri, vizyonu, misyonu, iş hedefleri ve kabul edilebilir risk skoru dikkate alınarak risklerin işlenmesi için aşağıda belirtilen aksiyonlardan biri gerçekleştirilir.

Riskin kabulü

Riskin var olduğu bilinerek aksiyon almadan çalışmaya devam etmektir. Riskin olasılık veya etkisini düşürecek aksiyon maliyetinin, riskin gerçekleşmesi durumunda bankaya vereceği zarardan daha fazla olması durumunda veya risk skorunun kabul edilen değer altında olması durumunda risk kabul edilir.

Riskin azaltılması

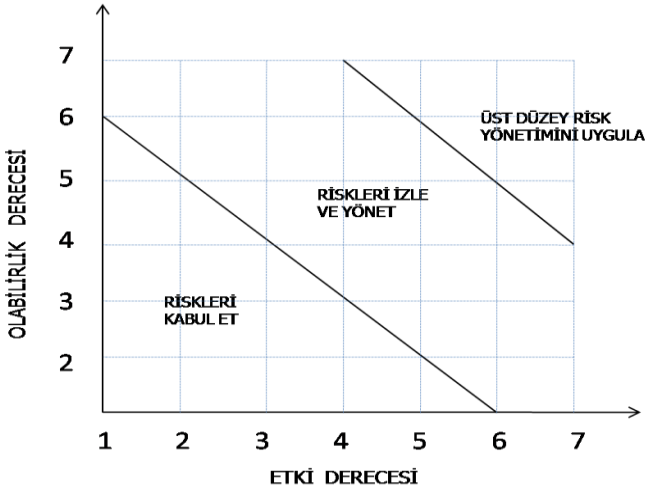
Riskin uygun kontrol noktaları seçilerek işlenmesi sonucunda mevcut risk derecesinin azaltılmasıdır. Risk skorunun kabul edilen değerden fazla olması, üst düzey risk yönetimi gerekmesi durumunda seçilebilir.

Riskten kaçınma

Riski oluşturan sebebin tamamen ortadan kaldırılması sonucunda riski tamamen elimine etmektir. Risk skorunun kabul edilen değerden fazla olması, üst düzey risk yönetimi gerekmesi durumunda seçilebilir.

Risk transferi

Riskin gerçekleşmesi durumunda ortaya çıkacak zararı tamamen kurumun dışına aktarılmasıdır. Sigorta yaptırmak veya ilgili riski üçünü parti firmaya transfer etmek örnek olarak verilebilir. Risk skorunun kabul edilen değerden fazla olması, üst düzey risk yönetimi gerekmesi durumunda seçilebilir.



Şekil 5.1. Risk Seviye Grafiği

Risk seviye grafiğinden anlaşılacağı üzere,

- Kontrol sonrası risk skoru 12 ve üstü olan riskler için üst düzey risk yönetimi uygulanır (Riskin azaltılması veya tamamen yok edilmesi için aksiyon alınır). Bu risklerle ilgili planlanan aksiyonlar, maliyet analizi çalışması ile birlikte hazırlanarak bankanın üst yönetimine sunulur.
- Kontrol sonrası risk skoru 8 ve 11 arasında olan riskler orta seviye risk skorlarına karşılık gelip bu riskler ve üzerlerindeki kontrollerin etkinliği teknik sahipleri tarafından devamlı olarak izlenir ve yönetilir.
- Kontrol sonrası genel kontrol değeri 7 ve küçük olanlar düşük seviyeli risk gruplarıdır ve bunlar kabul edilebilir riskler kategorisindedir. Normal şartlarda bunlar için herhangi bir aksiyon alınmaz.
- Tüm bunlara ek olarak, risk skoru 12'den düşük olan riskler için tekrar gözden geçirme ve ayar (tuning) uygulanabilir. Risk skoru düşük olup yasal uyumluluk açısından yok edilmesi ya da skorunun düşürülmesi gereken risklere yönelik aksiyon alınması mümkündür.
- Risklerin işlenmesinde önceliğin belirlenmesi için risk seviyeleri (GKD) yüksek, düşük ve orta olarak üç seviyede derecelendirilir. Uygulanan yaklaşım müdahale gerektiren en önemli riskleri ortaya çıkarıp öncelikle bu riskler üzerine odaklanılmasını sağlamak şeklindedir.

5.2. Bankanın Teknoloji Riski Yönetimi Süreci Hesaplamaları

Bu bölümde, çalışmamızı gerçekleştirdiğimiz bankanın teknoloji riski yönetimi süreci kapsamında risklerin belirlenip, değerlendirilerek takip edildiği süreçte varlık risk envanteri analiz ve hesaplamalarının nasıl yapıldığı, bankanın temel bankacılık hizmetleri için anlaşılabilir bir şekilde anlatılmaya çalışılmıştır. Bankanın herbir temel bankacılık hizmeti için belirlediği bir tehdit, bu tehdit için hesapladığı risk ve riskin gerçekleşmesi durumunda alacağı aksiyon yada aksiyonların neler olduğu bilgi sistemlerinin karmaşıklığı göz önüne alındığında temel bir düzeyde gösterilmiştir.

Teknoloji riski yönetimi süreci, varlık risk envanteri hesaplamaları için seçilen bankacılık hizmetleri aşağıdaki gibidir:

- Kredi hizmeti
- Çağrı merkezi hizmeti
- Debit kart (banka kartı) hizmeti
- ATM (automatic teller machine) hizmeti
- İnternet bankacılığı hizmeti
- Mevduat hizmeti
- Muhasebe hizmeti
- POS (point of sale) hizmeti

5.2.1. Kredi hizmeti risk hesaplamaları

Bankanın sağladığı kredi hizmetiyle ilgili kredi uygulamalarına “yetkisiz erişim” tehditinin detayları aşağıda gösterilmiştir.

Çizelge 5.4. Kredi hizmeti varlık risk envanteri tehdit belirleme

Hizmet	Varlık Kategorisi	Varlık	Tehdit	Açıklama
Kredi Hizmeti	Sunucular	Kredi Uygulamaları	Yetkisiz erişim	Yetkisiz olunan bilgilere erişilmesi güvenliği tehdit etmektedir.

Kredi uygulamalarına “yetkisiz erişim” tehditi için risk hesaplamaları aşağıda gösterilmiştir.

Çizelge 5.5. Kredi hizmeti varlık risk envanteri risk hesaplamaları

Hizmet	Kredi Hizmeti
Finansal	5,0
İtibar	5,0
Erişilebilirlik	5,0
Yasal Gereksinimler	2,0
Müşteriler	3,0
Kontrol Öncesi Olabilirlik	7,0
Kontrol Sonrası Olabilirlik	2,0
Risk Skor	12,0
Genel Kontrol Düzeyi	7,0
Risk İşleme Yöntemi	Riskleri kabul et

Kredi uygulamalarına “yetkisiz erişim” tehditi için gerekli kontroller, kabul edilen ve ortaya çıkabilecek riskin gerçekleşmesi durumunda alınacak aksiyonlar şu şekildedir.

Çizelge 5.6. Kredi hizmeti varlık risk envanteri aksiyon belirleme

Hizmet	Açıklama	Kontroller	Kesinti Anında Alınacak Aksiyon
Kredi Hizmeti	Yetkisiz olunan bilgilere erişilmesi güvenliği tehdit etmektedir.	• Şifre uygulaması • Yetkileri gözden geçirmek • Görevler ayrılığı ilkesini uygulamak	Sorun anında durum ilgili birimlere bildirilir. Eğer donanım sorunu varsa arızalı donanım devreden çıkarılır, yedek donanım ile devam edilir. Donanımın arızası tedarikçi listesindeki firmaya bildirilir ve sözleşmede belirtilen sürede değiştirilmesi sağlanır. Analiz sonucunda ortaya çıkan eksikliklerin giderilmesi için ilgili birimlere haber verilir. İç kaynaklarla yazılmış bir uygulama ise gözden geçirilerek problem giderilmeye çalışılır. Yazılım bir firmaya ait ise tedarikçi listesindeki firma ile temasa geçilir. Loglardan sorunun kaynağı araştırılır. İş dağılım tablolarında belirtilen yedek personel devreye sokularak sorunun giderilmesi sağlanır. Yedek personelin olmadığı durumlarda dokümanlar incelenir veya tedarikçi listesindeki firmalardan teknik yardım istenir. Sorunun tekrarlanmaması için gerekli önlemler alınır.

5.2.2. Çağrı merkezi hizmeti risk hesaplamaları

Bankanın sağladığı çağrı merkezi hizmetiyle ilgili çağrı merkezi uygulamasındaki (IVR) “eski teknoloji” tehditinin detayları aşağıda gösterilmiştir.

Çizelge 5.7. Çağrı merkezi hizmeti varlık risk envanteri tehdit belirleme

Hizmet	Varlık Kategorisi	Varlık	Tehdit	Açıklama
Çağrı Merkezi Hizmeti	Paket Yazılımlar	IVR (Çağrı merkezi uygulaması)	Eski teknoloji	Yeni teknolojileri desteklemeyen sistemler zaafiyetlere yol açabilir.

Çağrı merkezi uygulamasındaki “eski teknoloji” tehditi için risk hesaplamaları aşağıda gösterilmiştir.

Çizelge 5.8. Çağrı merkezi hizmeti varlık risk envanteri risk hesaplamaları

Hizmet	Kredi Hizmeti
Finansal	3,0
İtibar	4,0
Erişilebilirlik	4,0
Yasal Gereksinimler	2,0
Müşteriler	2,0
Kontrol Öncesi Olabilirlik	7,0
Kontrol Sonrası Olabilirlik	1,0
Risk Skor	11,0
Genel Kontrol Düzeyi	5,0
Risk İşleme Yöntemi	Riskleri kabul et

Çağrı merkezi uygulamasındaki “eski teknoloji” tehditi için gerekli kontrol, kabul edilen ve ortaya çıkabilecek riskin gerçekleşmesi durumunda alınacak aksiyon şu şekildedir.

Çizelge 5.9. Çağrı merkezi hizmeti varlık risk envanteri aksiyon belirleme

Hizmet	Açıklama	Kontroller	Kesinti Anında Alınan Aksiyon
Çağrı Merkezi Hizmeti	Yeni teknolojileri desteklemeyen sistemler zaafiyetlere yol açabilir.	• Teknoloji yatırımları yapmak	Yeni teknolojiler takip edilir ve gerekli değişimler yapılır.

5.2.3. Debit kart (banka kartı) hizmeti risk hesaplamaları

Bankanın sağladığı debit kart (banka kartı) hizmetiyle ilgili debit kart uygulamasındaki “eski teknoloji” tehditinin detayları şu şekildedir.

Çizelge 5.10. Debit Kart hizmeti varlık risk envanteri tehdit belirleme

Hizmet	Varlık Kategorisi	Varlık	Tehdit	Açıklama
Debit Kart Hizmeti	Sunucular	Debit Kart Uygulaması	Eski teknoloji	Kimlik doğrulama, kriptolama gibi yeni teknolojileri desteklemeyen sistemler zaafiyetlere yol açabilir.

Debit kart uygulamasındaki “eski teknoloji” tehditi için risk hesaplamaları aşağıda gösterilmiştir.

Çizelge 5.11. Debit Kart hizmeti varlık risk envanteri risk hesaplamaları

Hizmet	Debit Kart Hizmeti
Finansal	5,0
İtibar	5,0
Erişilebilirlik	5,0
Yasal Gereksinimler	2,0
Müşteriler	3,0
Kontrol Öncesi Olabilirlik	7,0
Kontrol Sonrası Olabilirlik	1,0
Risk Skor	12,0
Genel Kontrol Düzeyi	6,0
Risk İşleme Yöntemi	Riskleri kabul et

Debit kart uygulamasındaki “eski teknoloji” tehditi için gerekli kontrol, kabul edilen ve ortaya çıkabilecek riskin gerçekleşmesi durumunda alınacak aksiyon şu şekildedir.

Çizelge 5.12. Debit kart hizmeti varlık risk envanteri aksiyon belirleme

Hizmet	Açıklama	Kontroller	Kesinti Anında Alınan Aksiyon
Debit Kart Hizmeti	Kimlik doğrulama, kriptolama gibi yeni teknolojileri desteklemeyen sistemler zaafiyetlere yol açabilir.	• Teknoloji yatırımları yapmak	Sorun anında, durum ilgili birimlere bildirilir. Eğer donanım sorunu varsa, arızalı donanım devreden çıkarılır yedek donanım ile devam edilir. Donanımın arızası tedarikçi listesindeki firmaya bildirilir ve sözleşmede belirtilen sürede değiştirilmesi sağlanır. Analiz sonucunda ortaya çıkan eksikliklerin giderilmesi için ilgili birime haber verilir. İç kaynaklarla yazılmış bir uygulama ise gözden geçirilerek problem giderilmeye çalışılır. Yazılım bir firmaya ait ise tedarikçi listesindeki firma ile temasa geçilir. Loglardan sorunun kaynağı araştırılır. İş dağılım tablolarında belirtilen yedek personel devreye sokularak sorunun giderilmesi sağlanır. Yedek personelin olmadığı durumlarda dokümanlar incelenir veya tedarikçi listesindeki firmalardan teknik yardım istenir. Gerekli durumlarda firmalardan yardım alınır. Sorunun tekrarlanmaması için gerekli önlemler alınır.

5.2.4. ATM hizmeti risk hesaplamaları

Bankanın sağladığı ATM hizmetiyle ilgili ATM cihazlarındaki “data hattı kesintileri ve arızaları” tehditinin detayları şu şekildedir.

Çizelge 5.13. ATM hizmeti varlık risk envanteri tehdit belirleme

Hizmet	Varlık Kategorisi	Varlık	Tehdit	Açıklama
ATM Hizmetleri	ATM Sistemleri İletişim Cihazları	ATM Cihazları	Data hattı kesintileri ve arızaları	Data hattındaki kesintiler, olabilecek arızalar bilgi varlıklarını olumsuz etkilemektedirler.

ATM cihazlarındaki “data hattı kesintileri ve arızaları” tehditi için risk hesaplamaları aşağıda gösterilmiştir.

Çizelge 5.14. ATM hizmeti varlık risk envanteri risk hesaplamaları

Hizmet	ATM Hizmetleri
Finansal	3,0
İtibar	4,0
Erişilebilirlik	3,0
Yasal Gereksinimler	3,0
Müşteriler	2,0
Kontrol Öncesi Olabilirlik	7,0
Kontrol Sonrası Olabilirlik	4,0
Risk Skor	11,0
Genel Kontrol Düzeyi	8,0
Risk İşleme Yöntemi	Riskleri izle ve yönet

ATM cihazlarındaki “data hattı kesintileri ve arızaları” tehditi için gerekli kontrol, yönetilerek izlenilen ve ortaya çıkabilecek riskin gerçekleşmesi durumunda alınacak aksiyonlar aşağıda gösterilmiştir.

Çizelge 5.15. ATM hizmeti varlık risk envanteri aksiyon belirleme

Hizmet	Açıklama	Kontroller	Kesinti Anında Alınan Aksiyon
ATM Hizmetleri	Data hattındaki kesintiler, olabilecek arızalar bilgi varlıklarını olumsuz etkilemektedirler.	• Data hatlarının bakımı için ilgili firma ile sözleşme yapmak	Firma ile data hattı bakım onarım anlaşması kapsamında arızaları bildirmek. ATM'yi yedek hat ile çalıştırmak.

5.2.5. İnternet bankacılığı hizmeti risk hesaplamaları

Bankanın sağladığı internet bankacılığı hizmetiyle ilgili mobil bankacılık uygulamasındaki “güvenlik zafiyetlerinin yönetilememesi” tehditinin detayları şu şekildedir.

Çizelge 5.16. İnternet bankacılığı hizmeti varlık risk envanteri tehdit belirleme

Hizmet	Varlık Kategorisi	Varlık	Tehdit	Açıklama
İnternet Bankacılığı Hizmetleri	Uygulama Yazılımları	Mobil Bankacılık	Güvenlik zafiyetlerinin yönetilememesi	Bilgi varlıklarının maruz kaldığı zafiyetlerin zamanında tespit edilememesi ve giderilememesi.

Mobil bankacılık uygulamasındaki “güvenlik zafiyetlerinin yönetilememesi” tehditi için risk hesaplamaları aşağıda gösterilmiştir.

Çizelge 5.17. İnternet bankacılığı hizmeti varlık risk envanteri risk hesaplamaları

Hizmet	İnternet Bankacılığı Hizmetleri
Finansal	6,0
İtibar	7,0
Erişilebilirlik	3,0
Yasal Gereksinimler	1,0
Müşteriler	6,0
Kontrol Öncesi Olabilirlik	7,0
Kontrol Sonrası Olabilirlik	1,0
Risk Skor	14,0
Genel Kontrol Düzeyi	8,0
Risk İşleme Yöntemi	Riskleri izle ve yönet

Mobil bankacılık uygulamasındaki “güvenlik zafiyetlerinin yönetilememesi” tehditi için gerekli kontrol, yönetilerek izlenilen ve ortaya çıkabilecek riskin gerçekleşmesi durumunda alınacak aksiyon şu şekildedir.

Çizelge 5.18. İnternet bankacılığı hizmeti varlık risk envanteri aksiyon belirleme

Hizmet	Açıklama	Kontroller	Kesinti Anında Alınan Aksiyon
İnternet Bankacılığı Hizmetleri	Bilgi varlıklarının maruz kaldığı zafiyetlerin zamanında tespit edilememesi ve giderilememesi	• Düzenli olarak izlemek	Acil eylem planı uygulanacak.

5.2.6. Mevduat hizmeti risk hesaplamaları

Bankanın sağladığı mevduat hizmetiyle ilgili hazine uygulamasındaki (Reuters) "güvenlik zafiyetlerinin yönetilememesi" tehditinin detayları aşağıdaki gösterilmiştir.

Çizelge 5.19. Mevduat hizmeti varlık risk envanteri tehdit belirleme

Hizmet	Varlık Kategorisi	Varlık	Tehdit	Açıklama
Mevduat Hizmetleri	Paket Yazılımlar	Reuters (Hazine uygulaması)	Yazılımın çalışmaması	Yazılımın herhangi bir sebeple çalışmaması.

Hazine uygulamasındaki (Reuters) "güvenlik zafiyetlerinin yönetilememesi" tehditi için risk hesaplamaları aşağıda gösterilmiştir.

Çizelge 5.20. Mevduat hizmeti varlık risk envanteri risk hesaplamaları

Hizmet	Mevduat Hizmetleri
Finansal	7,0
İtibar	4,0
Erişilebilirlik	4,0
Yasal Gereksinimler	3,0
Müşteriler	6,0
Kontrol Öncesi Olabilirlik	7,0
Kontrol Sonrası Olabilirlik	2,0
Risk Skor	14,0
Genel Kontrol Düzeyi	9,0
Risk İşleme Yöntemi	Riskleri izle ve yönet

Hazine uygulamasındaki (Reuters) “güvenlik zafiyetlerinin yönetilememesi” tehditi için gerekli kontroller, yönetilerek izlenilen ve ortaya çıkabilecek riskin gerçekleşmesi durumunda alınacak aksiyonlar aşağıda gösterilmiştir.

Çizelge 5.21. Mevduat hizmeti varlık risk envanteri aksiyon belirleme

Hizmet	Açıklama	Kontroller	Kesinti Anında Alınan Aksiyon
Mevduat Hizmetleri	Yazılımın herhangi bir sebeple çalışmaması.	• Düzenli izlemek • Olağanüstü durum merkezinden çalışabilecek şekilde yedeklemek • Eğitimli personel	Sorun anında, durum ilgili birimlere bildirilir. Eğer donanım sorunu varsa, arızalı donanım devreden çıkarılır yedek donanım ile devam edilir. Donanımın arızası tedarikçi listesindeki firmaya bildirilir ve sözleşmede belirtilen sürede değiştirilmesi sağlanır. Analiz sonucunda ortaya çıkan eksikliklerin giderilmesi için ilgili birime haber verilir. İç kaynaklarla yazılmış bir uygulama ise gözden geçirilerek problem giderilmeye çalışılır. Yazılım bir firmaya ait ise tedarikçi listesindeki firma ile temasa geçilir. Loglardan sorunun kaynağı araştırılır. İş dağılım tablolarında belirtilen yedek personel devreye sokularak sorunun giderilmesi sağlanır. Yedek personelin olmadığı durumlarda dokümanlar incelenir veya tedarikçi listesindeki firmalardan teknik yardım istenir. Gerekli durumlarda firmalardan yardım alınır.

5.2.7. Muhasebe hizmeti risk hesaplamaları

Bankanın sağladığı muhasebe hizmetiyle ilgili dış ticaret işlemlerinin muhasebeleştirilmesi uygulamasındaki “eğitimsiz personel” tehditinin detayları şu şekildedir.

Çizelge 5.22. Muhasebe hizmeti varlık risk envanteri tehdit belirleme

Hizmet	Varlık Kategorisi	Varlık	Tehdit	Açıklama
Muhasebe	Sunucular	Dışticaret işlemleri muhasebe uygulaması	Eğitimsiz personel	Bilgi sistemlerini kullanma, yönetme ve işletme aşamasında eğitimsiz personel risk oluşturmaktadır.

Dış ticaret işlemlerinin muhasebeleştirilmesi uygulamasındaki "eğitimsiz personel" tehditi için risk hesaplamaları aşağıda gösterilmiştir.

Çizelge 5.23. Muhasebe hizmeti varlık risk envanteri risk hesaplamaları

Hizmet	Muhasebe
Finansal	5,0
İtibar	5,0
Erişilebilirlik	5,0
Yasal Gereksinimler	2,0
Müşteriler	3,0
Kontrol Öncesi Olabilirlik	7,0
Kontrol Sonrası Olabilirlik	2,0
Risk Skor	12,0
Genel Kontrol Düzeyi	7,0
Risk İşleme Yöntemi	Riskleri kabul et

Dış ticaret işlemlerinin muhasebeleştirilmesi uygulamasındaki "eğitimsiz personel" tehditi için gerekli kontroller, kabul edilen ve ortaya çıkabilecek riskin gerçekleşmesi durumunda alınacak aksiyon şu şekildedir.

Çizelge 5.24. Muhasebe hizmeti varlık risk envanteri aksiyon belirleme

Hizmet	Açıklama	Kontroller	Kesinti Anında Alınan Aksiyon
Muhasebe	Bilgi sistemlerini kullanma, yönetme ve işletme aşamasında eğitimsiz personel risk oluşturmaktadır.	• Eğitim planları yapmak • Düzenli eğitim aldırmak • İşe alım sırasında eğitim seviyesini kontrol etmek	Acil eylem planı uygulanacak.

5.2.7. POS (point of sale) hizmeti risk hesaplamaları

Bankanın sağladığı POS hizmetiyle ilgili merkezi sistem operatörlerindeki "kötü niyetli eylemler" tehditinin detayları şu şekildedir.

Çizelge 5.25. POS hizmeti varlık risk envanteri tehdit belirleme

Hizmet	Varlık Kategorisi	Varlık	Tehdit	Açıklama
POS Hizmetleri	İnsan	Merkezi Sistem Operatörleri	Kötü Niyetli Eylemler	Çalışanın kasıtlı hatalar sonucu bankanın zarara uğrama riskidir.

Merkezi sistem operatörlerindeki "kötü niyetli eylemler" tehditi için risk hesaplamaları aşağıda gösterilmiştir.

Çizelge 5.26. POS hizmeti varlık risk envanteri risk hesaplamaları

Hizmet	POS Hizmetleri
Finansal	2,0
İtibar	2,0
Erişilebilirlik	3,0
Yasal Gereksinimler	2,0
Müşteriler	2,0
Kontrol Öncesi Olabilirlik	1,0
Kontrol Sonrası Olabilirlik	1,0
Risk Skor	4,0
Genel Kontrol Düzeyi	4,0
Risk İşleme Yöntemi	Riskleri kabul et

Merkezi sistem operatörlerindeki “kötü niyetli eylemler” tehditi için gerekli kontroller, kabul edilen ve ortaya çıkabilecek riskin gerçekleşmesi durumunda alınacak aksiyon şu şekildedir.

Çizelge 5.27. POS hizmeti varlık risk envanteri aksiyon belirleme

Hizmet	Açıklama	Kontroller	Kesinti Anında Alınan Aksiyon
POS Hizmetleri	Çalışanın kasıtlı hatalar sonucu bankanın zarara uğrama riskidir.	• Sistem giriş yetkilerinin kontrollü verilmesi • Yapılan işlemlerin kayıt altına alınması • Kritik sistem değişikliklerinin onay mekanizması ile çalıştırılabilmesi	Yedek sunucuya geçmek.

6. SONUÇ

Küreselleşen dünyanın finansal piyasalarında yaşanan hızlı gelişmeler, bilgi teknolojilerinin gelişmesi ve finansal araçların çeşitliliğinin artması bankaların karşılaştığı risk türlerinde artışlara neden olmuş ve risk kavramının daha fazla dikkatle ele alınması gerektiğini göstermiştir.

Çalışmamızın ilk bölümünde risk ve risk yönetiminin kavramları anlatılarak bankacılık sektöründe bu kavramların önemine değinilmiş olup, bankaları etkileyebilecek risklerin neler olduğu detaylı bir şekilde irdelenmiştir.

Risk yönetimi, önleyici ve hızlı kararlar ve faaliyetler ile sürekli olarak risklerin belirlendiği, hangi risklerin öncelikle çözümlenmesi gerektiğinin değerlendirildiği, strateji ve planların geliştirilerek uygulandığı bir sistematiktir. Bu doğrultuda bankacılıkta risk yönetiminin amacı bankaların finansal durumlarını iyileştirmek ve geri dönüşü mümkün olmayan zararlarla karşılaşmalarını önlemektir.

İkinci bölümde bankaların maruz kaldıkları operasyonel riskler ve teknoloji risklerinin neler olduğu ve bu riskleri yönetmek için dünyada kabul görmüş standartlardan bahsedilmiştir.

Bankalar için bilgi teknolojileri üzerindeki güvenlik açıkları ya da hatalar ciddi krizlere ve itibar kayıplarına yol açabilmektedir. Bilgi teknolojileri riskleri kurumdaki tüm risklerin bir parçası olarak belirlenmeli, ölçülmeli ve yönetilmelidir.

Üçüncü bölümde bilgi teknolojilerini kullanıyor olmalarından dolayı kaynaklanan risklerin yönetilmesi ve gerekli önlemleri alma zorunluluğu bulunan bankaların bu amacına ulaşabilmelerini sağlayan uluslararası kabul görmüş COBIT standartının usul ve esasları anlatılmıştır.

COBIT'in dört ana alanın oluşturduğu yapı, bilginin bütün yönlerini ve bunu destekleyen teknolojileri kapsar. COBIT'in 34 süreç ve 318 detaylı kontrol hedefi dikkate alındığında, bilgi teknolojileri ortamı için uygun ve yeterli bir kontrol sisteminin kurulması sağlanabilecektir.

Çalışmamızın son bölümünde ise Türkiye'de büyük ölçekli bir bankanın teknoloji risklerinin belirlenip, değerlendirilerek takip edildiği sürecin belli bir kısım

aşamalarının teknik hesaplamalarına girilmiş olup basit bir düzeyde uygulaması yapılmıştır.

Sonuç olarak, bankalarda etkin ve etkili bir bilgi teknolojileri risk yönetimi yapılabilmesi için öncelikle uluslararası kabul görmüş bilgi teknolojileri risk yönetimi standartlarının gerektirdiği kontrollerin uygulanması, bankanın tüm sistemlerinin bir bütün olarak düşünülerek bilgi teknolojileri risklerinin tüm risklerin bir parçası olarak görülmesi ve tüm bunların üst yönetimce desteklenerek kabul görmesi gereklidir. Bilgi teknolojileri risk yönetimi süreci, sürekli devam eden kendini yenileyen ve belirli bir son noktası olmayan bir süreç olarak düşünülmelidir.

KAYNAKLAR

Alkin E., Savaş A.T. (2002). *A Modern Approach to Risk Management in Financial Intermediaries.* İstanbul: Filiz Kitabevi, 92.

Altıntaş, M.A. (2011). *Bankacılıkta Risk Yönetimi ve Sermaye Yeterliliği - 5411 Sayılı Bankacılık Kanunu, Basel I ve Basel II Düzenlemeleri Çerçevesinde.* Ankara: Turhan Kitap Evi, 3.

Artinyan, E. N.(2007). COBIT Çerçevesi. *Active Dergisi*, (54), 1.

Atan, M. (2002). *Risk Yönetimi ve Türk Bankacılık Sektöründe Bir Uygulama*, Doktora Tezi, Gazi Üniversitesi Sosyal Bilimleri Enstitüsü, Ankara..

Atay, M. B. (2010). *Operasyonel Risk Yönetimi ve Türk Bankacılık Sektöründe Bir Uygulama,* Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Aykın, H. (2009). Bankalarda Operasyonel Risk Yönetimi ve Bir Endeks Önerisi: Oryos Endeksi, Doktora Lisans Tezi, Kadir Has Üniversitesi Sosyal Bilimleri Enstitüsü, İstanbul.

Babuşçu, Ş. (2005). *Basel II Düzenlemeleri Çerçevesinde Bankalarda Risk Yönetimi* (1.Basım). Ankara: Akademi Consulting & Training, 4.

Bankacılık Düzenleme ve Denetleme Kurumu. (2002). Piyasa Riskinin Dahil Edildiği Yeni Sermaye Yeterliliği Rasyosunun Standart Metoda Göre Hesaplanmasına İlişkin Örnek. *Risk ve Gözetim Teknikleri Araştırma Dairesi,* 2.

Bankaların İç Sistemleri Hakkında Yönetmelik. Madde 3.

Bankaların Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik. Madde 3.

Basel Committee On Banking Supervision Report. (2000). *Principles For The Management Of Credit Risk*, 1.

Basel Committee on Banking Supervision. (2001). *Operasyonel Risk*. Consultative Document, 2.

Basel Committee on Banking Supervision.(2001). Operasyonel Risk. Consultative Document, 2.

Bayoğlu B.(2008). Bilgi Güvenliği Yönetim Sistemi Uygulama ve Denetleme Semineri Notları. Takasbank, *Tubitak Uekae: Ulusal Elektronik ve Kriptoloji Arastırma Enstitüsü,* 73.

Best P. (1999). *Implementing Value At Risk*. Chichester: John Wiley & Sons, 2.

Boyacıoğlu M. A.(2002). Operasyonel Risk ve Yönetimi. *Bankacılar Dergisi*, Sayı 43, 51.

Candan H., Özün A. (2009). *Bankalarda Risk Yönetimi ve Basel II* (2. Baskı). İstanbul: Türkiye İş Bankası Kültür Yayınları, 16.

Cannata, F. and Quagliariello, M. (2009). *The Role of Basel II in the Subprime Financial Crisis: Guilty or Not Guilty?*. Carefin Working Paper, Milan: Universita Bocconi, 4.

Çolak, Ö. F. (2001). *Finansal Piyasalar ve Para Politikası*. Ankara: Nobel Yayın Dağıtım, 17.

Global Technology Audit Guide (2008). Bilgi Teknolojisi Kontrolleri. *Uluslararası İç Denetim Ensititüsü,* 99.

Hacısüleymanoğlu, E. (2010). *Bilgi Teknolojileri Yönetişimi Yöntemleri ve COBIT ile Ulusal bir Bankada Uygulaması*, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

İnternet: Bağcı, B. (2010). Bilgi Teknolojileri Risk Yönetimine Genel Bakış. Deloitte. 1. Web: http://www.denetimnet.net/Pages/bilgiteknolojileririskyonetimi.aspx adresinden 8 Ocak 2014'de alınmıştır.

Kandır S. Y., Erişmiş A. (2010). Banka Hisse Senetlerinin Döviz Kuru Riskine Açıklığının İncelenmesi: İMKB Üzerine Bir Uygulama. *İMKB Dergisi*, 12(46), 50.

Köylüoğlu, H.U. (2001). Risk Yönetimi! Zaman Geçirmeden Neden? Nasıl?. *Active Bankacılık ve Finans Dergisi*, (17), 1.

Mandacı, P. E. (2003). Türk Bankacılık Sektörünün Taşıdığı Riskler ve Finansal Kriz Aşmada Kullanılan Risk Ölçüm Teknikleri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 5(1), 67-84.

Numanoğlu, M. (2009). Operasyonel risk yönetimi ve ölçümünde son gelişmeler. *TBB Eğitim ve Tanıtım Grubu Semineri*, İstanbul, 6.

Rodriquez, L. J. (2003). Banking Stability and The Basel Capital Standards. *Cato Institute*, 23(1),115-126.

Rumelili, Ö. M. (2006). Ödeme Sistemlerinde Bilgi Teknolojileri Riskleri, Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimleri Enstitüsü, Ankara.

Şahin, S. (2011). *Bankacılıkta Risk Yönetimi ve Operasyonel Risk*, Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimleri Enstitüsü, İstanbul.

Teker D. L. (2006). *Bankalarda Operasyonel Risk Yönetimi - Örnek Banka Uygulamalı* (1.Basım), İstanbul: Literatür Yayıncılık, 3.

Türkiye Bankalar Birliği Çalışma Grubu. (2006). Risk Yönetimi Prensipleri. *Bankacılar Dergisi*, (57), 15.

Wahler, B. (2005). *Process-Managing Operational Risk Developing a Concept for Adapting Process Management to the Needs of Operational Risk in the Basel II - Framework*. Hochschule für Bankwirtschaft and John Hopkins University Paul H.Nitze School of Advanced Internetional Studies, 16.

Yalçınkaya J., Ekinci A. (2007). Bankalarda Faiz Oranı Riskinin Ölçülmesi, *Eskişehir Osman Gazi Üniversitesi Sosyal Bilimler Dergisi*, 8(1), 21.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : BAYCAN, Şefik
Uyruğu : T.C.
Doğum tarihi ve yeri : 26.07.1985, Ankara
Medeni hali : Bekar
Telefon : 05324785074
Faks : -
e-mail : sefikbaycan@hotmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Yüksek lisans	Gazi Üniversitesi/İşletme	Devam ediyor
Lisans	Gazi Üniversitesi/Müh. Fakültesi (Endüstri Mühendisliği)	2008
Lise	Kocatepe Mimar Kemal Lisesi	2002

İş Deneyimi

Yıl	Yer	Görev
2011- devam ediyor	T.VAKIFLAR BANKASI T.A.O. Teftiş Kurulu Başkanlığı	Müfettiş

Yabancı Dil

İngilizce

Yayınlar

-

Hobiler

Bilgisayar, Teknolojik gelişmeler, Yüzme, Müzik dinlemek, Futbol

GAZİ GELECEKTİR..